

Interscience Research Network

Interscience Research Network

Conference Proceedings - Full Volumes

IRNet Conference Proceedings

12-2-2012

International Conference on Recent Trends in Engineering & Technology

Prof.Srikanta Patnaik Mentor

IRNet India, patnaik_srikanta@yahoo.co.in

Follow this and additional works at: https://www.interscience.in/conf_proc_volumes



Part of the [Engineering Commons](#)

Recommended Citation

Patnaik, Prof.Srikanta Mentor, "International Conference on Recent Trends in Engineering & Technology" (2012). *Conference Proceedings - Full Volumes*. 73.

https://www.interscience.in/conf_proc_volumes/73

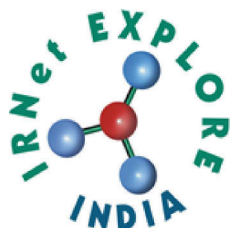
This Book is brought to you for free and open access by the IRNet Conference Proceedings at Interscience Research Network. It has been accepted for inclusion in Conference Proceedings - Full Volumes by an authorized administrator of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

Proceedings of International Conference on
RECENT TRENDS IN ENGINEERING & TECHNOLOGY



(ICRTET-2012)
2nd December, 2012
BANGALORE, India

Interscience Research Network (IRNet)
Bhubaneswar, India



[Home](#)



International Conference on Recent Trends in Engineering and Technology

ICRTET-2012
Bangalore, 2nd December, 2012

[Editorial](#)

Slno.	Titles & Authors	Page No.
1.	Wavelet Domain Image Resolution Enhancement With Fog Removal And Contrast Improvement Neethu Elizabeth Paul & J S Remya Krishna	1-4
2.	Removal of High and Low Density Impulse Noise Using Modified Median Filter T.M.Benazir & B.M.Imran	5-8
3.	Efficient Compression and encryption scheme for Secure Transmission of images and its Reconstruction Neethu Sara Raju & Jobins George	9-13
4.	A Contourlet Domain Watermarking Algorithm N.R.Brinta & P.R.Bipin	14-17
5.	An Algorithmic Approach to Travelling Salesman Problem Supriya Pandey, Shalini Singh & Rashmi Mishra	18-23
6.	Image Denoising Using Patch Based Technique and Fuzzy-C Means Algorithm Nimitha K E & Sapna Elizabeth Paul	24-27
7.	An Energy Aware Modified Leach Protocol For Energy Efficient Routing In Wireless Sensor Networks Nandakishor Sirdeshpande & Vishwanath Udupi	28-33
8.	Embedded Robot Control System Based on An Embedded Operating System, The Combination of Advanced RISC Microprocessor (ARM), DSP and ARM Linux Vaishak N L & Ramachandra C G	34-38
9.	Modified AES Using Dynamic S-Boxes Veena Desai, Sagar Dhavali & Sachin Katti	39-44
10.	A Comprehensive Survey On The Pervasion Of Android In The Design Of Sophisticated Embedded Devices Sharmila S P & A S Manjunath	45-50
11.	Diagnosis of Lung Cancer Disease Using Neuro-Fuzzy Logic A Malathi Palani	51-56
12.	A Machine Learning Approach For Identifying Disease-Treatment Relations In Short Texts Shivam Srivastava, Utkarsh Srivastava & Mithilesh Chaturvedi	57-61
13.	Chaotic Image Encryption Using-RC5 Dhanya B.Nair & Ruksana Maideen	62-64
14.	Data Encryption Standard Using Moddes Algorithm With Compression Winnie Eldhose & Manju Rani Mathew	65-68

- | | | |
|-----|---|-------|
| 15. | Enhanced Chaotic Image Encryption Algorithm Based On Trigonometric Functions
M.K Mohsina & Robin Abraham | 69-72 |
| 16. | Chaos-Based Compression And Encryption Scheme Using Artificial Neural Network
Geethi V & Chaithanya G Nair | 73-75 |
| 17. | A Secure Secret Key Steganographic Algorithm Through Optimization Of Pixel Pair Matching
Najeena K.S & B. Mohammed Imran | 76-78 |
| 18. | A survey on dynamic topology control-algorithms In manet
Krushna J. Pandit | 79-85 |
| 19. | Evaluation of Optimal Machining Parameters of Microfer C263 Alloy Using Response Surface Methodology While Turning on CNC Lathe Machine
Mohammed Wasif.G & Mir Safiulla | 86-91 |
| 20. | Analysis of Surface Roughness and Material Removal Rate (MRR) In Turning Operation of Super Alloy Nimonic 75
Danish Khan | 92-95 |



Copyright © 2012 All Rights Reserved Powered By IRNet

Editorial

The new economic millennium is surprisingly rushing with innovation and technology. There is a sharper focus on deriving value from the widespread global integration in almost all spheres of social, economic, political and technological subsystems. In the quest of making this earth a better place to live we have to make a strong hold upon sustainable energy source. Sustainable energy sources include all renewable energy sources, such as hydroelectricity, solar energy, wind energy, wave power, geothermal energy, bioenergy, and tidal power. It usually also includes technologies designed to improve energy efficiency. Energy efficiency and renewable energy are said to be the twin pillars of sustainable energy. Renewable energy technologies are essential contributors to sustainable energy as they generally contribute to world energy security, reducing dependence on fossil fuel resources, and providing opportunities for mitigating greenhouse gases. Although the discipline like electrical engineering has narrated academic maturity in the last decades, but the limitations of the non-renewable energy sources, turbulence and disturbances in the energy propagation cascades various insightfulness and stimulation in post classical electrical era. Evidence shows that there are phenomenal supplements in power generation and control after the introduction of Energy Management System (EMS) supported by Supervisory Control and Data Acquisition (SCADA). As there is increasing focus on strengthening the capacity of the power houses with the existing resources or constraints, some new dimensions like FACTS, optimal system generation, high voltage DC transmission system, power generation control, soft computing, compensation of transmission line, protection scheme of generator, loss calculation, economics of generation, fault analysis in power systems are emerging. Since the world is suffering with energy crisis, energy consumption has social relevancy.

The new integrated devices did not find a ready market. Users were concerned because the individual transistors, resistors, and other electronic circuit components could not be tested individually to ensure their reliability. Also, early integrated circuits were expensive, and they impinged on the turf that traditionally belonged to the circuit designers at the customer's company. Again, Bob Noyce made a seminal contribution. He offered to sell the complete circuits for less than the customer could purchase individual components to build them. (It was also significantly less than it was costing us to build them!) This step opened the market and helped develop the manufacturing volumes necessary to reduce manufacturing costs to competitive levels. To this day the cost reductions resulting from economies of scale and newer high-density technology are passed on to the user, often before they are actually realized by the circuit manufacturer. As a result, we all know that the high-performance electronic gadget of today will be replaced with one of higher performance and lower cost tomorrow.

The integrated circuit completely changed the economics of electronics. Initially looked forward to the time when an individual transistor might sell for Rs.10/today the same amount can buy tens of transistors as part of a complex circuit. This cost reduction has made the technology ubiquitous nearly any application that processes information today can be done most economically the next day. No other technology that one can identify, has undergone such a dramatic decrease in cost with the improved performance that comes from making things smaller and smaller.

In the advent of modern research there is a significant growth in Mechanical Engineering as Computer Aided Design has become instrumental in many

industrialized nations like USA, European Countries, Scotland and Germany Other CAE programs commonly used by Mechanical Engineers include Product Lifecycle Management (PLM) tools and analysis tools used to perform complex simulations. Analysis tools may be used to predict product response to expected loads, including fatigue life and manufacturability. These tools include Finite Element Analysis (FEA), Computational Fluid Dynamics (CFD), and Computer-Aided Manufacturing (CAM). Using CAE programs, a mechanical design team can quickly and cheaply iterate the design process to develop a product that better meets cost, performance, and other constraints. No physical prototype need be created until the design nears completion, allowing hundreds or thousands of designs to be evaluated, instead of a relative few. In addition, CAE analysis programs can model complicated physical phenomena which cannot be solved by hand, such as viscoelasticity, complex contact between mating parts, or non-Newtonian flows.

As Mechanical Engineering begins to merge with other disciplines, as seen in Mechatronics, Multidisciplinary Design Optimization (MDO) is being used with other CAE programs to automate and improve the iterative design process. MDO tools wrap around existing CAE processes, allowing product evaluation to continue even after the analyst goes home for the day. They also utilize sophisticated optimization algorithms to more intelligently explore possible designs, often finding better, innovative solutions to difficult multidisciplinary design problems.

Apart from Industrial Development there is also an hourly need for creation of an influential professional body which can cater to the need of research and academic community. The current scenario says there exists a handful of bodies like American Society of Mechanical Engineers (ASME). Hence we must strive towards formation of a harmonious professional research forum committed towards discipline of Mechanical Engineering.

In the current age of Scientific development Robotics takes a center stage in solving many social problems. As agriculture is the mainstay of many developing nations, efficiency building measures should be incorporated in the field to boost efficiency and productivity. In the context Robotics in Agriculture has attracted much attention in the recent years. The idea of Robotic Agriculture (agricultural environments serviced by smart machines), is not a new one. Many engineers have developed driverless tractors in the past but they have not been successful as they did not have the ability to embrace the complexity of the real World. Most of them assumed an industrial style of farming where everything was known before hand and the machines could work entirely in predefined ways, much like a production line. The approach is now to develop smarter machines that are intelligent enough to work in an unmodified or semi natural environment. These machines do not have to be intelligent in the way we see people as intelligent but must exhibit sensible behavior in recognized contexts. In this way they should have enough intelligence embedded within them to behave sensibly for long periods of time, unattended, in a semi-natural environment, whilst carrying out a useful task. One way of understanding the complexity has been to identify what people do in certain situations and decompose the actions into machine control.

The use of MATLAB is actually increasing in a large number of fields, by combining with other toolboxes, e.g., optimization toolbox, identification toolbox, and others. The Maths. Works Inc. periodically updates MATLAB and Simulink, providing more and more advanced software. MATLAB handles numerical calculations and high-quality graphics, provides a convenient interface to built-in state-of-the-art subroutine libraries, and incorporates a high-level programming language. Nowadays, the MATLAB/Simulink package is the world's leading mathematical computing software for Engineers and Scientists in industry and education.

Due to the large number of models and/or toolboxes, there is still some work or coordination to be done to ensure compatibility between the available tools. Inputs and outputs of different models are defined by each modeler, a connection between models from two different toolboxes can thus take some time. This should be normalized in the future in order to allow a fast integration of new models from other toolboxes. The widespread use of these tools is reflected by ever-increasing number of books based on the Maths.

The conference is designed to stimulate the young minds including Research Scholars, Academicians, and Practitioners to contribute their ideas, thoughts and nobility in these two integrated disciplines. Even a fraction of active participation deeply influences the magnanimity of this International event.

I must acknowledge your response to this Conference. I ought to convey that it is only a little step towards knowledge, network and relationship. I express best wishes to all the paper presenters. I extend my heart full thanks to the reviewers, editorial board members and programme committee members . If situations prevail in favour we will take the glory of organizing the second conference of this kind very soon.

Convener

Mr. Bikash Chandra Rout

Technical Editor, IOAJ

WAVELET DOMAIN IMAGE RESOLUTION ENHANCEMENT WITH FOG REMOVAL AND CONTRAST IMPROVEMENT

NEETHU ELIZABETH PAUL & J S REMYA KRISHNA

Department of P.G, Applied Electronics, ICET, Mulavoor

Abstract:- Foggy weather conditions can degrade images. Fog reduces the visibility of images. Restoration of foggy images is an important issue. The paper presents a method of image resolution enhancement in wavelet domain with defogging and contrast improvement. Resolution enhancement technique is based on the interpolation of the high-frequency subbands obtained by discrete wavelet transform (DWT) and stationary wavelet transform(SWT). The foggy image is corrected by subtracting the estimated airlight map from the degraded image. Estimation of airlight is done human visual model, wherein a human is more insensitive to variations of the luminance in bright regions than in dark regions.

Keywords:- Discrete wavelet transform, stationary wavelet transform, airlight map, luminance image.

I. INTRODUCTION

An image is represented by intensity at a particular point whose spatial coordinates are on generally x and y axis coordinates. digital image is a discretized i.e. it is defined on a discrete grid. It is a two dimensional collection of light values or gray values. Image processing is done to obtain better resolution. Interpolation is a commonly used technique for image resolution enhancement. Digital image processing has numerous applications in different studies and researches of science and technology. Some of fields that use digital image processing include: biological researches, finger print analysis in forensics, medical fields, photography and publishing fields, astronomy, and in the film and game industries. Image enhancement deals with contrast enhancement, spatial filtering, frequency domain filtering, edge enhancement and noise reduction[3]-[6].

II. DWT AND SWT BASED IMAGE RESOLUTION ENHANCEMENT

A one level DWT (with Daubechies 9/7 as wavelet function) is used to decompose an input image into different subband images[1]. The high frequency subbands (LH, HL, and HH) contain the high frequency components of the input image[2]. Bicubic interpolation with enlargement factor of 2 is applied to high frequency subband images. Down sampling in each of the DWT subbands causes information loss in the respective subbands. That is why SWT is employed to minimize this loss. The interpolated high frequency subbands and the SWT high frequency subbands have the same size which means they can be added with each other.

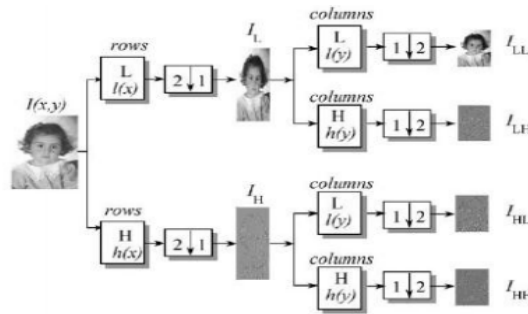


Fig.1. DWT decomposition

Bicubic interpolation with enlargement factor of 2 is applied to high frequency subband images. Down sampling in each of the The new corrected high frequency subbands can be interpolated further for higher enlargement. In the wavelet domain, the low resolution image is obtained by lowpass filtering of the high resolution image. In other words, low frequency subband is the low resolution of the original image. Using input image instead of low frequency subband increases the quality of the super resolved image. By interpolating input image high frequency subbands by 2 and then by applying inverse discrete wavelet transform (IDWT), the output image will contain sharper edges. Fig. 1 and Fig.2. shows different subbands obtained by DWT decomposition and reconstruction respectively.

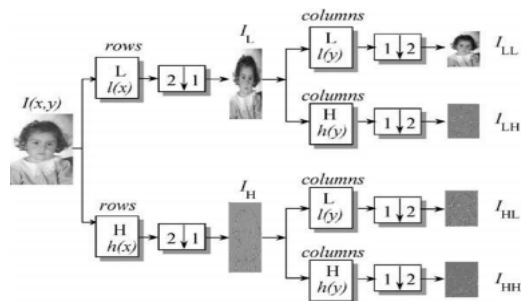


Fig. 2. DWT reconstruction

III. DEFOGGING OF DEGRADED IMAGE

Sometimes images taken will be degraded due to the presence of fog. The fog particles reduces the visual quality of images. Thus defogging is crucial in such occasions. In foggy weather conditions images become degraded due to the presence of airlight that is generated by scattering light by fog particles. Fog reduces visibility down to less than 1 km. In foggy weather, images also become degraded by additive light from scattering of light by fog particles. This additive light is called „airlight“. Airlight is estimated using cost function which is based on human visual model and an airlight map is generated.

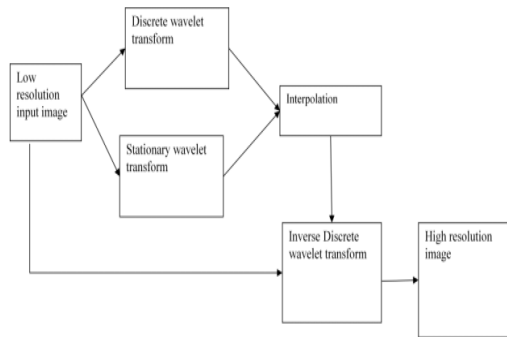


Fig .3. Block diagram of image resolution enhancement

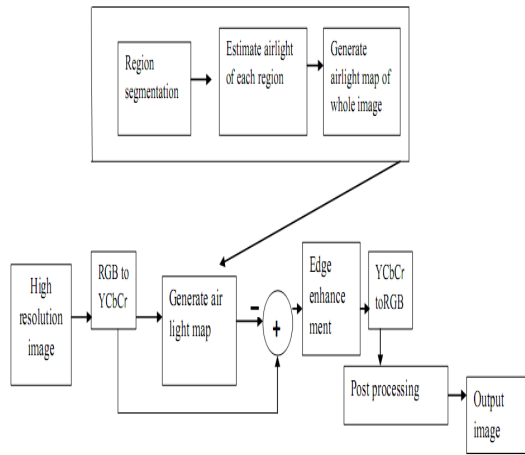


Fig .4. Block diagram for defogging

The luminance component of the foggy image is used to estimate the airlight[3]. The luminance image can be obtained by a fusion of the R, G, and B components. So, the color space is transformed from RGB to YCbCr.

$$Y'(i,j) = Y(i,j) + \lambda_Y(i,j) \quad (1)$$

where Y' and Y reflect the degraded luminance and clear luminance images respectively at position

(i,j) . $\lambda_Y(i,j)$ is the estimated airlight map for the luminance image. Restoration of the foggy image is done by estimating the airlight map and subtracting the airlight from the foggy image as in (2).

$$\hat{Y}(i,j) = Y'(i,j) - \hat{\lambda}_Y(i,j) \quad (2)$$

$\hat{Y}(i,j)$ represents the restored image and $Y(i,j)$ estimated airlight map. The human visual model is employed for the estimation of airlight map.[8] The airlight map is generated using multiple linear regression, which models the relationship between regional airlight and the coordinates of the image pixels. Weber's law explains that a human is more insensitive to variations of luminance in bright regions than in dark regions.

$$\Delta S = K \frac{\Delta R}{R} \quad (3)$$

where R is an initial stimulus, ΔR is the variation of the stimulus, and ΔS is a variation of sensation. We can estimate the existing stimulus in the image signal by the mean of the luminance within a region.[9] The variation between this and foggy stimulus can be estimated by the standard deviation within the region. Thus the human visual model would estimate the variation of sensation as

$$\frac{\text{STD}(Y)}{\text{mean}(Y)} = \frac{\sqrt{\frac{1}{n} \sum_{i=1}^n (y_i - \bar{Y})^2}}{\bar{Y}} \quad (4)$$

$$A(\lambda) = \frac{\text{STD}(Y - \lambda)}{\text{mean}(Y - \lambda)} \quad (5)$$

$$B(\lambda) = (\text{mean}(Y) - \lambda) \times \frac{\text{STD}(\text{ideal})}{\text{mean}(\text{ideal})^2} \quad (6)$$

The λ satisfying the above equation is the estimated airlight. The fog particles absorb a portion of the light in addition to scattering it. Ideal represents the ideal image having a uniform distribution from the minimum to the maximum of the luminance range. In general, the maximum value is 235 while the minimum value is 16. Edge enhancement is performed and contrast enhancement is performed to improve visual quality of the image. By changing the color space from YCbCr to RGB, RGB to R_{GB} , can be obtained. Therefore, after the color space conversion, histogram stretching is performed as a post-processing step.

$$\bar{I}_{R,G,B} = 255 \times \frac{I_{R,G,B} - \min(I_{R,G,B})}{\max(I_{R,G,B}) - \min(I_{R,G,B})} \quad (7)$$

$\bar{I}_{R,G,B}$ is the result of histogram stretching, $\max(I_{R,G,B})$ is the maximum value of $I_{R,G,B}$, that is an input for post-processing, and $\min(I_{R,G,B})$ is the minimum value of $I_{R,G,B}$.

IV. EXPERIMENTAL RESULTS

The proposed technique has been tested on several different images. The fig.5 shows subbands of obtained from DWT and



Fig.5. LL, LH, HL, and HH subbands obtained by using DWT and SWT.

SWT. Quantitative comparisons using Peak signal-to-noise ratio (PSNR) have shown superior results shown in Table I.

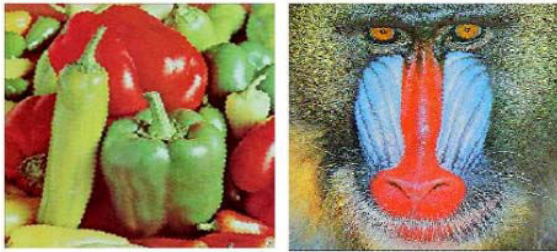


Fig .6.Enhanced output image with interpolation factor 2

PSNR IN DECIBELS				
WAVELET TYPE	Peppers	Lena	Baboon	Foggy tree
haar	12.1918db	11.3851db	10.8032db	9.8067db
db2	12.1781db	11.3554db	10.8052db	9.8307db
db97(proposed method)	32.99db	32.2187db	27.0291db	27.4285db

Table I Comparison of PSNR values for different wavelet types

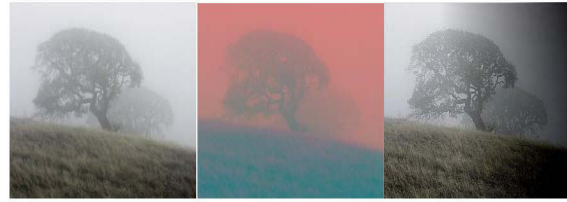


Fig.6.(a)foggy input image (b)YCbCr image (c) reconstructed image

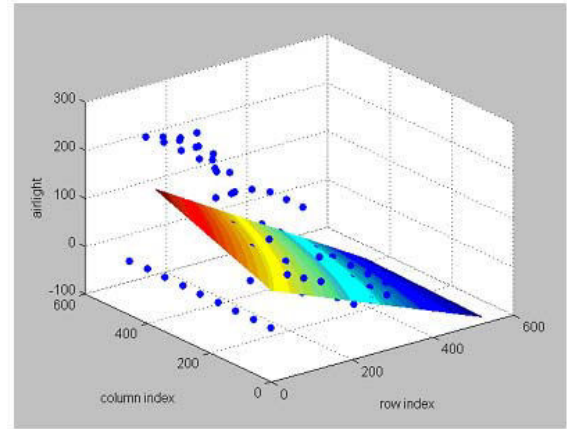


Fig.7.air light map of the image

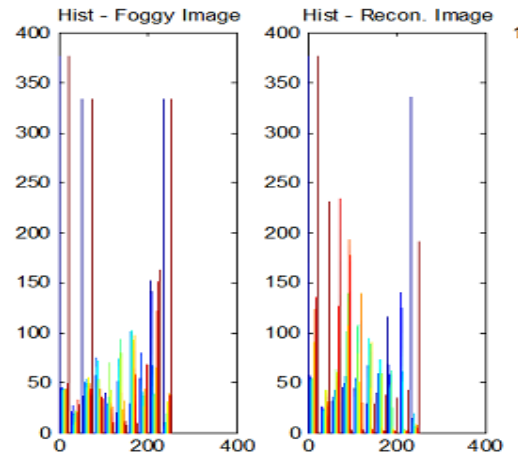


Fig. 8. Histogram comparison of foggy and reconstructed image

V. CONCLUSION

The work proposed an image resolution enhancement technique based on the interpolation of the high frequency subbands obtained by DWT, correcting the high frequency subband estimation by using SWT. The proposed technique has been tested on well-known benchmark images, where their PSNR and visual results show the superiority of proposed technique. Blurred image due to fog is restored by subtracting airlight map from degraded image. Thus defogging is done to improve the visual quality of image.

REFERENCES

- [1] Hasan Demirel and Gholamreza Anbarjafari, "Image Resolution Enhancement by Using Discrete and Stationary Wavelet Decomposition" IEEE Transactions on Image Processing, Vol. 20, NO. 5, MAY 2011.
- [2] W. K. Carey, D. B. Chuang, and S. S. Hemami, "Regularity-preserving image interpolation," IEEE Trans. Image Process., vol. 8, no. 9, pp.1295–1297, Sep. 1999.
- [3] Dongjun Kim, Changwon Jeon, Bonghyup Kang and Hanseok Ko, "Enhancement of Image Degraded by Fog Using Cost Function Based on Human Visual Model", IEEE International Conf. on Multisensor Fusion and Integration for Intelligent Systems, 2008
- [4] Y. Piao, I. Shin, and H. W. Park, "Image resolution enhancement using inter-subband correlation in wavelet domain," in Proc. Int. Conf. Image Process., 2007, vol. 1, pp. I-445–448.
- [5] H. Demirel and G. Anbarjafari, "Satellite image resolution enhancement using complex wavelet transform," IEEE Geoscience and Remote Sensing Letter, vol. 7, no. 1, pp. 123–126, Jan. 2010.
- [6] G. Anbarjafari and H. Demirel, "Image super resolution based on interpolation of wavelet domain high frequency subbands and the spatial domain input image," ETRI J., vol. 32, no. 3, pp. 390–394, Jun. 2010
- [7] Rafael C. Gonzalez, Richard E. Woods, Steven L. Eddins, Digital image processing using MATLAB.
- [8] Y. S. Zhai and X. M. Liu, "An improved fog-degraded image enhancement algorithm," Wavelet Analysis and Pattern Recognition, 2007. ICWAPR'07. International Conference on, vol. 2, 2007.
- [9] S. G. Narasimhan and S. K. Nayar, "Contrast restoration of weatherdegraded images," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, pp. 713-724, 2003.



REMOVAL OF HIGH AND LOW DENSITY IMPULSE NOISE USING MODIFIED MEDIAN FILTER

T.M.BENAZIR & B.M.IMRAN

Department of P.G, Applied Electronics, ICET, Mulavoor

Abstract:- Noise Suppression from images is one of the most important concerns in digital image processing. Impulsive noise is one such noise, which may corrupt images during their acquisition or transmission or storage etc. Noise should be removed in such a way that important information of image should be preserved. For removing salt and pepper noise from corrupted image we are using so many algorithms. In this paper an algorithm is proposed for the restoration of gray scale images that are highly corrupted by impulse noise (salt and pepper noise). The proposed algorithm consists of two phases. First phase detects whether the processing pixel is corrupted or not. In the Second phase it reconstructs the corrupted pixel by means of a filtering algorithm. This algorithm shows better results than the Standard Median Filter (MF), Center Weighed Median Filter(CWM) , Adaptive Median Filter(AMF), Adaptive Center Weighed Median Filter (ACWM) Decision Based Algorithm (DBA) and Modified Decision Based Unsymmetrical Trimmed Median Filter Algorithm(MDBUTMF).Obtained results with different grayscale images shows that proposed algorithm gives better Peak Signal-to-Noise Ratio (PSNR) and less Computational time and works well in removing salt and pepper noise at low, medium and high noise densities.

Key words: median filter, mid-point filter, salt and pepper noise, decision based unsymmetrical median.

I. INTRODUCTION

Noise is any undesired information that corrupts an image. Various types of noise introduces in digital images. For example, during image acquisition, light levels and faulty sensors are the major factors affecting the amount of noise in the resulting images and electronic transmission of image data can also introduce noise due to interference in the channel used in the transmission. Images are corrupted with noise modeled with a Gaussian, Impulse, Rayleigh or an erlang and speckle noise[1]. Impulse noise is a special type of noise where the intensity of the corrupted pixels has the tendency of being either relatively high or low. Impulse noise in images is present due to bit errors in transmission or introduced during the signal acquisition stage. There are two types of impulse noise, they are salt and pepper noise and random valued noise. Salt-and-pepper noise, a special case of impulse noise is the phenomenon where a certain percentage of individual pixels of an image are randomly digitized into the two extreme (maximum and minimum) intensities in the dynamic range. Its appearance is as white and black dots superimposed on the corrupted image and hence named salt and pepper noise. The information or data that was present in the original image may be damaged severely under the presence of salt-and-pepper noise. Therefore, removal of this type of noise is critical for the extraction of reliable and accurate information from a digital image[2].

Several nonlinear filters have been proposed for restoration of images contaminated by salt and pepper noise. Among these standard median filter has been established as reliable method to remove the salt and pepper noise without damaging the edge details. However, the major drawback of standard Median

Filter (MF) is that the filter is effective only at low noise densities. When the noise level is over 50% the edge details of the original image will not be preserved by standard median filter. In Weighed median(WM) filter and Center Weighed Median filter (CWM) weights are assigned to selected pixels in the filtering window in order to control the filtering behavior. However, these filters process all the pixels of an image without considering whether the current pixel is corrupted or not. In addition, local features of the image such as the possible presence of edges are also ignored. Therefore, when the noise level is high, these filters fail to recover the details and edges satisfactorily. Adaptive centre weighted median (ACWM) filter avoids the drawbacks of the CWM filters. Input data will be clustered by scalar quantization method, this results in fixed threshold for all of images[3].

The performance of Adaptive Median Filter AMF is good at lower noise density levels, due to the fact that there are only fewer corrupted pixels that are replaced by the median values. At higher noise densities, the number of replacements of corrupted pixel increases considerably; increasing window size will provide better noise removal performance; however, the corrupted pixel values and replaced median pixel values are less correlated. As a consequence, the edges are smeared significantly[4].

Decision based filter identifies the processed pixel as noisy, if the pixel value is either 0 or 255; else it is considered as not noisy. Under High noisy environment the DBA filter replaces the noisy pixel with neighborhood pixel. Due to repeated replacement of neighborhood pixel results in streaks in restored image. To avoid streaks in images an improved DBA (DBUTMF) is proposed with replacement of median of unsymmetrical trimmed

output, but under high noise densities all the pixel inside the current would take all 0's or all 255's or combination of both 0 and 255. Replacement of trimmed median did not fair well for above case[5]. Hence Modified decision based un-symmetric trimmed median filter (MDBUTMF) is proposed[6]. The above cause is eliminated by replacing the mean of the current window. When the noise densities scale greater than 80% the Smudging of edges occurs. All the algorithms fails well for low and medium density impulse noise but fails at high noise densities also these algorithms do not preserves edges. Hence a suitable algorithm which detects and eliminates impulse noise and preserves edges at high noise densities is proposed[1].

The rest of the paper is structured as follows. A brief introduction of unsymmetric trimmed median filter is given in Section II. Section III describes about the proposed algorithm and different cases of proposed algorithm. The detailed description of the proposed algorithm with an example is presented in Section IV. Simulation results with different images are presented in Section V. Finally conclusions are drawn in Section VI.

II. UNSYMMETRIC TRIMMED MEDIAN FILTER

The idea behind a trimmed filter is to reject the noisy pixel from the selected 3×3 window. Alpha Trimmed Mean Filtering (ATMF) is a symmetrical filter where the trimming is symmetric at either end. In this procedure, even the uncorrupted pixels are also trimmed. This leads to loss of image details and blurring of the image. In order to overcome this drawback, an Unsymmetric Trimmed Median Filter (UTMF) is proposed. In this UTMF, the selected 3×3 window elements are arranged in either increasing or decreasing order. Then the pixel values 0's and 255's in the image (i.e., the pixel values responsible for the salt and pepper noise) are removed from the image. Then the median value of the remaining pixels is taken. This median value is used to replace the noisy pixel. This filter is called trimmed median filter because the pixel values 0's and 255's are removed from the selected window. This procedure removes noise in better way than the ATMF[1].

III. PROPOSED ALGORITHM

The proposed algorithm processes the corrupted images by first detecting the impulse noise. The processing pixel is checked whether it is noisy or noisy free. That is, if the processing pixel lies between maximum and minimum gray level values then it is noise free pixel, it is left unchanged. If the processing pixel takes the maximum or minimum gray level then it is noisy pixel which is processed by filter. The steps of the algorithm are as follows.

ALGORITHM

Step 1: Select 2-D window of size 3×3 . Assume that the pixel being processed is $P(i,j)$.

Step 2: Check whether processing pixel $P(i,j)$ is corrupted or not.

Step 3: If $P(i,j)$ is an uncorrupted pixel and its value is left unchanged. This is illustrated in Case iii) of Section IV.

Step 4: If $P(i,j)$ is a corrupted pixel then two cases are possible as given in Case i) and ii). Case i): If the selected window contains all the elements as 0's and 255's. Then replace with the mean of the preprocessed neighborhood pixels by means of a midpoint filter. Case ii): If the selected window contains not all elements as 0's and 255's. Then eliminate 255's and 0's and find the median value of the remaining elements. Replace with the median value. Step 5: Repeat steps 1 to 4 until all the pixels in the entire image are processed. The pictorial representation of each case of the proposed algorithm is shown in Fig. 1. The detailed description of each case of the flow chart shown in Fig. 1 is illustrated through an example in Section IV.

IV. ILLUSTRATION OF PROPOSED ALGORITHM

The proposed algorithm consists of two phases. First phases detects whether the processing pixel is corrupted or not. In the second phase the corrupted pixels are reconstructed using the proposed algorithm. Each and every pixel of the image is checked for the presence of salt and pepper noise. Different cases are illustrated in this Section. If the processing pixel is noisy and all other pixel values are either 0's or 255's is illustrated in Case i). If the processing pixel is noisy pixel that is 0 or 255 is illustrated in Case ii). If the processing pixel is not noisy pixel and its value lies between 0 and 255 is illustrated in Case iii).

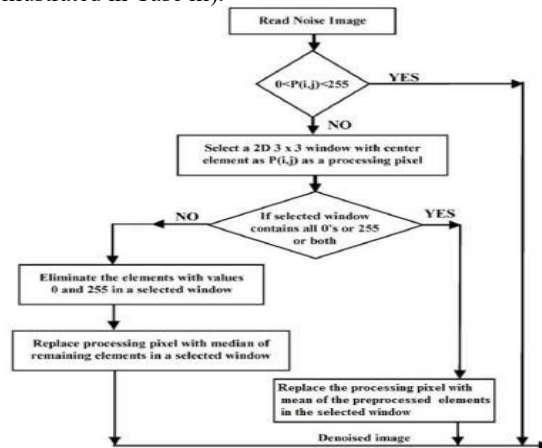


Fig 1: Proposed algorithm

Case i): If the selected window contains salt and pepper noise as processing pixel (i.e., 255/0 pixel value) and neighboring pixel values contains all pixels that adds salt and pepper noise to the image: An example is illustrated.

$$\begin{pmatrix} 0 & 255 & 0 \\ 0 & \langle 255 \rangle & 255 \\ 255 & 0 & 255 \end{pmatrix}$$

where “255” is processing pixel, i.e., $P(i,j)$. Since all the elements surrounding are 0’s and 255’s. If one takes the median value it will be either 0 or 255 which is again noisy. To solve this problem, the mean of the previously processed neighborhood pixels from the selected window is found and the processing pixel is replaced by the mean value. And for finding this mean value we go for a midpoint filter. Let P is the processing matrix and P' is the processed matrix. Consider a 3×3 window in the processing matrix as shown below. In cases where the processing pixel is corrupted and all the surrounding pixels are noisy, we replace that processing pixel by finding the mean of the previously processed neighborhood pixels filter and will replace the processing pixel by that value. Case ii): If the selected window contains salt or pepper noise as processing pixel (i.e., 255/0 pixel value) and neighboring pixel values contains some pixels that adds salt (i.e., 255 pixel value) and pepper noise to the image:

$$\begin{pmatrix} 78 & 90 & 0 \\ 120 & \langle 0 \rangle & 255 \\ 97 & 255 & 73 \end{pmatrix}$$

where “0” is processing pixel, i.e., $P(i,j)$. Now eliminate the salt and pepper noise from the selected window. That is, elimination of 0’s and 255’s. Here the elimination is unsymmetric and so it is unsymmetrical trimming. The 1-D array of the above matrix is [78 90 0 120 0 255 97 255 73]. After elimination of 0’s and 255’s the pixel values in the selected window will be [78 90 120 97 73]. Here the median value is 90. Hence replace the processing pixel by 90.

Case iii): If the selected window contains a noise free pixel as a processing pixel, it does not require further processing. For example, if the processing pixel is 90 then it is noise free pixel:

$$\begin{pmatrix} 43 & 67 & 70 \\ 55 & \langle 90 \rangle & 79 \\ 85 & 81 & 66 \end{pmatrix}$$

where “90” is processing pixel, i.e., $P(i,j)$. Since “90” is a noise free pixel it does not require further processing.

V. RESULTS AND COMPARISON

The performance of the proposed algorithm is tested with different grayscale images. The noise density (intensity) is varied from 10% to 90%. Denoising performances are quantitatively measured by the PSNR and MSE as defined in (1) and (2), respectively:

$$\text{PSNR in dB} = 10 \log_{10} \frac{255^2}{\text{MSE}} \quad (1)$$

$$\text{MSE} = \frac{\sum_i \sum_j (Y(i,j) - \hat{Y}(i,j))^2}{M \times N} \quad (2)$$

where MSE stands for mean square error, $M \times N$ is size of the image, Y represents the original image and denotes the denoised image.

The PSNR and MSE values of the proposed algorithm are compared against the existing algorithms by varying the noise density from 10% to 90% and are shown in Table I. From the Tables I, it is observed that the performance of the proposed algorithm (PA) is better than the existing algorithms at both low and high noise densities. A plot of PSNR against noise densities for Lena image is shown in Fig. 2.

Noise in %	MF	AC WM	AMF	DBA	MDB UTMF	PA
10	29.05	30.98	33.92	36.33	35.9	36.03
20	26.47	27.36	31.47	32.88	32.9	32.83
30	22.26	22.33	29.87	30.42	30	31.32
40	18.11	18.5	27.32	27.48	28.69	29.14
50	14.62	14.81	24.35	25.83	27.49	28.17
60	12	12.18	19.61	23.87	26.34	27.51
70	9.65	9.71	15.02	21.82	25.17	25.95
80	7.77	7.79	11.50	19.33	23.68	24
90	6.28	6.31	8.05	16.31	18.66	20.33

Table I Comparison of PSNR values of different algorithms for Lena image at different noise densities

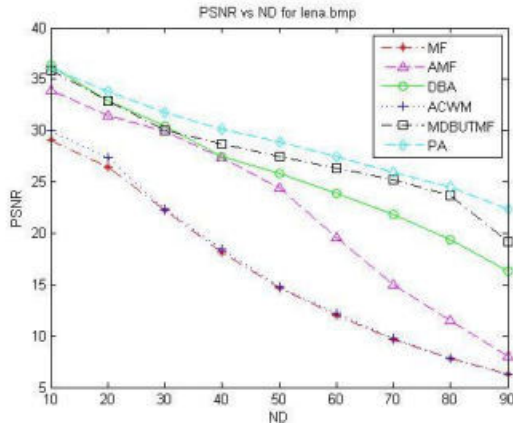


Fig 2: comparison of PSNR at different noise densities for Lena image

VI. CONCLUSION

In this paper the proposed algorithm presents a new approach to improve PSNR of highly corrupted images. This method gives an acceptable and recognizable restoration of image corrupted with noise as high as 90%. Unlike some filtering mechanisms which require iterations, and thus consumed lengthy processing time, the proposed filter only need to be applied once and is very efficient with its computational time. According to the experimental results, the proposed method is superior to the conventional methods in perceptual image quality, and it can provide quite a stable performance over a wide variety of images with various noise densities. One of the advantages of this method is that this method does not need the threshold parameter. Simulation results shows that this method always produces good output, even when tested with high level of noise. Thus, the proposed filter is able to suppress low to high density of salt and pepper noise, at the same time preserving fine image details, edges and textures well.

REFERENCES

- [1] Removal of High Density Salt and Pepper Noise Through Modified Decision Based Unsymmetric Trimmed Median Filter S. Esakkirajan, T. Veerakumar, Adabala N. Subramanyam, and C. H. PremChand, IEEE Signal Processing Letters, Vol. 18, No. 5, May 2011
- [2] Removal of Salt-and Pepper Noise in Images: A New Decision-Based Algorithm Madhu S. Nair, K. Revathy, and Rao Tataavarti, Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I, IMECS 2008, 19-21 March, 2008, Hong Kong
- [3] Adaptive Impulse Detection Using Center-Weighted Median Filters Tao Chen and Hong Ren Wu, IEEE Signal Processing Letters, Vol. 8, No. 1, January 2001
- [4] Hwang .H and Haddad .R.A, (1995) 'Adaptive median filters: new algorithms & results', IEEE transactions on image processing, Vol.no:4, pp.499-502.

- [5] S. Zhang and M. A. Karim, "A new impulse detector for switching median filters," IEEE Signal Process. Lett., vol. 9, no. 11, pp. 360–363, Nov. 2002.
- [6] Srinivasan .K.S., Ebenezer .D., (2007), 'A New Fast and Efficient Decision-Based Algorithm for Removal of High-Density Impulse Noises', IEEE Signal Processing Letters, Vol.no:14, pp.189 – 192.
- [7] Rafel.C.Gonzalez, and Richard.E.Woods, (2007). Digital Image Processing, Second Edition.



EFFICIENT COMPRESSION AND ENCRYPTION SCHEME FOR SECURE TRANSMISSION OF IMAGES AND ITS RECONSTRUCTION

NEETHU SARA RAJU & JOBINS GEORGE

ECE Department, ICET, Mulavoor

Abstract:- When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it. In this paper, we investigate the efficiency of reversing the order of these steps, i.e., first encrypting and then compressing, without compromise for compression efficiency or the information-theoretic security. A pseudorandom permutation and a linear encoding scheme is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, based on spatial correlation, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients and the linear decoding procedure.

Key Terms—Permutation, Linear encoding, Image compression, Image reconstruction.

I. INTRODUCTION

Consider the problem of transmitting redundant data over an insecure, bandwidth-constrained communication channel. It is desirable to both compress and encrypt the data. The traditional way to do this is to first compress the data to strip it of its redundancy followed by encryption of the compressed bit stream. The source is first compressed to its entropy rate using a standard source coder[3]. Then, the compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing the encrypted source. The compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data (also called ciphertext) without any knowledge of the original source[2],[3]. At the receiver, there is a decoder in which both decompression and decryption are performed in a joint step. The compression ratio and the quality of the reconstructed image are dependent on the values of compression parameters. Generally, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

Several techniques for compressing and decompressing encrypted data have been developed. In [1], proposes a novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image. It has been shown in [2] that, based on the theory of source coding, the performance of compressing encrypted data may be as good as that of compressing non encrypted data in theory. In [3], the encrypted image is decomposed in a progressive manner, and the most significant bits in high levels are compressed using rate-compatible punctured turbo codes. In [4], a compressive sensing

technique is introduced to achieve lossy compression of encrypted image data, and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. In [5], Compression of encrypted data is possible by using distributed source coding. Cipher text will be generated by adding a random key to the prediction errors.

In this work, we propose a novel system for lossy compression of encrypted image with flexible compression ratio, which is made up of image encryption, compression, and iterative decompression phases. The network provider may remove the redundant and trivial data from the encrypted image, and a receiver can retrieve the principal content of the original image using an iterative procedure.

II. ENCRYPTION, COMPRESSION AND RECONSTRUCTION

In the proposed scheme, a pseudorandom permutation and linear encoding scheme is used to encrypt an original image. Then, the encrypted data can be compressed by discarding the excessively rough and fine information of coefficients in the transform domain. When having the compressed data, the permutation way and secret key for linear encoding, with the aid of spatial correlation in natural image, the receiver can reconstruct the original image by iteratively updating the values of the coefficients.

A. Image Encryption

During encryption, assume the original image is in uncompressed format and each pixel with a gray value falling into $[0, 255]$ is represented by 8 bits. Denote the numbers of the rows and the columns in the original image as N_1 and N_2 , and the number of all pixels as $N=(N_1 \times N_2)$. So, the amount of bits of the original image is $8 \cdot N$. For image encryption, the data sender pseudorandomly permutes the N

pixels[5] and the permutation way is determined by a secret key.

In this scheme only the pixel positions are changed, but the pixel values are not masked. However, the number of possible permutation ways is $N!$, so that it is practical to perform a brute force search when N is fairly large. That means the attacker cannot recover the original content from the encrypted image with ordinary size and fluctuation.

To enhance the secrecy of permuted data, a linear encoding scheme[7] is used to change the pixel values as well. In this method, the image is first converted into a column vector and then the pixels are grouped into a particular size specified by a key-span. Each of these sets are then multiplied by a lower triangular matrix generated, which serves as the secret key for pixel value encryption. The multiplied values of pixels are then transformed to original image format and then transmitted as the encrypted image. Fig.1 illustrates the entire encryption procedure and Fig.2 illustrates linear encoding scheme in detail.

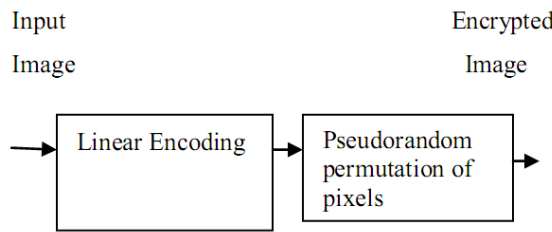


Fig. 1. Image Encryption Procedure

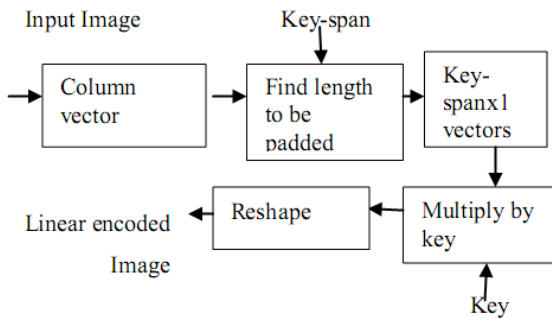


Fig. 2. Linear encoding

B. Compression of encrypted data

The compression technique to be proposed for the encrypted data is presented here. A lossy compression[1] is chosen for the compression of the encrypted image. In the compression procedure, a majority of pixels are converted to a series of coefficients using an orthogonal transform, and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount. In the compression procedure, a majority of pixels are converted to a series of coefficients using

an orthogonal transform, and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount. The detailed procedure is as follows.

1) When having the permuted pixel sequence, the network provider divides it into two parts: the first part made up of $\alpha.N$ pixels and the second one containing the rest of the $(1-\alpha).N$ pixels. Denote the pixels in the first part as p_1, p_2, p_3, \dots and the pixels in the second part as q_1, q_2, q_3, \dots . The value of α is within $(0, 1)$. Here, the data in the first part will be reserved while the data redundancy in the second part will be reduced. We call the pixels in the first part rigid pixels and the pixels in the second part elastic pixels.

2) Perform an orthogonal transform in the elastic pixels to calculate the coefficients

$$Q_1, Q_2, \dots, Q_{(1-\alpha).N}$$

$$[Q_1, Q_2, \dots, Q_{(1-\alpha).N}] = [q_1, q_2, \dots, q_{(1-\alpha).N}] \cdot H$$

Here, H is a public orthogonal matrix and it can be generated from orthogonalizing a random matrix.

