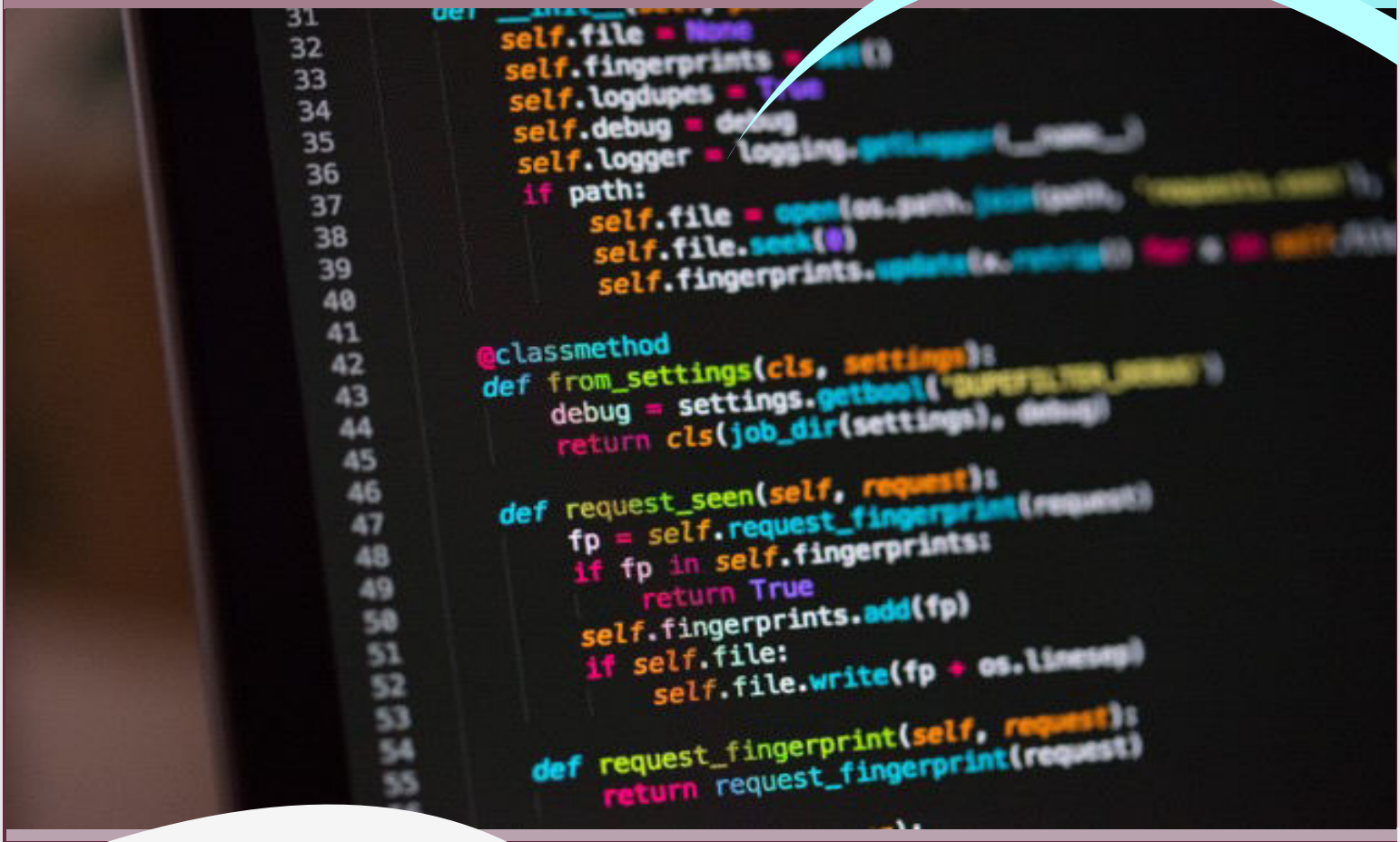
9-2-2012

International Conference on Computer Science & Information Technology

Prof.Srikanta Patnaik Mentor
IRNet India, patnaik_srikanta@yahoo.co.in

Proceedings of International Conference on

COMPUTER SCIENCE & INFORMATION TECHNOLOGY



(ICCSIT-2012)
2nd September, 2012
BANGALORE, India

Interscience Research Network (IRNet)
Bhubaneswar, India

International Conference on Computer Science & Information Technology

ICCSIT-2012

Bangalore, 2nd September, 2012.

Home Editorial

SECTION –II
ARTIFICIAL INTELLIGENCE & SOFT COMPUTING

Editorial

Over the past 50 years, innovation has been a key ingredient for success of Computer Science and Information Technology. The scope of today's amazing technology enables us to diffuse the ideas and transform the living conditions. The prospering dream to master over economic resources available the mankind has developed and categorized a concrete knowledge system that gives solutions and support to socio-economic and techno structural problems of our loving and enriching society. Some disciplines have their own theoretical foundations and some are derived. The thrust is to propagate new research and learning from experts, practitioners and avid scholars and improving the field of study for future development. The broad framework in which the conference is manifested is to augment and cater to the purpose of those silent laboratories and their relentless insistence for coming out with flying colours.

This ongoing innovation typically had a time constant of a decade from one innovation to the next in each domain. However, with the advent of the global Internet and the unprecedented number of innovations in web services and apps, innovation that used to be defined by years, now may take mere months or just days.

The conference designed to stimulate the young minds including Research Scholars, Academicians, and Practitioners to contribute their ideas, thoughts and nobility in these disciplines of engineering. It's my pleasure to welcome all the participants, delegates and organizer to this international conference on behalf of IOAJ family members. We received a great response from all parts of country and abroad .I sincerely thank you all the authors for their invaluable contribution to this conference. I am indebted towards the reviewers and team IOAJ for their generous gifts of time, energy and effort.

Editor-in-Chief
Dr. Srikanta Patnaik
Chairman, I.I.M.T., Bhubaneswar
Intersceince Campus,
At/Po.: Kantabada, Via-Janla, Dist-Khurda
Bhubaneswar, Pin:752054. Orissa, INDIA.

SECTION –I

COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm

[1]A.Yaganteeswarudu, [2]V.Chandra Sekher & [3]K.Siva Prasad

[1]Dept of CSE, SCET, Kurnool, Andhra Pradesh.
[2]Dept of CSE, SJCET, Yemmiganur, KurnoolAndhra Pradesh.
[3]Dept of CSE, SJCET, Yemmiganur, Kurnool.

Abstract- Phishing is a new type of network attack where the attacker creates a replica of an existing Web page to fool users (e.g., by using specially designed e-mails or instant messages) into submitting personal, financial, or password data to what they think is their service provides' Web site. In this project, we proposed a new end-host based anti-phishing algorithm, which we call Link Guard, by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the Anti-Phishing Working Group (APWG). Because it is based on the generic characteristics of phishing attacks, Link Guard can detect not only known but also unknown phishing attacks. We have implemented LinkGuard in Windows XP. Our experiments verified that Link Guard is effective to detect and prevent both known and unknown phishing attacks with minimal false negatives. LinkGuard successfully detects 195 out of the 203 phishing attacks. Our experiments also showed that Link Guard is light weighted and can detect and prevent phishing attacks in real time.