3) For each coefficient, calculate

$$S_k = \text{mod} \left[\text{round} \left(\frac{Q_k}{\Delta/M} \right), M \right], \quad k=1, 2, \dots, (1-\alpha)N$$

where Δ and M are system parameters. The round operation returns the nearest integer and the mod operation gets the remainder. By Q_k is converted into an integer S_k within $(0, M-1)$. With a small M , the data amount for representing the elastic pixels is reduced. As Q_k can be rewritten in the following manner

$$Q_k = r_k \cdot \Delta + s_k \cdot \Delta + \frac{t_k}{M}$$

Where r_k and S_k are integers and

$$0 \leq S_k \leq M-1; \quad -\Delta \leq \frac{t_k}{M} < \Delta$$

It can be seen that the rough information and the fine information are discarded, while only the information on the medium level remains. Note that the rough information will be retrieved by an iterative image reconstruction procedure, and the loss of the fine information cannot seriously affect the quality of the reconstructed image. 4) Since r_k and S_k are within, we can regard them as a set of digits in a notational system

with a base . Segment the set of into many pieces with digits and calculate the decimal value of each digit piece. Then, convert each decimal value into bits in a binary notational system, where $L_2 = L_1 \cdot \log_2 M$

5) Collect the data of rigid pixels, the bits generated from all pieces of , and the values of parameters including $N_1, N_2, \alpha, \nabla, M$ and L_1 and to produce the compressed data of encrypted image. Since the data amount of parameters is small, the compression ratio R , a ratio between the amounts of the compressed data and the original image data, is approximately

$$R = \frac{8 \cdot \alpha \cdot N + \log_2 M \cdot (1 - \alpha) \cdot N}{8 \cdot N} = \alpha + \frac{\log_2 M \cdot (1 - \alpha)}{8}$$

C. Image Reconstruction

The image reconstruction technique that is to be handled at the receiver side is presented here. With the compressed data and the secret key, a receiver can perform the following steps to reconstruct the principal content of the original image. 1) Initially decomposition of the compressed data is done and retrieve the rigid data and their positions. Then estimate the elastic pixels using the nearest rigid pixels. 2)Rearrange the estimated values of elastic pixels using the same permutation way and calculate the coefficients.

$$[Q_1', Q_2' \dots Q_{(1-\alpha) \cdot N}'] = [q_1', q_2' \dots q_{(1-\alpha) \cdot N}'] \cdot H; \text{ and}$$

$$dk = \text{mod} (Ok' / \lceil \Delta / M \rceil \cdot M) - Sk$$

3)Then modify the coefficients to the closest values consistent with the corresponding value.

$$Qk'' = \begin{cases} \{([Qk' / \Delta] + 1) \cdot \Delta + Sk \cdot (\Delta / M)\}; & \text{if } dk \geq M/2 \\ \{[Qk' / \Delta] \cdot \Delta + Sk \cdot (\Delta / M)\}; & \text{if } -M/2 \leq dk < M/2 \\ \{[Qk' / \Delta] - 1\} \cdot \Delta + Sk \cdot (\Delta / M); & \text{if } dk < -M/2 \end{cases}$$

4)Perform the inverse transformation

$$[q_1'', q_2'' \dots q_{(1-\alpha) \cdot N}''] = [Q_1'', Q_2'' \dots Q_{(1-\alpha) \cdot N}''] H^{-1}$$

5)Finally calculate the average energy of difference between the two versions of elastic pixels.

$$D = \frac{1}{(1-\alpha) \cdot N} \sum_{K=1} (qk'' - qk')^2$$

6)If the calculated value is less than a particular threshold T , then estimate the value of elastic pixel using four neighbouring rigid pixels. This value of T

is recommended to be 0.05, to ensure that the last two versions of elastic pixels are close enough and update doesn't improve the reconstructed result further.

7)To retrieve back the original pixel values, linear decoding operation is performed as in Fig.3. Here it uses the same secret key which is used at the encoder end. This secret key is used to find the key-span and then divide each set of multiplied values of pixels to get the original values of pixels.

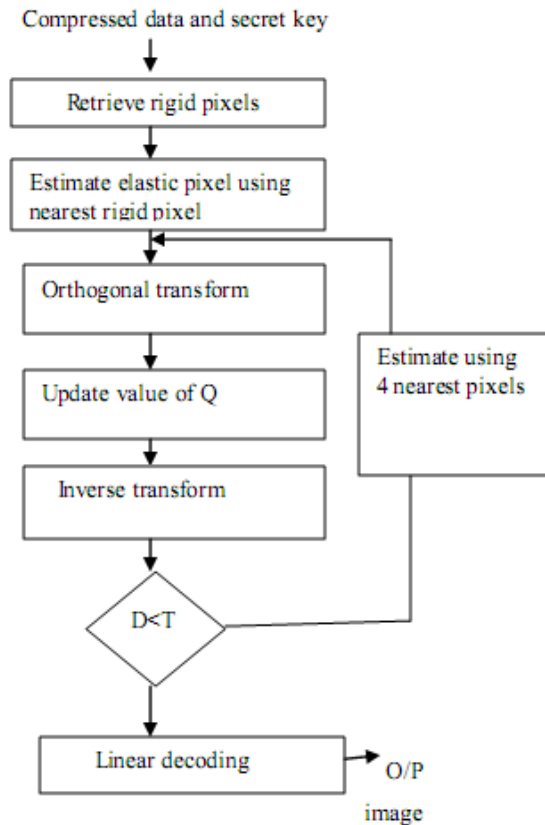


Fig.3. Image Reconstruction procedure

Fig.3 explains the complete reconstruction procedure and in Fig.4 the linear decoding method is illustrated in detail.

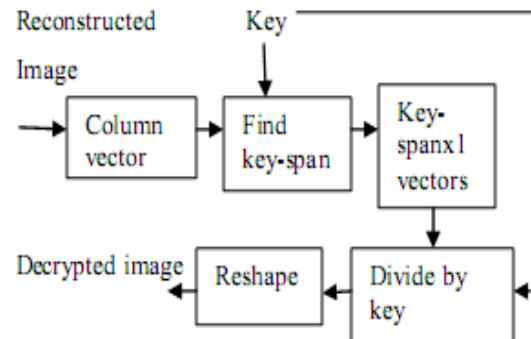


Fig.4. Linear Decoding

As long as we have an approximately estimated version as an initialization, the iterative procedure can produce a satisfactory reconstructed result. While the values of rigid pixels are used to give an initial estimation of elastic pixels, the values of sk provide more detailed information to produce a final reconstructed result with satisfactory quality. By the orthogonal transform, the estimation error of elastic pixels is scattered over all the coefficients. Since the coefficients are generated from all elastic pixels, the errors in a final reconstructed result are distributed over the image with an approximately uniform manner.

III. EXPERIMENTAL RESULTS AND DISCUSSION

The test image Lena was used for the experiment as the original image. The experiment was conducted with $\alpha = 0.99$, $\Delta = 80$ and $M = 4$. Fig. 5(a) shows the original image and Fig. 5(b) shows the encrypted image. With the compressed data, the receiver can retrieve the original content by using the image reconstruction procedure. Fig. 5(c) shows the medium reconstructed image by completing the reconstruction steps 1, 2 and 3. Fig. 5(d) shows the complete reconstructed result after completing steps 4 to 7. Here the compression ratio is found to be 0.98 and PSNR is found to be 43.7dB. It can be seen that the iterative procedure significantly improves the reconstruction quality.

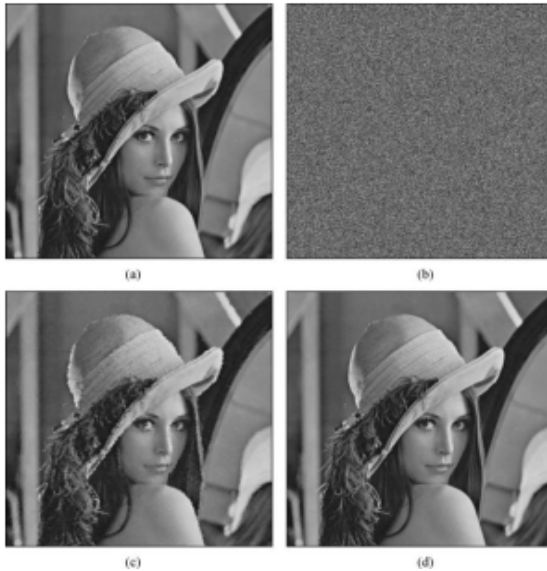


Fig.5 . (a) Original image Lena, (b) its encrypted version, (c) the medium reconstructed image from compressed data with PSNR 39.7dB, and (d) the final reconstructed image with PSNR 43.7dB.

Table 1 shows the values of compression ratio and PSNR for different values of α , Δ and M , for test image shown in Fig.6



Fig .6. Test Image for calculation of compression ratio and PSNR

		$\alpha = 0.15$	$\alpha = 0.10$	$\alpha = 0.07$
$M = 8$	$\Delta = 80$.48 , 36.5	.46 , 36.3	.43 , 36.1
$M = 8$	$\Delta = 60$.48 , 39.2	.46 , 38.4	.43 , 40.8
$M = 6$	$\Delta = 80$.45 , 34.3	.41 , 33.2	.39 , 32.8
$M = 6$	$\Delta = 60$.45 , 36.8	.41 , 35.8	.39 , 34.6
$M = 4$	$\Delta = 80$.39 , 33.6	.38 , 31.5	.35 , 31.6
$M = 4$	$\Delta = 60$.39 , 35.2	.38 , 34.3	.35 , 33.2

Table 1. Compression ratio R and PSNR (dB) in reconstructed image with different parameters

The quality of reconstructed image varies with different parameters chosen for different images. The compression ratio is determined by α & M , and the smaller α & M correspond to a lower R.

On the other hand, the larger the values of α & M , the iteration numbers are usually smaller and the qualities of reconstructed images are better since more rigid pixels and more detailed can be used to retrieve the values of elastic pixels. The compression ratio is independent of the value of Δ , and, generally speaking, a smaller Δ can result in a better reconstructed image since the receiver can exploit

more precise information for image reconstruction. However, more iterations are made for getting a final reconstructed result when using a smaller Δ , and, if the value of Δ is too small, the updating procedure is not convergent

IV.CONCLUSION

In this work, a new method for secure encryption of images is proposed which together with a lossy compression technique and iterative reconstruction method proves to be efficient for image storage and transmission. The encryption is done by a pseudorandom permutation of pixels and a linear encoding scheme that masks the pixel values, which is found to be highly secure. It is then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. In the reconstruction phase, an iterative updating procedure and linear decoding process will retrieve back the original image. The method is found to be highly secure and in general higher the compression ratio and smoother the original image, better will be the quality of reconstructed result. In future, advanced compression technique to improve the PSNR value,

can be incorporated with the scheme to improve its efficiency.

REFERENCES

- [1]. "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE transactions on information forensics and security, vol. 6, no. 1, MARCH 2011.
- [2]. "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pt. 2, pp. 2992–3006, Oct. 2004.
- [3]. "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
- [4]. "Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region 10 Conf. (TENCON 2009), 2009, pp. 1–6.
- [5]. "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization," Proc. Inst. Elect. Eng., Vis. Image Signal Process., vol. 147, no. 2, pp. 167–175, 2000.
- [6]. "Toward compression of encrypted images and video sequences," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, 2008.
- [7]. "Applications of linear algebra to cryptography", Proc. Inst. Adam Greleck, Math 208, 2004



A CONTOURLET DOMAIN WATERMARKING ALGORITHM

N.R.BRINTA & P.R.BIPIN

Department of P.G, Applied Electronics, Iahia College of Engineering & Technology, Muvattupuzha, Kerala, India

Abstract:-This paper presents a blind watermarking algorithm for digital images based on contourlet transform. After Contourlet transform, original image is decomposed into a series of multiscale, local and directional sub images. Each blocks of Arnold transformed watermark image, is embedded into suitable blocks of low pass coefficients of the contourlet transformed original image. Watermark is embedded using module arithmetic and odd-even quantization. The retrieving watermark algorithm is a blind detecting process, and it does not need original image. The experimental results show that the proposed watermarking algorithm is able to resist attacks, such as JPEG compression, noising, cropping and other attacks, and the watermarking is invisible and robust.

Keywords:-Arnold transform, blind watermarking, Contourlet transform, module arithmetic, quantization

I. INTRODUCTION

URING the past decade, with the development of information digitalization and internet, digital media increasingly predominate over traditional analog media. And also digital data can be shared by multiple users, distributed over network and is managed for longer period of time without any damage. However, as one of the concomitant side-effects, it is also becoming easier for some individual or group to copy and transmit digital products without the permission of the owner. Digital watermarking has been proposed as a solution to illegal copying or reproduction of digital data. The applications like copyright protection and authentication may mostly require the content owner or the authorized buyer to prove the authenticity without reference to the cover work. This creates a demand on blind watermarking techniques over non-blind watermarking techniques. For a watermarking scheme to be effective, it should have certain characters like imperceptibility, robustness, unambiguous. Wavelet based algorithms have been widely chosen for watermarking, since new image coding standards use wavelet domain representation and it models human visual systems as well. Wavelets are good at representing one dimensional signal. Two dimensional wavelet transform is a tensor product of a one dimensional wavelet, so they have limitation in capturing the geometry of image edges. Thus contourlet transform was defined to represent two dimensional signals more efficiently. Contourlet transform provides flexible multi-resolution, local and directional image expansion.[5] Contourlet D transform can also capture the intrinsic geometric structure which is the key in visual information. It is realized efficiently via a double iterated filter bank structure. In this double iterated filter bank structure, at first Laplacian Pyramid is used to capture point discontinuities and is followed by directional filter bank to link point discontinuities into linear structures [3]. Several digital image watermarking methods have been proposed. It includes both spatial and frequency domain techniques. Spatial-domain watermarking

technologies change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and with low computing complexity, because no frequency transform is needed. Frequency-domain watermarking embeds the watermark into the transformed image. Schyndel et al. [9] proposed a method for inserting information into original image using spatial domain technique. This method involves the embedding of the m-sequence on the LSB of the image data. The original 8 bit gray scale image data is capable of compression to 7 bits. But this method may be easily circumvented. Cox et al. [8] proposed a spread spectrum watermarking based on cosine transform in which watermark is embedded into perceptually most significant components of the data, thus the watermark is robust to signal processing operations. Maity et al. [4] proposed a blind spread spectrum watermarking scheme where watermark information is embedded redundantly in the multilevel wavelet coefficients of the cover image. High resiliency of the scheme is supported by good visual quality of the extracted watermark images from the several distorted watermarked images. Jayalakshmi et al. [2] proposed a relatively simple additive watermarking based on contourlet, the watermark is embedded into the high-pass coefficients of Contourlet transformed image, but the algorithm cannot to combine into the character of the carrier naturally, the visual quality decreased and the robustness are poor. Jingjing et al. [1] proposed a blind contourlet domain watermarking using module arithmetic, in which watermark is embedded into the low-pass coefficients of contourlet transformed, and it provides good robustness and invisibility. In order to increase robustness and invisibility, a new algorithm is proposed here. In this each blocks of watermark is embedded into that blocks of contourlet transformed original image which have optimum distance with the embedding watermark block. The paper is organized as follows. Section II, describes about Contourlet transform. And Section III describes the proposed algorithm. The simulation results of embedding and retrieval are given in Section IV. Conclusions are drawn in Section V.

II. CONTOURLET TRANSFORM

Contourlet transform gives flexible multi-resolution, local and directional image expansion. It is realized using Pyramidal Directional Filter Bank. Pyramidal Directional Filter Bank combines Laplacian Pyramid with Directional Filter Bank. Laplacian Pyramid captures the point discontinuities, and the directional filter bank links these discontinuities into linear structures [3]. Contourlet transform provides multi-scale decomposition of the image, which is obtained by using Laplacian Pyramid. Laplacian Pyramid at each level generates a down sampled low-pass version of the original and the difference between the original and prediction result in a band pass image [10]. The directional filter banks (DFB) are used to derive the high frequency sub bands with diverse directionality [7]. The DFB can be efficiently implemented via 1-level binary tree decomposition that leads to 21 sub bands with wedge-shaped frequency supports[6]. Contourlet transform extends to the different scales, orientation and height-width ratio support, which makes it approach to the image. In the frequency domain, Contourlet provides a multiscale decomposition, but it has a redundancy by 33%, the redundancy is generated by the LP. Contourlet transform is unique since the number of directional bands could be specified by the user at any resolution. Fig 1 shows the contourlet filter bank.

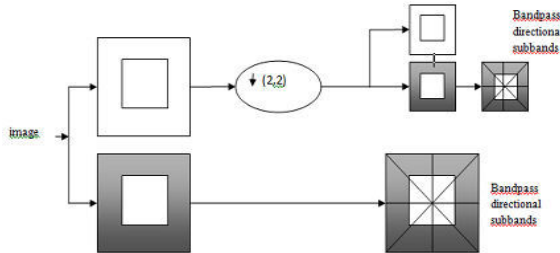


Figure 1. The contourlet filter bank: first, a multiscale decomposition by the Laplacian pyramid is computed, and then a directional filter bank is applied to each bandpass channel.

III. PROPOSED ALGORITHM

A. Watermark Embedding

Each blocks of watermark image is embedded into suitable blocks of original image, and save the block mappings on a table. Before embedding, each block of watermark image is scrambled using Arnold transform. And on each blocks of original image, perform two times of contour let transform, and then make module arithmetic on it, and choose the result of it as the location to embed watermark. The steps of the embedding process of the watermark are as follows:

1) Perform Arnold transform on the watermark image, then save the number K of the scrambling as a key.

- 2) Divide transformed watermark image into blocks.
- 3) Divide original image into blocks.
- 4) Consider one block from the watermark image and each block in original image one by one, then do the following steps. a) On the original image block, perform Contourlet transform of one layer, then perform a second transform the same as the first to the low-frequency of the last transform, then select the sub band for watermark embedding (D_m)

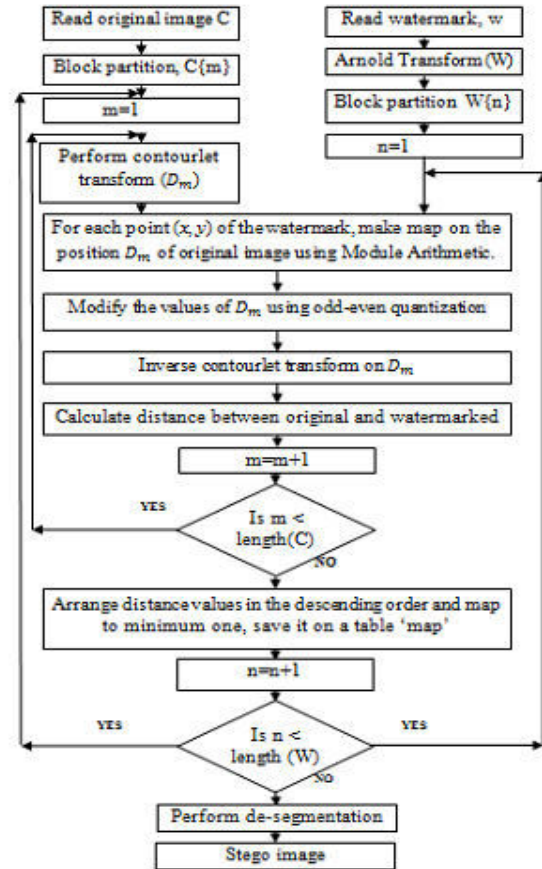


Figure 2. Watermark Embedding Algorithm

- b) Perform module arithmetic in the embedding domain, for each point (x, y) of the watermark, make a map on the position D_m , the map as follows:

$$i = \text{double}(x + 2 * y) \bmod (M_c / 4),$$

$$j = \text{double}(3 * x + 7 * y) \bmod (N_c / 4),$$

where M_c , N_c is the size of the original image. c) Modify the value of each D_m using the quantization method of odd-even, the rules are as follows:

$$D_m'(i, j) = \begin{cases} D_m(i, j) & \text{if } \text{Mod}(r(i, j), 2) = w(i, j) \\ [r(i, j) + 1] * \text{delta} & \text{if } \text{Mod}(r(i, j), 2) \neq w(i, j) \text{ and } w(i, j) = 1 \\ [r(i, j) - 1] * \text{delta} & \text{if } \text{Mod}(r(i, j), 2) \neq w(i, j) \text{ and } w(i, j) = 0 \end{cases}$$

$$r(i, j) = \text{round}(D_m(i, j) / \Delta)$$

Where, $D_m(i, j)$, $D_m'(i, j)$ are the values of the embedded points before and after the embedding

respectively, $W(i,j)$ means the relative (x, y) according to the map, $\text{round}(\bullet)$ represents the rounding operation, Δ represents the step size of the quantization.

- d) Perform 2 times of inverse contourlet transform.
- 5) After this, calculate the distance between original and watermarked image, and map watermark into that position of original image which have minimum distance, and also save the block mappings on a table.
- 6) Repeat steps 4&5 until all blocks of watermark image is considered
- 7) Perform de-segmentation on the blocks and result will be the watermarked image.

$$i = \text{double}(x + 2 * y) \bmod (M_c / 4),$$

$$j = \text{double}(3 * x + 7 * y) \bmod (N_c / 4),$$

where M_c, N_c are the size of the original image.

5) Modify the value of each D_m using the odd-even quantization method, the rules are as follows:

$$W_{s_n}(i,j) = \begin{cases} 0 & \text{if } \text{Mod}(r(i,j),2) = 0 \\ 1 & \text{if } \text{Mod}(r(i,j),2) = 1 \end{cases}$$

Where $r(i,j) = \text{round}(D_m(i,j) / \Delta)$ and $D_m(i,j)$ is the value of the extraction points having been found, $W_{s_n}(i,j)$ means the relative (x, y) according to the map.

- 6) Perform de-segmentation on the blocks of extracted Watermarks
- 7) Perform Arnold anti-scrambling on W_s , the scrambling number is K , and the result W is the extracted watermark.

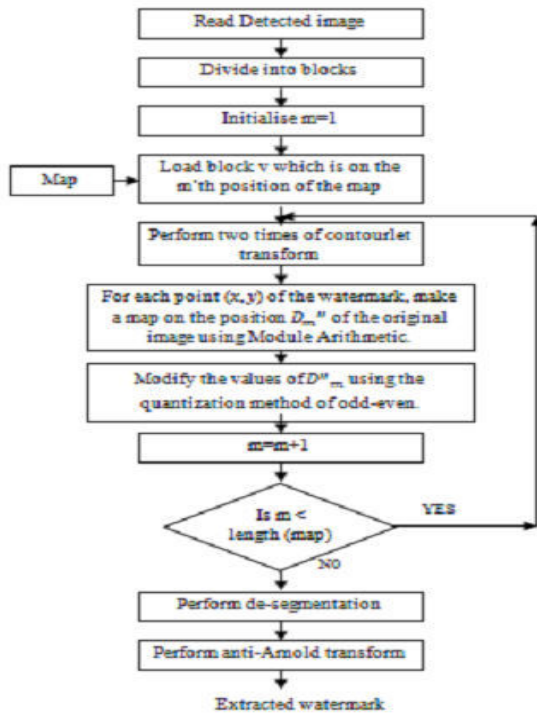


Figure 3. Watermark Extraction Algorithm

IV. RESULTS AND ANALYSIS

Simulation results with 400 x 400 Lena image and 48 x48 binary watermark are included here. In this simulation experiment, use a “9-7” pyramid filter of the LP, and use “pkva” orientation filter of DFB in the Contourlet transform. To measure the quality of embedded method and extracted watermark, we use Signal-to-noise ratio (PSNR) and Normalized Correlation (NC) respectively. They can be defined as follows.

$$PSNR = 10 \log((255^2 / MSE))$$

$$\text{Where } MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - I'(i,j))^2$$

$I(i,j)$ is the original image and $I'(i,j)$ is the watermarked image.

$$NC(w, w') = \frac{\sum_{i=1}^M \sum_{j=1}^N A(i,j)A'(i,j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N A(i,j)^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N A'(i,j)^2}}$$

$A(i,j)$ is the pixel value of the original watermark, $A'(i,j)$ is the pixel value of the extracted watermark. In this work, the step size of the quantisation is selected as 40. If we increase step size of quantisation, the image is robust although we got more distorted image. The variation of PSNR with step size of quantisation, Δ is shown in Fig 4. The watermark selected in this experiment is shown in Fig 3b. Watermarked image of Lena is shown in Fig 3c. The retrieved watermark from this image is also shown in Fig 3d. Figure indicates that after the watermark is embedded, the distortion of the image is small. When the image is not attacked, the value of PSNR is 39.40.

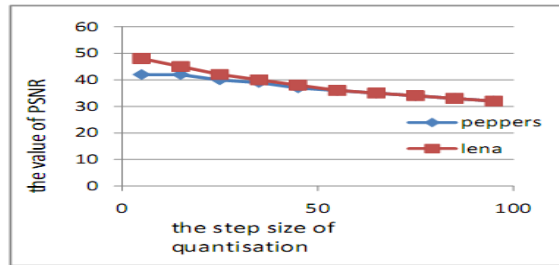


Figure 4. The relationship between PSNR and step size of quantisation



Figure 5. (a)original image, (b)Watermark, (c)watermarked images, (d)extracted watermark

Table 1 shows the PSNR of different images. Step size of quantisation is taken as 40 in both algorithms. From

this we can see that our algorithm will get a good visibility. Table II gives different NC under different attacks on Lena image, it also shows the comparison between our algorithm and reference [1] which uses the same original image and watermark, as shown in the table, our algorithm can resist a variety of attacks, and it has a better robustness.

TABLE I
THE PSNR OF DIFFERENT IMAGES

Image \ PSNR	Reference[1]	Our algorithm
Lena	38.45	39.40
Barbara	37.63	39.11
Boat	36.00	39.14
Peppers	34.89	38.63

TABLE II
THE COMPARISON BETWEEN OUR ALGORITHM AND REFERENCE 1

Attacks	Our algorithm	Reference[1]
JPEG compressed (50%)	1.0000	1.0000
Gaussian low pass filter	1.0000	1.0000
Gaussian noise (0.1%)	1.0000	1.0000
Salt and pepper noise (0.1%)	.9970	0.9900
Median filter	1.0000	1.0000
Wiener filter	1.0000	.9900

V. CONCLUSION

In this paper, we proposed a contourlet domain blind watermarking using module arithmetic and odd even quantisation with the help of distance method. This will give better performance in terms of PSNR. Since the contourlet transform used here can also capture contour information, the extracted watermark should be in a good visible pattern. This watermarking algorithm has good perceptual invisibility, since watermark is embedded using optimum mapping. Block based transform is used here, so robustness would be increased. From the experimental results, we can see that the proposed method is superior to the conventional methods in perceptual invisibility. The robustness of our algorithm is tested against various attacks and the results prove that the proposed algorithm is better than existing algorithm. By varying the value of delta, the step size of quantisation, we can change the value of PSNR. Different factors like the number of scrambling

times, the level of decomposition selected and the table representing optimum mapping determine the security of the algorithm.

VI. REFERENCES

- [1] Jingjing Wei, Shihua Yong, Xiaohu Ma, "Blind Digital Watermarking Algorithm based on Quantization in Contourlet Domain", IEEE 2nd International Conference on image processing, 2010.
- [2] Jayalakshmi M, Merchant S N, Desai U B. „Blind Watermarking in Contourlet Domain with Improved Detection“ Proceeding of 2006 IEEE International conference on Intelligent Information Hiding and Multimedia Signal Processing:449-452
- [3] Do, M.N., Vetterli, M. The contourlet transform: an efficient directional multiresolution image representation. IEEE trans. Image Processing2005, 14(2):2091 – 2106.
- [4] S. P. Maity and M. K. Kundu. "A blind cdma watermarking scheme in wavelet domain." IEEE Int. Conf Image Processing, pages 2633-2636, Oct. 2004.
- [5] M. Do, M. Vetterli, Contourlets: a directional multiresolution image representation, in: IEEE International Conference on Image Processing (ICIP'2002), vol.1, Rochester, 2002: 357-360.
- [6] Do M N, Vetterli M. Contourlets. Beyond Wavelets, Stoeckler J, Welland G V. Academic Press, 2002
- [7] M. N. Do and M. Vetterli, "Pyramidal directional filter banks and curvelets," in Proc. IEEE Int. Conf. on Image Proc., Thessaloniki, Greece, Oct. 2001.
- [8] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transaction on Image Processing 6(12): 1673-1687, 1997
- [9] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," in Proc. 1994 IEEE Int. Conf. on Image Proc., vol. II, (Austin, TX), pp. 86-90, 1994.
- [10] P. J. Burt and E. H. Adelson. The laplacian pyramid as a compact image codes. IEEE Trans. on Communications, 31:532- 540, Apr. 1983.



AN ALGORITHMIC APPROACH TO TRAVELLING SALESMAN PROBLEM

SUPRIYA PANDEY, SHALINI SINGH & RASHMI MISHRA

Department of Computer Science and Engineering, Institute of Technology and Management, GIDA
Gorakhpur, India

Abstract- Within scientific literature, the routing of vehicles on road transportation networks is an area of significant and great importance to transportation planners. This field includes well known and studied problems like traveling salesman problems or TSP, whose applications extend to other areas of transport and operations research. Computational results verified and further obtained from the test problems and statement taken from the literature indicate that this algorithm compares well in terms of accuracy with other existing algorithms, The TSP belongs to the class of NP-hard optimization problems. We conduct comprehensive experiments in order to assess the effects that these factors have on some of the best known algorithms for the TSP. We demonstrate that all these factors have a significant influence in solution time and quality.

Keyword- Routing, Linear Programming, Assignment Technique, Transportation.

1.INTRODUCTION

Travelling Salesman Problem: The traveling salesman problem or TSP for short is one of the most well known and thoroughly studied combinatorial optimization problems. The objective is to find the minimum cost (usually minimum distance) route visiting a set of n locations, where each location is visited exactly once. The tour must start and finish at the same location. A solution to the TSP problem is represented by a permutation of the n locations. The TSP is as well known NP-Hard problem. There are several practical uses for this problem, such as vehicle routing (with the additional constraints of vehicle's route, such as capacity's vehicles) [8] and drilling problems. This problem has been used during the last years as a comparison basis for improving several optimization techniques, such as genetic algorithms [1], simulated annealing [5], Tabu search [11], local search [4], ant colony [6] and neural networks[13], the latter used in this work. The principal types of neural network used to solve the TSP are: Hopfield's recurrent networks [13] and Kohonen's self organizing maps [9] communicating either [12]. Another way in which the TSP may lie in the high quality of results that can be obtained by traditional heuristics. The world of heuristics approaches to the TSP can be roughly divided into two classes. In addition to the *local search* approaches that are the topic, there are many different *successive augmentation* heuristics for the TSP. Such heuristics build a solution (tour) from scratch by a growth process (usually a greedy one) that terminates as soon as a feasible solution has been constructed. In the context of the TSP, we call such a heuristic a *tour construction* heuristic. Whereas the successive augmentation approach performs poorly for many combinatorial optimization problems, in the case of the TSP many tour construction heuristics do surprisingly well in practice. The best typically get

within roughly 10-15% of optimal in relatively little time. Furthermore, "classical" local optimization techniques for the TSP yield even better results, with the simple 3-Opt heuristic typically getting with 3-4% of optimal and the "variable-opt" algorithm of Lin and Kernighan [1973] typically getting with 1-2%. Moreover, for geometric data the above mentioned algorithms all appear to have running time growth rates that are $o(N^2)$, i.e., sub quadratic, at least in the range from 100 to 1,000,000 cities. These successes for traditional approaches leave less room for new approaches like Tabu search, simulated annealing, etc. to make contributions. Nevertheless, at least one of the new approaches, genetic algorithms, does have something to contribute if one is willing to pay a large, although still $o(N^2)$, running time price. The essence of the traveling salesman problem is evident within many practical applications in real life. From a mail delivery person trying to figure out the most optimal route that will cover all of his/her daily stops, to a network architect trying to design the most efficient ring topology that will connect hundreds of computers. In all of these instances, the cost or distance between each location, whether it be a city, building or node in a network, is known. With this information, the fundamental goal is to find the optimal tour. That is, to determine an order in which each location should be visited such that each location is visited only once, and the total distance traveled, or cost incurred, is minimal. In the general TSP, there are no restrictions on the distance/cost values. So, how and when did the traveling salesman problem first emerge within Mathematics and Computer Science studies? According to Lawler, Oestre, Rinnooy Kan & Shows [10], no one really knows. The origins range back to the 1920's, when a mathematician by the name of Karl Menger brought it to the attention of his colleagues in Vienna [2]. The problem then worked its way into Princeton's mathematical community during the 1930's [2].

Then, in the 1940's, mathematician Merrill Meeks Flood publicized the name, TSP, within the mathematical community at mass [10]. It was the year 1948 that Flood publicized the traveling salesman problem by presenting it at the RAND Corporation [10]; according to Flood "when I was struggling with the problem in connecting with a school-bus routing study in New Jersey" (Flood, 1956). The RAND Corporation is a non-profit organization that is the focus of intellectual research and development within the United States [14]. In its early days, RAND provided research and analysis to the United States armed forces, but then expanded to provide such services for the government and other organizations [14]. The TSP soon became very popular. This popularity was probably attributed to a few factors, one of which is the prestige of the RAND Corporation. Another factor is the connection between the TSP problem and the rising combinatorial problems within linear programming. Finally, its title is definitely a factor, which demonstrates relevance towards many tasks evident within people's daily lives. The TSP demonstrates all the aspects of combinatorial optimization. During the 1950's, Linear Programming was becoming a vital force in computing solutions to combinatorial optimization problems. This was due to the funding provided by the U.S. Air Force in the interest of obtaining optimal solutions to combinatorial transportation problems. As mentioned, this is one of the reasons why the TSP was in the interest of RAND. Attempts to solve the TSP were futile until the mid-1950's when Danzig, Fulkerson, and Johnson [7] presented a method for solving the TSP. They showed the effectiveness of their method by solving a 49-city instance [7]. However, it became evident, as early as the mid 1960's, that the general instance of the TSP could not be solved in polynomial time using Linear Programming techniques. In fact, it was conjectured that the TSP, and problems alike, posed such computational complexity that any programmable efforts to solve such problems would grow super polynomially with the problem size. These categories of problems became known as NP-hard, which will be discussed in more detail in chapter three. There has been a lot of progress in dealing with NP-hard problem such as the TSP. Solutions have been found to instances of the TSP with limited input. Polynomial time solutions have been found for special cases of the TSP. Researchers have even resorted to finding polynomial time approximation algorithms for NP-hard variations of the TSP, as discussed in chapters six and seven. However, until this very day, an efficient solution to the general case TSP, or even to any of its NP-hard variations, has not been found. Given a collection of cities and the cost of travel between each pair of them, the traveling salesman problem, or TSP for short, is to find the cheapest way of visiting all of the cities and returning to your starting point. In the

standard version we study, the travel costs are symmetric in the sense that traveling from city X To city Y costs just as much as traveling from Y to X.

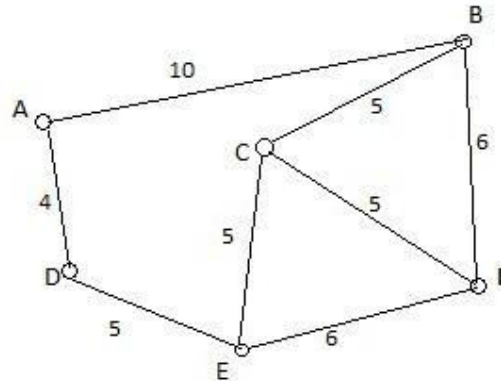


Figure.1: Graph Representation of TSP

In figure 1 each node in graph represents a city and each weighted edges in graph represents path from one city to other city. Weight is the cost to travel to reach city. Fitness function of the TSP will be

$$TCU = \sum_{k=1}^d C_{ij}$$

where C_{ij} is cost associated of path i to j and k is for the number of city or dimension.

2. NP COMPLETENESS

In order to understand NP-completeness, you must first understand the theory that is used to classify all computational problems and the algorithms used to solve them. That is the theory of Computational Complexity [13]. Recall that an algorithm is a set of step-by-step instructions that, when executed in the order specified, will solve a certain problem. Problems are basically classified as being within one of two categories. A problem is considered 'easy' if it can be solved by an algorithm that runs in polynomial time. On the other hand, a problem is considered 'hard' if it cannot be solved in polynomial time. Of course, these two classifications or definitions are not very elegant, but they are the basis of the computational complexity theory of problems that was developed.

The computational complexity theory divides problems into two classes. A complexity class is a set of all problems that can be solved in some certain amount of time, and that uses a certain amount of computing resources. An important note is that any problem that has been proven to be 'hard', in the sense that there exists only an exponential or super exponential solution to the problem, or that no algorithmic solution to the problem exists, does not fall within a complexity class. The reason for this is because it is not known how much time it will take for solution, and the computer's resources will probably run out by that time. In essence, algorithms for problems that are proven to be 'hard' are not practical and are very unpredictable.

3. SOLVING THE TRAVELLING SALESMAN PROBLEM

There have been many efforts to solve the travelling salesman problem ever since it was coined in 1930. The deterministic approaches strive to give an exact solution to the problem whereas the non deterministic try to provide a tour with a near minimal cost. This paper discusses few of such approaches in the following sub-section. A special case of a polynomial time non deterministic algorithm has also been proposed in this paper.

3. (A) DETERMINISTIC APPROACHES TO TSP

The assignment model can lead to infeasible solutions. Infeasibility removed by introducing additional constraints. One of the earliest deterministic solutions to TSP was provided by Danzig et al. [8], in which **linear programming (LP)** relaxation is used to solve the integer formulation by adding suitably chosen linear inequality to the list of constraints continuously. Held and Karp [10] presented a **dynamic programming formulation** for an exact solution of the travelling salesman problem, however it has a very high space complexity, which makes it very inefficient for higher values of N [9]. The **branch and bound technique** based algorithm published in [10] was able to successfully increase the size of the problem solvable without using any problem specific methods. The algorithm branches into the set of all possible tours while calculating the lower bound on the length of the tour for each subset. Eventually it finds a single tour in a subset whose length is less than or equal to some lower bound for every tour. The algorithm however grows exponentially in time with the input, but it is able to calculate the TSP for 40 cities with appreciable average time consumption as displayed by the authors. In the survey on exact algorithms for the Travelling Salesman problem, most attempts were found trying to address just a subset of the problem, instead of working on the complete problem space. This approach proved to be successful in almost all such cases, often slightly advantageous as far as time complexity is concerned. This happens due to the fact that not all problem instances are equally difficult. An efficient solution to the specific class of such instances can be used extensively by applications which deal mostly with these relatively easy instances only. The algorithm depicted in [15] solves the Travelling Salesman problem for graphs with degree at most 3 in exponential time. It has a slightly better time complexity of $O(2^{n-3})$ and a linear space complexity. However for a graph with n vertices and degree at most 4 this running time increases to

$$O((27/4 + \epsilon)^{n/2})$$

Although each of these algorithms become highly inefficient as we increase the number of cities in the tour.

3. (B) NON-DETERMINISTIC APPROACHES TO TSP

The exact solutions provide an optimal tour for TSP for every instance of the problem; however their inefficiency makes it unfeasible to use those solutions in practical applications. Therefore Non-Deterministic solution approach is more useful for the applications which prefer time of run of the algorithm over the accuracy of the result. There has been a vast research in past to solve the TSP for an approximate result. Some of the implemented approximate algorithms as described are listed here-[9]

3.1 Nearest Neighbor Algorithm

It follows a very simple greedy procedure: The algorithm starts with a tour containing a randomly chosen city and then always adds to the last city in the tour the nearest not yet visited city. The algorithm stops when all cities are on the tour.

3.2 Insertion Algorithms

All insertion algorithms start with a tour consisting of an arbitrary city and then choose in each step a city k not yet on the tour. This city is inserted into the existing tour between two consecutive cities i and j , such that the insertion cost (i.e., the increase in the tour's length) $d(i; k) + d(k; j) - d(i; j)$ is minimized. The algorithms stop when all cities are on the tour.

3.3 K-Opt Heuristics

The idea is to define a neighborhood structure on the set of all admissible tours. Typically, a tour t is a neighbor of another tour t' if t' can be obtained from t by deleting k edges and replacing them by a set of different feasible edges (a k -Opt move). In such a structure, the tour can iteratively be improved by always moving from one tour to its best neighbor till no further improvement is possible. The resulting tour represents a local optimum which is called k -optimal. Researchers have also taken help from literature on artificial intelligence and machine learning. Various algorithms optimizing the power of neural networks have been proposed for the approximation of the optimal cycle. Also a popular method is the Ant Colony optimization scheme.

3.4 Greedy Non-Deterministic Solution to TSP

A polynomial time non deterministic approach is being proposed here to solve the TSP in polynomial time. Although like other common greedy approaches, this approach too does not work as desired for some instances of the problem. However it halts in polynomial time for every instance and it provides an exact solution to the problem instances it works for. The algorithm combines the use of selective edge elimination from the graph and Wars halls algorithm to find the minimum Hamiltonian cycle in a graph. Wars halls algorithm is able to

determine the path matrix for a graph in n^3 time from the connectivity matrix. Thus it can determine if there is a path between any two vertices of the graph at any instant in polynomial time.

```

Procedure War shall ()
for (I = 0; i < max; I++)
for (j = 0; j < max; j++)
If (paths [I] [j] == 1)
for (k = 0; k < max; k++)
if (path[j][k] == 1)
path[I][k] = 1;
    
```

Figure 2: War shall Algorithm's Pseudo code

The algorithm starts from the starting node but works on the edges instead of the vertices. It picks up the largest unvisited edge repeatedly in the graph and removes it while taking care that the edge deletion should not make either of the 2 vertices adjacent due to that edge, disconnected from any of the other vertices in the graph. That is at every time step or every edge deletion there should be a path from every node in the graph to every other node. This condition is checked by running the Warshalls algorithm on the modified connectivity matrix of the graph at every time step. The algorithm halts after it has traversed all the edges in the original input graph. Since A graph with n nodes can have a maximum number of n^2 edges only, therefore the algorithm works in polynomial time ($O(n^5)$).Existence of a Hamiltonian Cycle in a graph means that at least a single path exists in the graph which connects all the vertices to each other and it will continue to exist even after the halting of the algorithm described. By executing this algorithm on the set of edges we are greedily removing the extra edges from the graph except the minimal cycle.

However, like any other greedy approach this algorithm also fails to deliver a solution for some problem instances. The algorithm halts with a minimum spanning tree of a graph instead of the Hamiltonian Cycle in a few cases. A major reason why greedy approaches although extremely efficient, do not work as required for some problem instances is due to the fact that in a greedy approach we always work on local minima while hoping to achieve the global minima by generalization. This approach fails terribly when there is a compromise required within the local minima's to achieve better global minima. Same phenomenon occurs in the execution of the proposed algorithm. Since here we are removing the heavier edges without considering their impact on possible Minimal Hamiltonian Cycle, hence assuming that such a cycle consists of only the minimum weighted edges of all the edges possible edges between two adjacent vertices. Thus the proposed algorithm will not work for cases where a compromise on the weight of the edge between 2 vertices

is required to achieve an overall minimum Hamiltonian Cycle Such a problem instance is shown in Figure 3.

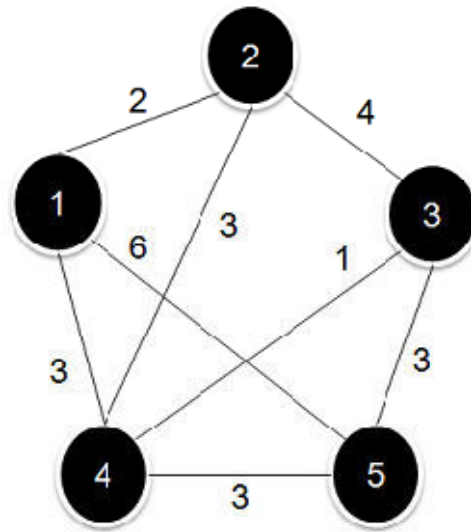


Figure 3: Example case when the proposed algorithm comes with a spanning tree instead of Hamiltonian Cycle.

4. RELATED WORK

A lot of work has been done in the area of Travelling Salesman Problem. The effect to the asymmetry of road transportation networks on the traveling salesman problem by Alejandro Rodriguez a,n, Rube'n Ruiz b [15].

For the solution of optimization tasks it is possible to use various algorithms. Some methods give better results and some give worse ones. We can obtain various methods for various tasks. The tests were done by twelve methods for the solution of travel salesmen problem. The tests include ten cities and it was searched the time of calculation, the value of fitness function, if the global minimum was found and the number of attempts. The tested algorithms are as follows: Exhaustive, Back Tracking, Random Search, Greedy, Hill Climbing, Simulated Annealing, Tabu Search, Ant Colony, Genetic Search and Particle Swarms.

Method	Time [sec]	Fit. f.	Count	Min
Exhaustive	426214	2,627	1	Y
Backtracking	21,549	2,627	1	Y
Random Search	0,019	3,438	20	Y
Greedy	0,020	2,627	1	Y
Hill Climbing	0,005	2,627	10	Y
Tabu Search	0,328	2,627	2	Y
Ant Colony	1,092	2,627	1	Y

The calculations which are done previously shows some of the following results:

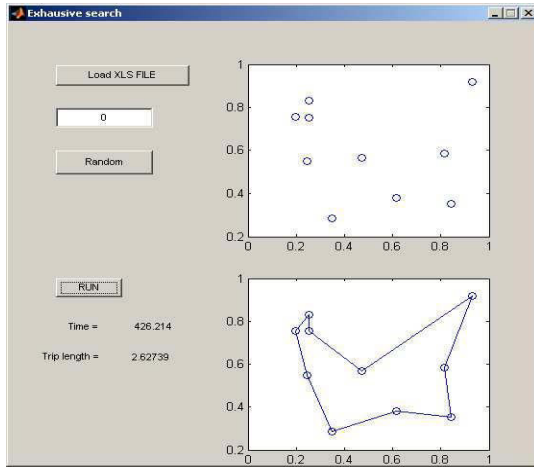


Figure.4:Exhaustive Search

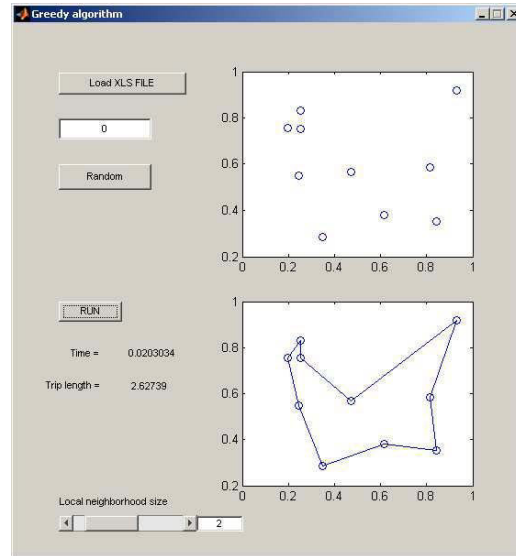


Figure.7: Greedy

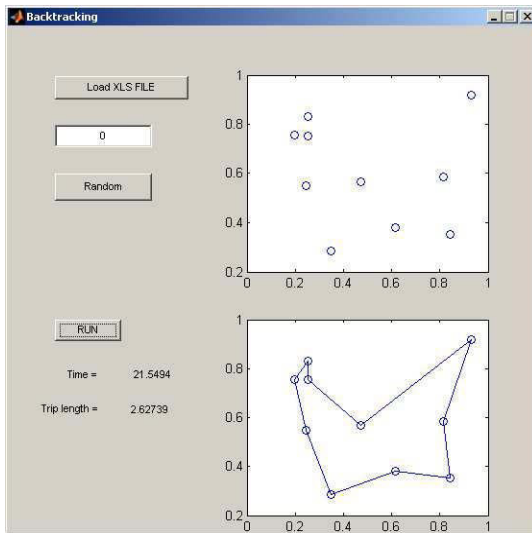


Figure.5 Backtracking

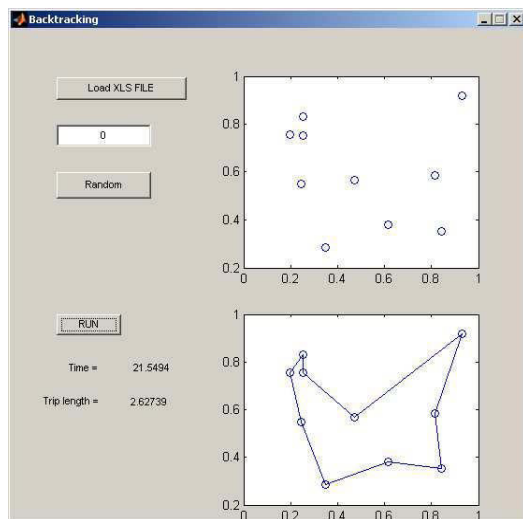


Figure.6:Random Search

And many others to go....So, the figures shows all about the previous done work on Travelling Salesman Problem. And the survey which is done on the literature material proves a long way go of Travelling Salesman Problem in many real-life problems too. One of the ultimate goals in computer science is to find computationally feasible exact solutions to all the known NP-Hard problems; a goal that may never be reached. Feasible exact solutions for the TSP have been found, but there are restrictions on the input sizes. An exact solution was found for a 318-City problem [Crowder & Pad berg, 1980]. As mention in [3], a 120-city problem by Gottschalk [1980], a 532-city problem by Pad berg and Renaldo [1987], a 666-city problem by Gottschalk and Holland [1991], a 1,002-city problem and a 2,392-city problem by Pad berg and Renaldo [1991].

5. CONCLUSION

In this paper, we got to know that we cannot use assignment technique to solve travelling salesman problem because it leads to infeasible solution. We can consider Greedy Algorithms, Ant Colony Algorithm etc. are the better solutions for TSP. Our main motive was vehicle routing which can easily be done by both the ways : deterministic or non-deterministic. In ant-colony, we adjust the routing strategy of the ant who worked better, that is to enhance the impact of pheromones in the route of this ant. Currently, if we focus then there are many ways of solving a problem statement using a number of methods. In our future work, we will investigate on a design or a problem statement which is real in application related to vehicle routing in big cities, to enhance the scope of TSP and implementation of various TSP algorithms. We also need to study how to reduce the complexity induced by our general algorithms. Moreover, we will deploy TSP to an

approach which will be total algorithmic with a blend of problems from real world and conduct more realistic experimental evaluations.

REFERENCES

- [1] M. Affenzeller, S. Wagner, A self-adaptive model for selective pressure handling within the theory of genetic algorithms, EUROCAST 2003, Las Palmas de Gran Canarias, Spain, 2003, Lect. Notes Comp. Sci. 2809 (1) (2003) 384–393.
- [2] D. AppleGate, R. Bixby, V. Chvatal and W. Cook. On the Solution of the Traveling Salesman Problems. Documenta Mathematica – Extra Volume ICM, chapter 3, pp. 645-656, 1998
- [3] Buthainah Fahren Al-Dulaimi, and Hamza A. Ali, "Enhanced Traveling Salesman Problem Solving by Genetic Algorithm Technique (TSPGA)", World Academy of Science, Engineering and Technology, Vol.38, pp. 296-302, 2008.
- [4] L. Bianchi, J. Knowles, J. Bowler, Local search for the probabilistic traveling salesman problem: Correction to the 2-p-opt and 1-shift algorithms, Eur. J. of Oper. Res. 162 (1) (2005) 206–219.
- [5] M. Budinich, A self-organizing neural network for the traveling salesman problem that is competitive with simulated annealing, Neural Comput. 8 (1996) 416–424
- [6] S.C. Chu, J.F. Roddick, J.S. Pan, Ant colony system with communication strategies, Inform. Sci. 167 (1–4) (2004) 63–76.
- [7] Hahsler, Michael; Hornik, Kurt (2007), "TSP Infrastructure for the Traveling Salesperson Problem
- [8] G. Laporte, The vehicle routing problem: an overview of exact and approximate algorithms, Eur. J. Oper. Res. 59 (2) (1992) 345–358
- [9] K.S. Leung, H.D. Jin, Z.B. Xu, An expanding self-organizing neural network for the traveling salesman problem, Neurocomputing 62 (2004) 267–292.
- [10] E. L. Lawler, J. K. Lenstra, A. H. G. Rinnooy Kan and D. B. Shmoys. The Traveling Salesman Problem: A Guided Tour of Combinatorial Optimization. John Wiley & Sons, 1985
- [11] G. Liu, Y. He, Y. Fang, Y. Oiu, A novel adaptive search strategy of intensification and diversification in tabu search, in: Proceedings of Neural Networks and Signal Processing, Nanjing, China, 200
- [12] G.C. Onwubolu, M. Clerc, Optimal path for automated drilling operations by a new heuristic approach using particle swarm optimization, Int.J. Prod. Res. 42 (3) (2004) 473–491.
- [13] R.L. Wang, Z. Tang, Q.P. Cao, A learning method in Hopfield neural network for combinatorial optimization problem, Neurocomputing 48 (4) (2002) 1021–1024
- [14] Wikipedia, the free encyclopedia - RAND. Retrieved November 10, 2006, from <http://en.wikipedia.org/wiki/RAND>
- [15] The effect to the asymmetry of road transportation networks on the traveling salesman problem by Alejandro Rodríguez a.n, Rube'n Ruiz b



IMAGE DENOISING USING PATCH BASED TECHNIQUE AND FUZZY-C MEANS ALGORITHM

NIMITHA K E & SAPNA ELIZABETH PAUL

Dept. of Electronics and Communication Engineering, Kerala ,India.

Abstract:-In the present scenario images play a vital role in many areas such as biomedical , space research etc...So for the efficient use of it ,the image it should be clear means free from noise. But there is chance for the addition of noise into the image during its access , process or transmission. For avoiding this different denoising methods are arised .This paper also deals with the image denoising. In this first its trying to minimize MSE by founding a statistical bound .Then a locally optimal Wiener filter where the parameters are learned from both geometrically and photometrically similar patches are designed. For this, the noisy image is first segmented into regions of similar geometric structure ,for this the Fuzzy c-means algorithm is used. The mean and the covariance of the patches within each cluster are then estimated. Next, for each patch, we identify photometrically similar patches and compute weights based on their similarity to the reference patch. These parameters are then used to perform denoising patchwise. To reduce artifacts, image patches are selected to have some degree of overlap (shared pixels) with their neighbor

Index Terms- Statistical bounds,Image denoising,,wiener filter, Clustering,Fuzzy -c means algorithm.

I. INTRODUCTION

RECENT years shown a great interest in the field of image denoising because of its wide need in many field such as biomedical ,weather forecasting, space research etc..Nowadays since most of the image capturing technique is in the digital domain and there is a great acceptability for the use of digital cameras. But due the competition ,the manufactures try to pack more number of pixels, which will decrease the quality of the captured image with the increase in the addition of noise .The present scenario clames for a wide varieties of image denoising methods , where one beets the other in any one feature such as the PSNR ,processing speed ,quality etc..So for to beet with this features, in this paper we are presenting a patch based image denoising by finding a statistical bound.Based on this bound we are then forming a patch based locally optimal Wiener filter ,the parameters for it ,such as the moments are trained from the geometrical and photometrically clustered patches . And for this parameters the clustering is performed using the Fuzzy -C means clustering algorithm which helps to improve the computational ability, for t

The challenge of any denoising algorithm is to suppress the noise without the lose of fine details. Severeal methods n has been emerged with the intention of this. The first modern adaptive method to successfully address these contradictory goals can be attributed to Tomasi *et al.* [3], where the authors proposed a generalization of the SUSAN filter [4], which itself was an extension of the Yaroslavky filter[5]. The authors there proposed denoising by weighted veraging pixels similar in intensity within a local neighborhood.Under strong noise, identifying such similar pixels can be challenging. In [6], Takeda *et al.* proposed a signal-dependent steering kernel

regression (SKR) framework for denoising.This method proved to be much more robust under strong noise. A patch-based generalization of the bilateral filter [3] was proposed in [7] and [8], where the concept of locality was extended to the entire image. Although the results there were encouraging, the true potential for this nonlocal means (NLM) method was only realized in [9] and [10]. Another patch redundancy-based framework, i.e., BM3D [11], adopts a hybrid approach of grouping similar patches and performing collaborative filtering in some transform [e.g., discrete cosine transform (DCT)] domain. It ranks among the best performing methods that define the current state of the art. In [1] and [2], we studied the problem from an estimation theory perspective to quantify the fundamental limits of denoising. The insights ained from that study are applied to develop a theoretically sound denoising method in this paper.

In this paper the statistical bounds are calculated and based on this the parameter for the Plow filtering is derived.The parameters are actually learned from the geometrically and photometrically similar patches.For ths at first the image is needed to be segmented into regions of similar geometrical stricter. The mean and the covariance of the patches within each cluster are then estimated. Next, for each patch, we identify photometrically similar patches and compute weights based on their similarity to the reference patch. These parameters are then used to perform denoising patchwise. To reduce artifacts, image patches are selected to have some degree of overlap (shared pixels) with their neighbors

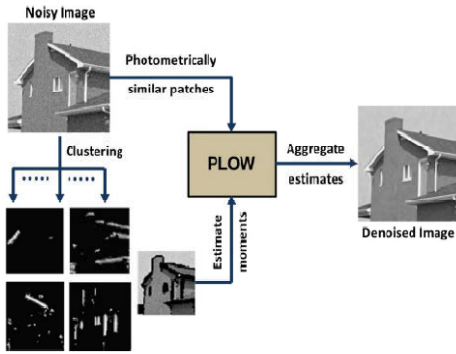


Fig 1.Flow of the proposed denoising method

II.STEP OF FLOW

A.Statistical Bound

From the noisy observation the intensity value of the each pixel can be given by

$$y_i = z_i + \eta_i, \quad i = 1, \dots, M. \quad (1)$$

based on this and the Bayesian cramer rao bound the MSE of denoising (estimating) any given patch in the image is bounded from below by

$$E[\|z_i - \hat{z}_i\|^2] \geq \mathcal{T}r[(J_i + C_z^{-1})^{-1}] \dots \dots \dots (2)$$

Where the J_i is the Fisher information matrix, C_z^{-1} is the inverse of covariance matrix. Then depending upon this bound the image is denoised. This covariance matrix captures the complexity of the patches and is estimated from all the geometrically similar patches present in the given image. Geometric grouping is done irrespective of the actual patch intensities. This is justified for intensity-independent noise when denoising performance is dictated by the complexity of patches, rather than their actual intensities.

The fisher information matrix give the information carried by the random variable, and it is influenced greatly by the noise characteristics. Photometric similarity among patches, as required to exploit redundancy, is a stricter condition than the geometric similarity property used for clustering.

B. GEOMETRIC CLUSTERING

When the image patches can be considerably noisy, we make use of the locally adaptive regression kernels (LARKs) as features for geometric clustering. Kernel regression as an effective tool for denoising. Kernel regression provides a rich mechanism for computing point-wise estimates of the function with minimal assumptions about global signal or noise models. Image patches within each cluster will exhibit similar structure, although the actual intensity values can be quite different. Then by applying the

kernels we can extract the features such as the mean and covariance and run the Fuzzy c means, and perform clustering. Thus we get the geometrically similar patches. Once the image is segmented into structurally similar regions, we estimate the moments, namely, mean and covariance, from the noisy member patches of each cluster. Since the noise patches are assumed to be zero mean i.i.d., the mean of the underlying noise-free image can be approximated by the expectation of the noisy patches within each cluster as

$$\bar{z} = E[y_i \in \Omega_k] \approx \frac{1}{M_k} \sum_{y_i \in \Omega_k} y_i \dots (2)$$

Then we calculate the covariance as

$$\hat{C}_z = [C_y - \hat{\sigma}^2 I]_+ \dots \dots (3)$$

, where $\hat{\sigma}$ is the standard deviation of noise

C. Photometrical similar patches

Upon this geometrically similar patch we again doing work to get photometrically similar patch. For this we take a reference patch from prefiltered noisy image. then find the patches which are similar to the reference patch by calculating the weight function as

The weight function is given as

$$w_{ij} \approx \frac{1}{\sigma^2} \exp \left\{ -\frac{\|y_i - y_j\|^c}{h^c} \right\} \dots \dots (4)$$

Where, h: smoothing parameter

D. The Algorithm

Thus by estimating the moments of geometrically similar patch and by finding photometrically similar patch by applying the bounds we can able to minimize the noise

One of the most widely used fuzzy clustering algorithms is the Fuzzy c- means (FCM) Algorithm. The FCM algorithm attempts to partition a finite collection of n elements $X = \{x_1, \dots, x_n\}$ into a collection of c fuzzy clusters with respect to some given criterion. Given a finite set of data, the algorithm returns a list of c cluster centres

$$C = \{c_1, \dots, c_c\} \text{ and a partition matrix } U = u_{i,j} \in [0, 1], \quad i = 1, \dots, n, \quad j = 1, \dots, c \dots \dots \dots (5)$$

, where each element u_{ij} tells the degree to which element x_i belongs to cluster c_j . Like the k-means algorithm, the FCM aims to minimize an objective function. The standard function is:

$$u_k(x) = \frac{1}{\sum_j \left(\frac{d(\text{center}_k, x)}{d(\text{center}_j, x)} \right)^{2/(m-1)}}.$$

.....(6)

which differs from the k-means objective function by the addition of the membership values u_{ij} and the fuzzifier m . The fuzzifier m determines the level of cluster fuzziness. A large m results in smaller memberships u_{ij} and hence, fuzzier clusters. In the limit $m = 1$, the memberships u_{ij} converge to 0 or 1, which implies a crisp partitioning. In the absence of experimentation or domain knowledge, m is commonly set to 2. The basic FCM Algorithm, given n data points (x_1, \dots, x_n) to be clustered, a number of c clusters with (c_1, \dots, c_c) the center of the clusters, and m the level of cluster fuzziness with

FUZZY C-MEANS CLUSTERING

In fuzzy clustering, each point has a degree of belonging to clusters, as in fuzzy logic, rather than belonging completely to just one cluster. Thus, points on the edge of a cluster, may be *in the cluster* to a lesser degree than points in the center of cluster. An overview and comparison of different fuzzy clustering algorithms is available.

Any point x has a set of coefficients giving the degree of being in the k th cluster $w_k(x)$. With fuzzy c -means, the centroid of a cluster is the mean of all points, weighted by their degree of belonging to the cluster:

$$c_k = \frac{\sum_x w_k(x)x}{\sum_x w_k(x)} \dots\dots\dots(7)$$

The degree of belonging, $w_k(x)$, is related inversely to the distance from x to the cluster center as calculated on the previous pass. It also depends on a parameter m that controls how much weight is given to the closest center. T

Algorithm

- 1.Give input noisy image
- 2.form them in to patches(n*n sized)(n=11)
- 3.compute The Lark features
- 4.Run Fuzzy-c-means algorithm, to perform clustering
- 5.Find the moments(mean &covariance) of each cluster

6.Find the photometrically similar PATCHES in each cluster by calculating the weights

7.Estimate denoised patch using photometrically similar patches

8.find the error covariance matrix

9.aggregate the multiple estimates

V.DISCUSSION OF RESULT

By using the Fuzzy c -means algorithm for clustering the denoising performance can be able to improve some how. By using the same and upon performing this for denoising the house image yield PSNR value of about 28.38.dB

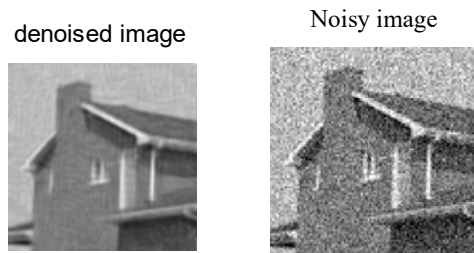


Fig 2. Result of Applying the Fuzzy c means clustering algorithm on denoising

Also the application of Fuzzy c -means algorithm will considerably help to improve the speed of denoising

Algorithm	K-means	Fuzzy -C Means
PSNR	28.33	28.38
Speed	75 s	Below this

VI. SUMMARY AND FUTURE WORK

In this paper, we have proposed a method of denoising motivated from the previous work in analyzing the performance bounds of patch-based denoising methods and patch based image denoising method. We have developed a locally optimal Wiener-filter-based method depend on fuzzy-c mean clustering and have extended it to take advantage of patch redundancy to improve the denoising performance. Our denoising approach does not require parameter tuning and is practical, with the added benefit of a clean statistical motivation and analytical formulation. We analyzed the framework in depth to show its relation to nonlocal means and residual filtering methods such as . Through

experimental validation, we have shown that our method produces results quite comparable with the state of the art. This method can be applicable to the colour images for the further enhancement

VII. REFERENCES

- [1] P. Chatterjee and P. Milanfar, "Is denoising dead?," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 895–911, Apr. 2010.
- [2] P. Chatterjee and P. Milanfar, "Practical bounds on image denoising: From estimation to information," *IEEE Trans. Image Process.*, vol. 20, no. 5, pp. 1221–1233, May 2011.
- [3] S. M. Smith and J. M. Brady, "SUSAN—A new approach to low level image processing," *Int. J. Comput. Vis.*, vol. 23, no. 1, pp. 45–78, May 1997.
- [4] L. P. Yaroslavsky, *Digital Picture Processing*. Secaucus, NJ: Springer-Verlag, 1985.
- [5] H. Takeda, S. Farsiu, and P. Milanfar, "Kernel regression for image processing and reconstruction," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 349–366, Feb. 2007.
- [6] A. Buades, B. Coll, and J. M. Morel, "A review of image denoising methods, with a new one," *Multiscale Model. Simul.*, vol. 4, no. 2, pp. 490–530, 2005.
- [7] S. P. Awate and R. T. Whitaker, "Unsupervised, information-theoretic adaptive image filtering for image restoration," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 3, pp. 364–376, Mar. 2006.
- [8] C. Kervrann and J. Boulanger, "Optimal spatial adaptation for patchbased image denoising," *IEEE Trans. Image Process.*, vol. 15, no. 10, pp. 2866–2878, Oct. 2006.
- [9] C. Kervrann and J. Boulanger, "Local adaptivity to variable smoothness for exemplar-based image denoising and representation," *Int. J. Comput. Vis.*, vol. 79, no. 1, pp. 45–69, Aug. 2008.
- [10] K. Dabov, A. Foi, V. Katkovnik, and K. O. Egiazarian, "Image denoising by sparse 3-D transform-domain collaborative filtering," *IEEE Trans. Image Process.*, vol. 16, no. 8, pp. 2080–2095, Aug. 2007.
- [11] N. A. Mohamed, "Modified fuzzy C-mean algorithm for medical image segmentation," M.Sc. thesis, Elect. Eng. Dept., Univ. Louisville, Louisville, KY, 1999.



AN ENERGY AWARE MODIFIED LEACH PROTOCOL FOR ENERGY EFFICIENT ROUTING IN WIRELESS SENSOR NETWORKS

NANDAKISHOR SIRDESHPANDE & VISHWANATH UDUPI

Department of Electronics and Communication, Gogte institute of technology, Belgaum

Abstract:-Wireless Sensor Networks (WSN) are networks of typically small, battery-powered, wireless devices, equipped with on-board processing, communication, and sensing capabilities. Especially wireless sensor network suffers from excessive packet loss, over hearing, retransmission of the packets due to node mobility and constant energy dissipation. A current technique for routing and data transmission does not take into account of optimizing the transmission through Energy Balancing. There are several power and energy aware algorithms that claim to compensate for the energy losses. The main fundamental of most of the techniques is to route the packets through the highest energy nodes which lead to quick battery drainage of those node. Therefore the network lifetime decreases. In this project we have proposed a unique protocol for Network lifetime improvement by modifying the Leach protocol. The fundamental of the protocol is to develop a cluster based routing where cluster heads should be selected based on maximum coverage and should have sufficient energy to prolong the communication. Clusters are dynamically formed and changed with transmission. The technique is compared with conventional LEACH. Result shows that the proposed system achieves high data delivery with extended lifetime

Keywords: *Energy Efficiency, Leach Protocol, Transmission Range.*

I. INTRODUCTION

Recent advances in wireless communication technologies and the manufacture of inexpensive wireless devices have led to the introduction of low-power wireless sensor networks. Due to their ease of deployment and the multi-functionality of the sensor nodes, wireless sensor networks have been utilized for a variety of applications such as healthcare, target tracking, and environment monitoring. The main responsibility of the sensor nodes in each application is to sense the target area and transmit their collected information to the sink node for further operations. Resource limitations of the sensor nodes and unreliability of low-power wireless links, in combination with various performance demands of different applications impose many challenges in designing efficient communication protocols for wireless sensor networks. Meanwhile, designing suitable routing protocols to fulfill different performance demands of various applications is considered as an important issue in wireless sensor networking. In this context, researchers have proposed numerous routing protocols to improve performance demands of different applications through the network layer of wireless sensor networks protocol stack. Most of the existing routing protocols in wireless sensor networks are designed based on the single-path routing strategy without considering the effects of various traffic load intensities. In this approach, each source node selects a single path which can satisfy performance requirements of the intended application for transmitting its traffic towards the sink node. Although route discovery through single-path routing approach can be performed with minimum computational complexity and resource utilization, the limited capacity of a single path highly reduces

the achievable network throughput. Furthermore, the low flexibility of this approach against node or link failures may significantly reduce the network performance in critical situations. For instance, whenever the active path fails to transmit data packets (as a result of limited power supply of the sensor nodes, high dynamics of wireless links and physical damages), finding an alternative path to continue data transmission process may cause extra overhead and delay in data delivery. Therefore, due to the resource constraints of sensor nodes and the unreliability of wireless links, single-path routing approaches cannot be considered effective techniques to meet the performance demands of various applications. In order to cope with the limitations of single-path routing techniques, another type of routing strategy, which is called the multipath routing approach has become as a promising technique in wireless sensor and *ad hoc* networks. Dense deployment of the sensor nodes enables a multipath routing approach to construct several paths from individual sensor nodes towards the destination. Discovered paths can be utilized concurrently to provide adequate network resources in intensive traffic conditions. Alternatively, each source node can use only one path for data transmission and switch to another path upon node or link failures. The latter one is mainly used for fault-tolerance purposes, and this is known as *alternative path routing*. In the past decade, multipath routing approach has been widely utilized for different network management purposes such as improving data transmission reliability, providing fault-tolerant routing, congestion control and Quality of Service (QoS) support in traditional wired and wireless networks. However, the unique features of wireless sensor networks (e.g., constrained power supply, limited computational capability, and low-memory capacity) and the characteristics of short-range radio communications (e.g., fading and

interference) introduce new challenges that should be addressed in the design of multipath routing protocols. Accordingly, existing multipath routing protocols proposed for traditional wireless networks (such as *ad hoc* networks) cannot be used directly in low-power sensor networks. During the past years, this issue has motivated the research community of wireless sensor networks to develop multipath routing protocols which are suitable for sensor networks.

There are several papers surveying proposed routing protocols for wireless sensor networks. These surveys describe and analyze the general routing strategies proposed for sensor networks. However, none of these literatures has provided a comprehensive taxonomy on the existing multipath routing protocols for wireless sensor networks. Al-Karaki *et al.* presented routing challenges and design issues in wireless sensor networks. They classified all the existing routing strategies based on the network structure and protocol operation. Alwan *et al.* provided a brief overview on the existing fault-tolerant routing protocols in wireless sensor networks and categorized these protocols into retransmission-based and replication-based protocols. Tarique *et al.* and Mueller *et al.* classified the existing multipath routing protocols in *ad hoc* networks based on the primary criterion used in their design. Accordingly, the principal motivation of conducting this research was lack of a comprehensive survey on the proposed multipath routing protocols for wireless sensor networks. To the best of our knowledge, this paper is the first effort to classify and investigate the operation as well as benefits and drawbacks of the existing multipath routing protocols in sensor networks.

RELATED WORK

In this section, highlighting the previous works on improving the lifetime of wireless sensor networks by using various scheduling algorithms and data aggregation techniques for sensors. Routing with data aggregation targets at jointly exploring the data structure and network topology to reduce energy consumption for data gathering in resource limited sensor networks. If the complete knowledge of all source correlations is available in advance at each source, theoretically the best approach is to use distributed source coding typified by Slepian-Wolf coding [3]. In this technique, compression is done at original sources in a distributed manner to achieve the minimum entropy and hence avoid the need for data aggregation on the intermediate nodes. In [4], an optimal rate allocation algorithm is proposed for nodes in the network and SPT is employed as the routing scheme. However, implementation of distributed source coding in a practical setting is still an open problem and likely to incur significant additional cost because of the aforementioned assumption. Routing-driven algorithms emphasize

source compression at each individual node and aggregation occurs when routes intersect. In [5] the directed diffusion scheme was proposed where sensors create gradients of information in their respective neighborhoods. If the gradients match the broadcasted interests from the sink and data is aggregated at the intersections. So the extra overhead is required. To improve path sharing a greedy incremental tree (GIT) is described in to adjust aggregation points on the routes. Energy-aware routing [6] shows that to use a set of sub-optimal paths occasionally to increase the lifetime of the network. These paths are chosen by means of a probability function, which depends on the energy consumption of each path. The approach shows that using the minimum energy path all the time will deplete the energy of nodes on that path. Instead, one of the multiple paths is used with a certain probability so that the whole network lifetime increases. The protocol assumes that each node is addressable through a class-based addressing which includes the location and types of the nodes. In addition, the approach requires gathering the location information and setting up the addressing mechanism for the nodes, which complicate route setup. Low-Energy Adaptive Clustering Hierarchy (LEACH) [7] is one of the most popular hierarchical routing algorithms for sensor networks. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. This will save energy since the transmissions will only be done by such cluster heads rather than all sensor nodes. LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it is not applicable to networks deployed in large regions. In Power Efficient Gathering in Sensors Information Systems (PEGASIS)[8] sensors form chains along which a node transmits and receives from a nearby neighbor. PEGASIS introduces excessive delay for distant node on the chain. In addition the single leader can become a bottleneck, which causes decreases of network lifetime WSNs. For example, every sensor needs to be aware of the status of its neighbour so that it knows where to route that data. Such topology adjustment can introduce significant overhead especially for highly utilized networks. In [9], the maximum lifetime data aggregation (MLDA) problem. The objective is to find a set of data gathering schedules to maximize the system lifetime a schedule is defined as a collection of directed spanning trees rooted at the sink node. MLDA is performing better than the other protocols in terms of system lifetime; the algorithm is computationally expensive for very large sensor networks. In [10], the impact of the data correlation on the routing schemes is studied and a static clustering scheme is showed that they achieve a near-optimal performance for various spatial correlations. The main goal of this project work is by jointly optimizing routing and data

aggregation, the network lifetime can be extended from two dimensions. One is to reduce the traffic across the network by data aggregation, which can reduce the power consumption of the nodes close to the sink node. The other is to balance the traffic to avoid overwhelming the bottleneck nodes. The energy consumption can be minimized if the amount of data that needs to be transmitted is also minimized. The solution to this is data aggregation. Data compression techniques are used to remove the redundancy information. Removing the redundancies results in transmitting fewer numbers of bits, and hence reduces energy Consumption and increases the network lifetime.

II. PRESENT SYSTEM MODEL

LEACH-distributed or LEACH [2] is a self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. LEACH makes some assumptions about both the sender nodes and the underlying network, being some of them very strong. LEACH assumes that all sensor nodes can adapt their transmission range. Furthermore, energy consumption during transmission scales exactly with the distance and every sensor node is able to reach a base station (BS). Moreover, nodes support several MAC layers and perform signal-processing functions. LEACH uses a distributed algorithm to determine the cluster heads in the set-up phase whereas in the steady phase nodes send their data according to the time schedule provided by their cluster heads. This operation of LEACH is divided into rounds as shown in figure1

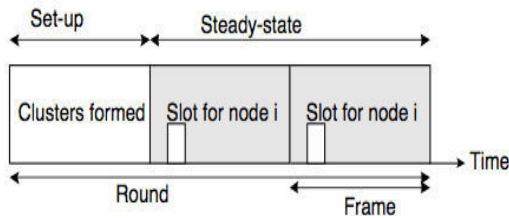


Figure 1: LEACH operations

A. Advertisement Phase

When clusters are created, each node n autonomously decides if it will be a cluster head for the next round. The selection is stochastic and each node determines a random number between 0 and 1. If this number is lower than a threshold $T(n)$, the node becomes a cluster head. $T(n)$ is determined according to the equation.

$$T_1(n) = \frac{P}{1 - P * (r \bmod \frac{1}{P})},$$

$$(1) T_1(n) = P/1-P*(r \bmod 1/P)$$

for nodes that have not been cluster head in the last $1/P$ rounds, otherwise $T(n)$ is zero. Here P is the desired percentage of cluster heads and r is the current round. Using this algorithm, each node will be a cluster head exactly once within $1/P$ rounds. After $1/P - 1$ rounds, $T(n) = 1$ for all nodes that have not been a cluster head. When a node has elected itself as a cluster head, it broadcasts an advertisement message telling all nodes that it is a cluster head. This advertisement is done using a CSMA MAC protocol. Non-cluster heads use these messages from the cluster heads to choose the cluster they want to belong for this round based on the received signal strength of the advertisement message.

B. Cluster Set-Up Phase

After each node has decided to which cluster it belongs, it must inform the cluster head node that it will be a member of its cluster. Each node transmits this information back to the cluster head again using CSMA MAC protocol. During this phase, all cluster head nodes must keep their receivers on.

C. Schedule Creation

The cluster head receives all the messages from the nodes that would like to join the cluster. Based on the number of nodes in the cluster, the cluster head creates a TDMA schedule telling each node when it can transmit the data. This schedule is broadcasted back to the nodes included in the cluster.

D. Data Transmission

Once the clusters are created and the TDMA schedule is fixed, nodes can start to transmit their data. Assuming nodes always have data to send, they send it during their allocated transmission time to the cluster head. This transmission uses the minimal amount of energy based on the received strength of the cluster head advertisement. The radio of each non-cluster head can be turned off until the node's allocated transmission time, thus minimizing energy dissipation. The cluster head node must keep its receiver on to receive all the data from the nodes in the cluster. Once all the data has been received, the cluster head performs optimization functions such as data aggregation or other signal processing functions to compress the data into a single signal. This composite signal, which is a high-energy transmission since the base station is far away, is then sent to the base station. The cluster heads send these data packets using a fixed spreading code with CSMA. This is the steady-state operation of LEACH networks. After a certain time, which is determined a priori, the next round begins with each node determining if it will become a cluster head for this round and advertising the decision to the rest of nodes as described in the advertisement phase.

III. PROPOSED MODEL

The fundamental of the protocol is to develop a cluster based routing where cluster heads should be selected based on maximum coverage and should have sufficient energy to prolong the communication. In proposed System we are routing through High Energy node and for cluster formation, selecting Node with High Node Energy. Clusters are dynamically formed and changed with transmission.

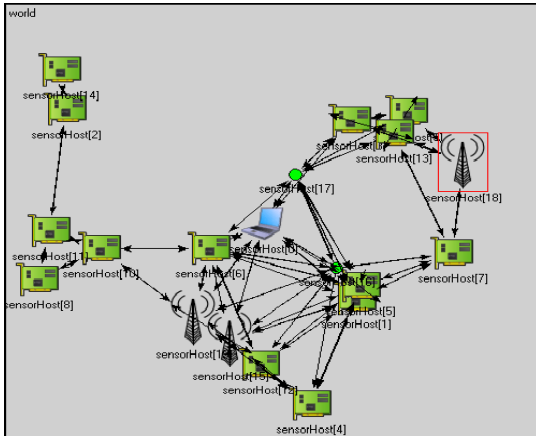


Figure 1.1

Algorithm: Modified LEACH Algorithm.

1. Let W, H be the Network width and Height. Network Area $A=W \times H$.
2. Let there be N nodes with E_i Energy at (X_i, Y_i) point.
3. Let Node 0 be the Sink node located at $W/2, H/2$.
4. The problem can be summarized as to get a connected graph $G=\{V, E\}$ from S number of sources such that V are the Nodes and E are set of all edges or Links, So as to maximize L where L is the Lifetime and is defined as time t_l when $E_i \leq 0$, where i can be any node other than the Sink.
5. Initially all node broadcast HELLO packets and let the other nodes know their Energy and Position.
6. Initially When Sink wants to gather data from Sources, It Selects the nodes with Maximum Neighbors and Sufficient Energy as Cluster Heads.
7. Each Cluster head is notified that it is cluster head.
8. Source generates RREQ packet.
9. A node forwards RREQ packet only if it is a cluster head.
10. Route is formed between each source to sink through cluster heads.
11. Data is transmitted from source to Sink.
12. Nodes loses Energy as $E_{loss} = E_{idle} + E_{transmit} + E_{receive}$

and $E = E_{idle} + E_{loss}$ where $E_{idle} = 1pJ/s$

$E_{transmit} = 3mJ/Packet$ (considering packet is of

Length 1024)

$E_{receive} = 1mJ/Packet$

13. During the Transmission if any E_i is less than 0, mark the time as Network Lifetime.
14. If a cluster head loses its energy below 30% of the Max energy, then it notifies the source. An alternative cluster head is selected, all the routes through previous cluster head generates RERR and new routes are formed.

A. Packet Delivery Ratio

Number of Packet delivered from source to sink/Number of Packets Generated at source Node.

B. Latency

Average time of Transmission of all packets from Source to Sink.

C. Control Overhead

Number of Control packet sent(RREQ,RERR, HELLO,RREP)/Number of data packet Delivered.

D. Average Energy Consumption

Avg $(E_{max} - E_i)$ where $i=1, 2, \dots, N$ and $i \neq Sink$.

IV. RESULTS

The analysis of the proposed cluster based routing scheme where cluster heads should be selected based on maximum coverage and should have sufficient energy to prolong the communication. is carried out using OMNeT++ to evaluate the energy consumption and maximize the lifetime of the sensor network. A sensing field of dimension $M \times M$ ($M = 500$ m) with a population of $N = 25, 50, 65$ nodes is considered for simulation. The system parameters used for nodes 25, 50, 65 for the simulation is listed in Table 1.

Area	500*500 m
Packet Size	512 Bytes
Packet Rate	500
Number of Active Session	14
Energy from MAC	0.003mJ/bit
Energy from Outside Module	0.001mJ/bit
Throughput LEACH	6.56
Throughput Proposed	5.102 Mbps
Clusterlife leach	15.796

Clusterlife Proposed	22.1676
Packet Delivery Ratio LEACH	1.1406
Packet Delivery Ratio PROPOSED	61.9543
Latency LEACH	0.004 Sec
Latency Proposed	0.008 Sec
Lifetime LEACH	744.77
Lifetime Proposed	1257.35

Table 1:Simulation parameters for 25 nodes.

rea	500*500 m
Packet Size	512 Bytes
Packet Rate	500
Number of Active Session	30
Energy from MAC	0.003mJ/bit
Energy from Outside Module	0.001mJ/bit
Throughput LEACH	5.7Mbps
Throughput Proposed	1.22Mbps
Cluster life LEACH	32.4851
Cluster life Proposed	56.7466
Packet Delivery Ratio LEACH	1.50869
Packet Delivery Ratio PROPOSED	64.3057
Latency LEACH	0.006 Sec
Latency Proposed	0.07 Sec
Lifetime LEACH	361.11

Table 2:Simulation parameter for 50 nodes.

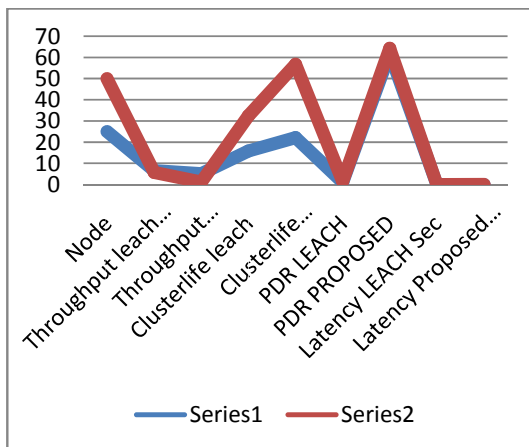


Figure : 1.2

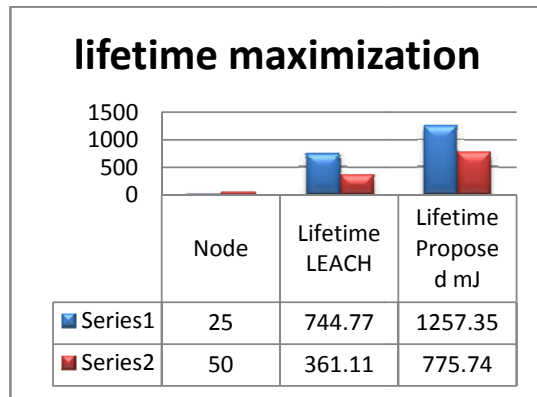


Figure: 1.3

V. CONCLUSION

There are several challenges in designing the routing and transmission for wireless sensor network. Sensors are small electronic devices with limited processing and transmission capabilities. Generally they are deployed over a wide area. Therefore continuously monitoring the energy of such nodes are difficult. Hence utmost care should be taken to ensure that in a communication scenario, the nodes do not loose too much energy and that the network remains active over longer period of time. The conventional sensor network protocols like direct diffusion and Leach fails to ensure the credibility of the network and fails to ensure longer lifetime. The lifetime maximization problem is generally seen as an isolated problem in comparison to QOS problem. In this work a QOS aware protocol is provided that ensures maximum lifetime of the edges through which routing is performed and thus minimizing the losses due to node mobility or collision, thereby enhancing the lifetime by minimizing the Energy losses. Result show that the lifetime of the proposed system is better than the conventional Leach. There are several other factors like bandwidth, delay that affects the performance of the network which are correlated. But resolving the acute relationships among the parameters are difficult. Hence the work can be further improved by incorporating fuzzy decisions along with hard decision Maximization problem.

REFERENCES

- [1] L. Akyildiz, W. Su, Y. Sankarasubramanian and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, vol. 40. no. 8, pp. 102-114, 2002.
- [2] G. N. Bravos and G. Efthymoglou, "MIMO-based and SISO multihop sensor network: Energy efficiency evaluation", *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2007
- [3] S. Cui, A. J. Goldsmith and A. Bahai, "Energy-efficiency of MIMO and cooperative techniques in sensor networks", *IEEE Journal on Selected Areas in Communications*, vol.22, no.6, pp. 1089-1098, 2004.

- [4] S. K. Jayaweera, "Energy analysis of MIMO techniques in wireless sensor networks", *Proceedings of Annual Conference on Information Sciences and Systems*, Princeton, NJ, 2004
- [5] X. Li, M. Chen and W. Liu, "Application of STBC-encoded cooperative transmissions in wireless sensor networks", *IEEE Signal Processing Letters*, vol.22, no.2, pp.134-137, 2005.
- [6] Y. Yuan, Z. He and M. Chen, "Virtual MIMO- based cross-layer design for wireless sensor networks", *IEEE Transactions on Vehicular Technology*, vol. 55, no.3, pp. 856 -864, 2006.
- [7] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", *IEEE Transactions on Wireless Communications*, vol.1, no .4, pp. 660 - 670, 2002.
- [8] W. Cheng, K. Xu, Z. Yang and Z. Feng, "An energy-efficient cooperative MIMO transmission scheme for wireless sensor networks", *Proceedings of International Conference on Wireless Communication, Networking and Mobile Computing*, pp. 1-4, 2006.
- [9] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs", *IEEE Transactions on Information Theory*, vol. 45, no.5, pp. 1456-1467, 1999.
- [10] A. Manjeshwar and D. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," In *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, San Francisco, CA, USA, April 2001.
- [11] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Proceedings of the 33rd Hawaii International Conference on System Science*, Vol. 2, Jan 2000.
- [12] Yuan Ping and B. Y. Wang Hao, "A Multipath Energy-Efficient Routing Protocol for Ad hoc Networks," *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, Vol. 3, pp. 1462-1466, Guilin, January 2007.
- [13] A. Manjeshwar and D. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," In *Proceedings of the 2nd International Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, pp. 195-202, Ft. Lauderdale, FL, April 2002.
- [14] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," *IEEE Trans. Mobile Computing*, Vol. 3, No. 4, pp. 366-379, Oct.-Dec. 2004.
- [15] Muruganathan, S.D. and Fapojuwo, A.O., "A Hybrid Routing Protocol for Wireless Sensor Networks Based on a Two-Level Clustering Hierarchy with Enhanced Energy Efficiency," *Wireless Communications and Networking Conference, 2008*, pp. 2051- 2056, Las Vegas, NV, April 2008.



EMBEDDED ROBOT CONTROL SYSTEM BASED ON AN EMBEDDED OPERATING SYSTEM, THE COMBINATION OF ADVANCED RISC MICROPROCESSOR (ARM), DSP AND ARM LINUX

VAISHAK N L & RAMACHANDRA C G

Department of Mechanical Engineering, Srinivas Institute of Technology Mangalore,
VTU University Belgaum, Karnataka, India

Abstract:-In this project, the configuration of the embedded system is introduced, and then presents a robot control system based on an embedded operating system and ARM. Based on the combination of advanced RISC microprocessor (ARM), DSP and ARM-Linux, this project involves development of embedded robot control systems through Wi-Fi. The design of embedded control system includes four aspects, i.e., system structure, functions, hardware, and software design. In the development of the system, some features are included such as hierarchy structure, modular hardware, and structured software, to make the system suitable for a variety of robots applications through some hardware adjustment and software customization only. The effectiveness of proposed approach has to be verified and tested.

Keywords- ARM; Embedded system; RISC; Wi-Fi;

I. INTRODUCTION

By the advancement of electronics, embedded technology has become a challenging field in this modern age. The single functioned, tightly constrained, reactive and real-time feature of these devices enhanced its importance in industrial, consumer applications. A robot arm is an Electro-mechanical device that performs various tasks ranging from simple mechanical jobs to highly complex tasks. It can be used to pick and place small parts on a production line. In a typical application, it can replace the human operator in feeding industrial process with discrete components. Robotic arms are used in diverse manufacturing processes including assembly, spot welding, laser processing, cutting, grinding, polishing, testing, painting and dispensing. Robots have proved to help automakers to be more agile, flexible and to reduce production lead times.

The robot arm using in this paper was designed with DC motors. DC motors are driven by the driver circuit and controlled by the control circuit. The controller using in this paper was based on ARM processor. The software part was developed by using embedded C. Existing system robot generally works with microcontroller and it is basically wired robots which works on CISC microprocessor. Proposed System introduces the configuration of the embedded system, and then presents a robot control system based on an embedded operating system and ARM. Based on the combination of advanced RISC microprocessor (ARM), DSP and ARM-Linux, this project involves development of embedded robot control systems through Wi-Fi. Here we use ARM controller as the heart of the system. ARM has high speed of execution and powerful information processing capability. The capacity of multi-parameter

execution, multi-level monitoring and networking of ARM processor makes it suitable for a wide variety of networking applications. It can also overcome the operation pressure on data reduction and is capable real-time applications. The RISC architectural feature and large memory space made us to choose this processor as the heart of the web server. Conventional PC web servers require uninterrupted 230V a.c power supply round the clock and the implementation and maintenance of these bulky systems are very high. When this is replaced by the low power embedded web server, the power consumption could be highly reduced since it requires only a low d.c power supply of 3.3V.

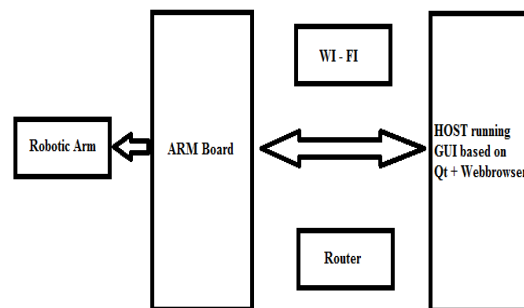


Figure 1. Functional Diagram

The system designed here is an example of embedded technology integrated with networking technology where communication and processing technology meets. Firmware development is done in embedded C language which is user friendly and also enhances the future development of the system. Front end of the EWS with external Ethernet Controller for user access is designed using Visual Basic and for EWS with integrated Ethernet is designed using HTML.

II. ARM ARCHITECTURE

The ARM is a 32-bit reduced instruction set computer (RISC) instruction set architecture (ISA) developed by ARM Holdings. It was known as the Advanced RISC Machine, and before that as the Acorn RISC Machine. The ARM architecture is the most widely used 32-bit ISA in terms of numbers produced. They were originally conceived as a processor for desktop personal computers by Acorn Computers, a market now dominated by the x86 family used by IBM PC compatible and Apple Macintosh computers. The relative simplicity of ARM processors made them suitable for low power applications. This has made them dominant in the mobile and embedded electronics market, as relatively low cost, and small microprocessors and microcontrollers.

The architecture has evolved over time, and starting with the Cortex series of cores, three "profiles" are defined:

- "Application" profile: Cortex-A series
- "Real-time" profile: Cortex-R series
- "Microcontroller" profile: Cortex-M series

Profiles are allowed to subset the architecture. The ARMv7 architecture defines basic debug facilities at an architectural level. These include breakpoints, watchpoints, and instruction execution in a "Debug Mode"; similar facilities were also available with Embedded ICE. Both "halt mode" and "monitor" mode debugging are supported.

A. Instruction set

To keep the design clean, simple and fast, the original ARM implementation was hardwired without microcode, like the much simpler 8-bit 6502 processor used in prior Acorn microcomputers.