Index Terms*—Network security, Phishing attacks, Hyperlink, Link Guard algorithm.*

I. INTRODUCTION

The word 'Phishing' initially emerged in 1990s. The early hackers often use 'ph' to replace 'f' to produce new words in the hacker's community, since they usually hack by phones.Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a faked Website by sending them faked e-mails (or instant messages), and stealthily get victim's personal information such as user name, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). The frequently used attack method is to send e-mails to potential victims, which seemed to be sent by banks, online organizations, or ISPs. In these e-mails, they will makeup some causes, e.g. the password of your credit card had been mis-entered for many times, or they are providing upgrading services, to allure you visit their Website to conform or modify your account number and password through the hyperlink provided in the e-mail. You will then be linked to a counterfeited Website after clicking those links. The style, the functions performed, sometimes even the URL of these faked Websites this work was supported by the National Natural Science Foundation of China (NSFC) under contract No. 60503049. are similar to the real Web site. It's very difficult for you to know that you are actually visiting a malicious site. If you input the account number and password, the attackers then Successfully collect the information at the server side, and is able to perform their next step actions with that information (e.g., withdraw money out from your account). to counterfeit the Bank of China (real Web site www.bank-ofchina.com, counterfeited Web site www.bank-offchina.com), the Industrial and Commercial Bank.cn, faked website www.1cbc.com.cn) , the Agricultural Bank of China (real website www.95599.com,faked Web site www.965555.com), etc. In this project, we study the common procedure of phishing attacks and review possible anti-phishing approaches. We then focus on end-host based antiphishing approach. We first analyze the common characteristics of the hyperlinks in phishing e-mails. Our analysis identifies that the phishing hyperlinks share one or more characteristics as listed below:

1) the visual link and the actual link are not the same; 2)the attackers often use dotted decimal IP address instead of DNS name; 3) special tricks are used to encode the hyperlinks maliciously; 4) the attackers often use fake DNS names that are similar (but not identical) with the target Website. We then propose an end-host based anti-phishing algorithm which we call LinkGuard, based on the characteristics of the phishing hyperlink. Since LinkGuard is character-based, it can detect and prevent not only known phishing attacks but also unknown ones. We have implemented LinkGuard in Windows XP, and our experiments indicate that LinkGuard is light weighted in that it consumes very little memory and CPU circles, and most importantly, it is very effective in detecting phishing attacks with minimal false negatives. LinkGuard detects 195 attacks out of the

203 phishing archives provided by APWG without knowing any signatures of the attacks.

The rest of this paper is organized as follows. In Section II, we give the general procedure of a phishing attack and provide the available methods to prevent phishing attacks. We then analyze the characteristics of the hyperlinks used in phishing attacks and present the LinkGuard algorithm in Section III.Section IV describes our implementation of the LinkGuard system and gives the experimental results. Section V concludes this project
.

II. PHISHING ATTACK PROCEDURE AND PREVENTION METHODS

In this project, we assume that phishers use e-mail as their major method to carry out phishing attacks. Nonetheless, our analysis and algorithm can be applied to attacks that use other means such as instant messaging.

A. The Procedure of Phishing Attacks

In general, phishing attacks are performed with the following
four steps:

1) Phishers set up a counterfeited Web site which looks exactly like the legitimate Web site, including setting up the web server, applying the DNS server name, and creating the web pages similar to the destination Website, etc.
2) Send large amount of spoofed e-mails to target users in the name of those legitimate companies and organizations, trying to convince the potential victims to visit their Web sites.
3) Receivers receive the e-mail, open it, and click the spoofed hyperlink in the e-mail, and input the required information.
4) Phishers steal the personal information and perform their fraud such as transferring money from the victims' account.

B. Approaches to Prevent Phishing Attacks

There are several (technical or non-technical) ways to prevent phishing attacks: 1) educate users to understand how phishing attacks work and be alert when phishing-alike e-mails are received; 2) use legal methods to punish phishing attackers; 3) use technical methods to stop phishing attackers. In this
project, we only focus on the third one.
Technically, if we can cut off one or several of the steps that needed by a phishing attack, we then successfully prevent that attack. In what follows, we briefly review these approaches.