B. RISC features

The ARM architecture includes the following RISC features:

- Load/store architecture.
- No support for misaligned memory accesses (now supported in ARMv6 cores, with some exceptions related to load/store multiple word instructions).
- Uniform 16×32 -bit register file.
- Fixed instruction width of 32 bits to ease decoding and pipelining, at the cost of decreased code density. Later, "the Thumb instruction set" increased code density.
- Mostly single-cycle execution. To compensate for the simpler design, compared with contemporary processors like the Intel 80286 and Motorola 68020, some additional design features were used:

- Conditional execution of most instructions, reducing branch overhead and compensating for the lack of a branch predictor.
- Arithmetic instructions alter condition codes only when desired.
- 32-bit barrel shifter which can be used without performance penalty with most arithmetic instructions and address calculations.
- Powerful indexed addressing modes.
- A link register for fast leaf function calls.
- Simple, but fast, 2-priority-level interrupts subsystem with switched register banks.

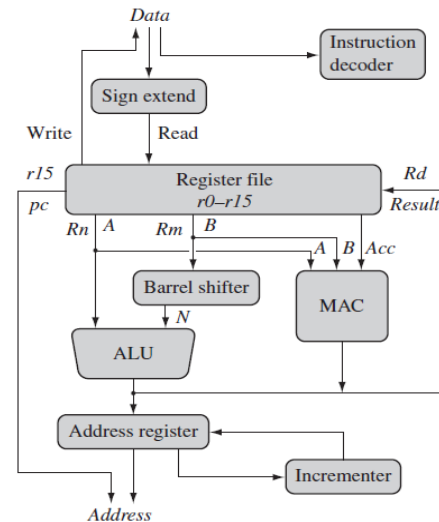


Figure 2. ARM Architecture

C. Conditional execution

The conditional execution feature (called predication) is implemented with a 4-bit condition code selector (the predicate) on every instruction; one of the four-bit codes is reserved as an "escape code" to specify certain unconditional instructions, but nearly all common instructions are conditional. Most CPU architectures only have condition codes on branch instructions. This cuts down significantly on the encoding bits available for displacements in memory access instructions, but on the other hand it avoids branch instructions when generating code for small if statements. One of the ways that Thumb code provides a more dense encoding is to remove that four bit selector from non-branch instructions.

D. Pipelines and other implementation issues

The ARM7 and earlier implementations have a three stage pipeline; the stages being fetch, decode, and execute. Higher performance designs, such as the ARM9, have deeper pipelines: Cortex-A8 has thirteen stages. Additional implementation changes for higher performance include a faster adder, and more extensive branch prediction logic.

E. Coprocessors

The architecture provides a non-intrusive way of extending the instruction set using "coprocessors" which can be addressed using MCR, MRC, MRRC, MCRR, and similar instructions. The coprocessor space is divided logically into 16 coprocessors with numbers from 0 to 15, coprocessor 15 (cp15) being reserved for some typical control functions like managing the caches and MMU operation (on processors that have one).In ARM-based machines, peripheral devices are usually attached to the processor by mapping their physical registers into ARM memory space or into the coprocessor space or connecting to another device (a bus) which in turn attaches to the processor.

F. Debugging

All modern ARM processors include hardware debugging facilities; without them, software debuggers could not perform basic operations like halting, stepping, and break pointing of code starting from reset.

G. Jazelle

Jazelle is a technique that allows Java Byte code to be executed directly in the ARM architecture as a third execution state (and instruction set) alongside the existing ARM and Thumb-mode. Support for this state is signified by the "J" in the ARMv5TEJarchitecture, and in ARM9EJ-S and ARM7EJ-S core names. Support for this state is required starting in ARMv6 (except for the ARMv7-M profile), although newer cores only include a trivial implementation that provides no hardware acceleration.

III. EMBEDDED WEB SERVER

An Embedded Web Server (EWS) is a Web server that runs on an embedded system with limited computing resources and serves embedded Web documents to a Web browser. By embedding a Web server into a network device, it is possible for an EWS to provide a powerful Web-based management user interface constructed using HTML, graphics and other features common to Web browsers. When applied to embedded systems, Web technologies offer graphical user interfaces, which are user-friendly, inexpensive, cross-platform, and network-ready. A Web server can be embedded in a device to provide remote access to the device from a Web browser if the resource requirements of the Web server are reduced. The end result of reducing the resource requirements of the Web server is typically a portable set of code that can run on embedded systems with limited computing resources. Embedded system can

be utilized to serve the embedded Web documents, including static and dynamic information about embedded systems, to Web browsers. This type of Web server is called an Embedded Web Server (EWS).EWSs are used to convey the state information of embedded systems, such as a system’s working statistics, current configuration and operation results, to a Web browser.

Boa is a single task of HTTP server, It is different from traditional Web server, It is not calls sub process to handle multiple connections produced simultaneously through the fork, but reprocesses all the ongoing HTTP connections that only fork calls CGI programs, automatic directory generation, and file compression implementation. This is vital important for embedded systems by saving the maximum extent possible system resources. Based on the above exposition, Boa applied to the embedded platform has many advantages; therefore Boa is used as Web server in this paper. Its architecture showed in Fig. 4.

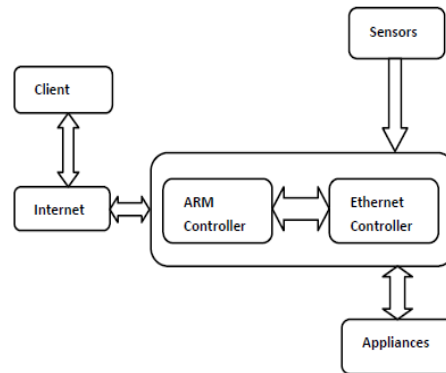


Figure 3. EWS with external Ethernet Controller

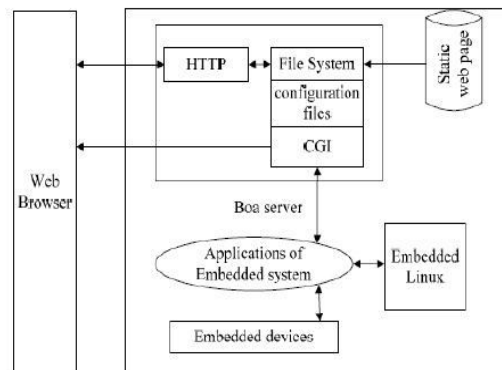


Figure 4. Architecture of Boa Server

If you need to improve system security or interact with users such as real-time status query and landing, then you have to use dynamic Web technologies. In such situation, either Boa or httpd can achieve these goals. In

the present research, we adopt Boa, the Web server suitable for embedded system, because thttpd has less function and needs far more resources to run.

A. The Principle Of Embedded Web Server Boa

Boa is a single task Web server. The difference between Boa and traditional Web server is that when a connection request arrives, Boa does not create a separate process for each connection, nor handle multiple connections by copying itself. Instead, Boa handles multiple connections by establishing a list of HTTP requests, but it only forks new process for CGr program. In this way, the system resources are saved to the largest extent. Like a common Web server, an embedded web server can accomplish tasks such as receiving requests from the client, analyzing requests, responding to those requests, and finally returning results to the client.

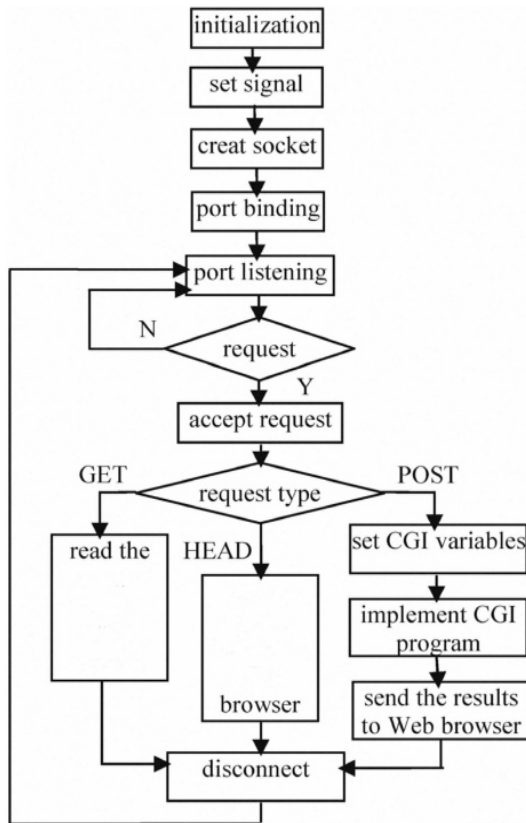


Figure 5. Embedded Web server flowchart

The following is its work process.

- Complete the initialization of the Web server, such as creating an environment variable, creating socket, binding a port, listening to a port, entering the loop, and waiting for connection requests from a client.
- When there is a connection request from a client, Web server is responsible for receiving the request and saving related information.

- After receiving the connection request, Boa analyzes the request, calls analysis module, and works out solutions, URL target, and information of the list. At the same time, it processes the request accordingly.

- After the corresponding treatment is finished, the Web server sends responses to the client browser and then closes the TCP connection with the client. For different request methods, the embedded Web server Boa makes different responses. If the request method is HEAD, the response header will be sent to the browser; If the request method is GET, in addition to sending the response header, it will also readout from the server the URL target file of the client request and send it to the client browser; If the request method is POST, the information of the list will be sent to corresponding CGI program, and then take the information as a CGI parameter to execute CGI program. Finally, the results will be sent to client browser. Boa's flowchart is shown in Fig. 5.

IV. BLOCK DIAGRAM

A. Design of the hardware system

S3C2440A1 processor is used as core of the hardware platform in this paper. Fig. 6 is the block diagram of hardware system. Include: serial port, Ethernet interface, JTAG port, storage systems and so on. The frequency Samsung S3C2440AL is 400MHz and can up to 533MHz in the maximum. According to its mode of internal circuit. 12MHz chosen for the crystal. JTAG (Joint Test Action Group) is an international test protocol standard, software simulation, single-step debug and u-boot download can be carried out through the JTAG port, it's a simple and efficient means of developing and debugging embedded systems. The SDRAM capacity in the system is 64MB, working voltage is 3.3V, data bus is 32-bit, clock frequency up to 100MHz, Auto-Refresh and Self-Refresh are both supported.

B. Design of the software system

Software development process based OS includes: the establishment of cross-compiler, the transplant of Boot loader, the transplant of embedded Linux, the development embedded Web server. To begin with, system cross-compiler environment using EABI-4.3.3 is established. what's more, uboot that developed by the German DEXN group is used as Boot loader. The function of Boot loader is to initialize the hardware devices, establish memory mapping tables, thus establish appropriate hardware and software environment and prepare for the final call to the operating system kernel. Besides, yaffs file system is made.

C. *The Transplant of Linux Kernel*

Linux is used as operating system because Linux system is a hierarchical structure and completely open its kernel source, the important feature of Linux is portability to support a wide range of hardware platforms, can run in most of the architecture. Contains a comprehensive set of editing, debugging and other development tools, graphical interface, a powerful network supporting and rich applications. In addition, the kernel can be reduced by configuring.

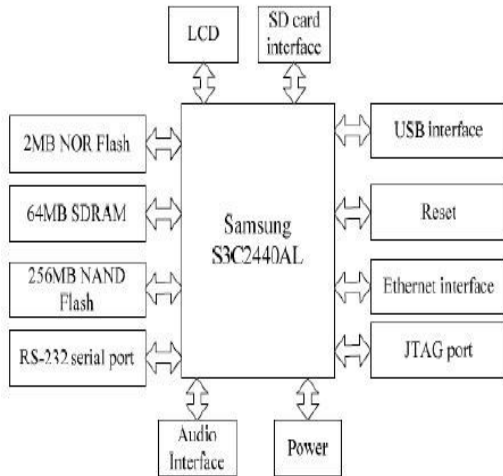


Figure 6. Block diagram of hardware system

V. CONCLUSION

When the case of monitoring multiple parameters comes, the EWS with integrated Ethernet is showing better performance when speed and reliability comes

into picture. Thus EWS with integrated Ethernet is suitable for real-time monitoring of Industrial appliances. Moreover this systems has a wide variety of Industrial applications such as supervisory data control, Fault diagnosis, remote monitoring and controlling etc. Since ARM processor has fast execution capability and Ethernet standard can provide internet access with reasonable speed, this system is suitable for enhancing security in industrial conditions by remotely monitoring various industrial appliances where high safety and care is a necessity. There is no doubt that this system will be useful for a wide variety of industrial applications.

REFERENCES

- [1]. Mo Guan, Minghai Gu, "Design And Implementation Of An Embedded Web Server Based On ARM" .pp. 612-615,2010.
- [2]. Yakun Liu; Xiaodong Cheng, "Design and implementation of embedded Webservice based on arm and Linux", 30-31 May 2010, 316 –319
- [3]. Zhan mei-qiong and Ji chang-peng; "Research and Implementation of Embedded Web Server," Inetrnational Conference on ultimedia and Information Technology, pp.123-125, Dec 2008.
- [4]. Alen Rajan, Aby K. Thomas, "ARM Based Embedded Web Server for Industrial Applications", International Conference on Computing and Control Engineering (ICCE 2012), 12 & 13 April, 2012
- [5]. Junhua Yang; Zhien Shang and Tao XinG, "Intelligence Monitoring System Based on ARM and Information Fusion," International Conference on Electric Information and Control Engineering, pp.487-490, April 2011.
- [6]. Alen Rajan, Aby K. Thomas, Rejin Mathew, "A Comparative Performance Analysis of ARM based Web Servers with Integrated and External Ethernet Interfaces for Industrial Applications", International Journal of Computer Applications (0975 – 8887) Volume 44– No.21, April 2012



MODIFIED AES USING DYNAMIC S-BOXES

VEENA DESAI, SAGAR DHAVALI & SACHIN KATTI

Department of Electronics and Communication Engineering, Gogte Institute of Technology, Belgaum, Karnataka, INDIA

Abstract:- Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. A block cipher takes as input a block of plaintext and a key, and outputs a block of cipher-text of the same size. Most of the block ciphers use substitution boxes (s-box) which obscure the relationship between the key and the cipher-text. AES is a symmetric block cipher developed by Joan Daemen and Vincent Rijmen (Rijndael)[1][2][3][4]. Rijndael is a symmetric byte-oriented iterated (each iteration is called a round) block cipher that can process data blocks of 128 bits (4 words), using keys with length of 128, 192 and 256 bits. Rijndael is capable of processing additional block sizes (160, 192 and 244 bits) and key lengths (160 and 244 bits), however they are not adopted in AES. Our implementation refers to AES algorithm that can process data blocks of 128 bits (4 words), using key with length 128 bits. In the original algorithm the S-BOXES used are static. We have modified the S-BOXES to be dynamic and they are generated from a unique sequence generated by finger prints. We compare the performance of both the algorithms on the parameters such as Hamming Distance, Balanced Output and Avalanche Effect.

Keywords:- AES, finger print, singular value decomposition, dynamic s-box generation.

I. INTRODUCTION

The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the internet.

Cryptography plays an important role in the security of data. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. The urgency for secure exchange of digital data resulted in large quantities of different encryption algorithms which can be classified into two groups: asymmetric encryption algorithms (with public key algorithms) and symmetric encryption algorithms (with private key algorithms). Symmetric key algorithms are in general much faster to execute electronically than asymmetric key algorithms.

The algorithm originates from the initiative of the National Institute of Standards and Technology (NIST) in 1997 to select a new symmetric key encryption algorithm. From the initial candidates, Rijndael algorithm was selected as the Advanced Encryption Standard (AES) due to the combination of security, performance, efficiency, ease of implementation and flexibility.

A case study of AES algorithm has been taken and implemented in MATLAB and modifications to the original AES using random sequences generated by finger prints is also implemented using MATLAB. A comparative study has been done on both implementations on the basis of parameters such as

Hamming distance, balanced output and Avalanche effect.

Rijndael is a symmetric byte-oriented iterated (each iteration is called a round) block cipher that can process data blocks of 128 bits (4 words), using keys with length of 128, 192 and 256 bits. The S-BOXES are modified to be dynamic and they are generated from a unique sequence. The unique sequence is generated by finger prints.

At the end we compare the two implementations using hamming distance, balanced output and avalanche criteria.

II. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is a symmetric block cipher which was developed by two Belgian cryptographers namely Joan Daemen and Vincent Rijmen[5][6][7]. AES was designed to have the following characteristics:

A. Flexibility

Candidate algorithms with greater flexibility will meet the needs of more users than less flexible ones, and therefore, inter alia, are preferable. However, some extremes of functionality are of little practical application (e.g. extremely short key lengths); for those cases, preference will not be given. Some examples of flexibility may include (but are not limited to) the following: The algorithm can accommodate additional key- and block-sizes (e.g., 64-bit block sizes, key sizes other than those specified in the Minimum Acceptability Requirements section, [e.g., keys between 128 and 256 that are multiples of 32 bits, etc.]). The algorithm can be implemented securely and efficiently in a wide variety of platforms and applications (e.g., 8-bit processors, ATM networks, voice & satellite communications, HDTV, B-ISDN, etc.). The algorithm can be implemented as a stream cipher, message authentication code (MAC) generator, pseudorandom number generator, hashing algorithm, etc.

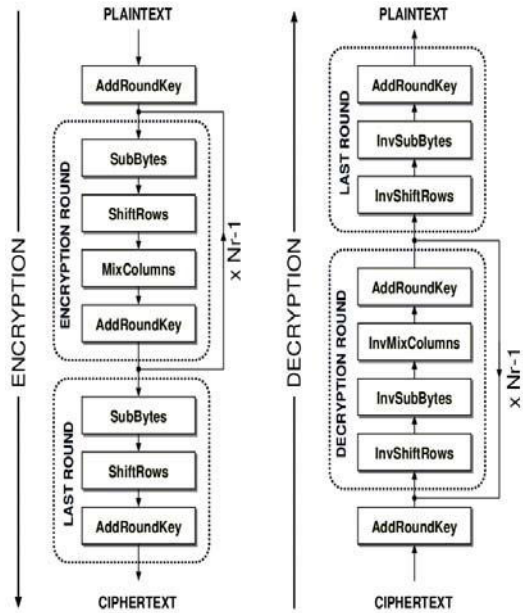


Figure 1. Overall Structure of AES

B. Hardware and Software Suitability

A candidate algorithm shall not be restrictive in the sense that it can only be implemented in hardware. If one can also implement the algorithm efficiently in firmware, then this will be an advantage in the area of flexibility.

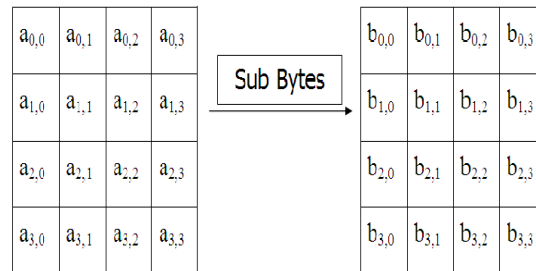
C. Simplicity

A candidate algorithm shall be judged according to relative simplicity of design. AES encrypts 128-bit blocks of plaintext into 128-bit blocks of cipher text. AES is implemented in numerous products and has received a fair amount of scrutiny. So far, the security of AES is unchallenged. The algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds as shown in Table 2. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key length. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: Sub Bytes, Shift Rows, Mix Columns and AddRoundKey. The AES algorithm uses a round function that is composed of four different byte-oriented transformations:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key.

1) Sub Bytes:

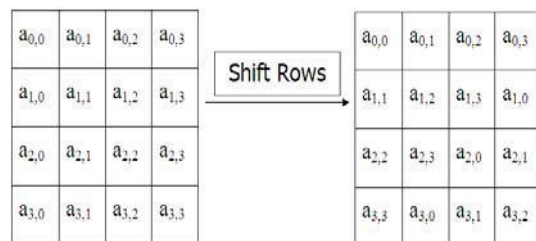
The forward substitute byte transformation, called Sub Bytes, is a simple table lookup. AES defines a 16 x 16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values. Each individual byte of state is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value. The inverse substitute byte transformation, called Inverse Sub Bytes, makes use of the inverse S-box.



2) Shift Rows:

The forward shift row transformation, called Shift Rows. The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed. The following is an example of Shift Rows.

The inverse shift row transformation, called Inverse ShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a one-byte circular right shift for the second row, and so on.



3) Mix Columns:

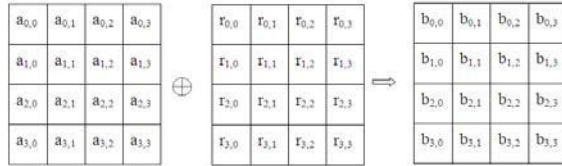
The forward mix column transformation, called Mix Columns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication on State.

The inverse mix column transformation, called Inverse Mix Columns, is determined by using Cramer's Rule.

$$\begin{bmatrix} a'_{0,0} & a'_{0,1} & a'_{0,2} & a'_{0,3} \\ a'_{1,0} & a'_{1,1} & a'_{1,2} & a'_{1,3} \\ a'_{2,0} & a'_{2,1} & a'_{2,2} & a'_{2,3} \\ a'_{3,0} & a'_{3,1} & a'_{3,2} & a'_{3,3} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$$

4) Add Round Key:

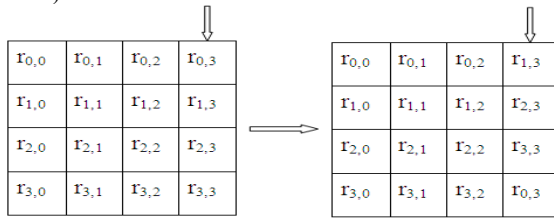
In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XOR-end with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation. The following is an example:



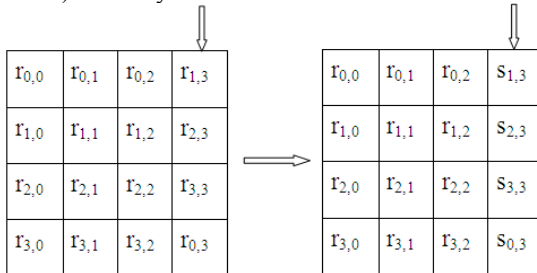
AES Key Expansion

There are 3 components in AES key expansion process viz.

1) Rotate last column:



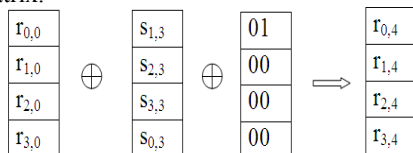
2) Sub Bytes



3) XOR-ing with RCON matrix RCON is a constant matrix which is defined as follows.

01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

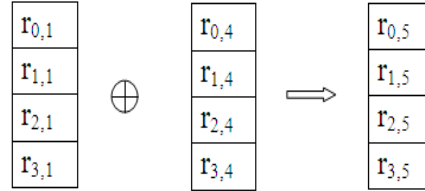
The first column of the key matrix is generated by XOR-ing the first column of the key with S-BOX substituted column and the first column of the RCON matrix.



The 2nd column of the key is generated by XOR-ing the 5th column of the key with the 2nd column of the key.

The 3rd column of the key is generated by XOR-ing the 6th column of the key with the 3rd column of the key.

The 4th column of the key is generated by XOR-ing the 7th column of the key with the 5th column of the key.



Now considering the newly generated key as the key matrix the steps 1, 2 and 3 are repeated and a new key is generated. In all 10 keys are generated and the total number of key including the original key account to 11 keys.

III. FINGER PRINTS AND SINGULAR VECTOR DECOMPOSITION

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity.

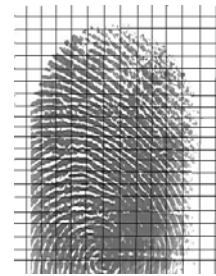


Figure 3: figure showing pixels and resolution

An image divided into pixels as shown in figure 3. The resolution of an image is calculated by multiplying number of row pixels into number of pixels in the column.

The svd function on an image computes the matrix singular value decomposition. $s = \text{svd}(X)$ returns a vector of singular values.

$[U, S, V] = \text{svd}(X)$ produces a diagonal matrix S of the same dimension as X, with nonnegative diagonal elements in decreasing order, and unitary matrices U and V so that $X = U*S*V'$.

The steps 1 to 12 give the algorithm for converting the fingerprint image to a unique key using SVD.

1. Read the finger print image using the command 'imread'. $A = \text{imread}(\text{'filename.fmt'})$ reads a image from the file specified by the string filename. If the

file is not in the current directory, or in a directory on the MATLAB path, specify the full pathname.

2. The finger print image is resized to a 48x48 matrix.
3. The SVD function is applied to the image which returns 3 matrices [U, S, V] each matrix is of the order 48x48.
4. The maximum values of S-matrix, obtained in the above step, copied into another matrix-C.
5. Apply SVD code to the matrix-U, obtained in step3, which returns another set of matrices [U1, S1, V1].
6. The maximum values of matrix-S1 are copied into a matrix-D.
7. Apply SVD function again to matrix-V, obtained in step-3, to get another set of matrices [U2, S2, V2].
8. The maximum values of matrix S2 are copied into another matrix-E.
9. Add the matrices C, D & E and store it in another matrix F.
10. A unique number is obtained by adding the diagonal elements of matrix F. This unique number decides the initial permutation (IP) which is explained in chapter 7.
11. Choose the 1st 16 elements of matrix F which are less than 255. These 16 elements form the key.
12. Reshape the key to 4x4 matrix. This forms the key for encryption and decryption processes.

IV. DYNAMIC S-BOX GENERATION

In the Rijndael AES algorithm the S-BOXES used for Encryption and Decryption are static i.e., they have a fixed value. The S-BOXES do not change with the key. The modification that we have implemented is that the S-BOXES used in our algorithm are dynamic. The word dynamic here means that S-BOXES are generated from the unique key.

TABLE I. INITIAL PERMUTATION I

Sequence	7	4	1	2	5	8	6	3	
Static S-BOX Element	1	0	0	1	0	1	0	1	95h
Dynamic S-BOX Element	0	1	1	0	0	0	1	1	63h

The steps involved in generating the dynamic S-BOXES are as follows.

1. The unique sequence is generated using the Randintrlv function. Randintrlv(data, state), rearranges the elements in data using a random permutation. Here data is the fixed sequence [1 2 3 4 5 6 7 8] and state is the unique number obtained at the end of SVD algorithm.
2. The unique sequence generated from the key is applied to each element of the S-BOX. This S-BOX is to which the unique sequence is applied

is always static. Since the sequence is unique for each key, the S-BOXES generated for two different keys are always different. The method employed in applying the sequence to each element is explained in the next step.

3. Let us assume that the unique sequence is [7 4 1 2 5 8 6 3]. Let the first element in the S-BOX be 95h. The element generated after applying the sequence is 63h.

The 1st bit of the static S-BOX Element is moved to the 7th position in the dynamic S-BOX element.

The 2nd bit of the static S-BOX Element is moved to the 4th position in the dynamic S-BOX element and so on.

4. Similarly this sequence is applied to each of the 256 elements of the static S-BOX. The new S-BOX generated is the dynamic S-BOX which is used for further reference in the Encryption process.

5. The inverse S-BOX is generated from the newly created dynamic S-BOX, which is used for further reference in the Decryption process.

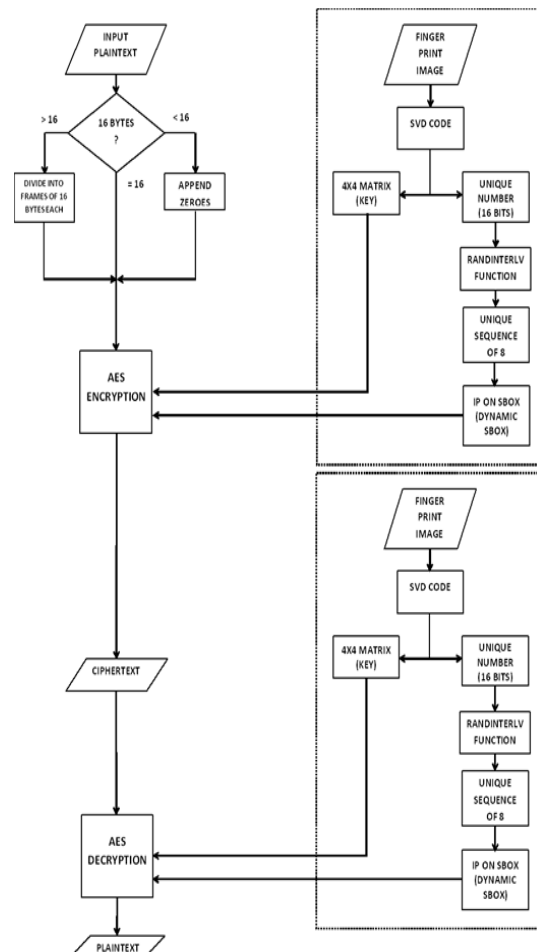


Figure 4: Flowchart of the implementation of modified AES

V. RESULT AND COMPARASION

The following parameters are used for comparison between both implementations.

A. Hamming distance:

In information theory, the Hamming distance between two strings of equal length is the number of positions for which the corresponding symbols are different. Put another way, it measures the minimum number of substitutions required to change one into the other, or the number of errors that transformed one string into the other.

The Hamming distance between two words a and b can also be seen as the Hamming weight of a-b for an appropriate choice of the - operator.

For binary strings and b the Hamming distance is equal to the number of ones in a XOR b.

B. Avalanche effect:

In cryptography, the avalanche effect refers to a desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions. The avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the cipher-text.

If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a cryptanalyst can make predictions about the input, being given only the output. This may be sufficient to partially or completely break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device.

C. Balanced Output:

Another measure for good block cipher is the balanced output. Balanced output means the number of ones and number of zeros in the cipher text should be nearly equal.

For example, if the cipher text is 10110010, then

No. of 1's = 4,

No. of 0's = 4.

The algorithm is good.

If, for example the cipher text is 10110110, then

No. of 1's = 5,

No. of 0's = 3.

The algorithm is poor.

TABLE II. IMAGES AND THEIR SVD SEQUENCES

SI no.	IMAGE	UNIQUE NUMBER	SEQUENCE
1	2.GIF	471	[8 4 6 1 7 3 5 2]
2	3.GIF	495	[6 3 2 8 5 1 4 7]
3	4.GIF	414	[6 5 3 4 7 8 2 1]
4	5.GIF	429	[4 8 7 2 1 6 5 3]

5	6.GIF	350	[3 6 4 2 1 5 8 7]
6	7.GIF	322	[3 8 2 1 6 7 5 4]
7	8.GIF	354	[3 5 2 7 8 1 4 6]
8	9.GIF	367	[3 8 6 2 7 4 5 1]
9	10.GIF	12675	[4 8 3 1 6 5 2 7]
10	11.GIF	13575	[4 7 1 6 3 2 5 8]

This sequence generated is used to modify the S-BOX. Since there are 8! (Eight factorial) permutations of this sequence there 8! possible S-BOXES. Hence the complexity of the modified algorithm is increased by a factor of 8!=40320 compared to the normal AES algorithm.

Results on the basis of Hamming distance (HD), balanced output and Avalanche effect:

PLAINTEXT=RAVISATTIGERI123			
AES		MODIFIED AES	
CIPHERTEXT=		CIPHERTEXT=	
225	208	206	156
40	113	23	160
191	9	27	244
40	85	172	129
HAMMING DISTANCE=62		HAMMING DISTANCE=52	
BALANCED OUTPUT ONES=58 ZEROS=70		BALANCED OUTPUT ONES=68 ZEROS=60	
AVALANCHE EFFECT 1 BIT VARIED PLAINTEXT=RAVISATTIGERI122			
CIPHERTEXT=		CIPHERTEXT=	
230	127	71	168
241	39	216	129
135	141	18	147
91	7	141	56
HAMMING DISTANCE=62		HAMMING DISTANCE=62	

PLAINTEXT=SACHINKATTI12345			
AES		MODIFIED AES	
CIPHERTEXT=		CIPHERTEXT=	
176	18	169	165
206	120	197	168
202	120	198	179
86	194	169	190
HAMMING DISTANCE=69		HAMMING DISTANCE=60	

BALANCED OUTPUT ONES=63 ZEROES=65	BALANCED OUTPUT ONES=66 ZEROES=62
AVALANCHE EFFECT 1 BIT VARIED PLAINTEXT= SACHINKATTI12344	
CIPHERTEXT= 5 89 9 63 172 52 86 108 214 160 79 89 106 106 182 92	CIPHERTEXT= 13 83 119 45 243 105 217 39 219 129 37 163 93 220 18 159
HAMMING DISTANCE=61	HAMMING DISTANCE=62

The modification made to the S-boxes using random sequence generated from finger prints has yielded better results compared to the original AES.

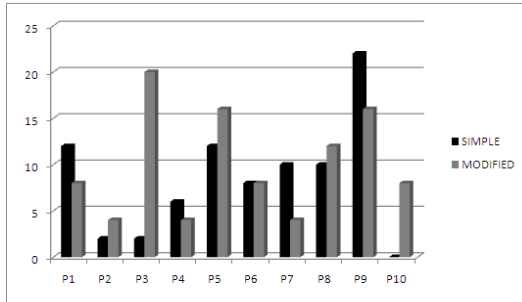
From the analysis and results, we conclude that, we should have a nonlinear relationship between plaintext and cipher text so that cryptanalysis must be very difficult or impossible to achieve. As such the encryption and decryption algorithms are public which are known to even the cryptanalysts also, it becomes imperative to initialize the S-boxes used in the ciphers using random sequences such that they become more secure and invulnerable.

As each individual has a unique finger print the random sequence generated by each finger print will be different, using finger print and password along with it provides double authentication and escalates complexity by a significant factor. Therefore we can conclude that modified AES algorithm using finger prints is more secure than original AES.

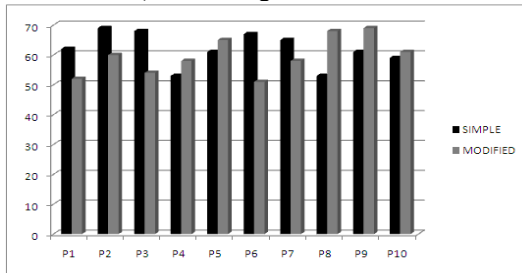
Modifications can be made in the project to generate the S-boxes of AES using any other strong random number generation algorithms. The random number generators using Neural Network function is proposed instead of the SVD code to compare the complexity of the algorithm. Once again different parameters stated above such as hamming distance, avalanche effect, balanced output can be used to test these implementations. A unique sequence generated by finger prints can be used as access codes or passwords to encrypt or authenticate for security of Biomedical Imaging.

Graphical Analysis

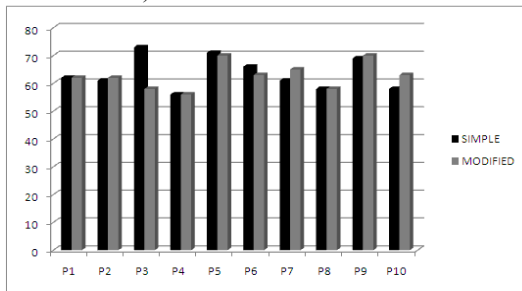
A) Balanced Output



B) Hamming Distance



C) Avalanche effect



VI. CONCLUSION

We have analyzed both the implementations and tested the algorithms based on various parameters. The parameters used are hamming distance between plaintext and cipher text, avalanche effect by flipping one bit in the plaintext and balanced output for the cipher texts.

REFERENCES

- [1] Cryptography and Network Security Principles and Practices, by William Stallings.
- [2] Comparative analysis of s-boxes based on graphical SAC by Iqtadar Hussain, Tariq Shah Mehmood from Quaid-i-azam University, Islamabad, Pakistan.
- [3] New Algorithm to Construct Secure keys for AES by Iqtadar Hussain, Tariq Shah Mehmood from Quaid-i-azam University, Islamabad, Pakistan.
- [4] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001 (**Error! Hyperlink reference not valid.** publications/fips/fips197/fips-197.pdf).
- [5] V. Rijmen: The block cipher Rijndael. <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>, (2001).
- [6] J.Daemen:Annex toAES proposal Rijndael. <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/PropCorr.PDF>
- [7] National Institute of Standards and Technology: Specification for the AdvancedEncryptionStandard.<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>



A COMPREHENSIVE SURVEY ON THE PERVASION OF ANDROID IN THE DESIGN OF SOPHISTICATED EMBEDDED DEVICES

SHARMILA S P & A S MANJUNATH

Dept. of Computer Science & Engg, SIT, Tumkur.

Abstract:-The benefits of Android in embedded systems are intensive. Android offers a very rich platform for application development and ease portability. It also eliminates the worries of developers that they had about the open source software. This paper presents our hands on experience and lesson learnt during our first phase of the work. Among three major categories of embedded systems Android is much known to the third category, sophisticated embedded devices like smart phones, tablets, notebooks etc. Studying the features of android necessary to move from smart phones to other embedded systems, we identify two major reasons for the pervasion of android in the designing of sophisticated embedded devices as commercial and technical requirements. This describes why Android is an attractive technology for diverse needs and ready to flourish on embedded systems beyond the mobile handset.

Keywords: *Android, Embedded devices, Smart phones*

1. INTRODUCTION:

Embedded Systems are computing devices hidden inside the vast array of everyday products and appliances such as toys, cell phones, hand held devices, PDAs, cameras etc. Since from the introduction of Android, the open source platform for mobile phones, there is a considerable amount of interest to customize and adapt android for other embedded platforms such as netbooks, set top boxes, car dashboards and others. This is the major motivation behind this work.

The entire paper is organized as follows; Section 2 contains a brief introduction regarding the embedded systems, its versatile definition, classifications and applications. Section 3 reviews the history, architecture, beneficiary features for the application of android on embedded devices. Section 4 takes an outlook on important existing and future features of smartphones, Section 5 discusses how android can be utilized for smart embedded devices. Finally the conclusion is as stated in Section 6.

2. EMBEDDED SYSTEMS:

A versatile definition of Embedded devices [1, 2, 3, 4, 5] is that they are the devices used to monitor, assist and control the operation of an equipment or a system. An embedded system itself is a computer system which will have dedicated functions often used in real time applications. It is a combination of computer hardware and software, and perhaps additional mechanical or other parts, designed to perform a dedicated or specific function. In some cases, embedded systems are part of a larger system or product, as in the case of an antilock braking system in a car.

An embedded system is a computer system designed for specific control functions within a larger system, often with real-time computing constraints. It is

embedded as part of a complete device often including hardware and mechanical parts. By contrast, a general-purpose computer, such as a personal computer (PC), is designed to be flexible and to meet a wide range of end-user needs. Embedded systems control many devices in common use today.

An embedded device may range from simple product to complex mission critical applications. Microsoft calls them "non-personal computer devices". Usually they cannot be modified by users, but often have interfaces to external devices such as sensors.

Broadly speaking, embedded systems can be classified [4] into Small scale, Median scale and Sophisticated Embedded systems, depending on the need of hardware and software requisites. Embedded implies that they are the constituent parts of the entire system. Embedded systems may be such that their presence is far from obvious to the casual observer. Major components of any embedded systems includes a hardware part, software part and the real time OS.

Most important characteristics of embedded systems responsible for their versatile applications are: They are designed for specific task. Hardware for embedded system is stored in ROM or flash memory At design time it can be used to minimize resources and maximizes robustness and they offer low power consumption in many situations and many other features.

The main focus here is on RTOS. Generally RTOS for embedded applications should have features like, open source, portable, ROMable, scalable, preemptive, multi tasking, deterministic, efficient memory management, good interrupt management, robust and reliable.[6,7]

The advances in microcontroller systems have undergone a tremendous evolution in recent years.

Microcontrollers and microprocessors are characterized by high integrated low power consumption, self sufficient and low cost. These features are used in sophisticated embedded systems which have vast advantages.

Applications of embedded systems may extend from a simple toy for a kid to a laptop for scientific researcher. Embedded systems have kept pace with developments in other fields of computing like pervasive and ubiquitous computing [25]. Even context aware applications have their main focus on sophisticated embedded devices. Some major fields of its applications includes medical electronics-healthcare[26,27], automotives, entertainment, localization and internationalization, military and aerospace application, medical electronics, communications, electronic applications and consumer devices, industrial automation and process control software.

3. ANDROID OPERATING SYSTEM:

Android[8] is a Linux based operating system for mobile devices such as smart phones and tablet computers. It is developed by the open handset alliance led by Google and other companies[9]. It delivers a complete set of software for mobile devices like an operating system, middleware and key mobile applications. Android means a lot in the highly technical world of today. Smart phones are very much known to android.

In 2005 August, android establishment was made as a property of integration of Google android incorporation of key people including Andry Rubin, Rich Miner and all. From 2007 to till now it went through various milestones for development. Andry rubin the founder of Android once quoted that, “Android started with phones, then grew to tablets and now it should grow to everything”. During the release of ice cream sandwich version of android, Google mentioned to unify tablets, phones and Google TV devices under a single version of operating systems. Now that aspect is taking a twist as Android is penetrating into embedded devices and home automation.

Thus we can say android circle is getting bigger and bigger. Android is extending beyond phones and tablets. It is moving into hackable devices and home automation with Android open accessory. Once in future everything may get androidified.

It has been discovered today that, Android open accessory Development Kit (ADK) embraces an android USB accessory which is based on Aurdino[10,11] prototyping platform and an android application can interact with it. Arduino is an open source electronics prototyping platform which is low

cost and easy to learn. With this it is easy to build our own electronics. Amarino[20] is a toolkit, consisting of android application and an Arduino library. This is needful to interface an android phone in a new dimension or to build our own interfaces. With this developers can build new and exciting hardware controlled by android. It is also feasible to make our smartphone sensors as accelerometer, light sensors or the touch screen to control the devices.

Some examples that are feasible with ADK are:

- Little robots controlled by an android device.
- In home automation with new android at home initiative where, lighting, power control and appliances interact with application running on android
- The giant wooden maze is the most dramatic example that is controlled by the tilting action of Motorola Xoom tablet

Thus android is a perfect software platform for creating professional and feature complete products with significantly reduced software development effort and improved over all time to market.

Features of Android which are much beneficial for embedded devices:

- Application framework of android enables reuse and replacement of components.
- Dalvik virtual machine[15] optimized for mobile devices.
- Integrated browser based on the open source web kit engine.
- Optimizes graphics powered by a custom 2D graphics library; 3D graphics based on the open GL ES 1.0 specification(hardware acceleration optional).
- SQLite for structured data storage.
- Media support for common audio, video and still image formats(MPEG4, J.26, MP3, AAC, AMR, JPG, PNG, GIF).
- GSM telephony(Hardware Dependent).
- Bluetooth, EDGE, 3G and WiFi.
- Rich development environment including device emulator tools for debugging memory and performance profiling and a plug-in for Eclipse IDE

Architecture of android:

Android Architecture [12, 13, 14, 15] can be divided into 4 layers. Application layer, Application framework layer, Libraries and Android runtime layer, and Linux kernel layer. Application layer contains built-in and custom applications developed in Java. Application developer can build new and rich applications since Application framework layer is component based, thus supports reusability. Android system provides C/C++ libraries which are accessible with the aid of Application framework. Android

runtime consists of core library and Dalvik Virtual Machine. Android is built on GPLv2 licensed 2.6 Linux kernel providing basic functionalities.

Customization [16] of android is also possible for other embedded platforms such as notebooks, set top boxes, car dash boards and others. There are lot of advantages if android is made available for multiple device platforms (so that application developed for one device could be made available for another platform with minimal or no porting needs).

Example: TiVo [17] recording client made available both on set top box and on user phone. Same application, same code but available on two devices to suit your mobility needs.

Android is Dalvik Virtual machine[15] based platform that runs on Linux based kernel. Therefore to port an android platform one needs to port the underlying Linux OS and then Android platform SDK as well.

As ARM[18] is one of the most popular platforms for embedded devices, we refer a need to understand how to port android platform to custom ARM based boards.

Prerequisites for this android porting activity according to [19] are :

- i) Android source code
- ii) Linux source code
- iii) Target platform
- iv) Cross development platform

Two major stages of porting android onto a ARM based platform are[19] :

- Porting Linux
- Porting Android

Android being the most popular and extensively used system has some weakness too, that includes huge android operating system battery drain and recharging of device over and over again after few hours[21,22]. The user should always check the percentage of power used by different departments. The device should be set for using 2G networks only. Cyanogenmod is also a leading power saving solution for better android battery usage. Another key is to put the phone on standby mode when not in use to avoid android operating system battery drain. Installation of custom ROM and custom Kernel makes phone smooth and more responsive. Chiefly the vibration factor of every phone consumes additional than normal battery, so turning off vibration makes the phone utilize less power

4. SMART PHONES:

Smartphone is a device that lets you make telephone calls, but also adds in features that, in the past, you would have found only on a personal digital assistant or a computer, such as the ability to send and receive e-mail and edit Office documents.

Cell phones were used for making calls, messaging and not much else; while PDAs, like the Palm Pilot, were used as personal, portable organizers. A PDA could store your contact info and a to-do list, and could synchronize with your computer.

Eventually, PDAs gained wireless connectivity and were able to send and receive e-mails. Cell phones, meanwhile, gained messaging capabilities, too. PDAs then added cellular phone features, while cell phones added more PDA-like (and even computer-like) features. The result was the Smartphone.

Available features of smartphones: Smart phones have smarter capabilities than mobile phones.

- i. Operating systems: Smart phones are based on operating systems that allow it to run extensive functions.
- ii. Applications: All cell phones include some sort of software, smart phone will have an ability to do more than that like, it can download applications.
- iii. Web access: Smart phones can access web at higher speed, which have influenced from 3G and 4G data networks. Some have free access to social networks too.
- iv. QWERTY keyboard: Smartphones have QWERTY keyboard. Keys are laid in the same manner as in computer.
- v. Messaging: Cell phones can send and receive text messages but what sets a Smartphone apart is its handling of e-mails and MMS. Smart phones can sync with personal and professional email account. Some supports multiple email accounts others include access to instant messaging services.
- vi. High definition cameras: Most smart phones support high definition cameras of several Mega Pixels.
- vii. High resolution display screens: Smart phones have large display screens making them suitable for even browsing.
- viii. Bluetooth and WiFi facility: This is also an important feature that made smart phone suitable for communication.

Technology surrounding Smartphone and cell phones is constantly changing. What constitutes a Smartphone today may change by next day, next week, next month or next year.

Anticipated features in Future smartphones: There are some features that are in anticipation for future smart phones. The consumer services are hopefully looking for such features.