1) Detect and block the phishing Web sites in time:

If we can detect the phishing Web sites in time, we then can block the sites and prevent phishing attacks. It's relatively easy to (manually) determine whether a site is a phishing site or not, but it's difficult to find those phishing sites out in time. Here we list two methods for phishing site detection. 1) The Web master of a legal Web site periodically scans the root DNS for suspicious sites (e.g. www.1cbc.com.cn vs. www.icbc.com.cn). Since the phisher must duplicate the content of the target site, he must use tools to (automatically) download the Webpages from the target site. It is therefore possible to detect this kind of download at the Web server and trace back to the phisher. Both approaches have shortcomings. For DNS scanning, it increases the overhead of the DNS systems and may cause problem for normal DNS queries, and furthermore, many phishing attacks simply do not require a DNS name. For phishing download detection, clever phishers may easily write tools which can mimic the behavior of human beings to defeat the detection.

2) Enhance the security of the web sites:

The business Websites such as the Web sites of banks can take new methods to guarantee the security of users' personal information. One method to enhance the security is to use hardware devices. For example, the Barclays bank provides a hand-held card reader to the users. Before shopping in the net, users need to insert their credit card into the card reader, and input their (personal identification number) PIN code, then the card reader will produce a onetime security password, users can perform transactions only after the right password is input . Another method is to use the biometrics characteristic (e.g. voice, fingerprint, iris, etc.) for user authentication. For example, Paypal had tried to replace the single password verification by voice recognition to enhance the security of the Web site. With these methods, the phishers cannot accomplish their tasks
even after they have gotten part of the victims' information .However, all these techniques need additional hardware to realize the authentication between the users and the Web sites, hence will increase the cost and bring certain inconvenience. Therefore, it still needs time for these techniques to be widely adopted.

3) Block the phishing e-mails by various spam filters:

Phishers generally use e-mails as 'bait' to allure potential victims. SMTP (Simple Mail Transfer Protocol) is the protocol to deliver e-mails in the Internet. It is a very simple protocol which lacks necessary authentication mechanisms. Information related to sender, such as the name and email address of the sender, route of the message, etc., can be

counterfeited in SMTP. Thus, the attackers can send out large amounts of spoofed e-mails which are seemed from legitimate organizations.

The phishers hide their identities when sending the spoofed e-mails, therefore, if anti-spam systems can determine whether an e-mail is sent by the announced sender (Am I Whom I Say I Am?), the phishing attacks will be decreased dramatically. From this point, the techniques that preventing senders from counterfeiting their Send ID (e.g. SIDF of Microsoft) can defeat phishing attacks efficiently.

SIDF is a combination of Microsoft's Caller ID for E-mail and the SPF (Sender Policy Framework) developed by Meng Weng Wong. Both Caller ID and SPF check e-mail sender's domain name to verify if the e-mail is sent from a server that is authorized to send e-mails of that domain, and from that to determine whether that e-mail use spoofed e-mail address. If it's faked, the Internet service provider can then determine that e-mail is a spam e-mail.

The spoofed e-mails used by phishers are one type of spam e-mails. From this point of view, the spam filters can also be used to filter those phishing e-mails. For example, blacklist, whitelist, keyword filters, Bayesian filters with self learning abilities, and E-Mail Stamp, etc., can all be used at the e-mail server or client systems. Most of these anti-spam techniques perform filtering at the receiving side by scanning the contents and the address of the received e-mails. And they all have pros and cons as discussed below. Blacklist and whitelist cannot work if the names of the spamers are not known in advance. Keyword filter and Bayesian filters can detect spam based on content, hence can detect unknown spasm. But they can also result in false positives and false negatives. Furthermore, spam filters are designed for general spam e-mails and may not very suitable for filtering phishing e-mails since they generally do not consider the specific characteristics of phishing attacks.

4) Install online anti-phishing software in user's computers:

Despite all the above efforts, it is still possible for the users to visit the spoofed Web sites. As a last defense, users can install anti-phishing tools in their computers. The antiphishing tools in use today can be divided into two categories: blacklist/whitelist based and rule-based.