- i. Augmented Reality(AR): It refers to what we perceive through our senses is enhanced through the use of computer generated sensory input as sound, video, graphics, and GPS data. AR makes more information as available for us by combining computer data to what we see in real life. Smartphones are capable to serve as a good platform for AR to work. Most AR apps available now utilize some form of GPS to facilitate location aware searches. An example on use of AR via smartphones is Apple's iPhone app using AR to replace ads with art.
- ii. Flexible screens: Smart phones are able to provide a large screen to watch and play your favorite movie and games while maintaining a pocketable size. Screens can be folded or unfolded by using organic light emitting diode (OLED) technology. Paper thin screens can even project future feature smartphones from both sides of the screen. Some companies have plans to make wearable smartphones for masses. Research on concept Morph is still on process.
- iii. In built projector: Smartphone integrated with a projector. Existing example is Samsung Galaxy Beam has a built in digital light projection(DLP) VVVGA projector which is able to project at up to 50 inches in size at 15 lumens
- iv. Interactive gaming consoles: Without a need of TV screen but we need a surface instead of a physical controller we use our body or voice. A smart camera or voice control function can capture our movement and voice commands to let you interact with objects on the phone or the projected screen.
- v. Self charging capacity: With all the extensive feature applications a smart phone is meant to consume lot of battery. To drain out the issues in battery life of smart phones we can make use of photovoltaic cells that uses solar energy to recharge or piezoelectric materials that converts the vibrations into energy[24] that can be used to recharge a smart phone economically.
- vi. Seamless voice control: This is existing in some mobile phones. Instead of recognizing commands via sound waves like most voice recognition systems, it is necessary to use natural language interface to recognize however we speak. This would be more effective and accurate. Seamless voice control combined with gestures may bring interactivity to a new level for smart phones and their uses.
- vii. 3D screens: Mobile companies are moving from 2D feature smart phones to 3D. This provides resolution that is sharper than what human eye can perceive. A couple of 3D smart phones in market are LG optimus, Motorola MT810, Samsung AMOLED 3D.
- viii. Holograms: The next path from 3D is obviously holographic projections. It is a combination of 3D smartphones and projections from smartphones. 3D display can be integrated with the elements of movement when it comes to user interaction with the phones.
- ix. Real time face detection applications: Much like the human visual system, embedded computer vision systems perform the same visual functions of analyzing and extracting information from video in a wide variety of products. In embedded portable devices such as smart phones, digital cameras, and camcorders, the elevated performance has to be delivered with limited size, cost, and power.

Although it is exciting to expect these above said and many more features in future smartphones but it becomes expensive and pricey to pay for such smartphones too.

5. PERVASION OF ANDROID IN EMBEDDED DEVICES:

Reasons for Android to move from smart phones to a broader range of embedded devices can be based on commercial requirements and technical requirements.

Commercial requirements cannot reflect on all android requirements but some reasons for embedded android.

- i) License for software components: Emedded software development using open source technology need licenses for embedded software components. If modified version of source code is generated then license may not be required under the terms of original license.
- ii) Source code management: A comprehensive set of source code is provided by Google's android. This

code is actively managed by a vibrant community. Anybody can get a benefit who wants to optimize the components. This reduces team's learning curve.

- iii) Release rhythm: Major releases of android are very frequent. It has rapid release cycles because we can see multiple releases per year. The rate of innovation is always a plus point for the developer.
- iv) Support of ecosystem: Most android products were based on ARM architecture. These hardware providers help to speed up time to market and thus advantageous. Rather than driving only into application layer but also into middleware components is critically important from both augmentation and optimization perspective in order to continue the evolution of android.
- v) Documentation and training: Android is not free. In the sense that in order to get our team enabled an up to date documentation is needed. Android community offers a diversity of tutorials, videos, extensive blogs, and independent companies providing academies.

Technical requirements intensively focuses on top engineering based reasons that make embedded developers to move towards android.

- i) Android java and DVM: Programming language is one of the decision criteria. It is associated with upper and middle layer of software stack. Java is common programming language and android is based on java. It has its own virtual machine, Dalvik Virtual Machine similar to JVM. Any java programmer can easily work with it.
- ii) Hardware reference platforms: The wide availability of hardware platforms for prototyping and benchmarking purposes resulted in popularity of android. The primary choice is ARM based platform. ARM based android development phones are most suitable for Android compliance test suite. Some other platforms include Texas, Zoom Beagleboard systems etc., A new class of form-factor-approximate development devices for embedded android systems are designed for set top boxes, tablets etc.
- iii) Technical frameworks: Android has a new technical framework. Some devices require larger screens than Smartphone or even multiple screens. Google and its partner community are investing on frameworks that enabled specific application needs.
- iv) NDK support: Native development kit is a toolset to embed components that make use of native C/C++ code in android applications. NDK support

was added to standard android software development kit to moderate the limitations of java based application development. This gave a way for creating performance and graphics sensitive applications which is a tremendous benefit for developers.

- v) Development and debug tools: Open source development environment and debug tools allow us to rapidly switch to an android development. Eclipse offers dedicated plug in for android that is ADT plug in. his lets us to create application specific user interfaces, add components, debug and then export .apks.

6. CONCLUSION:

Android is gaining popularity in a very rapid way for both smart phones as well as embedded devices. A systematic estimation of technical features of android culminates the idea that android is superior for design of competitive embedded systems. The systematized and well organized API and innovative life cycle of application made it very ease for starting development of the system.

After studying Android SDK and its available tools and resources, it can be reviewed that there is some considerations for applying android beyond conventional and formal routine mobile handsets like for example medical devices, consumer devices, military aerospace systems etc. but more emphasis can be given in the application of android in the in-home automation and sophisticated embedded devices. Android's ultimate market acceptance will be based on how quickly the commercial and technical requirements can be capitalized in order to overcome its newness with the platform.(N.B.: All Web links in 'References' below have been last checked and working on 12 November 2012.)

REFERENCES:

- [1] Patrick Schaumont, Anand Raghunathan : Guest Editors' Introduction: Security and Trust in Embedded-Systems Design ; In Proc: Design and Test of ICs for Secure Embedded Computing, 2007 IEEE Copublished by the IEEE CS and the IEEE CASS IEEE Design & Test of Computers, Pages 518-520
- [2] Prof. Sorin Alexander Huss, : The DEVS Model of Computation – A Foundation for a Novel Embedded Systems Design Methodology, Plenary Talk I: Wednesday, November 30, 2011
- [3] Karim Yagmour.; Building Embedded Linux systems 2008
- [4] Raj kamal.: Embedded Systems Architecture, Programming and Design, – 2nd Edition The McGrawHill publications 2009
- [5] Aleksander Malinowski, and Hao Yu.; Comparison of Embedded System Design for Industrial Applications: IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 2, MAY 2011
- [6] Catherine: A survey on Embedded OS ;: IEEE Transactions on Embedded computing 2002

- [7] S. Baskiyar, Ph.D. and N. Meghanathan : A Survey of Contemporary Real-time Operating Systems Dept. of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA; Informatica 29 (2005) 233–240
- [8] What is Android?: <http://www.android.com/about/>
- [9] Mobile Operators: <http://www.openhandsetalliance.com/>
- [10] Arduino Prototyping Platform: <http://www.arduino.com>
- [11] Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. <http://www.code.google.com/p/arduino>
- [12] Cláudio Maia, Luis Miguel Nogueira, Luis Miguel Pinho.: Technical Report Evaluating Android OS for Embedded Real-Time Systems; HURRAY-TR-100604 Version: Date: 06-29-2010
- [13] Suman Kumar S.P and Vijay Anand : A Robust Client Architecture On Android To Cater End-2-End Real-Time Content Management And Personalized Iptv Services To Mobile Internet Devices; International Journal of Next-Generation Networks (IJNGN) Vol.2, No.3, September 2010
- [14] Paul POCATILU.: Developing Mobile Learning Applications for Android using Web Services ; Informatica Economica vol. 14, no. 3/2010
- [15] David Ehringer.: The Dalvik Virtual Machine Architecture , March, 2010
- [16] Karim Yaghmour.:Porting Android to New Hardware; Android Builders Summit – April 14th 2011
- [17] Release notes for TiVo client SDK for AS3 v0.9 2012
- [18] Micheal J pont and Chisanga Mwelwa; In Proc: VikingPLoP 2003, Developing reliable embedded systems using 8051 and ARM processors: towards a new pattern language
- [19] Hughes Systique Corporation: Android porting guide for embedded platforms, 03/16/2009 Rel. 2.0 HSC Restricted
- [20] Bonifaz Kaufmann: Design andImplementation of a Toolkit for the Rapid Prototyping of Mobile Ubiquitous Computing ; MASTER THESIS, Computer Science, University of Klagenfurt August 2010
- [21] Aaron Carroll, Gernot Heiser.: An Analysis of Power Consumption in a Smartphone-2011
- [22] G.P. Perrucci, F.H.P Fitzek, J. Widmer Survey on Energy Consumption Entities on the Smartphone Platform-Nokia Research Center
- [23] Maged NK Boulos, Steve Wheeler, Carlos Tavares and Ray Jones.: How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX
- [24]Scott Meninger, Jose Oscar Mur-Miranda, Rajeevan Amirtharajah, Anantha P. Chandrakasan, and Jeffrey H. Lang.: Vibration-to-Electric Energy Conversion; IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 9, No. 1, February 2001
- [25] Eleanor Toye, Richard Sharp, Anil Madhavareddy, and David Scott.: Using Smart Phones to Access Site-Specific Services, IEEE Pervasive Computing, Mobile and Ubiquitous systems Vol. 4, No. 2 April–June 2005
- [26] A Mendoza Garcia, M Rodriguez Huizar, B Baumgartner, U Schreiber, A Knöll.: Embedded Platform for Automation of Medical Devices, Computing in Cardiology 2011; 38:829–832.
- [27] Roozbeh Jafari.: Medical Embedded Systems - A dissertation submitted in partial satisfaction of the requirements for the degree Doctor of Philosophy in Computer Science, University of alifornia, Los Angeles, 2006



DIAGNOSIS OF LUNG CANCER DISEASE USING NEURO-FUZZY LOGIC

A MALATHI PALANI

Department of Computer Science, M.S Ramaiah College of Arts, Science and Commerce, Bangalore.

Abstract:- Artificial Neural Network and fuzzy logic are the branch of Artificial intelligence, have been accepted as a new technology in computer science. Neural Networks and fuzzy logic has rapidly become one of the most successful of today's technologies especially in the field of medicine, particularly in the fields of radiology, urology, cardiology, oncology and etc. In this paper, an attempt has been made to make use of neural networks and fuzzy logic in the medical field (carcinogenesis (pre-clinical study)). In carcinogenesis, neuro-fuzzy have been successfully applied to the problems in both pre-clinical and post-clinical diagnosis. In this study, a fuzzy logic-based system for diagnostic decision support for pre-clinical diagnosis of cancer diseases is presented.

Keywords: *Neural networks, fuzzy logic, carcinogenesis, lung cancer, rule extraction, back propagation, medical decision making, decision support systems, rule extraction, membership function, fuzzy inference model, Machine learning, etc.,*

INTRODUCTION

Neuro-fuzzy applications are used in a wide range medical diagnosis. Even today, the diagnosis cancer disease represents a serious clinical problem. The medical knowledge in this field is characterized by uncertainty, imprecision and vagueness. Medical diagnosis is one of major problem in medical application.

Several research groups are working world wide on the development of neural networks in medical diagnosis. A detailed study on Artificial Neural Network (ANN) can be seen in "Neural and Adaptive Systems: Fundamentals Through Simulations" by Principe, Euliano, and Lefebvre(2000). Paulo J. Lisboa and Azzam F.G. Taktak (2006) had done a systematic review on artificial neural networks in decision support in cancer. This paper reports on a systematic review that was conducted to assess the benefit of artificial neural networks (ANNs) as decision making tools in the field of cancer. This paper reviews the clinical fields where neural network methods figure most prominently, the main algorithms featured, methodologies for model selection and the breast cancer diagnosis. Kiyani and Yildirim(2003) employed Radial Basis Function, General Regression Neural Network and Probabilistic Neural Network in order to get the suitable result.

CANCER DISEASE PRE-CLINICAL DETECTION AND NEURAL NETWORKS

Carcinogenesis (*the creation of cancer*), is the process by which normal cells are transformed into cancer cells. (In other words, uncontrolled and dangerous cell growth). Cancer is the general name for over 100 medical conditions involving uncontrolled and dangerous cell growth. One of the major determinants of an individual susceptibility to cancer is sex - An obvious distinction that accounts for much of the variation in cancer g known carcinogens. Compared to

need for rigorous evaluation of results. Theakos N (2004), developed a fuzzy system to understand a disturbance occurred after a diagnosing. Zarkadakis G (1989), Monitored the arterial acid-base status of ICU patients. He measured and calculated the acid-base variables pH, the partial pressure of carbon-dioxide (PCO₂) and the bicarbonate-ion concentration ([HCO₃]). Based on these values he had developed a computer program for the multivariate evaluation and graphical monitoring. A composite index is introduced for the monitoring of all three laboratory values.

Jari J. Forsström, Kevin J. Dalton (1995) developed connectionist models such as neural networks, which define relationships among input data that are not apparent when using other approaches. They also reviewed the use of neural networks in medical decision support. Paulo J. Lisboa, Azzam F. G. Taktak(2006) assess the benefit of artificial neural networks (ANNs) as decision making tools in the field of cancer. In the work of G Wilym s. Lodwick, M.D., Richard Connors and Charles A. Harlow (1979), an efficient neural network model has been developed to diagnosis the carcinogenesis. Neural network have been applied to nonsmokers, men who smoke are about 23 times more likely to develop lung cancer and women who smoke are about 13 times more likely. Smoking causes about 90% of lung cancer deaths in men and almost 80% in women. (For women, the risk of cervical cancer increases with the duration of its incidence. There are a number of cancers to which only males are susceptible or to which only females are susceptible. For eg., females have no risk of ever experiencing cancer of prostate, penis and males are not threatened by ovarian, endometrial or cervical cancers. The next factor of susceptibility to cancer is age - Susceptibility to cancer is low for persons under thirty years of age and increases steadily in subsequent age groups, while middle aged persons and particularly older persons are more susceptible to cancer. The third factor is genetic

predisposition - Some adult cancers show the effects of genetic transmission of susceptibility although other factors may be more prominently associated with their development. Lung cancer is an example of such inherited susceptibility. In case of female breast cancer, close relatives of breast cancer patients have a high risk of breast cancer two or three times that of women with no family history of breast cancer. The fourth factor considered is geographic variations - Scientists suggest that some cancer is caused by environmental conditions. Today, cancer constitutes a major health problem. Penedo *et al* (1998) developed a system that employed an artificial neural network to detect suspicious regions in a low-resolution image and employed another artificial neural network to deal with the curvature peaks of the suspicious regions, which was used in the detection of lung nodules found on digitized chest radiographs. Bartfay (2006) proposed a neural network model. Utilizing data on patients from two National Cancer Institute of Canada clinical trials, he compared predictive accuracy of neural network models and logistic regression models on risk of death of limited-stage small-cell lung cancer patients.

CANCER DISEASE PRE-CLINICAL DETECTION AND FUZZY

Today, cancer constitutes a major health problem. Lung cancer is one of the most common and deadly diseases in the world. It is the second leading cause of death. The most common risk factor for lung cancer is smoking, due to the harmful *carcinogens* found in tobacco smoke. Lung cancer is one of the most common and deadly diseases in the world. Detection of lung cancer in its early stage is the key of its cure. Several hundreds papers based on fuzzy set theory in medicine were published in different aspects of application: diagnosis, differential diagnosis, therapy, image analysis, pattern recognition, patient monitoring, medical data analysis, data bank, text analysis and etc.. John, R.I (2005) describes a fuzzy approach to computer-aided medical diagnosis in a clinical context. It introduces a formal view of diagnosis in clinical settings and shows the relevance and possible uses of fuzzy cognitive maps. A lightweight fuzzy process is described and evaluated in the context of diagnosis of two confusable diseases. The process is based on the idea of an incremental simple additive model for fuzzy sets supporting and negating particular diseases. These are combined to produce an index of support for a particular disease. The process is developed to allow fuzzy symptom information on the intensity and duration of symptoms. Results are presented showing the effectiveness of the method for supporting differential diagnosis. Elpiniki I. Papageorgiou (2009) developed a new approach for the construction of Fuzzy Cognitive Maps augmented by knowledge through fuzzy rule-extraction methods for medical

decision making is investigated. The system proposed is based on diagnosis cells that depending upon the type of knowledge, can be fuzzy inference systems, neural networks, neuro-fuzzy networks, other type of hybrid systems or even simple fuzzy or crisp mathematical formulas.

NEURO FUZZY SYSTEM - NEURAL MODEL

Neural Network Model

The construction of the neural network involves three different layers with feed forward architecture. This is the most popular network architecture in use today. The input layer of this network is a set of input units, which accept the elements of input feature vectors. The input units (neurons) are fully connected to the hidden layer with the hidden units. The hidden units (neurons) are also fully connected to the output layer. The output layer supplies the response of neural network to the activation pattern applied to the input layer. The information given to a neural net is propagated layer-by-layer from input layer to output layer through (none) one or more hidden layers.

Important issues in MultiLayer Perceptrons (MLP) design include specifications of the number of hidden layers and the number of units in these layers. The number of input and output units is defined by the problem the number of hidden units of use is far from clear. That is the amount of hidden layers and their neurons is more difficult to determine. A network with one hidden layer is sufficient to solve most tasks. There is no theoretical reason ever to use more than two hidden layers. It is also been seen that for the vast majority of principal problems. Those problems that require two hidden layers are only rarely encountered in real life situations. Using more than one hidden layer is almost never beneficial. It often slows dramatically when more hidden layers are used. None of the known problems needs a network with more than three hidden layers in order to be solved error. Choosing an appropriate number of hidden nodes is important.

In the network the input neuron values are the demographic data concerns information such as patient's age, sex etc. The hidden neuron values are based on heuristic diagnostic knowledge represents experience accumulated through years and concerns the way an expert uses the patient data to make diagnoses.

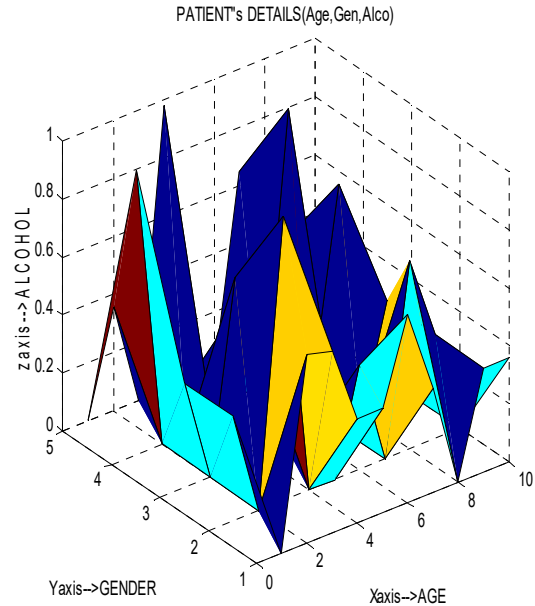
Training the model

Once a network has been structured for a particular application, that network is ready to be trained. To start this process the initial weights are chosen randomly. Learning techniques are often divided into supervised, unsupervised and reinforcement learning. Nominal variables are used to represent the input values in the the nodes of the input layer. Nominal variables may be two-state or many-state. A two-state nominal variables is easily represented by

transformation into a numeric value .For e.g, Male =0 , Female=1.Many-state nominal later. In order to test the real generalization abilities of a network to unknown data, it must be tested by classified, but yet unknown data, the *test data* that should not contain samples coming from patients of the training data. We have to face the fact that patient data is very individual and it is difficult to generalize from one patient to another. Ignoring this fact would pretend better results than a real system could practically achieve. Initially 100 lung cancer patients data has been collected from various hospitals and trained with the neural networks. It gives more than 87% of accuracy .

Data description and Training data using neural – network model

MATLAB is derived from MATrix LABoratory. The MatLab programming language is exceptionally straightforward since almost every data object is assumed to be an array It is an interactive, matrix-based system for scientific and engineering numeric computation and visualization. It includes high-level functions for two-dimensional and three-dimensional data visualization, image processing, animation, and presentation graphics. Initially 100 lung cancer patients data has been collected from various hospitals and trained with the neural networks. It gives more than 87% of accuracy. The results are found to be better using back propagation algorithm. For e.g age<35={1,0,0}, age>=35<=55 ={0,1,0}, age>55={0,0,1}.Similarly the other input values are represented .Neural networks has facilities to convert both two-state and many-state nominal variables equals the number of possible values ;one of the N variables is set and the others are cleared..



NEURO FUZZY SYSTEM- FUZZY MODEL

Fuzzy system is highly useful for medical diagnostic problems due to the inherent imprecision and uncertainty in the medical data. The proposed fuzzy system consists of two levels of lung cancer risk, first level lung cancer risk (FLLCR) and second level lung cancer risk (SLLCR). The inputs used factors to find FLLCR are: age, gender, smoking, alcohol and the inputs for the second level to find SLLCR are: FLLCR , cough , vomiting , loss of weight and chest pain. The models of FLLCR and SLLCR are shown in figure 1 & 2

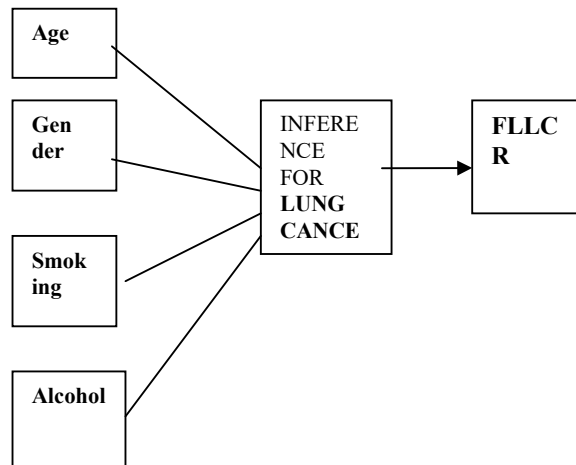
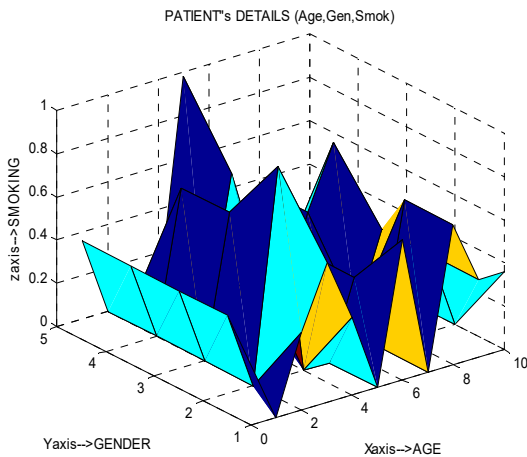


Fig 1 - Model of First Level Lung Cancer Risk

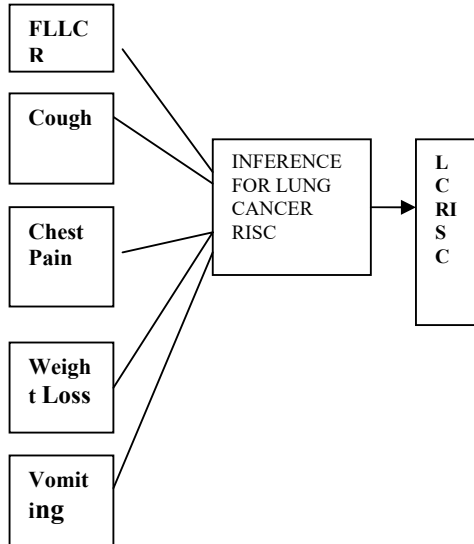


Fig 2 - Model of Second Level Lung Cancer Risk

FLLCR- FIRST LEVEL LUNG CANCER RISK

The first level lung cancer risk is based on the patient history , such as age, gender, smoking and alcohol. Fuzzy system (first level) works with 54 rules . This gives a total of 54 output pairs. It is necessary to find the exact level of risk of the patient. This will also aid in the development of automated systems that can precisely classify the risk level of the lung cancer patient under observation. Hence an optimization of the outputs of the fuzzy system is necessary. This will improve the classification of the patient. The fuzzy rules are , For example, Rule 1, Rule 2,Rule 52, Rule 53 and Rule 54 can be interpreted as follows:

Rule 1	If age = Young and gender = F and Smoking = No and Alcohol = No then Cancer Risk = Low.
Rule 2	If age = Young and gender = F and Smoking = No and Alcohol = Occasional then Cancer Risk = Low
Rule XXX	----- ----- -----
Rule 54	If age = Old and gender = M and Smoking = Regular and Alcohol Regular then Cancer Risk = High

Table 1 – FLLCR Rules

SLLCR – Second Level Lung Cancer Risk

The second level lung cancer risk is based on the output of first level and clinical symptoms, such as cough , chest pain ,loss of weight and vomiting with 48 rules . This gives a total of 48 output pairs. The outputs of these proposed fuzzy systems are optimized. For example, Rule 1, Rule 2,Rule 40, Rule 47 and Rule 48 can be interpreted as follows:

Rule 1	If FLLCR = low and cough =yes and chest pain = yes and loss of weight =yes and vomiting =yes then Lung Cancer Risk = Medium
Rule 2	If FLLCR = low and cough =yes and chest pain = yes and loss of weight =yes and vomiting =no then Lung Cancer Risk = Low.
Rule XXX	----- -----
Rule 48	If FLLCR = high and cough =no and chest pain =no and loss of weight =no and vomiting =no then Lung Cancer Risk = Low.

Table 2 – SLLCR Rules

Linguistic variables

Fuzzy logic uses linguistic variables to describe a system. Linguistic variables are described by words, rather than a value like normal Boolean variables. For instance, the linguistic variable "age" may have "young," "middle," and "old" defining its range of values. Linguistic rules describing the control system consist of two parts; an antecedent block (between the IF and THEN) and a consequent block (following THEN). Membership functions are used to convert non-fuzzy data to fuzzy data. Moreover, membership functions are a set of fuzzy variables. For example, a range of gender values may be represented by a fuzzy variable subset "F" and "M". Each input feature is classified into various fuzzy linguistic levels A typical fuzzy controller is composed of membership functions, rules, and a defuzzification unction. This mapping produces a fuzzy membership function. For example the value if FLLCR is 0.00867143 (low) and SLLCR is 0.523469 (medium) after defuzzification. The corresponding calculated values of FLLCR and SLLCR are given below:

<i>Age</i>	<i>Age*W</i>	<i>Gen</i>	<i>Gen*W</i>	<i>Smok</i>	<i>Smok*W</i>	<i>Alco</i>	<i>Alco*W</i>	<i>FLLCR</i>	<i>FLLCR</i>
0.071429	-0.07143	0.4	0.08	0	0	0.001	0.0001	0.00867	Low

Table 3 – FLLCR values for an Input

FLLCR	cough	Gen chest pain	weight loss	vomiting	SLLCR	FLLCR
0.008671	0.6	0.4	0.2	0.1	0.523469	Low

Table 4 – SLLCR values for an Input

COMPARISON OF NEURAL NETWORKS MODEL AND FUZZY MODEL

Chin-Teng Lin and C. S. George Lee (1991) proposed neural-network (connectionist) model for fuzzy logic control and decision systems. This connectionist model, in the form of feedforward multilayer net, combines the idea of fuzzy logic controller and neural-network structure and learning abilities into an integrated neural-network-based fuzzy logic control and decision system.

In our proposed neuro-fuzzy model patient details are compared with neural network model and fuzzy model. In neural network model, for example the patient age is 30, gender is male and smoking habit is no and the alcohol is no then the chance (output) of getting cancer is 0.15 (almost nil). In fuzzy model, for the same input values the chance of getting cancer is low. Similarly comparing the details of various patient's demographic data the neural and fuzzy model gives 82% of accurate results.

CONCLUSION

Lung cancer is one of the most common and deadly diseases in the world. Detection of lung cancer in its early stage is the key of its cure. The automatic diagnosis of lung cancer is an important, real-world medical problem. In this paper we have introduced the use of fuzzy methodology and fuzzy system for pre-clinical lung cancer. The main advantage of the model is its simplicity and good accuracy. The study has made use of common data obtained from the patients of KMC and M S Ramaiah hospital, Bangalore.

In this paper the author has shown how neuro – fuzzy system is used in actual clinical diagnosis of lung cancer. In this work, the performance of neural network structure was investigated for lung cancer diagnosis problem.

REFERENCES

[1]. Anagnostou T, Remzi M, Lykourinas M, Djavan B (2003). "Artificial neural networks for decision-making in urologic oncology". Eur Urol. 2003 Jun;43(6):596-603. Review.

[2] B.D. Ripley (1996). "Pattern Recognition and Neural Networks". Cambridge University Press, Cambridge, 1996.

[3] B.D. Ripley and R.M. Ripley(2001). "Neural networks as statistical methods in survival analysis". In R. Dybowski and V. Gant, editors, Clinical Applications of Artificial Neural Networks, chapter 9. Cambridge University Press, Cambridge. In press. [4] Brown, Robert J (1987)., "An Artificial Neural Network Experiment", Dr. Dobbs Journal, April 1987.52. Rawtani,J LRana &A K Tiwari-Number Hidden Nodes for Shape Preserving ANN Representation of a Curve,Maulana Azad College of Technology ,Dept. of Electronics and Computer Science & Engineering,Bhopal,India

[5] C.A. Galletly, C.R. Clark, and A.C. McFarlane (1996). Artificial neural networks: "A prospective tool for the analysis of psychiatric disorders". Journal of Psychiatry & Neuroscience, 21(4):239–47, 1996.

[6] Chiou YSP, Lure YMF (1993), Ligomenides PA. "Neural network image analysis and classification in hybrid lung nodule detection (HLND) system". In: Proceedings of the IEEE-SP Workshop on Neural Networks for Signal Processing, 1993.

[7] C.M. Bishop, M. Svensen, and C.K.I. Williams (1997). GTM: "The generative topographic mapping". Neural Computation, 10(1):215–234, 1997.

[8] C.Pappas, N.Maglaveras and J.R.Scherrer(1998), "The computational capabilities of three-layered neural networks"- IOS press, Thessalonike, Greece.were proven by Hornik et al.,10

[9] C. Robert, C. Guilpin, and A. Limoge (1998). "Review of neural network applications in sleep research". Journal of Neuroscience Methods, 79(2):187–193, 1998.

[10] Derong Liu; Zhongyu Pang; Lloyd S.R (2008) –"A Neural Network Method for Detection of Obstructive Sleep Apnea and Narcolepsy"- Based on Pupil Sizeand EEG.2008 V-19 I-2

[11] Djoussé L et al.(2002) Alcohol Consumption and Risk of Lung Cancer: "The Framingham Study". J Natl Cancer Inst 2002;94:1877-82.

[12] Dreifus LS (1956). "A clinical correlative study of the electrocardiogram in electrolyte imbalance". Circulation.1956; 14: 815-825.E. BARTFAY, PHD, ASSOCIATE PROFESSOR 1,

[13] Eberhart, R. Micheli-Tzanako, E (1990).-"Neural

- networks for engineering in medicine and biology “,Appl. Phys. Lab., Johns Hopkins Univ., Laurel, MDIEEETransactionson Volume 1, Issue 4,Dec1990Page(s):305 – 306
- [14] E.O. Madu, V. Stalbovskaya, B.Hamadicharef, E.C. Ifeachor- Preoperative Ovarian Cancer using Neuro – Fuzzy Approach,Univ. of Plymouth,UK.
- [15] Fausett, L (1994). “Fundamentals of Neural Network: Architectures, Algorithms and Applications”. Prentice Hall; Englewood Cliffs(1994).
- [16] Fogel DB, Wasson EC (1995) 3rd, Boughton EM: “Evolving neural networks for detecting breast cancer”. *Cancer Lett*, 1995; 96(1): 49-53
- [17] Garibaldi, J.M. & Ozen, T.- Uncertain Fuzzy Reasoning: A Case Study in Modelling Expert Decision Making , *IEEE Transactions on Fuzzy Systems*, (2007) Pages 16-30, 2007.
- [18] Greenlee RT, Murray T, Bolden S(2000), et al.: *Cancer statistics 2000*. *CA Cancer J Clin* 2000, 50:7–33
- [19] G Wilyms(1). Lodwick,M.D.,Richard Conners(2) ,Ph.D and Charles A. Harlow(2),Ph.D-(!) Dept. of Radiology ,Univ. of Missouri , Columbia (@)Dep of Electrical Engg. ,Louisiana state univ.,Louisiana -IEEE 1979
- [20] Heine H. Hansen, MD(1990)- Lung Cancer—“A Changing Picture”,National University Hospital, The Finsen Center 5072,9 Blegdamsvej, Copenhagen DK-2100, 1990 ,Denmark.E-mail: hansenhh@iaslc.org
- [21] Hernandez, C.A. et al (1993)., "How to Choose the Training Data for Neural Network Medical Diagnosis Systems", *ISA*, pp. 283-290 (1993)
- [22] Hornik K, Stinchcomb X(1989), White X. “Multilayer feedforward networks are universal approximators”. *Neural Net* 1989;2: 359–66.
- [23] Ismail SARITAS ,Novruz ALLAHVERDI and Ibrahim Unai SERT(2003) – “A Fuzzy System Design for diagnosis of Prostrate Cancer”,*International Conference on Computer systems and Technologies-CompSysTech’2003*
- [24] J.P. Hogge, D.S. Artz, and M.T. Freedman(1997). “Update in digital mammography.Critical Reviews in Diagnostic Imaging”, 38(1):89–113, 1997.
- [25] Kornel papik ,Zalan,Dombovari,Zsolt tulassay ,Janos feher and Bela molnar(1998) – Dept of medicine,Semmaleveis medical university,Hungary and Raier Schaefer- Germany - “Applications of neural networks in medicine”-a review 1998-Vol 4.
- [26] L. Tarassenko(1995). “Neuralnetworks”. *Lancet*, 346:1712, 1995.Martens, J.-P. Weymaere, N (2002)-“An equalized error backpropagation algorithm for the on-line training of multilayer perceptrons”.*Electronics & Inf. Syst.*, Ghent Univ., Gent; *IEEE trans*,2002.
- [27] Moul JW, Snow PB, Fernandez EB, Maher PD, Sesterhenn IA(1995)- “Neural network analysis of quantitative histological factors to predict pathological stage in clinical stage I nonseminomatous testicular cancer”. *J Urol*, 1995; 153(5): 1674-5 Philip
- [28] M.R. Brickley, J.P. Shepherd, and R.A. Armstrong(1998). *Neural networks: “A new technique for development of decision support systems in dentistry”*. *Journal of Dentistry*, 26(4):305–309, 1998.
- [29] Nguyen Hoang Phuong-Fuzzy SetTheory and Medical Expert Systems:Survey and Model,Institute of Computer Scienre (1995) Vol 2, Page 182 .
- [30] Penedo MG, Carreira MJ, Mosquera A, Cabello D(1998).” Computer-aided diagnosis: a neural-network-based approach to lung nodule detection”. *IEEE Trans. Medical Imaging* 1998; 17(6)
- [31] Penny W etc(1996).” *Neural networks in clinical medicine”*. *Med Decis Making*. 1996; 16:386-398.
- [32] Ktonas(1996). “Computer-based recognition of EEG patterns”. –*Electroencephalography & Clinical Neurophysiology – Supplement*, 45:23–35, 1996.



A MACHINE LEARNING APPROACH FOR IDENTIFYING DISEASE-TREATMENT RELATIONS IN SHORT TEXTS

SHIVAM SRIVASTAVA · UTKARSH SRIVASTAVA & MITHILESH CHATURVEDI

Dept. of Computer Science & Engineering ITM Gida, Gorakhpur

Abstract - Machine learning offers a principled approach for developing sophisticated, automatic, and objective algorithms for analysis of high-dimensional and multimodal biomedical data. The Machine Learning (ML) is almost used in any domain of research and now it has become a reliable tool in the medical domain. The models that we use represent a combination of lexical and syntactic features, medical semantic information, terms extracted from a vector-space model created using a random projection algorithm, and additional contextual information extracted at sentence-level. The potential value of this paper stands in the ML settings that we propose and in the fact that we outperform previous results on the same data set. **Keywords** - *Machine Learning, relation classification, natural language processing.*

1. INTRODUCTION

Machine learning, a sub discipline in the field of artificial intelligence (AI), focuses on algorithms capable of learning and/or adapting their structure based on a set of observed data, with adaptation done by optimizing over an objective or cost function. Natural Language Processing (NLP) and Machine Learning (ML) are the techniques that are used here. The ultimate aim is to show what representation of information and algorithms used to identify and provide relevant healthcare information in short texts. Currently text categorization is applied in many contexts, ranging from document indexing depending on a managing vocabulary, to document filtering, automated metadata creation, vagueness of word sense, population of and in general any application needs document organization or chosen and adaptive document execution. As the field of machine learning has matured, greater effort has gone into developing a deeper understanding of the theoretical basis of the various algorithmic approaches. In fact, a major difference between machine learning and statistics is that machine learning is concerned with theoretical issues such as computational complexity, computability, and generalization and is in many respects a marriage of applied mathematics and computer science. The contributions that we bring with our work stand in the fact that we present an extensive study of various ML algorithms and textual representations for classifying short medical texts and identifying semantic relations between two medical entities: diseases and treatments. The traditional healthcare system is also becoming one that embraces the Internet and the electronic world. Moreover, identifying relations between medical entities in clinical data can help in stratifying patients by disease susceptibility and response to therapy, reducing the size, duration, and cost of clinical trials, leading to the development of new treatments, diagnostics, and prevention therapies. Since healthcare providers need to

be up-to-date with all new discoveries about a certain treatment, in order to identify if it might have side effects for certain types of patients. The results that we obtained show that it is a realistic scenario to use NLP and ML techniques to build a tool which is capable of identifying and disseminating information which are related to diseases and treatments. Machine learning and statistical pattern recognition have been the subject of tremendous interest in the biomedical community because they offer promise for improving the sensitivity and/or specificity of detection and diagnosis of disease, while at the same time increasing objectivity of the decision-making process.

2. RELATED WORKS

This work presents various Machine Learning (ML) and information for classification of short texts and finds the relation between diseases and treatments. According to ML technique the information are shown in short texts when identifying relations between two entities such as diseases and treatment. The main focus of their work is on entity recognition for diseases and treatments. The authors use Hidden Markov Models and maximum entropy models to perform both the task of entity recognition and the relation discrimination. The tasks addressed in our research are information extraction and relation extraction. From the wealth of research in these domains, we are going to mention some representative works. The task of relation extraction or relation identification is previously tackled in the medical literature, but with a focus on biomedical tasks. In this work user can give their symptoms, the server will extract the information from various articles related to those symptoms. Then it classifies that information based on the symptoms and then provides the cure, preventive measures and side-effects for those symptoms. The main task in this work is to extract healthcare information and the relation details. In this research work, it focuses on diseases and treatment

information, and the relation that exists between these two entities. So this approach works well even with fewer amounts of data. Concerning relation extraction the rule checks whether the text information contains any relation or not. For this relation extraction the statistical approach uses bag-of-words technique. Some researchers combined this technique with POS which provides two sources of information such as relation between entities and their specific contexts. And it is proved that simple technique coproduce accurate results. The most relevant related work is the work done by Rosario and Hearst [1]. The authors of this paper are the ones who created and distributed the data set used in our research. The data set consists of sentences from Medline5 abstracts annotated with disease and treatment entities and with eight semantic relations between diseases and treatments. The tasks addressed in our research are information extraction and relation extraction. From the wealth of research in these domains, we are going to mention some representative works. The task of relation extraction or relation identification is previously tackled in the medical literature, but with a focus on biomedical tasks: subcellularlocation (Craven, [2]), gene-disorder association (Ray and Craven, [3]), and diseases and drugs (Srinivasan and Rindflesch, [4]). Syntactic rule-based relation extraction systems are complex systems based on additional tools used to assign POS tags or to extract syntactic parse trees. It is known that in the biomedical literature such tools are not yet at the state-of-the-art level as they are for general English texts, and therefore their performance on sentences is not always the best (Bunescu et al. [5]). Representative works on syntactic rule-based approaches for relation extraction in Medline abstracts and full-text articles are presented by Thomas et al. [6] The semantic rule-based approaches suffer from the fact that the lexicon changes from domain to domain, and new rules need to be created each time. Certain rules are created for biological corpora, medical corpora, pharmaceutical corpora, etc. Systems based on semantic rules applied to full-text articles are described by Friedman et al. [7], on sentences by Pustejovsky et al. [8], and on abstracts by Rindflesch et al. [9]. Various learning algorithms have been used for the statistical learning approach with kernel methods being the popular ones applied to Medline abstracts (Li et al. [10]). Our work differs from the ones mentioned in this section by the fact that we combine different textual representation techniques for various ML algorithms.

3. PROPOSED SYSTEM

3.1 Tasks and Data Sets

The two tasks used in this paper are the basis for the development of information technology framework. This framework helps to identify the medical related information from abstracts. The first task deals with extraction all information regarding diseases and treatments while the task deals with extraction of related information existing between disease and treatments. The framework developed with these tasks are used by healthcare providers, people who needs to take care of their health related problems and companies that build Systematic views. Applied machine

Relationship	Definition and Example
Cure 810 (648, 162)	TREAT cures DIS <i>Intravenous immune globulin for recurrent spontaneous abortion</i>
Only DIS 616 (492, 124)	TREAT not mentioned <i>Social ties and susceptibility to the common cold</i>
Only TREAT 166 (132, 34)	DIS not mentioned <i>Flucticasome propionate is safe in recommended doses</i>
Prevent 63 (50, 13)	TREAT prevents the DIS <i>Statins for prevention of stroke</i>
Vague 36 (28, 8)	Very unclear relationship <i>Phenylbutazone and leukemia</i>
Side Effect 29 (24, 5)	DIS is a result of a TREAT <i>Malignant mesodermal mixed tumor of the uterus following irradiation</i>
NO Cure 4 (3, 1)	TREAT does not cure DIS <i>Evidence for double resistance to permethrin and malathion in head lice</i>
Total relevant: 1724 (1377, 347)	
Irrelevant 1771 (1416, 355)	Treat and DIS not present <i>Patients were followed up for 6 months</i>
Total: 3495 (2793, 702)	

Table 1. Original data set

learning based text categorization for disease treatment relations titled “A Machine Learning Approach for Identifying Disease-Treatment Relations in Short Texts”.

With the reference of their proposal the authors debated that The Machine Learning (ML) field has won place in almost any domain of research and of lately become a reliable tool in the medical field. The empirical domain of automatic learning is used in tasks like medical decision support, medical imaging, protein-protein interaction, extraction of medical knowledge, and for total patient management care. ML is pursued as a tool by which computer-based systems can be combined with healthcare field in order to get a better, more efficient medical care.

Task 1: In this three models have been built. Each model is focused on relation and provides the difference

between the sentences that contain information that do not contain.

Task 2: Unlike in setting 1 it has only one model. This model focus on three relation (cure, prevent and side effects). It distinguishes relations in three-class tasks and contains label in each sentence that has any one semantic relation. The most important thing is that they can be combined in pipeline so that it provides solution to framework which identifies all related information. This proposed pipeline approach first deals task1 and then carries out with task2 so that it can give only informative sentences based on three relations. The logic behind to go with pipeline approach is to identify the best model to identify and extract the reliable healthcare information. With this pipeline task some problems can be removed due to the fact that unwanted information can be the potential factor to classify the sentences into three semantic relations.

3.2 Classification Algorithms and Data Representations

While working with ML technique two challenges should be considered. One is to find the exact model. ML provides a better model that can be used. To find the model one should rely on empirical studies and should gain knowledge in healthcare domain. The next one is to provide better data representation and to do feature engineering, because feature increase the performance of the model. Finding the exact feature for the predictive model is a crucial task that should be considered. These two challenges can be achieved by using various algorithms and textual representation that suits for the tasks. In ML, as a field of empirical studies, the acquired expertise and knowledge from previous research guide the way of solving new tasks. The models should be reliable at identifying informative sentences and discriminating disease-treatment semantic relations. The research experiments need to be guided such that high performance is obtained. The experimental settings are directed such that they are adapted to the domain of study (medical knowledge) and to the type of data we deal with (short texts or sentences), allowing for the methods to bring improved performance. There are at least two challenges that can be encountered while working with ML techniques. One is to find the most suitable model for prediction. The ML field offers a suite of predictive models (algorithms) that can be used and deployed. The task of finding the suitable one relies heavily on empirical studies and knowledge expertise. The second one is to find a good data representation and to do feature engineering because features strongly influence the performance of the models. Identifying the right and sufficient features to represent the data for the

predictive models, especially when the source of information is not large, as it is the case of sentences, is a crucial aspect that needs to be taken into consideration.

	Training		Test	
	Positive	Negative	Positive	Negative
Cure	554	531	276	266
Prevent	42	531	21	266
SideEffect	20	531	10	266

Table 2. Data Sets Used for the Second Task

3.2.1 Bag-of-Words Representation

This representation is commonly used for text classification. It is use ad to represent the features which are chosen among the words. There are two most common feature representations for bag-of-words representation. The bag-of-words is the name commonly used to classification of tasks. It is a representation in which features are selected among the words that are present in the training data. And then selection techniques are used in order to identify the most suitable words as features. Once the feature is identified, each training and test instance is mapped to this feature representation by providing values to each feature for a specific instance. Two most common feature value representations for Bag-of-Words (BOW) representation are: binary feature values or frequency feature values. The binary feature value is the value of a feature can be either 0 or 1, where 1 represents the fact that the feature is present in the instance and 0 otherwise. The frequency feature value is the value of the feature is the number of times it appears in an instance or 0 if it did not appear. Here we use frequency feature value. There is no that much difference between binary feature values and frequency feature values because there is only twenty words in each sentence of short texts. The advantage of using frequency feature values is that the feature's value will be greater than other features since it captures the number of feature appeared once in a sentence. It keeps words that appear at least three times in training data and have at least one alphanumeric.

3.2.2 NLP and Biomedical Concepts Representation

Unlike above representation this representation is based on syntactic information such as nouns, phrases, healthcare related points in the sentence. The NLP representation is based on the syntactic information such as noun-phrases, verb-phrases and biomedical

concepts. The Genia tagger is used to extract this type of information. This tagger is specially used for the biomedical text. Here the Genia tagger will run on the entire data set. Then we extract only the noun-phrases, verb-phrases and biomedical concepts. A tool called Genia tagger is used to extract information. The tagger is specifically designed for biomedical text such as Medline abstracts. It analyzes the sentences to generate base forms, chunk tags, part of speech tags. The phrases and nouns obtained by tagger is used in second representation method. While running the Genia tagger it extracts only nouns, phrases and healthcare related concepts from each sentence of data set. The steps to be followed to obtain the final feature for classification are: removing features that contains punctuations and considering lemma-based forms. Lemma is used because there is lot of words that has plural forms. Lemmatized form gives the base form of the word. Another reason to use lemma is to reduce the sparseness problem. Lemma forms remove the problem of representing only a few features in short text forms.