Category II: this category of tools uses certain rules in their software, and checks the security of a Website according to these rules. Examples of this type of tools include Spoof Guard developed by Stanford, Trust Watch of the GeoTrust, etc. Spoof Guard checks the domain name, URL (includes the port number) of a Web site, it also checks whether the browser is directed to the current URL via the links in the contents of e-mails. If it finds that the domain name of the visited Web site is similar to a well-known domain name, or if they are not using the standard port, Spoof Guard will warn the users. In TrustWatch, the security of a Web site is determined by whether it has been reviewed by an independent trusted third party organization. Our work differs from in that: 1) LinkGuard is based on our careful analysis of the characteristics of phishing hyperlinks whereas Spoof Guard is more like a framework; 2) LinkGuard has a verified very low false negative rate for unknown phishing attacks whereas the false negative proper of Spoof Guard is still not known. In next section, we first study the characteristics of the hyperlinks in phishing e-mails and then we propose the LinkGuard algorithm.

II. LINKGUARD

A. Classification of the hyperlinks in the phishing e-mails

In order to (illegally) collect useful information from potential victims, phishers generally tries to convince the users to click the hyperlink embedded in the phishing e-mail. A hyperlink has a structure as follows.

 Anchor text <\a>

where 'URI' (universal resource identifiers) provides the necessary information needed for the user to access the networked resource and 'Anchor text' is the text that will be displayed in user's Web browser. Examples of URIs are http://www.google.com, https://www.icbc.com.cn/login.html, ftp://61.112.1.90:2345, etc. 'Anchor text' in general is used to display information related to the URI to help the user to better understand the resources provided by the hyperlink. In the following hyperlink, the URI links to the phishing archives provided by the APWG group, and its anchor text "Phishing Archive" informs the user what's the hyperlink is about.

<a href"http://www.antiphishing.org/phishing archive.html"> Phishing Archive

Note that the content of the URI will not be displayed in user's Web browser. Phishers therefore can utilize this fact to play trick in their 'bait' e-mails. In the rest of the project, we call the URI in the hyperlink the actual link and the anchor text the visual link.

After analyzing the 203 (there are altogether 210 phishing e-mails, with 7 of them with incomplete information or with malware attachment and do not have hyperlinks) phishing email archives from Sep. 21st 2003 to July 4th 2005 provided by APWG . We classified the hyperlinks used in the phishing e-mail into the following categories:

1) The hyperlink provides DNS domain names in the

anchor text, but the destination DNS name in the visible link doesn't match that in the actual link. For instance, the following hyperlink:

<ahref+http://www.profusenet.net/checksession.php> "http://www.profusenet.net/checksession.php"> https://secure.regionset.com/EBanking/logon/ appears to be linked to secure.regionset.com, which is the portal of a bank, but it actually is linked to a phishing site www.profusenet.net.

2) Dotted decimal IP address is used directly in the URI or the anchor text instead of DNS name. See below for an example.

 SIGN IN

3) The hyperlink is counterfeited maliciously by using certain encoding schemes. There are two cases:

a)The link is formed by encoding alphabets into their corresponding ASCII codes. See below for such a hyperlink.

 www.citibank.com while this link is seemed pointed www.citibank.com, it actually points to http://4.34.195.41:34/l/index.htm.

b) Special characters (e.g. @ in the visible link) are used to fool the user to believe that the e-mail is from a trusted sender. For instance, the following link seems is linked to amazon, but it actually is linked to IP address 69.10.142.34.http://www.amazon.com:fvthsgbljhfcs83infoupdate @69.10.142.34.

4) The hyperlink does not provide destination information in its anchor text and uses DNS names in its URI. The DNS name in the URI usually is similar with a famous company or organization. For instance, the following link seems to be sent from paypal, but it actually is not. Since paypal-cgi is actually registered by the phisher to let the users believe that it has something to do with paypa <a href= "http://www.paypal-cgi.us/webscr.php?cmd=LogIn"> Click here to confirm your account

5) The attackers utilize the vulnerabilities of the target Web site to redirect users to their phishing sites or to launch CSS (cross site scripting) attacks. For example, the following link <a href="http://usa.visa.com/track/dyredir.jsp?rDirl= http://200.251.251.10/.verified/"> Click here <a> Once clicked, will redirect the user to the phishing site 200.251.251.10 due to a vulnerability of usa.visa.com.