Inhibition	Inhibition	NN	B-NP	O
of	of	IN	B-PP	O
NF-kappaB	NF-kappaB	NN	B-NP	B-protein
activation	activation	NN	I-NP	O
reversed	reverse	VBD	B-VP	O
the	the	DT	B-NP	O
anti-apoptotic	anti-apoptotic	JJ	I-NP	O
effect	effect	NN	I-NP	O
of	of	IN	B-PP	O
isochamaejasmin	isochamaejasmin	NN	B-NP	O
.	.	.	O	O

Table 3. Example of Genia tagger output

3.2.3 Medical Concepts (UMLS) Representation

In order to work with a representation that provides features that are more general than the words in the abstracts (used in the BOW representation), we also used the unified medical language system⁷ (here on UMLS) concept representations. We use the Unified Medical Language system (UMLS) for the medical concept representation. UMLS is a source of knowledge which is developed at the US National Library of Medicine. UMLS contains about 1 million medical concepts and also about 5 million concepts which are organized hierarchical. UMLS is a knowledge source developed at the US National Library of Medicine (hereafter, NLM) and it contains a met thesaurus, a semantic network, and the specialist lexicon for biomedical domain. The met thesaurus is organized around concepts and meanings; it links alternative names and views of the same concept and identifies useful relationships between different concepts.

4. RELATION CLASSIFICATION

Identifying the interactions between proteins is one of the most important challenges in modern genomics, with applications throughout cell biology, including expression analysis, signaling, and rational drug design. Most biomedical research and new discoveries are available electronically but only in free text format, so automatic mechanisms are needed to convert text into more structured forms. We tackled an important and difficult task, the classification of different interaction types between proteins in text. A solution to this problem would have an impact on a variety of important challenges in modern biology. We used a protein-interaction database to automatically gather labeled data for this task, and implemented graphical models that can simultaneously perform protein name tagging and relation identification, achieving high accuracy on both problems.

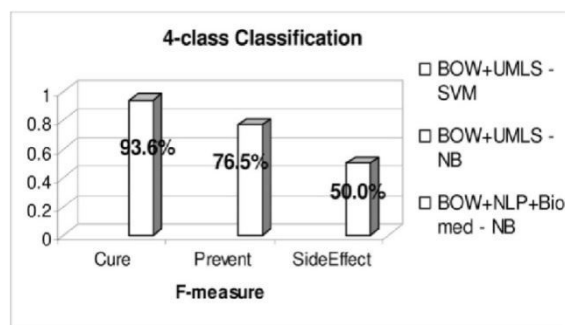


Fig 1. F-measure results for four-class classification

5. CONCLUSION AND FUTURE WORK

Machine learning has emerged as a field critical for providing tools and methodologies for analyzing the high volume, high dimensional and multi-modal data generated by the biomedical sciences. The interests are inline with the tendency of having a personalized medicine, one in which each patient has its medical care tailored to its needs. The conclusions of our study suggest that domain-specific knowledge improves the results Probabilistic models are stable and reliable for the classification of short texts in the medical domain. The representation techniques highly influence the results, common for the ML community, but more informative representations. Where the ones that consistently obtained the best results.

As future work, we would like to extend the experimental methodology when the first setting is applied, and to use additional sources of information as representation techniques.

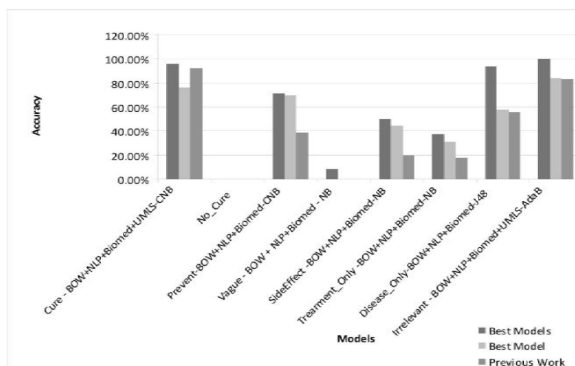


Fig. 2. Results for all annotated relations in the data set.

6. REFERENCE

[1]. B. Rosario and M.A. Hearst, "Semantic Relations in Bioscience Text," Proc. 42nd Ann. Meeting on Assoc. for Computational Linguistics, vol. 430, 2004

[2]. M. Craven, "Learning to Extract Relations from Medline," Proc. Assoc. for the Advancement of Artificial Intelligence, 1999.

[3]. S. Ray and M. Craven, "Representing Sentence Structure in Hidden Markov Models for Information Extraction," Proc. Int'l Joint Conf. Artificial Intelligence (IJCAI '01), 2001.

[4]. P. Srinivasan and T. Rindflesch, "Exploring Text Mining from Medline," Proc. Am. Medical Informatics Assoc. (AMIA) Symp., 2002.

[5]. M. Ould Abdel Vetah, C. Ne'dellec, P. Bessie' res, F. Caropreso, A.-P. Manine, and S. Matwin, "Sentence Categorization in Genomics Bibliography: A Naive Bayes Approach," Actes de la Journe'e Informatique etTranscriptome, J.-F. Boulicaut and M. Gandrillon, eds., Mai 2003.

[6]. J. Thomas, D. Milward, C. Ouzounis, S. Pulman, and M. Carroll, "Automatic Extraction of Protein Interactions from Scientific Abstracts," Proc. Pacific Symp. Biocomputing, vol. 5, pp. 538-549, 2000.

[7]. C. Friedman, P. Kra, H. Yu, M. Krauthammer, and A. Rzhetsky, "GENIES: A Natural Language Processing System for the Extraction of Molecular Pathways from Journal Articles," Bioinformatics, vol. 17, pp. S74-S82, 2001.

[8]. J. Pustejovsky, J. Castan` o, J. Zhang, M. Kotecki, and B. Cochran, "Robust Relational Parsing over Biomedical Literature: Extracting Inhibit Relations," Proc. Pacific Symp. Biocomputing, vol. 7, pp. 362- 373, 2002.

[9]. T.C. Rindflesch, L. Tanabe, J.N. Weinstein, and L. Hunter, "EDGAR: Extraction of Drugs, Genes, and Relations from the Biomedical Literature," Proc. Pacific Symp. Biocomputing, vol. 5, pp. 514-525, 2000.

[10]. J. Li, Z. Zhang, X. Li, and H. Chen, "Kernel-Based Learning for Biomedical Relation Extraction," J. Am. Soc. Information Science and Technology, vol. 59, no. 5, pp. 756-769, 2008.



CHAOTIC IMAGE ENCRYPTION USING-RC5

DHANYA B.NAIR & RUKSANA MAIDEEN

Dept of Electronics & Communication Engg, Ilahia College of Engineering and Technology
Muvattupuzha, Kerala, India

Abstract:-In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption techniques. Many methods have been developed to perform image encryption. The use of chaotic map for image encryption is very effective, since it increase the security, due to its random behavior. The highly unpredictable and random-like nature of chaotic signals is the most attractive feature of deterministic chaotic systems that may lead to novel (engineering) applications. This paper introduces a new cascaded structure of chaotic encryption scheme with RC-5 algorithm. In this paper 'Triple key' is used to encrypt and decrypt the data. Three different parameters which are decided by user are used to scramble the image data and so hackers get many difficulties to hack the data hence providing more security. Cascading RC-5 with triple key chaotic image encryption increases the security and the histogram can be made more uniform. For simulation MATLAB software is used. The experimental results shows that algorithm successfully perform the cryptography and highly sensitive to the small changes in key parameters.

Keywords— image encryption; chaotic neural network; chaotic logistic map; RC5.

I. INTRODUCTION

Recently, with the great demand in digital signal transmission and the big losses from illegal data access, data security has become a critical and imperative issue in the multimedia data transmission applications. In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption techniques. The data encryption techniques make the images invisible to undesirable readers and can be applied to protect the frames in the digital versatile disk (DVD) and the cable TV. Cryptography is exchanging the information between the related persons without leakage of information by unauthorized one. For this secure transmission or communication, data is encrypted at transmitter and decrypted at receiver. The encryption is obtained by scrambling the phase spectrum of original one, reverse process is used for decryption. If the same key is used at both for encryption and decryption then it is called as secret or symmetric cryptography and if different key is used then called public cryptography. In the 'Triple Key Image Encryption' [1], both position permutation and value transformation is performed. It has the potential of high data security. Here we are using three keys for encryption and decryption. In the proposed method we are combining this triple key method with RC-5 algorithm to increase the security, without affecting the quality of encryption. So in the proposed method we have four keys: three of chaotic method and one of the RC-5. Since the number of keys is increased the security also increases.

The features that make chaotic logistic maps and RC5 desirable for image encryption have been described in the following section. Then, the algorithm of the "Chaotic Image Encryption using RC5" is elaborated.

The observations and results of this image encryption method are provided next.

II. FEATURES OF CHAOTIC LOGISTIC MAPS

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems that are highly sensitive to initial conditions that is similar to random behavior, and continuous system. The properties of chaotic systems are [2]: (i) Deterministic, this means that they have some determining mathematical equations ruling their behavior. (ii) Unpredictable and non-linear, this means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes. (iii) Appear to be random and disorderly but in actual fact they are not. Beneath the random behavior there is a sense of order and pattern.

A simple 1D map that exhibits complicated behavior is the logistic map $[0,1] \rightarrow [0,1]$, parameterized by μ :

$$X_i = \mu * X_{i-1} (1 - X_{i-1})$$

In the logistic map, as μ is varied from 0 to 4, a period doubling bifurcation occurs. In the region $\mu \in [0, 3]$, the map possesses one stable fixed point. As μ is increased past 3, the stable fixed point becomes unstable and two new stable periodic points of period 2 are created. As μ is further increased, these stable periodic points in turn become unstable and each spawns two new stable periodic points of period 4.

Thus the period of the stable periodic points is doubled at each bifurcation point. Moreover, at a finite μ , the period doubling episode converges to an infinite number of period doublings at which point chaos is observed. This is depicted in the bifurcation

diagram in Fig. 1. The extreme amount of confusion can be seen to pervade at the end of the spectrum.

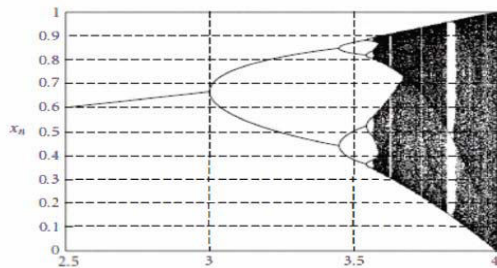


Figure 1. Bifurcation diagram of one-dimensional logistic map

III. FEATURES OF RC5

The RC5 encryption algorithm [3] is a block cipher that converts input data blocks of 16, 32, and 64 bits into cipher text blocks of the same length [8-10]. It uses a key of selectable length b (0, 1, 2, ..., 255) byte. The algorithm is organized as a set of iterations called rounds r that takes values in the range (0, 1, 2, ..., 255)

An expanded key array is created out from the original key by means of a key schedule. The expanded key array is used with both encryption/decryption routines and its length is dependent on the number of rounds. The operations performed on the data blocks include bitwise exclusive-OR of words, data-dependent rotations by means of circular left and right rotations and two's complement addition/subtraction of words, which is modulo- $2w$ addition/subtraction, where w is the word size in bits. They always affect a complete 16, 32 or 64-bit data block at a time. There are two inputs to the encryption function, which are the image to be encrypted and the expanded secret key.

For RC5 image encryption, the image header is extracted from the image to be encrypted and the image data stream is divided into blocks of 64-bit length. The first 64-bit block of image is entered as the plain image to the encryption function of RC5. The second input the RC5 encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by the key schedule. Then, the next 64-bit plain image block follows it, and so on.

In the decryption process, the encrypted image (cipher image) is also divided into 64-bit blocks. The 64-bit cipher image is entered to RC5 decryption algorithm and the same expanded secret key is used to decrypt the cipher image but the expanded secret key is applied in a reverse manner. Then the next 64-bit cipher image block follows it, and so on

IV. ALGORITHM

A. Forming Binary Image

1. Read the input image which is to be encrypted and convert it into binary image matrix d_{ij} .

B. Generate the Chaotic Sequence

2. The session key K consisting of 20 hexadecimal characters viz. 0 to 9 and A to F is entered.

$$K = k_1 k_2 \dots k_{20}$$

3. Each hexadecimal character in the session key is converted into binary equivalent of four bits so that session key consists of 80 bits.

$$\text{Let } k_1 = k_{11} k_{12} k_{13} k_{14}, \quad k_2 = k_{21} k_{22} k_{23} k_{24} \dots, \\ k_{20} = k_{201} k_{202} k_{203} k_{204}$$

4. The bits are extracted from the session key to create intermediate keys $X01$ and $X02$

$$X(1) = (X 01 + X 02 + X 03) \bmod 1.$$

$$\text{Where, } X 01 = (k_{11} * 2^0 + \dots + k_{204} * 2^{79}) / 2^{80}$$

$$X 02 = (k_{11} + k_{21} + \dots + k_{20}) / (16 * 20)$$

$$X 03 = \text{user entry key.}$$

5. Enter control parameter μ .

6. Generate the chaotic sequence

$$X(n + 1) = \mu X(n) (1 - X(n))$$

The values of the chaotic sequence are normalized and are converted into binary matrix B . The number of elements in the chaotic sequence is equal to the number of pixels in the image. B is used to compute the weights and biases of the chaotic neural Network.

C. Construction of Neural Network

Using the elements in B (b_{ij}), the weight matrix (W) and bias matrix (θ) are found out

$$W_{ij} = 0 \quad ; \quad \text{for } i \neq j$$

And for $i = j$

$$W_{ij} = -1 \quad ; \quad \text{if } b_{ij} = 1$$

$$\theta = 1/2 \quad ; \quad \text{if } b_{ij} = 0$$

$$\theta = -1/2 \quad ; \quad \text{if } b_{ij} = 1$$

$$d_{ij}' = \text{sign} (\sum W_{ij} * d_{ij} + \theta)$$

$$\text{sign} (x) = 1 \quad ; \quad x \geq 0 \quad \& \quad \text{sign} (x) = 0 \quad ; \quad x < 0$$

Each row of d_{ij}' is converted to its corresponding decimal value. Now, d_{ij}' contains values ranging from 0 to 255. The one-dimensional array is converted to a three dimensional array which belongs to the chaotic encrypted image.

C. RC5 Algorithm

7. Enter the RC5 key and create an expanded key array.

8. Do RC5 Encryption, to create the final encrypted image.

D. Decryption

Decryption procedure is same as the encryption procedure, but takes place only when the RC5 key session key, initial parameter key and control parameter key are correctly entered.

V. ANALYSIS

Simulation was done using MATLAB to explore the efficiency of this image encryption method. The results presented here contain both simulation diagrams and mathematical results. Simulation diagrams provide a physical feel of the encryption method, while the mathematical results provide statistical data. Simulation diagrams include 1) Encrypted Image Analysis 2) Histogram Analysis. Mathematical results are depicted using two new parameters: Correlation Index and Quality of Encryption.

From the encrypted image and histogram analysis as shown in Fig.2, it is clear that it is impossible to map encrypted image to the original image. Also the histogram of the encrypted image is more uniform compared to the input, showing better encryption. Correlation is a measure of the similarity that exists between two adjacent pixels in an image.

$$Cr = \frac{N \sum_{j=1}^N (x_j * y_j) - \sum_{j=1}^N x_j * \sum_{j=1}^N y_j}{\sqrt{(N \sum_{j=1}^N x_j^2 - (\sum_{j=1}^N x_j)^2) * (N \sum_{j=1}^N y_j^2 - (\sum_{j=1}^N y_j)^2)}}$$

CI refers to the correlation index, Ch the correlation between horizontally adjacent pixels and Cv the correlation between vertically adjacent pixels.

$$CI = Ch + Cv / 2$$

The correlation coefficient of encrypted image is very less compared to input image and is shown in Table 1. The quality of encryption is determined from the following equation Higher the value of QoE better will be the encryption.

$$QoE = (1 - CI) * 100\%$$

VI. CONCLUSION

In this paper, we have presented a new method of image encryption by cascading triple key method with RC5. Here the system strength increases by including more secret keys and by maintaining good quality of encryption. We can conclude that proposed system is very effective, as good security is achieved between two parties in case of secret communication.

VII. REFERENCES

- [1]. "Triple Key Method of Image Encryption": Srividya.G, Nandakumar.P IEEE Transactions On Circuits And Systems- I:
- [2]. Salleh. M., S. Ibrahim and I. F. Isnin. 2002. "Ciphing Key Of Chaos Image Encryption" Proceeding of International Conference on AI and Engineering Technology.
- [3]. "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems". International Journal of Information Technology Volume 3 Number 4.

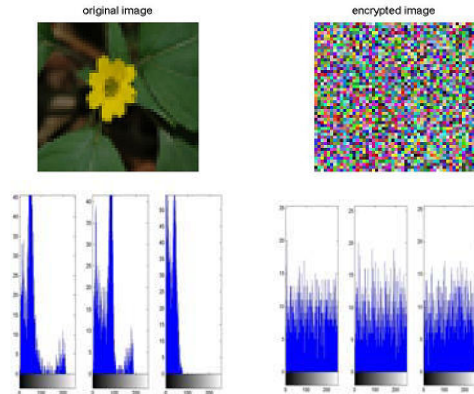


Figure2. Encrypted Image Analysis and Histogram Analysis

Table 1. Sensitivity to Keys

Sl No:	Keys		CII	CIO	QoE (%)
1	Session key	ABCDEF12345	0.5512	0.0285	97.1
	Initial parameter key	3.5			
	Control parameter key	3.9			
	RC5 key	12345			
2	Session key	1AB23C4B5CB6C7	0.5512	0.0556	94.4
	Initial parameter key	2.9			
	Control parameter key	3.81			
	RC5 key	ZXCVBNM			



DATA ENCRYPTION STANDARD USING MODDES ALGORITHM WITH COMPRESSION

WINNIE ELDBHOSE & MANJU RANI MATHEW

Dept of Electronics & Communication Engg, Ilahia College of Engineering and Technology, Muvattupuzha, Kerala, India

Abstract:-When data needs to be transmit securely an encryption standard is required. Different algorithm can be used for encryption and decryption of data. Encryption using MODDES algorithm uses two stacks for its operation. One having a set of operators and other with a set of delimiters. A lookup table is used for the selection of this stack elements using some mathematical logic. With MODDES algorithm the cipher text will be of larger length and it takes a larger encryption time. With the same plain text and same key we can produce different cipher text, therefore prone to replay attacks. In this paper a compression technique is introduced for compressing the text length . LZW compression is used for compressing the data which uses the MODDES Algorithm. We can compress the original text as well as the cipher text also, thereby achieving a larger compression ratio and security. When compression is used, the text length can be reduced, thereby increasing the encryption as well as decryption speed. With larger text length, more compression ratio can be achieved and data will be more secured also. This method is successfully tested on text files, image and audio files.

Keywords:-MODDES, delimiters, operators, LZW Compression, Compression ratio

I. INTRODUCTION.

Cryptography is an art of transforming information to make them more secure. To be secured, information which are going to transmit needs to be hidden from unauthorized access, should be protected from unauthorized change, and available to authorized entity when it is needed. With a suitable encryption standard we can make the data more secure. Most of standard encryption algorithm will produce same cipher text, when encrypted by same key on same plain text and it will be fully dependent on the encryption key. So there will be chance for replay attacks. In most of the algorithms, iteration of the key value is required and depending on the key value the message is deciphered [1].

Encryption using MODDES algorithm uses two stacks for its operation. MODDES-Multi Operator Delimiter based Data Encryption standard. This algorithm uses operator stack and delimiter stack. Different combination of operators and delimiters and can be used for its operation. These stack elements are selected using a look up table concept. To be more secured MODDES Algorithm is extended to include transposition, substitution and Binary operation to get X-MODDES(eXtended MODDES) [1].

When MODDES algorithm is used for encryption, the cipher text will be of larger length. So the transmission bit rate will be larger and will take longer time for its encryption as well as decryption. In the proposed model a compression technique is introduced for the original message as well as the cipher text. With this double compression the text length as well as cipher length are compressed considerably and encryption as well as decryption speed can be increased. So the transmission bit rate also get reduced. The rest of the paper is structured as

follows. An introduction MODDES Algorithm is discussed in Section II. Section III deals with the Proposed model. Detailed description of LZW Compression is discussed in Section IV. Experimental results of text, image as well as audio files are given in the Section V. Finally Section VI deals with conclusion.

II. MODDES ALGORITHM

Computational steps like Transposition, Substitution and Binary Operation can be include before MODDES algorithm to be more secured.

Encryption Procedure using MODDES

- i) After the transposition, substitution and binary operation, read a character from the text file corresponding to a text, audio or image to be encrypted.
- ii) Product of random number and key sum is done and with this mod value is taken to get the look up indices.
- iii) Look-up values is be selected and corresponding stack elements can be selected for stack operation.
- iv) From the operator stack, each operator is taken and operation is performed same with delimiter stack also.
- v) Continue steps(i) to (iv) until end of file is reached.

Decryption Procedure of MODDES

- i) Key is verified and character before delimiter is noted and ASCII is calculated.

- ii) From the cipher, look-up index is noted and with this, corresponding stack element can be selected.
- iii) Reverse mathematical operation is performed here. And repeat all the steps till end.
- iv) Plain text received at the end is converted back to respective audio or image or text files using softwares like MATLAB 7.5.

III. PROPOSED MODEL.

Encryption: The plain text , image or audio files which needs to be transmit is first compressed using LZW compression. This compressed file, then goes for a transposition operation. Transposed output will undergo for a substitution operation. Then comes the binary operation. After binary operation, the file is encrypted using MODDES algorithm. The algorithm output is then again compressed to get a larger compression ratio. Finally obtained output is the cipher text which needs to be transmit to the receiver side for decryption.

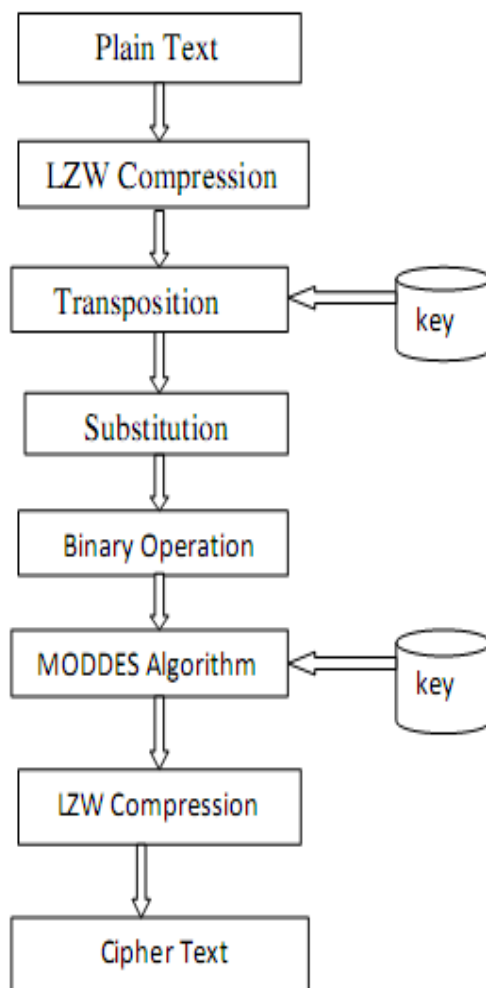


Figure 1. Block diagram for the encryption of proposed model.

The Plain text which is used for transmission has to be undergone compression first. Compression used here is LZW (Lempel-Ziv-Welch) compression. LZW compression is a lossless data compression and it does not require any advance knowledge of the input. As it is a lossless compression , data can be recovered back in the decryption side. The compressed output then undergoes a transposition operation. Transposition method used here is Key Based Random Permutation (KBRP). This permutation is based on the key which we used for encryption. Here we are considering all the elements in the key for this permutation. The process involves three steps [3]. Init(), Eliminate(), Fill() Init(): This step involves the initialization of the permutation array. Array length is of the size of text length which we are used for encryption. First the array is filled with all ASCII values of the elements in the key. Then need to fill the remaining part of the array by adding ASCII value of two consecutive elements of the array. If N is the length of the array, set the elements of the array with values in the range from 1 to N by taking the mode operation on each element of the array. Eliminate (): Second step involved in the permutation is the elimination process. After taking the mode operation in the first step, there will be some repeated values in the array. Repeated values are replaced with zeros.

Fill(): In this step, zero values in the array are replaced by nonzero values which are not present in that array. Now array will contain nonzero and distinct values in the range from 1 to N. Based on this permutation , units in the plain text can be arranged and thus transposition is achieved. The Transposed output file then undergoes substitution operation. In substitution operation the units of plain text are replaced with cipher text according to regular pattern. Replacement can be done by a left shift or right shift or by any other operation also. In this paper substitution is done by shifting letters three position left.

The substituted output then undergoes binary operation. Output of binary operation is given to MODDES Algorithm, where mathematical operation is performed with stack elements. After encrypted with MODDES Algorithm, the result is again compressed using LZW Compression, resulting is the cipher text which is sent to receiver side. Decryption: In the decryption, the inverse operation of encryption is performed. The cipher text obtained at the receiver side needs to decompress first. After decompressing, the output file needs to pass through MODDES Decryption Algorithm. Then Reverse Binary, Substitution and Transposition operation needs to take place. Again the transposed output needs to be decompressed for getting the original message which has transmitted.

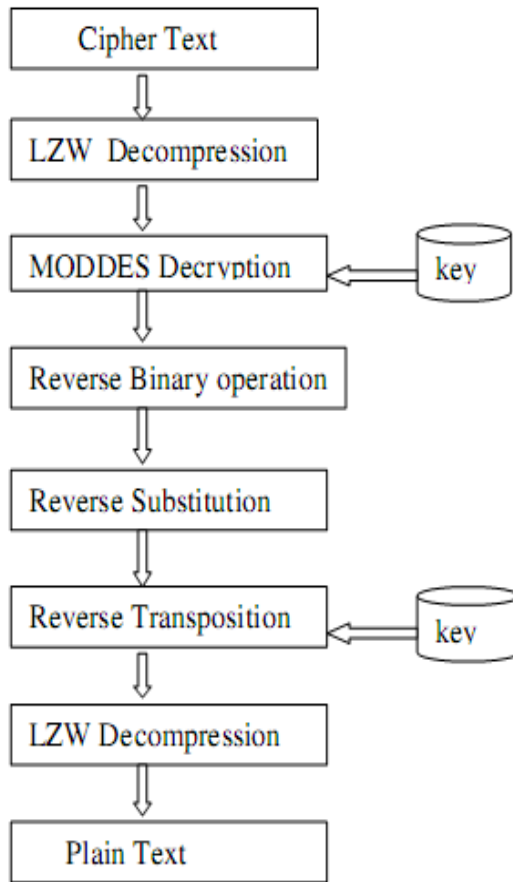


Figure 2. .Block diagram for the decryption of proposed model.

IV. DESCRIPTION OF LZW COMPRESSION.

Unlike other coding schemes LZW (Lempel-Ziv-Welch) do not require prior knowledge of the input used for compression. LZW can compress the input in a single pass. Being a lossless compression, the information which is compressed can be retrieved back during decryption. LZW has faster execution than other compression. LZW can compress repetitive sequence of data. When text length is larger, a larger compression ratio can be achieved. With the compression we can reduce the text length which is being transmitted and execution speed can be increased.

LZW Encoding

LZW compression uses a dictionary or a code table for its operation. Initially code table has entries from 0 to 255. So when encoding starts, code table will contain only these 256 entries. As encoding begins LZW will check for the repeated sequence in the message. It will take consecutive two character and check if it is present in the code table. If it is not present in the code table it will be added to the code table. Otherwise next characters are added and again check for its presence.

Algorithm steps is as follows

Initialize the code table with 256 entries

Let X be the first input character.

While not end of file

Let Y be the next input character.

If X+Y is in the code table

$X=X+Y$

Else

Output the code for X

X+Y is added to the code table

X=Y

End while

Output the code for X.

LZW Decoding

Code table which is created in the encoder is not transmitted to decoder. The code table is created in the decoder. Initially code table is initialized to have 256 entries. Except for the first one, for each and every time the string table is updated.

Algorithm steps is as follows

Initialize the code table with 256 entries.

Let X be the first input code.

Display the output translation for X

While not end of file

Let Y be the next input bit

If Y is not in the string table

S=Translation of X

S=S+N

Else

S= translation of Y

Output S

Let Y be the first character of S

X+N is added to string table

X=Y

End while

V. RESULTS

With the LZW compression , a compression ratio in the range from 80%-90% can achieved for larger text length. Compression Ratio is calculated by using (1).

$$\text{Compression ratio} = \frac{\text{text length after compression}}{\text{text length before compression}} * 100 \quad (1)$$

When greater compression ratio is attained, the encryption speed also increases. In Figure 3. We can see algorithm and compression applied for plain message. Time taken for encryption of this plain text is very much reduced. In Figure 4,algorithm and compression is applied to image file. In Figure 5,result obtained after compressing and encrypting the audio file can be seen. There also encryption speed is increased.

MODDES algorithm is a unique independent approach which uses several computational steps along with string of operators.

Plain text

~pU@(* @#0&P@P*%@(*@#)AS(^(A P@P* %0@ #0&A@(* -AS(^(A OpUX@P*@((* @P* @ (* OpU D@P* Ix&^H# @(* %0@ #0& 0@ (* @@ (* u&^# # 8@P* =%U Ç@U p@(*&^# =% @0&@# #0& &^H# %@ (* +&^H# ΔS(^(A @ S(^(A ^@ (* V0& 0@ #0&8&^H# I@Uh@ #X&^@ #0& I&^&

Output of Algorithm

~pU @(* @#0&P@P@)AS(^(A X (%@jUMA^m#Z^q^H %@#xÇ@ P@P<# p#u5V@#@e%h82G2

Output of LZW compression

MODDES algorithm is a unique independent approach which uses several computational steps along with string of operators.

Plain text

Figure 3.Data encryption standard for Plain text




Image file

S@-#&S@-#*@#N&3Z&^*#&%SS&^S@-#8^S@-#)0S-%6^È&%SSB@#N&zS @-%ç2@#N&1&%S ΔS@-#1&^*# SS@<#x'&%SS [S-%^+S@-#eXS-%6^ S@-#S-%^uS-%^uS-%6^94^@#0&0^@#0&&%SSÖD&^#;&#-h&%SS00@#0 &@4&%BSS00@#0&j&^*#0@#0&hS-%6^h^@#0&ZÆ@#iz&^*#E^S-%T^Vü&%BSS-%6^ eS@-#Ú&^*#b(S-%6^

Output of Algorithm

-yex' [_ÉDÓ ñBCH)RP)#IT, é-Á é-
%À\;Ód±o0È#^1W^N×01;:h+ÜLJ6-Ö

Output of LZW Compression

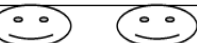


Image file

Figure 4 .Data encryption standard for image file.

135 135 134 132 130 126 123 123 121 120 119 119 122 123 123
123 124 123 124 123 123 128 128 132 134 136 140 138 136 133
130 130

Plain Text

3È&%SS&%SSr0@#0V@#&l&%BS:S@-#3* &^#IS-%6^Fü&^#uS-%6^
H&%SS(0&^H#|^S@-#00@#&S-%6^0&&%BSS-%6^YAS3È&%SS&%SSr0@
#AS-%^S-%6@-# O&^# ÖS@<# qAS@

Output of Algorithm

ÄMøYü/8/p#A9p -3 äFu' w_]éanâ [è"kkÇ2\$L uOp%4éÄ;1ç/4

Output of LZW Compression

135 135 134 132 130 126 123 123 121 120 119 119 122 123 123
123 124 123 124 123 123 128 128 132 134 136 140 138 136 133
130 130

Plain Text

Figure 5.Data encryption standard for Audio file

VI. CONCLUSION.

In this paper we have introduced a new encryption standard. By compressing the text as well as the cipher, a larger compression ratio has achieved and encryption speed also got increased. More than that the encryption became more complex. With same plain text and key, algorithm produce different cipher text and hence security is assured.

REFERENCES.

- [1] eXtended Multi Operator Delimiter based Data Encryption Standard(X-MODDES) 2010 Second International Conference on Future Networks.
- [2] Multi Operator Delimiter based Data Encryption Standard (MODDES) ICCNT 2009. [3] Key Based Random Permutation(KBRP) ISSN 1549-3636 2006 Science Publication.
- [4] W.Stallings “Cryptography and Network Security Principles and Practices”,Fourth edition,Prentice hall,2007



ENHANCED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON TRIGONOMETRIC FUNCTIONS

M.K MOHSINA & ROBIN ABRAHAM

Department of P.G, Applied Electronics, ICET, Mulavoor.

Abstract:- The advent of wireless communications, both inside and outside the home-office environment has led to an increased demand for effective encryption systems. The encryption of images is quite different from that of the texts due to the bulk data capacity and high redundancy of images. Traditional methods are difficult to handle the image encryption because of their small space of pseudo random sequence. At present, the chaotic maps have been widely used in image encryption for their extreme sensitivity to tiny changes of initial conditions. The chaos based algorithms have suggested a new and efficient way to deal with the problem of fast and highly secure image encryption. In this paper, we propose an algorithm in which two one-dimensional chaotic maps are used instead of a one-dimensional chaotic map. We also use an external secret key of 96-bits. Thereby it significantly increases the resistance to statistical and differential attacks. The results of experiment, statistical analysis, correlation coefficient analysis and key sensitivity tests show that the algorithm is of great security and practicability.

Keywords:- *Chaos; Pseudo Random Sequence; Chaotic Map; Trigonometric Function; Image Encryption*

I. INTRODUCTION

The amazing developments in the field of network communications during the past years have created a great requirement for secure image transmission over the Internet. Internet is a public network and is not so secure for the transmission of confidential images. To meet this challenge, cryptographic techniques need to be applied. Cryptography is the science of protecting the privacy of information during communication, under hostile conditions. In recent days, Chaos based methods are used for image Encryption. Chaos word has been derived from the Greek, which refers to unpredictability and it is defined as a study of nonlinear dynamic system. Chaos theory is a mathematical physics which was developed by Edward Lopez. Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics. The combination of chaotic theory and cryptography forms an important field of information security. In the past decade, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic maps have been proposed. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods.

Based on chaos functions, a variety of image encryption algorithms have been proposed during the past decade. In [3], a chaotic key-based algorithm (CKBA) was proposed for image encryption /decryption. The algorithm first generates a chaotic sequence by the 1-D chaos map (the logistic map), and then uses it to create two keys--two binary sequences. According to the binary sequence generated above, four operations were selected to shuffle the image pixels. They are the combination of

the image pixels XOR or XNOR operation with the selected key. This method is simple but exist obvious defects in security. The defects of CKBA were pointed out in [4]: the method is very vulnerable to the chosen/known-plain-text attack with only one plain-image, and its security to brute-force cipher-text-only attack is questionable. In [5], an enhanced CKBA algorithm was proposed. The enhanced CKBA replaces the 1-D chaotic Logistic map with the piece wise linear chaotic map (PWLCM) so as to improve the balance property. It also increases the key size to 128 bits, adds two more cryptographic primitives and extends the scheme to operate on multiple rounds so that the chosen/known-plain-text attacks are no longer possible. In [7], to overcome the drawbacks of small key space and weak security in the widely used one-dimensional Logistic systems, this paper presented a new nonlinear chaotic algorithm that uses power function and tangent function instead of linear function. In [8] an algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data is introduced. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algorithm is tested with two different maps and performance analysis is done to select best suited map for encryption.

In this paper, a new image encryption algorithm based on two different chaotic maps is proposed. In the proposed algorithm, the plain-image is first encrypted by using a chaotic trigonometric function and then the shuffling of image pixels is carried out using another trigonometric function. The rest of this paper is organized as follows. In section II, a new algorithm is suggested for fast and secure image encryption based on the trigonometric functions. Section III provides a large quantity of experiment

data and makes performance analysis to the algorithm.

II. PROPOSED ENCRYPTION ALGORITHM

In this section, an algorithm based on the trigonometric function is introduced. We'll use the following trigonometric function (TF) as chaotic map for encrypting the plain image.

$$y = \frac{1}{2}(\sin(4\pi x) + 1) \quad (1)$$

After encrypting the plain image, the following sine map is used to shuffle the image pixels.

$$X_{n+1} = 0.99 \sin(\pi X_n) \quad (2)$$

A. ENCRYPTION ALGORITHM

Assume that we'll encrypt a 24 bit color image fp (plain image). The image size is [M,N,Z]. The encryption steps are as follows Step 5. Shuffle fpm according to the perturb rule sets fl.

Step 5.1 Transform the rows of fpm.

Step 1. Randomly generate a 96-bit long binary sequence and change it into 12 ASCII codes. The K is our secrecy Key.

$$K = K1K2K3 \dots K12(\text{ASCII})$$

Step 2. Generate the initial value x0, l0 of formula (1) and z0 of formula (1) according to K. Get K1K2...K6, K7K8...K12 then calculate x0 and l0 according to formulas (3), (4)

$$X0 = (K1 * 2^{40} + K2 * 2^{32} + K3 * 2^{24} + K4 * 2^{16} + K5 * 2^8 + K6) / 2^{48} \quad (3)$$

$$l0 = (K7 * 2^{40} + K8 * 2^{32} + K9 * 2^{24} + K10 * 2^{16} + K11 * 2^8 + K12) / 2^{48} \quad (4)$$

Calculate z0 according to formula (6)

$$R = \sum_{i=1}^{12} K_i / 256 \quad (5)$$

$$z0 = R - \text{floor}(R) \quad (6)$$

Step 3. Generate the chaos mask fm and perturb rule sets fl.

Step 3.1 Generate fm. Use x0 as the initial value, and iterate the trigonometric function (1) 150 times so as to make the chaos system steady, then use the output as the initial value, continue iterating the trigonometric function (1) M*N*Z times, store M*N*Z output values in fm.

Step 3.2 Generate fl. Use l0 as the initial value, and iterate the trigonometric function (1) 150 times so as to make the chaos system steady, then use the output as the initial value, continue iterating the trigonometric function (1) 2*(M+N) times, store 2*(M+N) output values in fl.

Step 4. Generate fpm.

$$fpm = fp \oplus fm$$

There are 2*(M+N) values in fl. We divide them into four parts fl1, fl2, fl3 and fl4.

$$fl1 = fl(1) \dots fl(M)$$

$$fl2 = fl(M+1) \dots fl(M+N)$$

$$fl3 = fl(M+N+1) \dots fl(2M+N)$$

$$fl4 = fl(2M+N+1) \dots fl(2(M+N))$$

The fl1 and fl3 are used to confuse the rows of fpm. The fl2 and fl4 are used to confuse the columns of fpm. According to table 1, we divide the region [0,1] into 10 groups. Each group has a specific operation for encryption/decryption. For example, we need to confuse the row r1. We first get the value fl(r1). If fl(r1)=0.176. We look it up in table 1 and find the group number is 8. The corresponding operation is nonequivalent.

Group number	The range that value belonged to	Corresponding operations for Encryption/decryption
1	[0.00,0.01) (0.10,0.11)... (0.90,0.91)	Right shift this row according to the value stored in fl
2	[0.01,0.02) (0.11,0.12)... (0.91,0.92)	Use the value stored in fl as the initial value of trigonometric function and get the same number of values(Xr,Xg,Xb) as the image size in a row. Then $R \oplus X_r, G \oplus X_g, B \oplus X_b$
3	[0.02,0.03) (0.12,0.13)... (0.92,0.93)	Left shift
4	[0.03,0.04) (0.13,0.14)... (0.93,0.94)	$R \oplus X_r, G \oplus X_g, B \oplus X_b$
5	[0.04,0.05) (0.14,0.15)... (0.94,0.95)	Right shift
6	[0.05,0.06) (0.15,0.16)... (0.95,0.96)	$R \oplus X_r, G \oplus X_g, B \oplus X_b$
7	[0.06,0.07) (0.16,0.17)... (0.96,0.97)	$\text{NOT}(R), \text{NOT}(G), \text{NOT}(B)$
8	[0.07,0.08) (0.17,0.18)... (0.97,0.98)	$R \oplus X_r, G \oplus X_g, B \oplus X_b$
9	[0.08,0.09) (0.18,0.19)... (0.98,0.99)	Left shift
10	[0.09,0.10) (0.19,0.20)... (0.99,1.00)	$R \oplus X_r, G \oplus X_g, B \oplus X_b$

Table 1: Table showing various operations for encryption and decryption

We get the value from fl(M+N+r1), and use it as the initial value to iterate the trigonometric function N*Z times and get N*Z values. Here Z is 3. We divide the N*Z value into 3 parts "X1, X2, X3" with the number N in each. Then get $X_r = X1 * 255, X_g = X2 * 255, X_b = X3 * 255$. At last, we do nonequivalent operation as follows. $R \oplus X_r, G \oplus X_g, B \oplus X_b$

Step 5.2 Transform the columns of fpm. The step is similar to step 5.1. In order to ease the operations, we can transpose the image array. Change the column operations to row operations and we get the encrypted image.

Step 6. Separate R,G, B matrix of the encrypted Image and convert each R,G,B matrix in to single array ($1 \times MN$).

Step 7. The Sine map in formula (2) is iterated for $n=1$ to $M \times N \times Z$ times to generate the required elements using the initial condition z_0 . Now divide the generated elements into three blocks of each equal to $M \times N$.

Step 8. Now sort the elements of each block in ascending or descending order and compare the misorder between the original and sorted elements of each block and tabulate the index change. We have got three series of index change values in according to three blocks.

Step 9. According to the obtained index, we change the intensity position to get the final encrypted image.

B. DECRYPTION PROCESS

The process of decryption is similar to the encryption. It is the inverse process of the encryption processing with the same key.

III. EXPERIMENTAL RESULTS AND

SECURITY ANALYSIS

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. To prove the robustness of the proposed image encryption procedure, we have performed statistical analysis, correlation coefficient analysis, security of key and key space analysis. If correlation coefficient is nearer to zero for an encrypted image, then algorithm is said to be better. To prove that decryption is possible only with one key, key sensitivity is calculated. In this section, we'll use the proposed algorithm to encrypt the image lena with size of $128 \times 128 \times 3$.

A. STATISTICAL ANALYSIS

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. Histogram is widely used to evaluate the statistic feature of an image. We use the secret key "AC1FB58E3907AD45AB1FB41C" to encrypt the image. Figure 1 shows the histograms. It is clear that the histograms of the encrypted image are fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image.

B. CORRELATION COEFFICIENT ANALYSIS

Correlation coefficient ' ' is the measure of extent and direction of linear combination of two random

variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related.

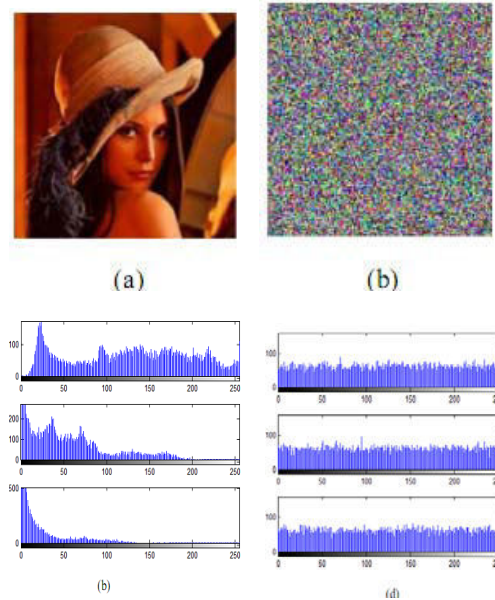


Figure 1. Histogram analysis: Frame (a) shows a plain-image. Frame (b) shows the encrypted image. Frames (c) and (d) shows the histograms of red, green and blue channels of the plain-image and cipher image respectively.

The coefficient can be calculated by the following formulas. Where x and y are gray values of two adjacent pixels in an encrypted image. We randomly select 1000 pairs of vertically and horizontally adjacent pixels and calculate the correlation coefficients in two directions separately. The correlation coefficients among adjacent pixels of plain-image in three directions come out to be 0.9120 and 0.8645 respectively. The values of correlation coefficients obtained in encrypted images are listed in Table 2. The values of correlation coefficients show that the two adjacent pixels in the plain-image are highly correlated to each other and correlation coefficients are almost 1 whereas the values of correlation coefficients in the encrypted images are close to 0, this means that the adjacent pixels in the encrypted images are highly uncorrelated to each other.

$$\gamma(x, y) = \frac{COV(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (7)$$

$$COV(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)] \quad (8)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \quad (9)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (10)$$

Direction	Plain -Image	Cipher -Image
Vertical	0.9120	-0.0271
Horizontal	0.8645	-0.0089

Table 2. Correlation Coefficients of Two Adjacent Pixels In The Plain-Image And Cipher-Image.

These data prove that the chaotic encryption algorithm leads to a more secured encryption process.

C. SECURITY OF KEY AND KEY SPACE

ANALYSIS

Figure 2 shows the cipher-image encrypted by 96-bit key “AC1FB58E3907AD45AB1FB41C”, the decrypted images by the correct key “AC1FB58E3907AD45AB1FB41C” and the wrong key “AC1FB58E3907AD45AB1FB41A”. Frame (c) shows that the image can be decrypted correctly by the correct key. Frame (d) shows that the image

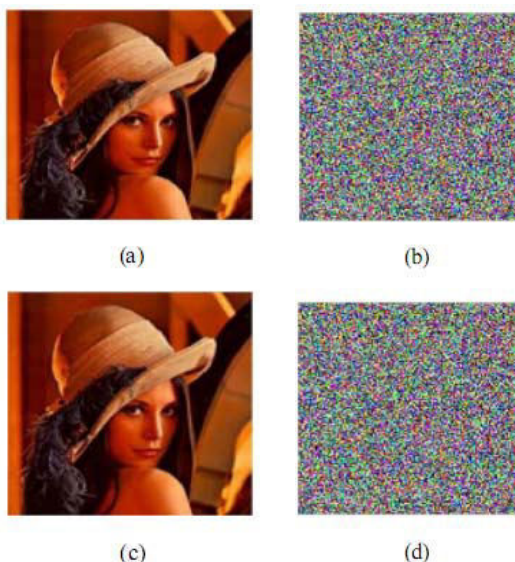


Figure 2 : Image encryption and decryption experiment result: Frame (a) plain-image, Frame (b) cipher-image encrypted by key “AC1FB58E3907AD45AB1FB41C”, Frame (c) image decrypted by correct key “AC1FB58E3907AD45AB1FB41C”, Frame (d) image decrypted by wrong key “AC1FB58E3907AD45AB1FB41A”

cannot be decrypted by the wrong key, and the decrypted image by the wrong key is of the same security feature to the cipher-image. We cannot get any useful information to attack from it.