Table 1 summarizes the number of hyperlinks and their percentages for all the categories. It can be observed that most of the phishing e-mails use faked DNS names (category 1,44.33%) or dotted decimal IP addresses (category 2, 41.87%). Encoding tricks are also frequently used (category 3a and 3b,17.24%). And phishing attackers often try to fool users by setting up DNS names that are very similar with the real ecommence sites or by not providing Destination information in the anchor text (category 4). Phishing attacks that utilize the vulnerability of Web sites (category 5) are of small number (2%) and we leave this type of attacks for future study.

Note that a phishing hyperlink can belong to several categories at the same time. For instance, an attacker may use tricks from both categories 1 and 3 at the same time to increase his success chance. Hence the sum of percentages is larger than 1.

Category	Number of Links	Percentage
1	90	44.33%
2	85	41.85%
3.a	19	9.36%
3.b	16	7.8%
4	67	33%
5	4	2%

TABLE I

THE CATEGORIES OF HYPERLINKS IN PHISHING E-MAILS.

Once the characteristics of the phishing hyperlinks are understood, we are able to design anti-phishing algorithms that can detect known or unknown phishing attacks in real-time. We present our LinkGuard algorithm in the next subsection.

B. The LinkGuard algorithm

LinkGuard works by analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted site. The algorithm is illustrated in Fig. 1. The following terminologies are used in the algorithm.

v_link: visual link;
a_link: actual_link;
v_dns: visual DNS name;
a_dns: actual DNS name;
sender_dns: sender'sDNS name.

```
int LinkGuard(v_link, a_link} {
1 v_dns = GetDNSName(v_link);
2 a_dns = GetDNSName(a_link);
3 if ((v_dns and a_dns are not
4 empty) and (v_dns != a_dns))
5 return PHISHING;
6 if (a_dns is dotted decimal)
7 return POSSIBLE_PHISHING;
8 if(a_link or v_link is encoded)
9 {
10 v_link2 = decode (v_link);
11 a_link2 = decode (a_link);
12 return LinkGuard(v_link2, a_link2);
13 }
```

```
14 /* analyze the domain name for
15 possible phishing */
16 if(v_dns is NULL)
17 return AnalyzeDNS(a_link);
}
```

Fig. 1. Description of the LinkGuard algorithm.

The LinkGuard algorithm works as follows. In its main routine *LinkGuard*, it first extracts the DNS names from the actual and the visual links (lines 1 and 2). It then compares the actual and visual DNS names, if these names are not the same, then it is phishing of category 1 (lines 3-5). If dotte decimal IP address is directly used in actual dns , it is then a possible phishing attack of category 2 (lines 6 and 7). We will delay the discussion of how to handle possible phishing attacks later. If the actual link or the visual link is encoded

```
int AnalyzeDNS (actual_link) {
/* Analyze the actual DNS name according
to the blacklist and whitelist*/
18 if (actual_dns in blacklist)
19 return PHISHING;
20 if (actual_dns in whitelist)
21 return NOTPHISHING;
22 return PatternMatching(actual_link);
}
int PatternMatching(actual_link){
23 if (sender_dns and actual_dns are different)
24 return POSSIBLE_PHISHING;
25 for (each item prev_dns in seed_set)
26 {
27 bv = Similarity(prev_dns, actual_link);
28 if (bv == true)
29 return POSSIBLE_PHISHING;
30 }
31 return NO_PHISHING;
}
float Similarity (str, actual_link) {
32 if (str is part of actual_link)
33 return true;
34 int maxlen = the maximum string
35 lengths of str and actual_dns;
36 int minchange = the minimum number of
37 changes needed to transform str
38 to actual_dns (or vice verse);
39 if (thresh<(maxlen-minchange)/maxlen<1)
40 return true
41 return false;
}
```

Fig. 2. The subroutines used in the LinkGuard algorithm.

PatternMatching:

Pattern maching is designed to handle unknown attacks (blacklist/whitelist is useless in this case). For category 5 of the phishing attacks, all the information we have is the actual link from the hyperlink (since the visual link does not contain DNS or IP address of the destination site), which provide very little information for further analysis. In order to resolve this problem, we try two methods: First, we extract the sender email address from the e-mail. Since phishers generally try to fool users by using (spoofed) legal DNS names in the sender e-mail address, we expect that the DNS name in the sender address will be different from that in the actual link. Second, we proactively collect DNS names that are manually input by the user when she surfs the Internet and store the names into a *seed set*, and since these names are input by the user by hand, we assume that these names are trustworthy. *PatternMatching*
then checks if the actual DNS name of a hyperlink is different from the DNS name in the sender's address (lines 23 and 24), and if it is quite similar (but not identical) with one or more names in the *seed set* by invoking the *Similarity* (lines 25-30) procedure.

Similarity checks the maximum likelihood of actual dns and the DNS names in *seed set*. As depicted in Fig. 2, the similarity index between two strings are determined by calculating the minimal number of changes (including insertion, deletion, or revision of a character in the string) needed to transform a string to the other string. If the number of changes is 0, then the two strings are identical; if the number of changes is small, then they are of high similarity; otherwise, they are of low similarity. For example, the similarity index of 'Microsoft' and 'micr0s0ft' is 7/9 (since we need change the 2 '0's in micr0s0ft to 'o'. Similarly, the similarity index of 'paypal' and 'paypal-cgi' is 6/10 (since we need to remove the last 4 chars from paypal-cgi), and the similarity index of '95559' and '955559' is 5/6 (since we need to insert a '5' to change '95559' to '955559').

B. False positives and false negatives handling

Since LinkGuard is a rule-based heuristic algorithm, it may cause false positives (i.e., treat non-phishing site as phishing site) and false negatives (i.e., treat phishing site as nonphishing site). In what follows, we show that LinkGuard may result in false positives but is very unlikely to cause harmful false negatives.

For phishing attacks of category 1, we are sure that there is no false positives or false negatives, since the DNS names of the visual and actual links are not the same. It is also easy to observe that LinkGuard handles categories 3 and 4 correctly since the encoded links are first decoded before further analysis.

For category 2, LinkGuard may result in false positives, since using dotted decimal IP addresses instead of domain names may be desirable in some special circumstances (e.g., when the DNS names are still not registered). For category 5,

LinkGuard may also result in false positives. For example we know that both 'www.iee.org' and 'www.ieee.org' are legal Web sites. But these two DNS names have a similarity index of 3/4, hence is very likely to trigger a false positive.

When it is a possible false positive, LinkGuard will return a POSSIBLE PHISHING. In our implementation (which will be described in the next section), we leverage the user to judge if it is a phishing attack by prompting a dialogue box with detailed information of the hyperlink. The rationale behind this choice is that users generally may have more knowledge of a link than a computer in certain circumstances (e.g., the user may know that the dotted decimal IP address is the address of his friend's computer and that www.iee.org is a respected site for electrical engineers).

For category 5, LinkGuard may also result in false negatives. False negatives are more harmful than false positives, since attackers in this case will succeed in leading the victim to the phishing sites. For instance, when the sender's e-mail address and the DNS name in the actual link are the same and the DNS name in the actual link has a very low similarity index with the target site, LinkGuard will return NO PHISHING. For instance, PatternMatching will treat the below link as NO PHISHING.

<ahref="http://fdicsecure.com/application.htm">
Click here

with "securehq@fdic-secure.com" as the sender address. We note that this kind of false negatives is very unlikely to result in information leakage, since the end user is very unlikely to have information the attack interested (since the DNS name in this link is not similar with any legal Web sites).