IV. CONCLUSION

In this paper, a new way of image encryption scheme have been proposed which utilizes two chaotic maps and an external key of 96-bits. The initial conditions for both the maps are derived using the external

secret key. In the proposed encryption process, several different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the trigonometric chaotic map. To make the cipher more robust against any attack, the pixel position of the encrypted image is changed according to the randomness of the chaotic elements, which is derived by comparing sorted and unsorted chaotic elements generated from sine map. We have carried out statistical analysis, correlation coefficient analysis and key space analysis to demonstrate the security of he new image encryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

REFERENCES

- [1] R. Matthews, “On the derivation of a chaotic encryption algorithm,” *Cryptologia*, 1989, 8(1):29-41.
- [6] T. Uehara, R. Safavi-Naini and P. Ogunbona, “Securing wavelet compression with random permutations,” In: *IEEE Pacific Rim Conference on Multimedia*, 2000, p. 332-5.
- [7] H.J. Gao, Y.S. Zhang, S.Y. Liang and D.Q. Li, “A new chaotic algorithm for image encryption,” Published by Elsevier Ltd, 2005.
- [8] “Chaos Image Encryption using Pixel shuffling” Manjunath Prasad and K.L.Sudha, DSCE, Bangalore,



CHAOS-BASED COMPRESSION AND ENCRYPTION SCHEME USING ARTIFICIAL NEURAL NETWORK

GEETHI V & CHAITHANYA G NAIR

Dept of Electronics & Communication Engg. Ilahia College of Engineering and Technology Muvattupuzha, Kerala, India

Abstract:- An algorithm for improving the security of an existing chaos-based compression and encryption scheme is proposed. The basic idea is to encrypt each character of the message as the integer number of iteration performed in the logistic equation. The lookup table used for encryption is determined adaptively by the probability of occurrence of plaintext symbols. The lookup table used for encryption is dynamically updated in the searching process. Then expansion of the cipher text is avoided, and the compression ratio is improved. In this paper, the chaotic mask used for encryption is generated by using an artificial neural network. As a result, the complexity is increased in mask mode encryption and the overall security of the system is improved.

Keywords:- Chaos, compression, cryptography, chaotic neural network.

I. INTRODUCTION

IN RECENT years, the size of multimedia files as well as the need for the secure transmission of confidential data over public networks keep rising. The efficiency and security requirements of information transmission lead to a substantial amount of research work in data compression and encryption. In order to improve the performance and the flexibility of multimedia applications, it is worthwhile to perform compression and encryption in a single process [3],[5]. The approach based on multiple Huffman tables simultaneously performs encryption and compression by a key-controlled swapping of the left and right branches of the Huffman tree.

In recent years, there is an increasing trend of designing ciphers based on chaos. This is because chaotic systems are sensitive to the initial condition and the system parameters. These properties are desirable in cryptography. Moreover, the knowledge on chaos and nonlinear dynamics can be applied in the field of cryptography. A chaos-based cipher designed by Baptista [2] searches the plaintext symbol in the lookup table using a key-dependent chaotic trajectory and treats the number of iterations on the chaotic map as the ciphertext. However, it suffers from the problem of ciphertext expansion. In the existing scheme [5], for improving the compression Performance, the lookup table used for encryption is dynamically updated in the searching process, so that encryption process has two modes- search mode and mask mode. As a result, the number of iterations required for encryption is reduced. The ciphertext is shortened, and a better compression performance is achieved. In this scheme, an algorithm for improving the security of an existing chaos-based compression and encryption scheme [5] is introduced. The mask used for encryption [3] is

generated using artificial neural network (ANN). ANN gives a complex relationship between input and output. Thus the mask become more complex and an intruder cannot easily attack the system. Thus the security is improved.

II. FEATURES OF ARTIFICIAL NEURAL NETWORK

In the existing scheme, the encryption process includes search mode and mask mode. The mask used for encryption is a stream cipher that masks the plaintext by a pseudorandom bitstream. Mask is generated by iterating the chaotic function,

$$x_{n+1} = b x_n(1 - x_n),$$

where $x_n \in [0, 1]$ is the output at discrete time $n = 0, 1, 2, \dots$. The control parameter b should be a real number between 3.6 and 4 for generating chaotic output sequences. Its security is determined by the randomness of the occurrence of the numbers or bits in the mask stream [3]. An Artificial neural network is a mathematical model used to form a complex relationship between its input and output. By using an artificial neural network to form the mask, the mask become more complex and it cannot easily attack by an intruder. As a result, the overall security of the system is improved.

The output of the ANN (mask) is given by the equation,

$$\text{Out_seq.} = \text{sign}(\sum(W_{ij} * \text{Inp_seq.}) * \theta_j)$$

Here the input sequence is a Henon map sequence so that Henon map sequence is a chaotic sequence.

III. ALGORITHM

A. Determination of probability of occurrence of each symbol in the message.

Scan the whole plaintext sequence once to find out the number of occurrence for each possible plaintext symbol. Then, sort them in descending order and select the top M symbols, S1, S2, S3....SM.

B. Construction of look-up table

Divide the phase space of the chaotic map into N equal-width partitions, with $N > M$. Starting from $j=1$, map the selected plaintext symbols to the N partitions according to the below equation, until all the partitions are mapped

$$n(s_j) = \left\lfloor \frac{N * u(s_j)}{\sum_{i=1}^M u(s_i)} \right\rfloor + 1$$

Where $u(s_j)$ and $n(s_j)$ are, respectively, the number of occurrence and the number of partitions mapped to symbol s_j . The mapping should be random so that the partitions mapped to a particular symbol spread over the whole phase space of the chaotic map. In general, the selection of the partitions for mapping can be determined by iterating a chaotic map and record the partitions that the chaotic trajectory falls in. Since the number of partitions mapped to a plaintext symbol must be an integer, the truncated value is taken in the equation and then added by 1. As a result, there may be the case that all the partitions are mapped and nothing is left for the last few probable plaintext symbols. However this is not a matter as the more probable symbols should have higher priorities. \

C. Encryption with compression

1. Search mode Encryption

Encrypt each plaintext symbol sequentially. First of all, check whether the plaintext symbol in concern is one of the M selected symbols. If this is the case, sequentially encrypt each symbol in the plaintext by searching in the lookup table using a secret chaotic trajectory. If the symbol being encrypted is found, the number of iterations of the chaotic map is considered as the cipher text. Otherwise, the lookup table will be updated using a new process based on the model of sampling without replacement. If the partition just visited maps to a non target symbol, all the partitions associated with that symbol need to be reassigned to another symbol. With the considerations of compression ratio and simplicity of the encryption process, those partitions are assigned to the non visited symbol with the highest probability. However, it should be noticed that the partitions can be randomly assigned to other symbols to increase the

difficulty of attack. In the next iteration, the chaotic trajectory continues to search the target symbol in the updated lookup table until the symbol is found. When the current plaintext symbol has been encrypted, the lookup table is initialized again according to the symbols' probabilities of occurrence. After that, the next symbol is encrypted using the same procedures. If the selected plain text symbol is not present in the M selected symbols, then it is padded with zero.

2. Compression using Huffman tree

After all the plaintext blocks have been processed, a Huffman tree is built for all the collected number of iterations, including zero. When the Huffman tree is built, the number of iterations and the special symbol are replaced by the corresponding variable-length Huffman code to form the intermediate sequence.

3. ANN Mask mode Encryption

The formed intermediate sequence is again encrypted by the mask mode. The mask is the output sequence of an artificial neural network. It is given by the equation,

$$\text{Out_seq.} = \text{sign}(\sum(W_{ij} * \text{Inp_seq.}) * \theta_j)$$

Here

$$\text{sign}(x) = 1; x \geq 0 \quad \& \quad \text{sign}(x) = 0; x < 0$$

1. Inp_seq. is a Henon map sequence and is given by the equation,

$$X_{n+1} = Y_n + 1 - P X_n^2,$$

$$Y_{n+1} = Q X_n; \text{ where } (X_n, Y_n) \in [-1, 1]$$

and

$$P=1.4, Q=0.3; \text{ for the chaotic behavior.}$$

2. Create a chaotic sequence by performing the equation,

$$x_{n+1} = b x_n(1 - x_n).$$

The values of the chaotic sequence are normalized and are converted into binary matrix C. The number of elements in the chaotic sequence is equal to the length of intermediate sequence. C is used to compute the weights and biases of the chaotic neural Network.

$$W_{ij} = 0; i \neq j$$

$$W_{ij} = 1 - 2C_{nj}; i = j \quad \text{and}$$

$$\theta_j = -1/2, C_{nj} = 0$$

$$\theta_i = 1/2, C_{ni} = 1$$

The resultant output sequence will be the mask. Then an XOR operation is done between mask and the intermediate sequence. The output will be the cipher text.

D. Decryption with Decompression

Before starting the decryption, the key and the plaintext specific information must be delivered to the receiver secretly. The secret key includes the parameters and the initial values of the chaotic map and Henon map. The plaintext-specific information includes the name and length of the plaintext file, the encryption mode, the probable plaintext symbols and their number of occurrence, and the Huffman tree. Iterate the chaotic map using the shared secret parameters and the initial conditions to regenerate the chaotic trajectory as used in encryption. Then, extract the mask bits. Unmask the cipher text to get the output sequence.

Scan the intermediate sequence sequentially. Decode the variable-length Huffman code using the shared Huffman tree to find out the number of iterations required. If the number is zero, this means that the block was encrypted in mask mode. No decoding operation is required and the block is copied directly as the output. Otherwise, iterate the chaotic map with the nonzero number of iterations and determine the final partition visited by the chaotic trajectory. The plaintext symbol is obtained from looking up the corresponding mapping table. It should be noticed that the mapping table should be cyclic shifted appropriately after decoding each plaintext block, so as to synchronize with the changes made in encryption. The same symbol replacement process needs to be performed so as to synchronize with the encryption part. Thus the original plaintext sequence is reconstructed.

IV. ANALYSIS

The proposed algorithm is implemented and simulation was done using MATLAB. In the logistic map the parameter b is set to be 3.8 and the initial condition is set to be 0.232323. The maximum number of iterations is chosen as 255. In the case of Henon map, the initial values of X_n and Y_n are set to be 0 and 0.9 respectively. The following results are obtained after simulation.

A. Key sensitivity

Very small change in the initial parameters of the logistic equation results large change in the cipher. A tiny change in the values of 'b' and 'X0' cause a considerable change in the values of the generated chaotic sequence. Then the cipher text is also changed.

B. Plane text sensitivity

To evaluate the plaintext sensitivity, a bit is changed at different positions of the plaintext sequence, which is then encrypted using the same key. The two resultant cipher text sequences are compared bitwise. A tiny change in the plane text affects cipher text block and the encryption process. This is because the lookup table is disturbed by the plane text.

C. Compression Ratio

In this scheme the lookup table is updated in the searching process. Then less number of iteration is

needed. Then the length of cipher text is also reduced. Compression Ratio = (cipher text length / plain text length) * 100. Thus the compression performance is increased by (10-17) %

V. CONCLUSION

The existing approach of embedding compression in the chaos-based cryptosystem suffers from some security problems. In this paper an ANN algorithm is introduced to increase complexity of the system. As a result the security of the overall system is improved by increasing the secret keys and also the quality is improved.

VI. REFERENCES

- [1] C. M. Ou, "Design of ciphers by simple chaotic functions," IEEE Comput. Intell. Mag., vol.3, no.2, pp.54-59, May 2008
- [2] M.S. Baptista, "Cryptography with chaos", Phys.Lett.A, vol.240,no.1/2,pp.50-54,Mar.1998
- [3] K.W. Wong and C.H. Yuen, "Embedding compression in chaos based cryptography", IEEE Trans. Circuits Syst.II,Exp.Briefs, vol.55,no.11,Nov 2008
- [4] H. Kim, J. Wen & J. Villasenor, "Secure arithmetic coding," IEEE Trans. Signal Process., vol. 55, no. 5, pp. 2263-2272, May 2007
- [5] Jianyong Chen, Junwei Zhou & Kwok-Wo-Wong, "A Modified chaos based joint compression and encryption scheme", IEEE Transactions on Circuits and systems-II: Express briefs, vol. 58, no. 2, February 2011



A SECURE SECRET KEY STEGANOGRAPHIC ALGORITHM THROUGH OPTIMIZATION OF PIXEL PAIR MATCHING

NAJEENA K.S & B. MOHAMMED IMRAN

Dept of Electronics & Communication Engg, Ilahia College of Engg & Technology
KERALA, INDIA

Abstract:- Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. Both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Presently we have very secure methods for both cryptography and Steganography – chaotic algorithm is a very secure technique for cryptography and the Steganography methods, which use spatial domain, are highly secured. The encrypted data is embedded in to the cover media based on pixel pair matching technique. Therefore, the idea of applying both of them together is presented with more security levels and got a very highly secured system for data hiding.

Keywords:- *APPM; chaotic system; public steganography; encryption; scrambling.*

I. INTRODUCTION

There are many techniques available for secure data transmission. Cryptography and steganography are two popular methods used for enhancing the security of network communication. Cryptography is a technique in which the secret data is scrambled into undetectable fashion so that it become impossible for any external person to decrypt the secret data. Steganography enhances the security of data transfer by hiding the image within another cover media having large size compared to stego image. Among the traditional encryption algorithms like AES, RSA cannot be used for real time image encryption as these algorithms require large computational time and computational overhead. Among them chaotic sequence based encryption algorithms provides high speed, complex system. Steganography exist in spatial domains and frequency domains where spatial domain techniques are used for data hiding applications that require high payload and invisibility. LSB substitution, optimum pixel adjustment process are the common techniques for data embedding which is mainly focused on LSB modification of cover pixels. Pixel pair matching is a good technique where the embedding unit is a pair of pixels. Exploiting modification direction EMD and diamond encoding DE algorithms embed each bit of secret information in to a pair of pixels of cover image. Instead of embedding the data directly the secret bit act as a parameter, which determines the new pixel pair by which the original pixel pair is to be replaced. By combining the data encryption technique with steganography enhances the security of data embedding. Eventhough the individual encryption and steganographic techniques are secure, the combined algorithm provide multiple stages of security.

II. RELATED WORK

Steganography allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected. Various digital steganographic techniques are implemented which are capable of producing a secret-embedded image that is indistinguishable from the original image to the human eye. In OPAP method the pixel values are adjusted after hiding the secret data is done to improve the quality of the stego image without disturbing the data hidden. The “pixel value differencing” (PVD) method that computes the difference value between two neighboring pixels to determine how many secret bits should be embedded into a cover pixel. The main idea of the EMD embedding scheme is that each $(2n + 1)$ -ary notational secret digit is carried by n cover pixels, and only one pixel value increases or decreases by 1. The basic idea of the PPM-based data-hiding method is to use pixel pair (x, y) as the coordinate, and searching a coordinate (x', y') within a predefined neighborhood set $\Phi(x, y)$ such that $f(x', y') = SB$, where f is the extraction function and SB is the secret message bit in a B -ary notational system to be concealed. Pure steganographic algorithms discussed above can be combined with good encryption algorithms to enhance the security of data transmission.

Among the encryption techniques chaotic based encryption techniques possess good combination of speed, security, complexity, suited to real time applications. The system appear to be random and disorderly but in actual there is a sense of order and pattern. The 1-dimensional map that exhibits complicated behavior is the logistic map from the interval $[0, 1]$ in to $[0, 1]$ parameterized by μ .

$$X_i = \mu * X_{i-1} (1 - X_{i-1}) \text{ where } 0 \leq \mu \leq 4.$$

In this project we are developing a system where we introduce a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module.

III. PROPOSED METHOD

The design for combining two different techniques is purely based on the idea- distort the message and hide the existence of the distorted message and for getting back the original message –retrieve the distorted message and regain the actual message by reversal of the distortion process. The proposed system includes three subsystems: cryptosystem, stego system and security system. The first cryptosystem encrypt and shuffle the secret message. Encryption and scrambling is purely based on the features of chaotic sequence. The initial parameter for the chaotic system is calculated from the secret key of user. Scrambling of cipher message is performed to decrease the correlation among the pixels where scrambling is based on the index of sorted chaotic sequence. In natural images the values and position of the neighbouring pixels are strongly correlated. The proposed method breaks this correlation increasing entropy of the position and entropy of pixel values using shuffling and encryption by chaotic sequence respectively. The second system called security system contributes extra security module through key based random permutation algorithm. KBRP algorithm generates a random sequence characterized by mutually exclusive elements from 1- P where Size of sequence: $P = \frac{1}{2} * \text{size of cover image}$ and Elements of sequence varies from 1 to

P. Original cover image is split up in to even and odd pixel matrix so that any adjacent pixel pairs can be randomly selected from it. The stego system finally embeds the cipher message bits in to the random pixel pairs of the cover image whose position is determined from the random sequence generated by KBRP algorithm. The data embedding and extraction procedure is based on adaptive pixel pair matching technique. In APPM the original pixel pair in the cover image is replaced by another pixel pair in its compact neighbourhood set such that the MSE between two pixel pairs is minimum. Thus the embedding procedure is protected by two secret keys: one is used for chaotic sequence generation and the other for KBRP sequence generation. The extraction procedure is exactly the reverse operation of embedding technique. The decrypted message in B ary notational system is converted back into binary notation.

IV. ALGORITHM FOR THE PROPOSED SYSTEM

In the proposed technique we hide the message in an image with the help of two secret keys. These two keys are secret keys and the receiver needs to know

these correctly to retrieve the original encrypted message.

A. Procedure for hiding data:

Cover image I of size $M \times N$, Secret image S

1. Convert the secret message in to B ary notational system SB such that all secret bits can be safely embedded. $B \geq \lceil \log_B |S| \rceil$ where $M \times N/2 \log B \geq |S|$
2. Encrypt the message using chaotic algorithm. Enter an external key k. calculate X0
3. Scramble encrypted message based on the index of sorted chaotic sequence
4. Create a random sequence Q using key based random permutation algorithm Size of $Q = M \times N/2 = P$. split up the cover image I to I1 & I2

Where I1 : hold odd pixel values I2 : even pixel matrix

5. Select a pixel pair (x,y) in cover image using Random sequence Q. Calculate the new co-ordinate (x',y') using APPM algorithm
6. Replace (x,y) by (x',y')
7. Repeat procedure until all encrypted message bits are embedded.

B Procedure for retrieving data:

Stego image I' secret key1, secret key 2

1. Construct random sequence Q using secret key 2.
2. Select pixel pair (x',y') according to the embedding sequence Q.
3. Calculate extraction function $f(x',y')$, result is the encrypted & scrambled cipher bit
4. Repeat step 2 & 3 until all cipher bits are extracted.
5. Apply reverse scrambling and decryption algorithm to get the original secret message in B-ary notation
6. Convert message bits into binary bit stream.

IV. RESULTS & ANALYSIS

When data is embedded into a cover image, image is distorted as its pixel values are modified. so an ideal steganographic scheme to keep the stego image away from drawing attention of an opponent should maintain better stego image quality. We measure mean square error between the cover image and stego

image as a parameter for analyzing stego image quality. minimum MSE results better stego image quality

$$MSE = \frac{1}{M \times N} \sum \sum (p_{ij} - p'_{ij})^2$$

Where $M \times N$ denotes the image size, and p_{ij} denote the pixel values of the original image and the stego image, respectively.

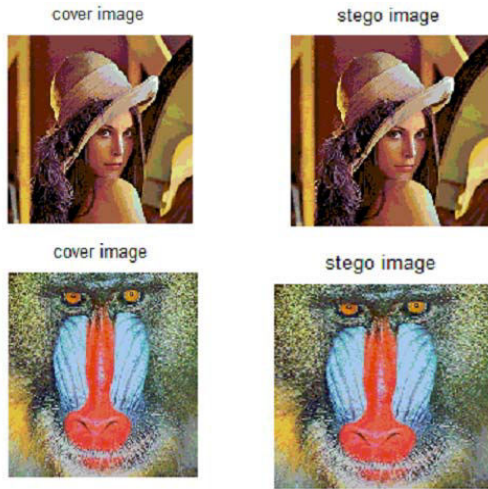
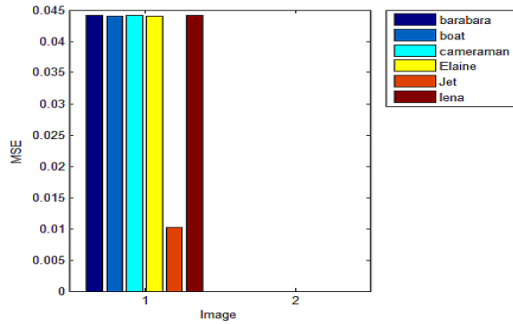


Fig 1 Test images and Stego images

VI. CONCLUSION

In this paper, we have presented a novel method of integrating cryptography and steganography by combining chaotic encryption with APPM embedding. The system strength increases by including secret keys, which enables us to change the cover pixel pairs randomly. We can conclude that proposed system is very effective as good security is achieved between two parties in case of secret communication.

VII REFERENCES

- [1] A novel data embedding method using adaptive pixel pair matching :Wien Hong and Tung-Shou chen IEEE transactions on information forensics and security, vol. 7, NO. 1, february 2012
- [2] A. Cheddad, J. Condell, K. Curran, and P. McKeivitt, "Digital image steganography: Survey and analysis of current methods," SignalProcess., vol. 90, pp. 727–752, 2010.
- [3] A survey on digital image steganography Amritha P, Gireeshkumar T
- [4] Image encryption algorithm using chaotic mapping mazleena salleh1, subariah ibrahim2 & ismail fauzi isnin3 chaotic mapping , university of malaysia, journal teknologi 2003



A SURVEY ON DYNAMIC TOPOLOGY CONTROL-ALGORITHMS IN MANET

KRUSHNA J. PANDIT

Department of M.E. Computer Engineering, Alpha College of Engineering & Technology,
Gujarat Technological University, Ahmedabad, Gujarat, India

Abstract:- Many solutions have been proposed for topology control in MANETs. A systematic & hierarchical study of these solutions allows better understanding and making improvements. In MANETs the nodes are free to move among network, causes the dynamic change in topology of network. Thus, in MANETs the dynamic topology control is required. Large variety of algorithms has been devised having focus of different performance metrics. This paper presents the topology control with its schematics and describes its available solution in analytical, sophisticated & hierarchical manner.

Keywords: MANET, Topology control, clustering, Ad hoc networks, centralized, distributed.

INTRODUCTION

The proliferation of mobile computing & communication technology is rapidly evolving with time, from common network computing- where workstations communicate via shared server, to a heterogeneous-scenario where different mobile-hosts (nodes) communicate over different network platforms. In such environment, the mobile devices/nodes adapt & do the self-reconfigure individually and collectively, in order to support the network functions. We are moving from the “Personal computer” age to the “ubiquitous computing” age which utilizes and the concept of accessing different network platforms in order to access the services.

In accordance with recent trends in networking, by the nature of communication, the networks can be classified in 2 main categories: Wired network & Wireless/Infrastructure less network. Due to the emergence of affordable, portable wireless communication and computation devices and the contribution of advances in the communication infrastructure have resulted in rapid growth of mobile wireless networks [1]. This technology allows network nodes (also referred to as mobile hosts) to communicate with each other via wireless transceivers directly by single/multiple hop without the need for a fixed infrastructure.

The “Mobile ad hoc network” (MANET) is an autonomous system of mobile nodes connected by single/multi-hop wireless scenario & Communicating over wireless links, which are relatively bandwidth-constrained, with limited battery power and highly dynamic in nature. Non-Infrastructure based MANET are expected to become a crucial part in the 4G architecture, as shown in the figure [3].

As in the figure, the research activities are grouped into 3 main areas:

- ❖ Enabling technologies
- ❖ Networking
- ❖ Middleware and applications

In MANET, the mobile-nodes are required to provide the services (all/specific-ones), which were being provided by the infrastructure of the wired-network. Since the MANETs help realizing network services for mobile-users in areas with no preexisting infrastructure & also for wireless extension for such infrastructures, it is gaining the favor of choice globally. And its mobile-nodes can also be linked to a fixed backbone network via use of a dedicated gateway device enabling targeted (i.e. IP) networking services in the areas where they (i.e. Internet etc) are not available [4]. Such applicability makes MANETs a promising solution & an attractive option for future of wireless networks.

ISSUES INVOLVED IN AD-HOC NETWORKING

MANETs represents complex distributed systems that comprise wireless mobile nodes that can freely & dynamically self-organize into arbitrary and temporary “ad-hoc” network topologies. Despite the flexibility & convenience being provided by the ad-hoc networks, it has several flaws.

Since MANET is a wireless network, it inherits the general problems relating to the wireless communications, which are: [5]

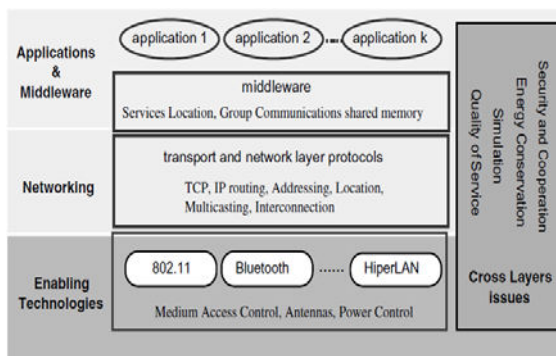


Fig 2– Simple MANET Architecture

- No absolute/observable network boundaries (no absolute/static measure of coverage area)
- Less reliable in comparison with wired media
- Security-level is low
- Time variant & asymmetric properties
- Hidden-terminal & exposed terminal problems

Some salient characteristics of MANET are enlisted & described as below: [4]

- **Autonomous & Infrastructure-less:** Each node operates as an independent-router and operates in distributed, self-induced & peer-to-peer mode. Due to which the network management is introduced to problem of fault-detection & management.
- **Multi-hop routing:** routes between nodes may include multiple hops in order to deliver the service to the node, which is out of source node's range.
- **Dynamic Topologies:** Nodes are free to move arbitrarily, which causes the network topology to change randomly and rapidly at predictable/unpredictable times (may have either unidirectional or bidirectional links).
- **Energy constrained operation:** Due to the limited power supply, processing power is limited, which causes to limit the services & applications that can be supported. In MANET each node is acting as both an end-system & router, which causes the energy constraint to be a bigger issue.
- **Bandwidth-constrained and variable capacity & capability links:** These links will continue to have significantly lower capacity than their hard-wired counterparts. Each node being equipped with one or more radio interfaces that have varying transmitting/receiving capabilities and operate across different frequency bands. This heterogeneity in node radio capabilities can result in possibly asymmetric links.
- **Network scalability:** The current trend of designing for network management algorithms is of fixed or relatively small wireless networks. Many MANET applications involve large (i.e. # of nodes) networks, for which scalability is critical to the successful deployment.

Among the many challenges for ad hoc network designers, mobility seems an especially difficult issue. In particular, when the nodes are allowed to move, wireless links between nodes may not be maintained all the time, hence network connectivity is not guaranteed at any time during the movement.

DYNAMIC TOPOLOGY CONTROL

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computing environment or biological network. The topology of a multi-hop wireless network is a "set of communication links between node-pairs used either explicitly or implicitly for the routing operation" [5]. Topology can

depend on uncontrollable factors (i.e. node mobility, weather, interference, noise) as well as controllable factors (i.e. transmission power, directional antennas, and multi-channel communications). Inappropriate topology for network can reduce the impact of network capacity by limiting spatial reuse of the communication channel and decrease network robustness. The main purpose of topology control is to - save energy, reduce interference between nodes & extend lifetime of the network.

Motivations for Topology control

- **Energy conservation:** Suppose node u must send a packet to node v , which is at distance d (see Figure 1). Node v is within u 's transmitting range at maximum power, so direct communication between u and v is possible. However, there exists also a node w in the region C circumscribed by the circle of diameter d that intersects both u and v (see Fig-3). Since $\delta(u,w) = d_1 < d$ and $\delta(v,w) = d_2 < d$, sending the packet using w as a relay is also possible. Instead of using long, energy inefficient path, it can take place along a multi-hop path composed of short edges.
- **Network capacity:** As depicted in Fig-4, node u is transmitting a packet to node v using certain transmit power P ; at the same time, node w is sending a packet to node z using the same power P . Since $\delta(v,w) = d_2 < \delta(v,u) = d_1$, the power of the interfering signal received by v is higher than that of the intended transmission from u , and the reception of the packet sent by u is corrupted. The max-power communication graph, that is, the graph obtained when the nodes transmit at maximum power, can be properly pruned in order to maintain only 'capacity-efficient' edges.

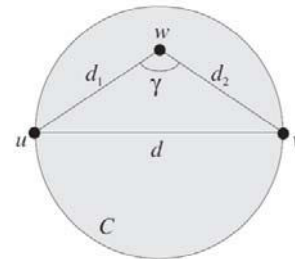


Fig 3- The case for multi-hop communication: node u must send a packet to v , which is at distance d ; using the intermediate node w to relay u 's packet is preferable from the energy consumption's point of view.

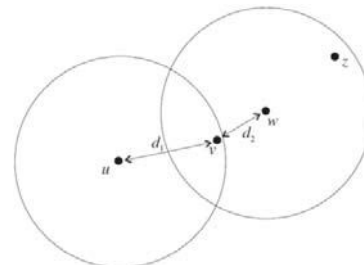


Fig 4- Conflicting wireless transmissions. The circles represent the radio coverage area with transmit power P .

2 steps of Topology control process (Topology creation & maintenance)

In recent trends, topology control has been divided into 2 sub problems.

Topology- construction, in charge of the initial reduction. There are many different ways to perform topology construction:

- Modification in transmission range of the nodes
- Clustering
- Turn-off nodes from the network
- Create a communication backbone, etc.

Topology-maintenance, in charge of the maintenance of the reduced topology so characteristics like connectivity & coverage are satiable for performance of network. There are different ways for topology maintenance:

- Global Vs. Local
- Dynamic Vs. Static Vs. Hybrid
- Triggered by time, energy, density, random, etc.

CLASSIFICATION OF TOPOLOGY CONTROL ALGORITHMS

A clear definition of the Topology control has not been introduced yet, but informally-it's the art of coordinating decisions regarding the transmitting ranges of the nodes, for generating a network with desired properties (i.e. connectivity)while reducing node energy consumption and/or increasing network

Table 1–The centralized topology control algorithms

Algorithms	Complexity	Strategy	Pros	Cons
RNG	$O(N \log N)$	Cone based search	Low power topology	Low fault tolerance & high articulation points
MST	$O(E + N \log N)$	Tree information	Low power topology	Low fault tolerance, high articulation points & high overheads
Connect	$O(N^2 \log N)$	Iterative cluster migration	Low power topology	Low fault tolerance & high overheads
NTC	$O(E^2 \log E)$	DT graph formation & sorting edges	High fault tolerance	High overheads
minR	$O(N^2P)$	Search for minimum power to maintain overall network connectivity	High fault tolerance(due to high power redundancy) & low articulation points	Same transmission power for all nodes, high overheads
Biconn-Augment	$O(N^2 \log N)$	Iterative cluster migration & DFS	High fault tolerance & low articulation points (due to bi-connectivity)	High overheads

Table 2-The distributed topology control algorithms

Algorithms	Complexity	Strategy	If-Articulation points?	No. of tables used
LINT	$O(N)$	Maintaining a specific node-degree	No	1
LILT	$O(2N+E)$	Maintaining a specific node degree & checking for APs	Yes	1

capacity(i.e. scalability, heterogeneity). The definition does implicate that - the topology control doesn't impose any constraint on the nature of the mechanism used to curb the network topology [6].

A number of algorithms for Topology control have already been proposed in the literature, generally they are classified in 2 types: Centralized algorithms- rely on global topology information to make adaptive decisions & Distributed algorithms- rely on partial link state information (i.e. density of neighboring-nodes for maintenance-in-network).

Note: Centralized algorithms suffer the problem of high connectivity overhead and scalability, therefore distributed topology control algorithms are generally preferred over centralized topology control algorithms.

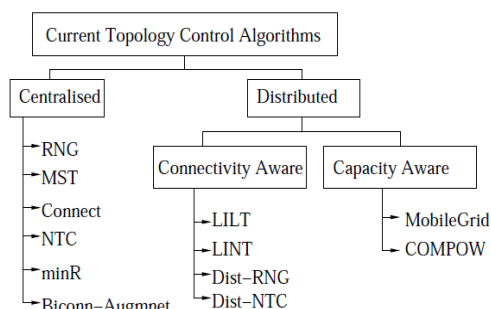


Fig 5- Categorization of topology control algorithms [5]

In the tables below, we discuss the characteristics of the centralized and distributed topology control algorithms. [7-12]

Dist- NTC	O(NL)	Maintaining a specific node degree & computing local DT graphs	No	1
Dist- RNG	O(N log N)	Maintaining local RNGs	No	1
MobileGrid	O(N)	Maintain CI	No	1
COMPOW	O(PN)	Evaluating an optimum power level	No	P

Note: E= total number of edges, N= total number of nodes, P= number of power increments, L=total number of non-basic links.

Clustering in MANETs

For some scenarios, topology control techniques are considered as mechanisms used to super-impose a network structure on an otherwise flat network organization [6]. This is the case, for instance, of clustering algorithms, which organize the network into a set of clusters, which are used to ease the task of routing messages between nodes and/or to better balance the energy consumption in the network.

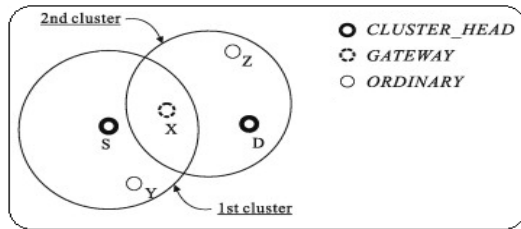


Fig 6- Cluster classification in MANET

Basically the clustering scheme in MANET is for classifying the network in a hierarchy of several nodes in the network by criteria for their specific role in network. The network nodes can be classified into 3-types of nodes in the MANETs.

1. Cluster Head node: which manages & maintains a given cluster w.r.t. given environment parameters (controllable i.e. or-uncontrollable)
2. Gateway node: used for routing between clusters

3. Ordinary node: simple elementary node of a cluster, which is other than gateway or cluster head node

In general, for a clustering protocol, first a distributed leader election algorithm is executed in each cluster on the basis of criteria i.e. available energy, communication quality, power consumption etc, or their combination. Then for message routing, the message to be sent is forwarded to clusterhead, which decides whether the routing is to be done in 2 level-hierarchies:

1. Inter cluster communication: forward the message to another cluster head via gateway node
2. Intra cluster communication: forward the message to another ordinary node in cluster or directly send it to the destination

Classification of the Clustering algorithms:

Below we enlist some common schemes for clustering in MANET infrastructure: [25]

1. Identifier based clustering
2. Connectivity based clustering
3. Mobility aware clustering
4. Low cost of maintenance clustering
5. Power aware clustering
6. Combined weight based clustering

Now we shall explain the available algorithms for each scheme of clustering: [13-24]

Table- Identifier based clustering (A unique ID is assigned to each node)

Algorithm	Scheme	Pros	Cons
Lowest ID Cluster Alg.	Concerned with only the lowest ID nodes (cluster heads), which are assigned arbitrarily.	Simple design	Due to long duration clusterhead, it is prone to power drainage
Max-min d-cluster formation Alg.	<ul style="list-style-type: none"> ➤ Cluster is a collection of nodes, with d-hops away from clusterhead ➤ No. of messages sent from each node is limited to a multiple of 'd' ➤ CHs are chosen on the basis of their degree of connectivity 	<ul style="list-style-type: none"> ➤ Clock synchronization overhead is avoided ➤ Guaranteed controlled message delivery, CH election & its density ➤ Minimizes the amount of data for exchange in clusterhead 	

Table- Connectivity based clustering

Algorithm	Scheme	Pros	Cons
Highest connectivity clustering Alg.	<ul style="list-style-type: none"> ➤ Degree of node is counted on basis of the distance from others & only 2 node type in this scheme-CH & ordinary ➤ Node with highest degree is chosen as CH & max inter-cluster node distance is 2-hops 	Low rate of clusterhead change	<ul style="list-style-type: none"> ➤ Low throughput & decrease with added no of nodes ➤ Reaffiliation count of nodes is high due to mobility
K-hop	➤ To elect CH we consider 2 criterions (connectivity &	➤ Combines 2 Alg. Lowest	One node can be

connectivity ID clustering (K-CONID)Alg.	<ul style="list-style-type: none"> lower ID of nodes) ➤ First of a node starts flooding for clustering-REQ to all other nodes ➤ All nodes at k-hops from the CH form the cluster 	<ul style="list-style-type: none"> ID & highest degree heuristics ➤ Minimizes no. of clusters in the network 	exhausted due to serving as a CH for longer duration to many mobile hosts
Adaptive cluster load balance method	<ul style="list-style-type: none"> ➤ In this scheme, 'hello' message format includes a specific "Options" item ➤ CH node sets its value to the no. of other nodes which are its neighbors in cluster & Ordinary node resets its value to 0 	<ul style="list-style-type: none"> ➤ Better resource utilization ➤ Distributed information transmission & resource consumption 	
Adaptive multihop clustering	The node broadcasts its information (ID, CH-ID & its status) to its cluster neighbors & Periodical-exchange of information with neighboring gateways	Upper and lower bounds for no of clustermembers	No scheme for proper selection of a node as a clusterhead

Table- Mobility aware clustering

Algorithm	Scheme	Pros	Cons
Mobility based d-hop clustering	<ul style="list-style-type: none"> ➤ It partitions the ad-hoc network into d-hop clusters ➤ Based on mobility metric & cluster diameter, adaptable w.r.t. node-mobility ➤ Requires calculation of 5 terms: <u>D</u>istance estimate & <u>R</u>elative mobility between nodes, <u>V</u>ariation of distance estimate over time, <u>L</u>ocal stability and <u>E</u>stimated mean distance ➤ Most stable node is chosen as CH 	Simple design	
Mobility based metric for clustering	<ul style="list-style-type: none"> ➤ In order to form a cluster, it uses a "variance of mobile node's speed relative to each its neighbors" ➤ Aggregate value of local speed of each node is estimated ➤ Timer is used for reduction of re-clustering in the maintenance of clusters 	Effective usage in group mobility based models	Mobility criterion is somewhat ignored during maintenance phase of clusters
Mobility based frame-work for adaptive clustering	<ul style="list-style-type: none"> ➤ It partitions a no. of mobile nodes into multihop clusters based on a special criteria(a,t), which indicate- every node in a cluster has a path to every other node, that will be available over some-time period 't' with probability of 'a' ➤ Adaptive framework dynamically organizes all the nodes 	<ul style="list-style-type: none"> ➤ More responsive & effective with low mobility ➤ More efficient with high node mobility 	

Table- Low cost of maintenance clustering

Algorithm	Scheme	Pros	Cons
Least cluster change Alg.	<ul style="list-style-type: none"> ➤ It follows 2 step procedure: cluster formation & maintenance ➤ Cluster formation is done by using a LIC Alg. ➤ In cluster maintenance, re-clustering is event driven & triggered <ol style="list-style-type: none"> 2 CH move into range of each others A mobile node is laid abstract 	Improves stability of cluster	Higher complexity for highly mobile scenarios
Adaptive clustering for mobile wireless network	<ul style="list-style-type: none"> ➤ Each node contains its own ID & the ID of its direct neighbors in a set G_i and the node with lowest ID is chosen a CH with its ID be the CID-cluster ID ➤ CID information (node ID & its CID) is used for cluster formation only, where each node finds its associated CH to form a cluster ➤ If 2 nodes in a cluster have moved 2 hops distance to each-other, then the node with highest intra-cluster connectivity is kept in & other one is revoked and maybe used as neighboring cluster inclusion or create a new cluster, if necessary 	Reduces the cluster formation overhead	Decrease in cluster size as well as increase in no. of clusters
3-hop between adjacent clusterheads (3-hBAC)	<p>Note: 1) The neighborhood of a lowest ID- node considered as node-MO. 2) A cluster-member/ direct neighbor of a node with status "unspecified" aren't considered to be candidates of becoming CH.</p> <ul style="list-style-type: none"> ➤ In MO's proximity highest degree node is chosen to be 1st CH with its direct neighbors be its members ➤ In parallel, node which is not deniable as CH, declares a new CH with highest degree neighbor ➤ For cluster-maintenance, 2 hops away CH distance is considered ➤ When node moves out of all cluster-range, can be included as "CG" 	<ul style="list-style-type: none"> ➤ New cluster generation is avoided in case of node location be abstract ➤ Reduce no. of clusters ➤ Eliminate small unnecessary clusters 	Bias for non-changing cluster topology

Passive clustering	<p>Note: 1) Does not use dedicated control packets/signals for clustering specific decisions. 2) Only node with value “initial” can be made CH by claiming to the neighbors via piggybacking its state</p> <ul style="list-style-type: none"> ➤ 4 available states for mobile-nodes : initial, CH, gateway, ordinary ➤ The neighboring nodes gain knowledge of CH-claim by monitoring the packet and recording the CID & packet receiving time ➤ The ordinary nodes are time bound with messages from other nodes in packets 	Self controlling for each node to maintain the cluster structure in order to manage the communication	
--------------------	---	---	--

Table- Power aware clustering

Algorithm	Scheme	Pros	Cons
Load balancing clustering	<ul style="list-style-type: none"> ➤ Balances the load on elected CHs on the basis of budget constraint ➤ Use variable number of virtual IDs(VID) 	Load distribution	Bias in CH selection may not derive optimum results
Power-aware connected dominant set(DS) clustering	DS consumes more battery-energy for specific operations of CH in network	Energy efficient (If DS reduced)	Inability to balance load between the CH and ordinary nodes
Clustering for energy conservation (single & double phase-clustering)	Master-slave paradigm, in which the channel is predefined & paging is used for communication with slaves	Reduces energy for transmission	More energy spent on paging itself than actual transmission

Table- combined weight based clustering

Algorithm	Scheme	Pros	Cons
Entropy-based weighted clustering	For evaluating route stability uses the entropy	Better indicator of stability & mobility	
Vote-based clustering	<ul style="list-style-type: none"> ➤ Uses a vote as a parameter, in the ‘Hello’ message (which is sent randomly during hello-cycle), to decide CH ➤ Uses an ‘Options’ field in hello-message to balance load between CH 	Easier CH selection	<ul style="list-style-type: none"> ➤ Extra communication overhead ➤ Clustering is followed by global weight determination policy at node level
Weight-based adaptive clustering	<ul style="list-style-type: none"> ➤ Uses transmission-power & rate, mobility, battery power and degree for CH-selection ➤ Automated response for node mobility (CH=higher than 1 hop, gateways=2/more CH ordinary-node=1 hop to CH) 	Self decisive & energy efficient	<ul style="list-style-type: none"> ➤ Uses GPS which becomes costly and overhead in maintenance ➤ Biased CH selection
Connectivity, energy & mobility driven weighted clustering	<ul style="list-style-type: none"> ➤ 2 stage procedure: To choose CH & To construct CH members ➤ In stage-1, quality for node-comparison is based on-lowest mobility, highest degree & battery energy etc. 	<ul style="list-style-type: none"> ➤ Adaptive in nature ➤ Relatively less CH-alteration 	No specific control over metrics

Note: REQ= request, CH=cluster-head, CG=Cluster-Guest, MH=mobile-host, MO= Mode of operation

CONCLUSION

We have studied the topology control in MANETs, also reviewed the hierarchy of available solutions for TC (topology control), which is concerned with organizing, controlling & co-coordinating MHs in MANETs. Here we have analyzed a clustering algorithms for TC in a hierarchical manner and reviewed their characteristics and schematics of the availed solutions. With this survey we see that topology control has many dimensions yet to be explored and does have many domains for further researches in TC for MANETs. It does outline several important issues which, we discussed for cluster-based MANETs, i.e. cluster-stability of structure, transmission rate, control the load of cluster construction & maintenance, energy consumption in different tasks, fairness of service in case of failures, resource utilization.

REFERENCES

- [1]. P. Senthilkumar , M. Baskar and K. Saravanan “A STUDY ON MOBILE AD-HOCK NETWORKS (MANETS)” in JMS- September 2011
- [2]. Dave Cavalcanti, Dharma Agrawal, Carlos Cordeiro, Bin Xie and Anup Kumar “Issues in integrating cellular networks, wlans, and manets: a futuristic heterogeneous wireless network “in IEEE 2005
- [3]. Marcin Szczodrak and Dr. Jinwoo Kim “4G and MANET, Wireless Network of Future Battlefield”
- [4]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”
- [5]. Paolo santi “Topology control in wireless Ad-hoc and sensor networks” IEEE – 2005
- [6]. Wang, Lee “PassCAR: A passive clustering aided routing protocol for VANET” Science Direct -August 2012

- [7]. Jerzy W. Jaromczyk and Godfried T. Toussaint, "The relative neighborhood graphs and their relatives," in *Proceedings of the IEEE*, Vol. 80, No9, Sept. 1992
- [8]. Chi-Fu Huang, Yu-Chee Tseng, Shih-Lin Wu, and Jang-Ping Sheu, "Distributed topology control algorithm for multihop wireless networks," in *Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on*, Vol.1, Pages: 355-360, 2002
- [9]. Kenneth J. Supowit, "The relative neighbourhood graph with application to minimum spannig trees," in *Journal of the ACM*, vol. 30, no. 3, pp 428- 448, 1983
- [10]. Hu L, "Topology control for multihop packet radio networks," in *Communications, IEEE Transactions on*, Vol.41, Iss.10, Pages: 1474- 1481, 1993
- [11]. Jilei Liu and Baochun Li, "Mobilegrid: capacity-aware topology control in mobile ad hoc networks," in *Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on*, Vol., Pages: 570- 574, 2002
- [12]. Narayanaswamy S., Kawadia V., Sreenivas R.S., and Kumar P.R., "Power Control in Ad-Hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol," in *Proceedings of the European Wireless Conference, Next Generation Wireless Networks: Technologies, Protocols, Services and Applications*, Feb. 2002
- [13]. A.D. Amis, R. Prakash, T.H.P Vuong, D.T. Huynh. "Max-Min DCluster Formation in Wireless Ad Hoc Networks". In proceedings of *IEEE Conference on Computer Communications (INFOCOM)* Vol. 1. pp. 32-41, 2000
- [14]. G. Chen, F. Nocetti, J. Gonzalez, and I. Stojmenovic, "Connectivity based k-hop clustering in wireless networks". Proceedings of the *35th Annual Hawaii International Conference on System Sciences*. Vol. 7, pp. 188.3, 2002
- [15]. F. Li, S. Zhang, X. Wang, X. Xue, H. Shen, "Vote- Based Clustering Algorithm in Mobile Ad Hoc Networks", In proceedings of *International Conference on Networking Technologies*, 2004
- [16]. T. Ohta, S. Inoue, and Y. Kakuda, "An Adaptive Multihop Clustering Scheme for Highly Mobile Ad Hoc Networks," in proceedings of *6th ISADS'03*, Apr. 2003
- [17]. I. Erland W. Seah. "Mobility-based d-hop clustering algorithm for mobile ad hoc networks". *IEEE Wireless Communications and Networking Conference* Vol. 4. pp. 2359-2364, 2004
- [18]. C. R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks," *IEEE JSAC*, vol. 15, pp. 1265-75, Sept. 1997
- [19]. J. Y. Yu and P. H. J. Chong, "3hBAC (3-hop between Adjacent Clusterheads): a Novel Non-overlapping Clustering Algorithm for Mobile Ad Hoc Networks," in proceedings of *IEEE Pacrim'03*, vol. 1, pp. 318-21, Aug. 2003
- [20]. A. D. Amis and R. Prakash, "Load-Balancing Clusters in Wireless Ad Hoc Networks," in proceedings of *3rd IEEE ASSET'00*, pp. 25-32 Mar. 2000
- [21]. Yu-Xuan Wang, Forrest Sheng Bao, "An Entropy-Based Weighted Clustering Algorithm and Its Optimization for Ad Hoc Networks," wimob, pp.56, *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007)*, 2007
- [22]. F. Li, S. Zhang, X. Wang, X. Xue, H. Shen, "Vote- Based Clustering Algorithm in Mobile Ad Hoc Networks", proceedings of International Conference on *Networking Technologies*, 2004
- [23]. S.K. Dhurandher and G.V. Singh" Weight-based adaptive clustering in wireless ad hoc networks" *IEEE* 2005
- [24]. F.D.Tolba, D. Magoni and P. Lorenz " Connectivity, energy & mobility driven Weighted clustering algorithm " in proceedings of *IEEE GLOBECOM 2007*
- [25]. R. Agarwal & Dr. Motwani "Survey of clustering algorithms for MANET" in *IJCSE* 2009



EVALUATION OF OPTIMAL MACHINING PARAMETERS OF Nicrofer C263 ALLOY USING RESPONSE SURFACE METHODOLOGY WHILE TURNING ON CNC LATHE MACHINE

MOHAMMED WASIF.G & MIR SAFIULLA

Dept of Mechanical Engg. Ghousia College Engineering, Ramanagaram

Abstract The objective of the present work was to investigate the effects of the various machining (turning) process parameters on the machining quality and to obtain the optimal sets of process parameters so that the quality of machined parts can be optimized. The working ranges and levels of the machining process (turning) parameters are found using three factors. Cutting speed (V_c - m/min), feed rate (f - mm/rev) and depth of cut (d - mm). The Design-Expert software has been used to investigate the effects of the Machining process parameters and subsequently to predict sets of optimal parameters for optimum quality characteristics. The response surface methodology (RSM) in conjunction with second order central composite rotatable design has been used to develop the empirical models for response characteristics. Desirability functions have been used for simultaneous optimization of performance measures. Also, the ANOVA technique and utility function have been used for response optimization. Confirmation experiments are further conducted to validate the results.

Keywords: Cutting parameters; turning process; feed force; RSM(Response Surface Methodology); ANOVA; Nicrofer c-263, TiAlN coated carbide tool.

INTRODUCTION:

A manufacturing engineer or machine setup technician is often expected to utilize experience and published shop guidelines for determining the proper machining parameters to achieve a specified level of surface roughness. This must be done in a timely manner to avoid production delays, effectively to avoid defects, and the produced parts monitored for quality. Therefore, in this situation, it is prudent for the engineer or technician to use past experience to select parameters which will likely yield a surface roughness below that of the specified level, and perhaps make some parameter adjustments as time allows or quality control requires. A more methodical, or experimental, approach to setting parameters should be used to ensure that the operation meets the desired level of quality with given ambient conditions and without sacrificing production time. Rather than just setting a very low feed rate to assure a low surface roughness, for example, an experimental method might determine that a faster feed rate, in combination with other parameter settings, would produce the desired surface roughness.

LITERATURE REVIEW

- H.H. Habeeb, K. Kadrigama, M.M. Noor, M.M. Rahman, B. Mohammed, R.A. Bakar and K. A. Abouel Hossein, et al. ,2010, pages 2322-2327, Journal Of Applied Science, Journal “ Machining of Nickel Alloy 242 with Cubic Boron Nitride Tools” discusses the development of first and second order of surface roughness prediction model when machining Haynes 242 alloy with Cubic Boron Nitride (CBN). The relationship between the cutting parameters (cutting speed,

axial depth and feed rate) with surface roughness are discussed. Response Surface Method (RSM) has been selected to optimize the cutting parameters and reduce the number of experiments. Surface roughness obtained in these experiments ranged from 0.052-0.08 μm , which consider as an extremely fine finish. Increase in cutting speed from 70 to 300 m/min, the roughness getting finer. On the other hand, increase in feedrate (0.1 to 0.3 mm/tooth) and axial depth (0.025 to 0.075 mm) surface roughness become rougher.

- Aman Aggarwal, Hari Singh, Pradeep Kumar, Manmohan Singh, et al., 11 September 2007, pp 373-384, Journal Of Materials Processing Technology, Journal “Optimizing power consumption for CNC turned parts using response surface methodology and Taguchi’s technique—A comparative analysis” presents the findings of an experimental investigation into the effects of cutting speed, feed rate, depth of cut, nose radius and cutting environment in CNC turning of AISI P-20 tool steel. Design of experiment techniques, i.e. response surface methodology (RSM) and Taguchi’s technique; have been used to accomplish the objective of the experimental study. L27 orthogonal array and face centered central composite design have been used for conducting the experiments. Taguchi’s technique as well as 3D surface plots of RSM revealed that cryogenic environment is the most significant factor in minimizing power consumption followed by cutting speed and depth of cut. The effects of feed rate and nose radius were found to be insignificant compared to other factors. Though both the techniques.

EXPERIMENTAL PROCEDURE:

1) First of all preliminary tests are done in order to find out the levels of machining parameters. First feed rate and depth of cut is kept constant and cutting speed is varied. The surface roughness of specimen is measured after each trial and it was found that optimum roughness is lying in between 50 to 100 m/min range of cutting speed. Next Speed is kept constant and feed rate is varied and surface roughness of the specimen is measured after each trial. The feed rate was found to be lying between 0.10 to 0.20 mm/rev for optimum surface roughness. Since according to literature depth of cut does not affect the surface roughness to a greater extent hence depth of cut levels were chosen according to the suitability.

2) After finding levels of parameters, design matrix as shown in table 5 was prepared with the help of Design Expert V 8.0 software.

3) Experiments were done as per the design matrix. The surface roughness was measured after each trial with the help of handysurf and all the data was recorded.

EXPERIMENTAL PLAN PROCEDURE:

Design Matrix with Responses:

RUN ORDER	STANDARD ORDER	SPEED (m/min)	FEED (mm/rev)	DOC (mm)	SURFACE ROUGHNESS (µm)
1	17	50.00	0.15	0.125	0.79
2	16	100.00	0.20	0.150	1.1
3	2	50.00	0.10	0.100	0.72
4	11	100.00	0.10	0.150	0.77
5	18	100	0.15	0.125	0.86
6	28	75	0.15	0.125	0.63
7	4	100	0.10	0.100	0.69
8	25	75	0.15	0.125	0.63
9	1	50	0.10	0.100	0.67
10	21	75	0.15	0.100	0.65
11	24	75	0.15	0.125	0.65
12	3	100	0.10	0.100	0.71
13	5	50	0.20	0.100	0.97
14	19	75	0.10	0.125	0.72
15	7	100	0.20	0.100	0.94
16	26	75	0.15	0.125	0.64
17	8	100	0.20	0.100	0.96
18	13	50	0.20	0.150	0.95
19	10	50	0.10	0.150	0.72
20	12	100	0.10	0.150	0.87
21	9	50	0.10	0.150	0.68
22	6	50	0.20	0.100	0.98
23	15	100	0.20	0.150	0.97
24	22	75	0.15	0.150	0.67
25	27	75	0.15	0.125	0.69
26	23	75	0.15	0.125	0.66
27	14	50	0.20	0.150	0.94
28	20	75	0.20	0.125	0.79

The data tabulated in the table 5.0 is analyzed with Design Expert V8.0 software. The analysis is shown and discussed here.

Table 5.1: Model Summary Statistics

Sequential	Lack of Fit	Adjusted	Predicted		
Source	p-value	p-value	R-Squared	R-Squared	
Linear	0.0011	< 0.0001	0.4185	0.3330	
2FI	0.7368	< 0.0001	0.3736	0.1927	
Quadratic	< 0.0001	0.0631	0.8884	0.7845	Suggested
Cubic					Aliased

Table 5.1 shows that quadratic model has to be applied for the observed sets of reading of surface roughness. It clearly shows that the quadratic model is the best suggested model for surface roughness with larger R2 statistics value.

Table 5.2 - ANOVA for Surface Roughness Quadratic Model

Source	Sum of Squares	df	MEAN SQUARE	F VALUE	p-value Prob > F	
Model	0.48	9	0.053	24.88	< 0.0001	Significant
A-Speed	0.011	1	0.011	5.25	0.0342	
B-Feed	0.23	1	0.23	107.91	< 0.0001	
C-DOC	8.022E-003	1	8.022E-	003 3.74	0.0689	
AB	9.000E-004	1	9.000E-004	0.42	0.5251	
AC	0.013	1	0.013	6.17	0.0230	
BC	1.225E-003	1	1.225E-003	0.57	0.4593	
A2	0.056	1	0.056	25.91	< 0.0001	
B2	0.016	1	0.016	7.48	0.0136	
C2	1.701E-003	1	1.701E-003	0.79	0.3847	
Residual	0.039	18	2.143E-003			
Lack of Fit	0.020	5	3.993E-003	2.79	0.0631	not significant

Pure Error	0.019	13	1.431E-003		
Cor Total	0.52	27			

Table II shows that speed (A), feed rate (B) and two-level interaction effect of speed and depth of cut (BC) and A2, B2 have significant effect on the surface roughness. But the effect of feed rate (B) is the most significant factor associated with surface roughness. This is anticipated as it is well known that for a given tool nose radius, the theoretical surface roughness ($R_a = f^2 / (32 \times r_e)$) is mainly a function of the feed rate (Shaw, 1984). The Model F value of 24.88 implies the model is significant. There is only a 0.01% chance that a "Model F-Value" this large could occur due to noise. Values of "Prob > F" less than 0.0500

indicate model terms are significant. In this case A, B, AC, A2, B2 are significant model terms. Values greater than 0.1000 indicate the model terms are not significant. If there are many insignificant model terms (not counting those required to support hierarchy Model reduction may improve our model. The "Lack of Fit F-value" of 2.79 implies there is a 6.31% chance that a "Lack of Fit F-value" this large could occur due to noise. Lack of fit is bad -- we want the model to fit.

Std. Dev.	0.046	R-Squared	0.9256
Mean	0.79	Adj R-Squared	0.8884
C.V.%	5.88	Pred R-Squared	0.7845
PRESS	0.11	Adeq Precision	14.782

The "Pred R-Squared" of 0.7845 is in reasonable agreement with the "Adj R-Squared" of 0.8884. "Adeq Precision" measures the signal to noise ratio. A ratio greater than 4 is desirable. Ratio of 14.782 indicates an adequate signal.

There are many insignificant terms in the equation and it can also be deduced from ANOVA table. Hence removing the insignificant terms and again analyzing ANOVA table we get,

Final Equation in Terms of Actual Factors:

$$R_a = 1.70386 - 0.037551 \text{ Speed} - 5.45880 \text{ Feed} + 8.27622 \text{ DOC} - (6.00000E-003) \text{ Speed} \times \text{Feed} + 0.046 \text{ Speed} \times \text{DOC} - 7.00 \text{ Feed} \times \text{DOC} + 2.24673E-004 \text{ Speed}^2 + 30.16822 \text{ Feed}^2 - 9.32710 \text{ DOC}^2$$

Table 5.4 - ANOVA for Response Surface Reduced Quadratic Model

Source	Sum of Squares	df	MEAN SQUARE	F VALUE	p-value Prob > F	
Model	0.48	6	0.079	39.30	< 0.0001	Significant
A-Speed	0.011	1	0.011	5.57	0.0280	
B-Feed	0.23	1	0.23	114.53	< 0.0001	
C-DOC	8.022E-003	1	8.022E-003	3.97	0.0594	
AC	0.013	1	0.013	6.55	0.0183	
A2	0.057	1	0.057	28.45	< 0.0001	
B2	0.014	1	0.014	7.16	0.0142	
Residual	0.042	21	2.019E-003			
Lack of Fit	0.024	5	2.974E-003	2.08	0.1159	Not significant
Pure Error	0.019	13	1.431E-003			
Cor Total	0.52	27				

Table 5.5 - Various R2 statistics for Surface Roughness for Reduced Quadratic Model

Std. Dev.	0.045	R-Squared	0.9182
Mean	0.79	Adj R-Squared	0.8949
C.V.%	5.71	Pred R-Squared	0.8305
PRESS	0.088	Adeq Precision	19.227

The various R2 statistics (i.e. R2, adjusted R2 (R2 adj) and predicted R2 (R2 pred)) of the surface

roughness are given in Table 5.5. The value of R2 = 0.9182 for surface roughness indicates that 91.82 %

of the total variations are explained by the model. The adjusted R2 is a statistic that is adjusted for the “size” of the model; that is, the number of factors (terms). The value of the R2 adj = 0.8949 indicates that 89.49 % of the total variability is explained by the model after considering the significant factors. R2 pred = 0.8305 is in good agreement with the R2 adj and shows that the model would be expected to explain 83.05% of the variability in new data (Montgomery, 2001). ‘C.V.’ stands for the coefficient of variation of the model and it is the error expressed as a percentage of the mean ((S.D./Mean)×100). Lower value of the coefficient of variation (C.V. = 5.71%) indicates improved precision and reliability of the conducted experiments.

Final Equation in Terms of Actual Factors:

$$\text{Surface Roughness (Ra)} = 2.33372 - 0.036045 \times \text{Speed} - 5.58070 \times \text{Feed} - 2.60556 \times \text{DOC} + 0.046 \text{ Speed} \times \text{DOC} + 2.08632 \times 10^{-4} \text{ Speed}^2 + 26.15789 \times \text{Feed}^2$$

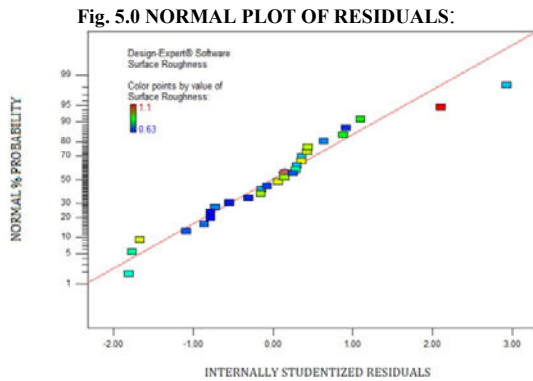


Fig. 5.0 the normal probability plot of the residuals (i.e. error = predicted value from model–actual Value) for surface roughness is shown in Fig. 5.0, Fig. 5.0 reveals that the residuals lie Reasonably close to a straight line, giving support that terms mentioned in the model are the only significant (Montgomery, 2001).

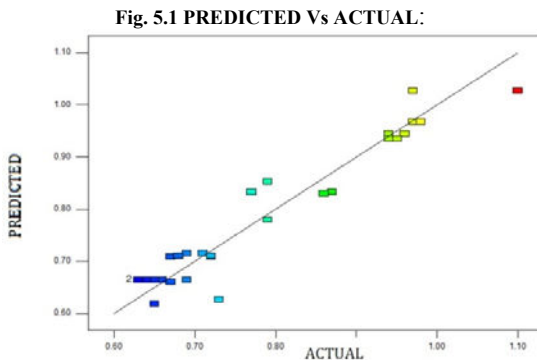


Fig. 5.1: Shows the actual values i.e. obtained through experimentation and the predicted valued i.e. values obtained from the model made for the surface roughness.

Fig. 5.2 PERTURBATIONS:

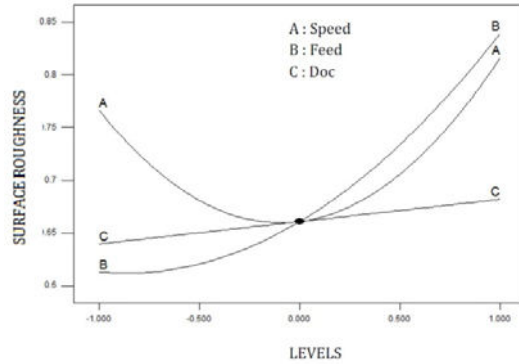


Fig 5.2 shows the variation of surface roughness with speed, feed and depth of cut. It can be observed from the fig that increasing depth of cut increases the surface roughness marginally and it can be considered not affecting surface roughness for this range. It can also be seen from the graph that surface roughness decreases with increase in cutting speed upto a certain point then further increase in cutting speed leads to increase in surface roughness. Increasing feed increases the surface roughness, this is anticipated as it is well known that for a given tool nose radius, the theoretical surface roughness ($Ra = f^2 / (32 \times re)$) is mainly a function of the feed rate (Shaw, 1984).

Fig. 5.3 CONTOUR:

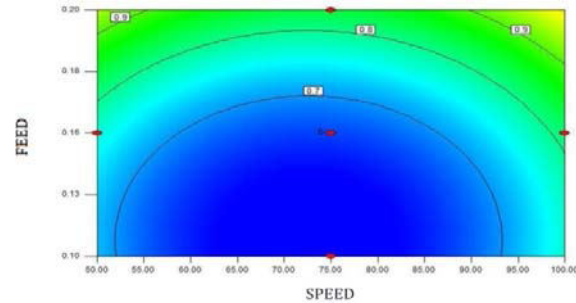


Fig. 5.4 3D SURFACE:

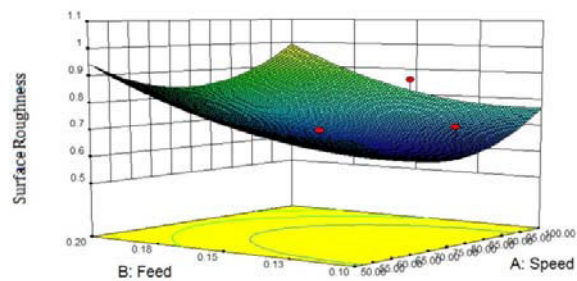


Figure 5.4 - Surface roughness 3D surface in cutting speed and feed rate plane at depth of cut of 0.1mm

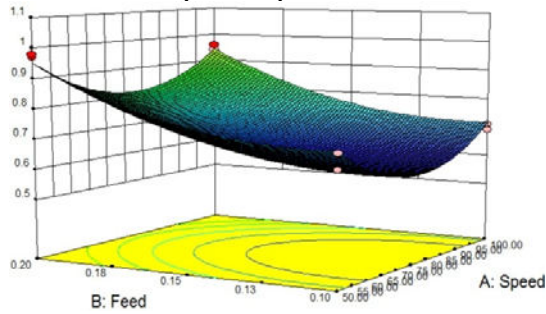


Figure 5.5 - Surface roughness 3D surface in cutting speed and feed rate plane at depth of cut of 0.125mm

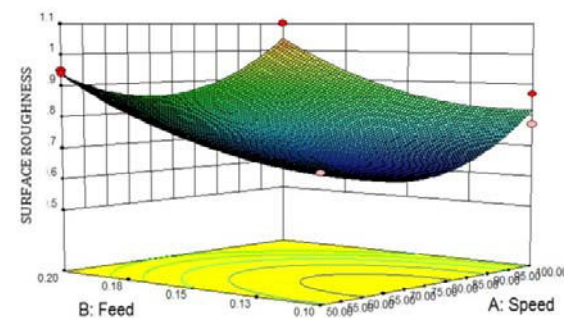


Figure 5.6 - Surface roughness 3D surface in cutting speed and feed rate plane at depth of cut of 0.150mm

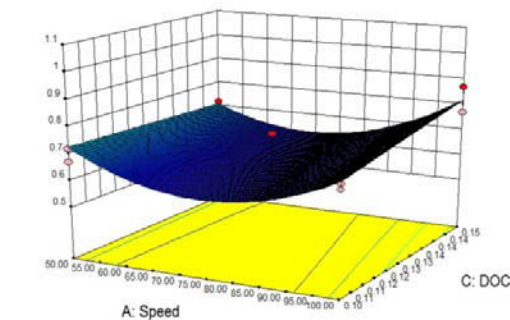


Figure 5.7 - Surface roughness 3D surface in cutting speed and depth of cut plane at feed of 0.01 mm/rev

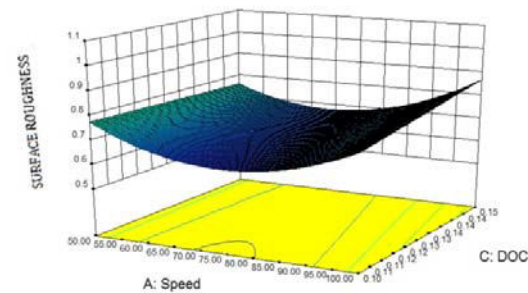


Figure 5.8 - Surface roughness 3D surface in cutting speed and depth of cut plane at feed of 0.015 mm/rev

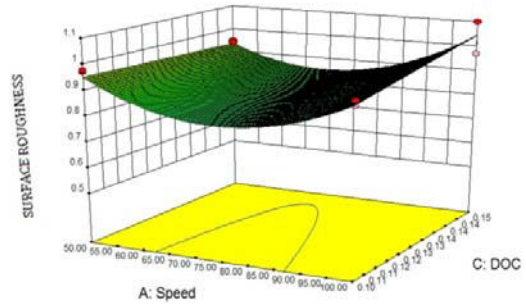


Figure 5.9 - Surface roughness 3D surface in cutting speed and depth of cut plane at feed of 0.02 mm/rev

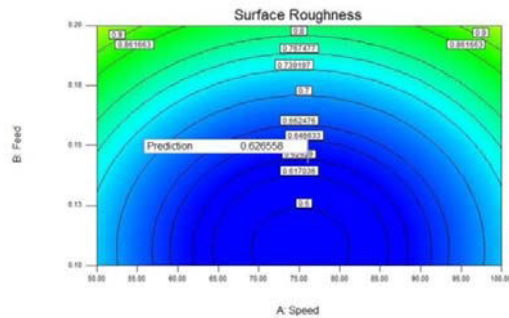


Figure 5.10- Optimization contour highlighting optimized (lowest) value of surface roughness at a Particular setting.

Figure 5.4, 5.5, 5.6 shows the Surface roughness in 3D surface in cutting speed and feed rate plane at three depth of cuts (0.100, 0.125, 0.150 mm) respectively. All have curvilinear profile in accordance to the quadratic model fitted. It can clearly be seen that surface roughness is increasing with increase in the feed rate and it varies with cutting speed, first decreases then increases as discussed before.

Figure 5.7, 5.8, 5.9 - shows the Surface roughness in 3D surface in cutting speed and depth of cut plane at three feed rates (0.10, 0.15, 0.2 mm/rev) respectively. It can clearly be seen that surface roughness does not vary much with the increase in depth of cut.

Figure 5.10 - Shows the optimization contour for surface roughness in feed and cutting speed plane. The figure shows the predicted optimized value (minimum value) of surface roughness which can be obtained in the given sets of feed, speed, depths of cut. The solution obtained through the Design Expert software is shown below. At this set of speed, feed and depth of cut one can get the lowest value of surface Roughness.

Table 5.7- Solution:

Surface Roughness	0.626558 μm
Feed	0.14mm/rev
DOC	0.102 mm
Speed	76.10 m/min

Thus the minimum value of roughness that can be achieved in given ranges of parameter values is $0.626558 \mu\text{m}$, which is obtained when feed is approximately at medium level (0.15mm/rev), depth of cut is near to lower level (0.10mm) and speed is also at medium level (75m/min).

SCOPE FOR FUTURE WORK:

- One of the important facts is whether the system contains a maximum or a minimum or a saddle point, which has a wide interest in industry. Therefore, RSM is being increasingly used in the industry. Also, in recent years more emphasis has been placed by the chemical and processing field for finding regions where there is an improvement in response instead of finding the optimum response (Myers, Khuri, and Carter). In result, application and development of RSM will continue to be used in many areas in the future.
- Since C-263 is a High temperature material it is always in use of aircrafts and industrial gas turbines. It can be used in space industry, where temperature goes on high counts. An adjustment in composition is still a very important way to improve the properties.

CONCLUSION:

This project presents the findings of an experimental investigation of the effect of cutting speed, feed rate and depth of cut on the surface roughness in turning of Nicrofer C-263 alloy using PVD TiAlN coated carbide tool and following conclusions are drawn. Quadratic model is fitted for surface roughness. The results show that the surface roughness does not vary much with experimental depth of cut in the range of 0.1 to 0.15 mm. A quadratic model best fits the

variation of surface roughness with feed rate, speed and depth of cut. Feed rate is the dominant contributor, accounting for 69.06% of the variation in surface roughness whereas cutting speed accounts for 3.30% and depth of cut 2.41%. Secondary contributions of interaction effect between speed and depth of cut (3.90%), second order (quadratic) effect of cutting speed (17.11%) and feed (4.2 %). Good surface finish can be achieved when depth of cut is set nearer to lower level of the experimental range (0.1mm), feed rate at mid level of the experimental range (0.15mm/rev) and cutting speed also at mid level of experiment range (75 m/min). Contour plots can be used for selecting the cutting parameters for providing the given desired surface roughness. The values of feed, speed, depth of cut has been found for best surface finish (lowest surface roughness). These are 0.14 mm/rev .76.10 m/min and 0.102 mm respectively. The value of surface roughness at these setting is predicted as $0.626558 \mu\text{m}$.

REFERENCES:

- [1]. Aman Aggarwal, Hari Singh, Pradeep Kumar, Manmohan Singh, et al., 11 September 2007, pp 373–384, Journal Of Materials Processing Technology, Journal “Optimizing power consumption for CNC turned parts using response surface methodology and Taguchi’s technique—A comparative analysis”.
- [2]. A. Karmakar et al., 1970, pp. 123–128, Proceedings of the Fourth All India Machine Tool Design and Research Conference , “Factors influencing surface finish during fine turning”.
- [3]. C. Courbon, D. Kramar, P. Krajnik, F. Pusavec, J. Rech, J. Kopac, et al., 2009, pp. 1114–1125, International Journal of Machine Tools & Manufacture, Journal “Investigation of machining performance in high-pressure jet assisted turning of Inconel 718: An experimental study”.



ANALYSIS OF SURFACE ROUGHNESS AND MATERIAL REMOVAL RATE (MRR) IN TURNING OPERATION OF SUPER ALLOY NIMONIC 75

DANISH KHAN

Department of Mechanical Engg. Ghousia College of Engg. Ramanagram Karnataka

Abstract:-The objective of the present work is to analyse the surface roughness and material removal rate(MRR) in turning operation of super alloy NIMONIC 75 so that the quality of machined parts can be optimized. The working ranges and levels of the machining process (turning) parameters are found using three factors. Cutting speed (V_c - m/min), feed rate (f - mm/rev) and depth of cut (d - mm). The Design-Expert software has been used to investigate the effects of the Machining process parameters and subsequently to predict sets of optimal parameters for optimum quality characteristics. The response surface methodology (RSM) in conjunction with second order central composite rotatable design has been used to develop the empirical models for response characteristics. Desirability functions have been used for simultaneous optimization of performance measures. Also, the ANOVA technique and utility function have been used for response optimization. Confirmation experiments are further conducted to validate the results.

Keywords: *Cutting parameters; turning process; feed force; RSM(Response Surface Methodology); ANOVA; Nimonic 75, TiAlN coated carbide tool, DOE(Design Expert Software v 8),*

INTRODUCTION:

Significant advances have been made in understanding the behaviour of engineering materials when machining at higher cutting conditions from practical and theoretical standpoints. This approach has enabled the aerospace industry to cope with constant introduction of new materials that allow the engine temperature to increase at a rate of 100C per annum since the 1950s. Improvements achieved from research and development activities in this area have particularly enhanced the machining of difficult-to-cut nickel base and titanium alloys that have traditionally exhibited low machinability due to their peculiar characteristics such as poor thermal conductivity, high strength at elevated temperature, resistance to wear and chemical degradation, etc. A good understanding of the cutting tool materials, cutting conditions, processing time and functionality of the machined component will lead to efficient and economic machining of nickel and titanium base superalloys. Rather than just setting a very low feed rate to assure a low surface roughness, for example, an experimental method might determine that a faster feed rate, in combination with other parameter settings, would produce the desired surface roughness.

LITERATURE REVIEW

1. M.Y. Noordin, Y.C. Tang and D. Kurniawan et al. 2007 observed that the introduction of hard turning has provided an alternative to the conventional processing technology used to manufacture parts made from hardened steels. Shorter product development time along with being more environmentally friendly are among the benefits offered by hard turning, which potentially results in lower manufacturing cost per part. However, common tool materials

for hard turning applications are expensive. Due to the continuous developments in cutting tool materials and coating technology, inexpensive coated carbide cutting tools are being investigated to determine the potential of using them for use in extreme conditions as in hard turning. TiAlN coated carbide tool was selected to finish machine hardened steel. Performing hard turning dry at various cutting conditions, that is, cutting speed and feed rate, revealed that satisfactory tool life values and surface finish values that meet the strict range of finish machining were obtained when finish machining hardened steel of 47-48 HRC hardness.

2. Yen et al. (2004) studied the effects of edge preparation of the cutting tool (round/hone edge and T- land/chamfer edge) on cutting forces using finite element analysis in orthogonal machining. Jawahir et al. (1992) carried out experimental studies on finish turning of low and medium carbon steel (AISI1018 and 1045) with cermet tool for investigating machinability parameters such as chip breakability, surface roughness and specific cutting pressure.

EXPERIMENTAL PROCEDURE:

- 1) Since depth of cut has least significance on surface roughness so there were no preliminary tests were performed on depth of cut.
- 2) Selection of speed and feed were taken by preliminary pilot experiments.

Table below shows results for pilot experiments:

5.2.2 Preliminary Experiments for Feed

S.No.	Speed	Feed	DOC	R _{a1}	R _{a2}	R _{avg}
1.	175	0.015	0.15	0.24	0.21	0.23
2.	175	0.02	0.15	0.19	0.26	0.24
3.	175	0.025	0.15	0.27	0.31	0.29
4.	175	0.03	0.15	0.25	0.37	0.31
5.	175	0.035	0.15	0.54	0.47	0.51
6.	175	0.04	0.15	0.83	0.69	0.76

S.No.	Speed	Feed	DOC	R _{a1}	R _{a2}	R _{avg}
1.	50	0.02	0.15	0.51	0.65	0.58
2.	100	0.02	0.15	0.39	0.46	0.43
3.	150	0.02	0.15	0.23	0.19	0.22
4.	200	0.02	0.15	0.17	0.24	0.21
5.	250	0.02	0.15	0.43	0.49	0.46

- 3) After finding levels of parameters, design matrix as shown in table 5.3 was prepared with the help of Design Expert V 8.0 software.
- 4) Experiments were done as per the design matrix. The surface roughness was measured after each trial with the help of handysurf and all the data was recorded.

Table below shows Design Matrix with Responses using DOE software:

Standar d Order	Run Order	Speed mmi n	Feed mm/ rev	DOC mm	R _{a1} micro on	R _{a2} micro on	R _{avg} micro on	MRR ₁ mms/mi n	MRR ₂ mms/mi n	MRR _{avg} mms/mi n
1	18	100	0.02	0.1	0.35	0.40	0.375	199.38	199.36	199.37
2	20	100	0.02	0.1	0.33	0.25	0.29	199.37	199.38	199.38
3	9	250	0.02	0.1	0.43	0.38	0.405	496.45	496.45	496.45
4	12	250	0.02	0.1	0.20	0.32	0.26	496.54	496.37	496.46
5	8	100	0.04	0.1	0.68	0.76	0.72	398.78	398.77	398.78
6	19	100	0.04	0.1	0.37	0.60	0.485	398.74	398.72	398.73
7	1	250	0.04	0.1	0.50	0.65	0.575	996.95	996.86	996.91
8	10	250	0.04	0.1	0.28	0.70	0.49	996.95	996.87	996.91
9	17	100	0.02	0.15	0.36	0.30	0.33	298.62	298.58	298.60
10	13	100	0.02	0.15	0.31	0.28	0.285	298.58	298.59	298.59
11	5	250	0.02	0.15	0.39	0.43	0.41	746.63	746.43	746.53
12	15	250	0.02	0.15	0.23	0.57	0.40	746.58	746.31	746.45
13	2	100	0.04	0.15	0.70	1.00	0.85	597.20	597.14	597.17
14	16	100	0.04	0.15	0.73	0.83	0.78	597.31	597.20	597.26
15	14	250	0.04	0.15	0.76	0.73	0.745	1493.14	1492.95	1493.05
16	6	250	0.04	0.15	0.66	0.79	0.725	1493.22	1492.99	1493.11
17	3	175	0.03	0.125	0.26	0.46	0.36	653.82	653.64	653.73
18	7	175	0.03	0.125	0.44	0.22	0.33	653.68	653.70	653.69
19	4	175	0.03	0.125	0.20	0.24	0.22	653.74	653.67	653.71
20	11	175	0.03	0.125	0.20	0.27	0.235	653.73	653.60	653.67
21	28	100	0.03	0.125	0.41	0.47	0.44	373.58	373.48	373.53
22	23	250	0.03	0.125	0.43	0.49	0.46	933.88	933.81	933.85
23	27	175	0.02	0.125	0.15	0.26	0.205	435.81	435.74	435.78

The data tabulated in the table 5.4 is analyzed with Design Expert V8.0 software. The analysis is shown and discussed here.

Table 5.4: Model Summary Statistics for surface roughness.

	Sequential	Lack of Fit	Adjusted	Predicted	
Source	p-value	p-value	R-Squared	R-Squared	
Linear	<0.0001	0.0084	0.5959	0.5056	
2FI	0.3207	0.0073	0.6083	0.4847	
Quadratic	0.0008	0.2564	0.8229	0.6629	Suggested
Cubic	0.3930	0.1332	0.8274	-1.5856	Aliased

Table 5.8 shows that quadratic model has to be applied for the observed sets of reading of surface roughness. It clearly shows that the quadratic model is the best suggested model for surface roughness with larger R2 statistics value.

Table 5.8 below shows the ANOVA analysis for Response Surface Quadratic model

Source	Sum of Squares	df	Mean Square	F Value	p-value Prob > F	
Block	0.014	1	0.014			
Model	0.80	9	0.89	14.42	<0.0001	Significant
A-Speed	4.014E-004	1	4.014E-004	0.065	0.8020	
B-Feed	0.54	1	0.54	87.15	<0.0001	
C-DOC	0.044	1	0.044	7.11	0.0162	
AB	0.015	1	0.015	2.48	0.1340	
AC	1.914E-003	1	1.914E-003	0.31	0.5853	
BC	0.034	1	0.034	5.46	0.0320	
A ₂	0.034	1	0.034	5.48	0.0316	
B ₂	0.037	1	0.037	5.99	0.0256	
C ₂	1.208E-003	1	1.208E-003	0.20	0.6641	
Residual	0.11	17	6.186E-003			
Lack of fit	0.041	5	8.143E-003	1.52	0.2564	Not significant
Pure error	0.064	12	5.370E-003			
Cor Total	0.92	27				
Std Dev:	0.078649		C.V. %:	17.50545	Adj R-Squared:	0.822884
Mean:	0.449286		R-Squared:	0.884193	Pred R-Squared:	0.662933

The Model F-value of 14.42 implies the model is significant. There is only a 0.01% chance that "Model F-Value" this large could occur due to noise.

- Values of "Prob > F" less than 0.0500 indicate model terms are significant. In this case B,C, BC, A₂, B₂ are significant model terms. Values greater than 0.1000 indicate the model terms are not significant. If there are many insignificant model terms (not counting those required to support hierarchy), model reduction may improve your model.
- The "Lack of Fit F-value" of 1.52 implies the Lack of Fit is not significant relative to the pure error. There is a 25.64% chance that a "Lack of Fit F-value" this large could occur due to noise. Non-significant lack of fit is good -- we want the model to fit.
- The various R2 statistics (i.e. R2, adjusted R2 (R2adj) and predicted R² (R^{2pred})) of the surface roughness are given in Table 5.8. The value of R2 = 0.884193 for surface roughness indicates that 88.41% of the total variations are explained by the model.
- The adjusted R2 is a statistic that is adjusted for the "size" of the model; that is, the number of factors (terms). The value of the R2adj = 0.822884 indicates that 82.28% of the total variability is explained by the model after considering the significant factors.

Final Equation in Terms of Actual Factors:

$$\begin{aligned}
 \text{Surface Roughness} = & +1.30374 - (6.48994E-00 * \text{Speed}) - (68.32068 * \text{Feed}) + (3.86029 * \text{DOC}) - \\
 & (0.04125 * \text{Speed} * \text{Feed}) + (5.83333E-003 * \text{Speed} * \text{DOC}) + (183.75000 * \text{Feed} * \text{DOC}) \\
 & + (1.98152E-005 * \text{Speed}^2) + (1164.60396 * \text{Feed}^2) - (33.66337 * \text{DOC}^2) \\
 & \dots (5.1)
 \end{aligned}$$

There are many insignificant terms in the equation and it can also be deduced from ANOVA table. Hence removing the insignificant terms and again analyzing ANOVA table we get:

Table 5.9 below shows the Reduced or Pooled ANOVA table for surface roughness after excluding insignificant terms i.e. A, AB, AC, C²

Table 5.9: ANOVA for Response Surface Reduced Quadratic Model (Surface roughness)						
Source	Sum of Squares	df	Mean Square	F-Value	p-value Prob > F	
Block	0.014	1	0.014			
Model	0.78	5	0.16	26.56	<0.0001	Significant
B-Feed	0.54	1	0.54	91.30	<0.0001	
C-DOC	0.044	1	0.044	7.45	0.0125	
BC	0.034	1	0.034	5.72	0.0262	
A ²	0.034	1	0.034	5.74	0.0259	
B ²	0.037	1	0.037	6.31	0.0202	
Residual	0.12	21	5.905E-003			
Lack of Fit	0.060	9	6.617E-003	1.23	0.3601	Not significant
Pure Error	0.064	12	5.370E-003			
Cor Total	0.92	27				
Std. Dev: 0.079		C.V. %: 17.50		Adj R-Squared: 0.8231		
Mean: 0.45		R-Squared: 0.8639		Pred R-Squared: 0.7305		

Final Equation in Terms of Actual Factors:

$$\text{Surface Roughness} = +1.80482 - (6.52062E-003 * \text{Speed}) - (70.93346 * \text{Feed}) - (3.53472 * \text{DOC}) + (183.75 * \text{Feed} * \text{DOC}) + (1.84505E-005 * \text{Speed}^2) + (1087.83784 * \text{Feed}^2) \dots (5.2)$$

Equation 5.2 is based on final table 5.9

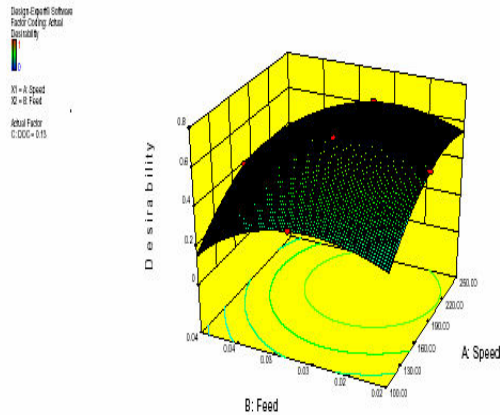


Figure 5.15: 3D Surface Graph of Desirability for speed and feed

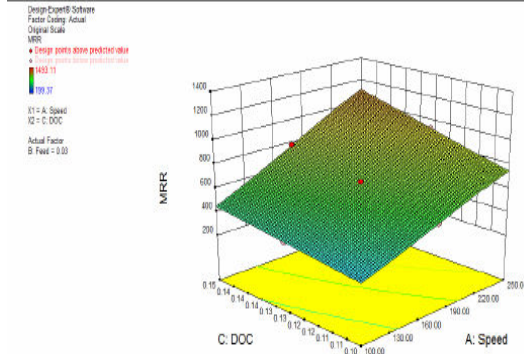
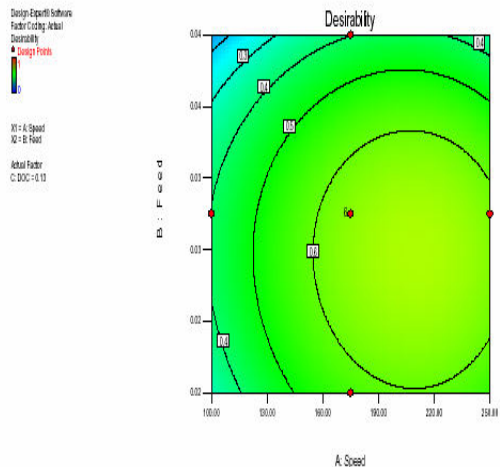


Figure 5.12: Response surface between Speed, DOC and MRR

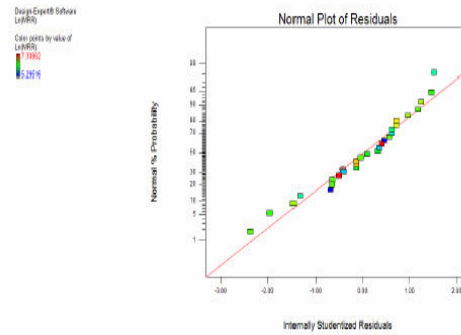


Figure 5.13: Normal Probability curve for MRR

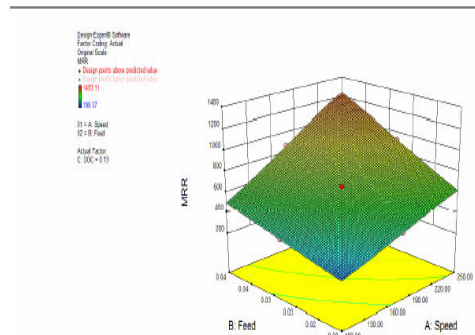


Figure 5.10: Response surface between Speed, Feed and MRR

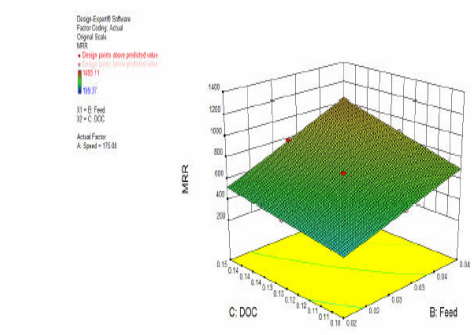


Figure 5.11: Response surface between DOC, Feed and MRR

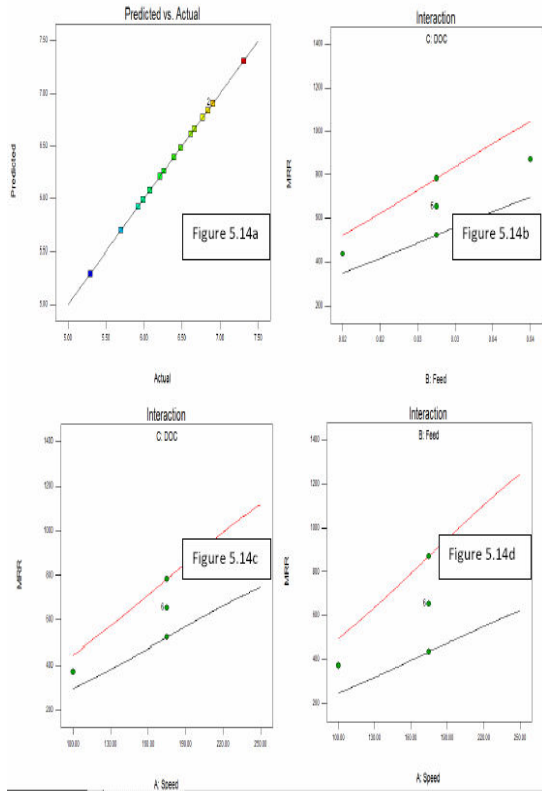


Figure 5.14: Actual v/s Predicted & Interaction curves

Table 5.7- Solution:

Feed	0.02 mm/rev
DOC	0.1mm
Speed	175 m/min

Above table shows the final result to achieve optimum surface finish in machining of nimonic 75.

SCOPE FOR FUTURE WORK:

- One of the important facts is whether the system contains a maximum or a minimum or a saddle point, which has a wide interest in industry. Therefore, RSM is being increasingly used in the industry. Also, in recent years more emphasis has been placed by the chemical and processing field for finding regions where there is an improvement in response instead of finding the optimum response (Myers, Khuri, and Carter). In result, application and development of RSM will continue to be used in many areas in the future.
- Since C-263 is a High temperature material it is always in use of aircrafts and industrial gas turbines. It can be used in space industry, where temperature goes on high counts. An adjustment in composition is still a very important way to improve the properties.

CONCLUSION:

The surface roughness follows the quadratic trend in the given ranges of speed (100 to 250 m/min), feed (0.02 to 0.04 mm/rev) and depth of cut (0.1mm to 0.15mm). The material removal rate undergone natural log transformation and fitted to the quadratic model in the given range of parameters. Feed rate is the most significant parameter in judging the surface roughness. Feed rate is contributing 58.69% to the surface roughness. Optimum value of parameters to maximize the material removal rate is Cutting speed = 250 m/min, Feed = 0.04 mm/rev & Depth of cut = 0.15 mm Optimum value of parameters to minimize the value of surface roughness is Cutting speed = 175 m/min, Feed = 0.02 mm/rev & Depth of cut = 0.1mm. Optimum value of parameters to optimize the multiple responses by using desirability function on giving more importance to surface roughness (5 units) and less importance to MRR (2 units) is Cutting speed = 204 m/min, Feed = 0.03 mm/rev. and Depth of cut = 0.15 mm At higher speed (250 m/min), a lot of heat was generated which accelerated the tool wear rate. The coefficient of friction of PVD TiAlN coating is 0.35 and micro hardness is 2300-2500HV. But if some better coating with higher micro hardness and lower coefficient of friction is used then the tool life can be extended.

REFERENCES:

- [1]. E.O. Ezugwu, Z.M. Wang, A.R. Machad, 1999. The machinability of nickel-based alloys: a review. Journal of Materials Processing Technology 86 (1999) 1-16
- [2]. E.O. Ezugwaa, J. Bonney, Y.Yamane, 2002. An overview of the machinability of aeroengine alloys. Journal of materials processing technology 134 (2003), 233 -253.
- [3]. E.O. Ezugwu, 2005. Key improvements in the machining of difficult -to-cut aerospace superalloys. International Journal of Machine Tools & Manufacture 45 (2005) 1353 -1367
- [4]. R.S. Pawade, Suhas S. Joshi, P.K. Brahmkankar, M. Rahman, 2007. An investigation of cutting forces and surface damage in high-speed turning of Inconel 718. Journal of Materials Processing .