IV. IMPLEMENTATION AND VERIFICATION OF LINKGUARD

We have implemented the LinkGuard algorithm in Windows XP. It includes two parts: a whook.dll dynamic library and a LinkGuard executive. The structure of the implementation is depctied in Fig 3

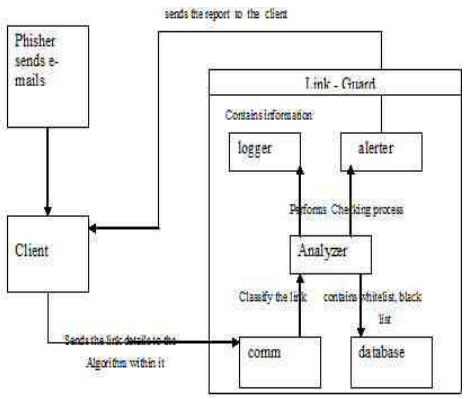


Fig. 3. Link Guard Alogrithm

whook is a dynamic link library, it is dynamically loaded into the address spaces of the executing processes by the operating system. whook is responsible for collecting data, such as the called links and visual links, the user input URLs. More specifically, whook.dll is used to: 1) install a BHO (browser helper object) for IE to monitor user input URLs; 2) install an event hook with the *SetWinEventHook* provided by the Windows operating system to collect relevant information; 3) retrieve sender's e-mail address from Outlook; 4) analyze and filter the received windows and browser events passed by the BHO and the hook, and pass the analyzed data to the LinkGuard executive.

LinkGuard is the key component of the implementation. It is a stand alone windows program with GUI (graphic user interface). Analyzer, Alerter, Logger, Comm, and Database. The functionalities of these 5 parts are given below:

Comm: Communicate with the whook.dll of all of the monitored processes, collect data related to user input fromother processes (e.g. IE, outlook, firefox, etc.), and sendthese data to the Analyzer, it can also send commands (suchas block the phishing sites) from the LinkGuard executiveto whook.dll. The communication between the LinkGuardprocess and other processes is realized by the shared memory mechanism provided by the operating system.

Database: Store the whitelist, blacklist, and the user inputURLs.

Analyzer: It is the key component of LinkGuard, whichimplements the LinkGuard algorithm,. It uses data provided by Comm and Database, and sends the results to the Alertand Logger modules.

Alerter: When receiving a warning messages from Analyzer, it shows the related information to alert the users and send back the reactions of the user back to the Analyzer.

Logger: Archive the history information, such as user events, alert information, for future use.

After implemented the LinkGuard system, we have designed experiments to verify the effectiveness of our algorithm. Since we are interested in testing Link Guard's ability to detect unknown phishing attacks, we set both whitelist and blacklistto empty in our experiments. Our experiments showed that PhishgGuard can detect 195 phishing attacks out of the 203APWG archives (with detection rate 96%). For the 8 undetected attacks, 4 attacks utilize certain Web site vulnerabilities. Hence the detecting rate is higher than 96% if category 5 is notincluded. Our experiment also showed that our implementation used by small amount of CPU time and memory space of the system. In a computer with 1.6G Pentium CPU and 512MBmemory, our implementation consumes less than 1% CPU time and its memory footprint is less than 7MB.Our experiment only used the phishing archive provided by APWG as the attack sources. We

are planning to use LinkGuard in daily life to further evaluate and validate its effectiveness. Since we believe that a hybrid approach may be more effective for phihsing defense, we are also planning to include a mechanism to update the blacklist and whitelist in real-time.

V. CONCLUSION

Phishing has becoming a serious network security problem,causing finical lose of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally,phishing has made e-commerce distrusted and less attractive to normal consumers. In this paper, we have studied the characteristics of the hyperlinks that were embedded in phishinge-mails. We then designed an anti phishing algorithm, Link-Guard, based on the derived characteristics. Since Phishig-Guard is characteristic based, it can not only detect known attacks, but also is effective to the unknown ones. We have implemented LinkGuard for Windows XP. Our experiment showed that LinkGuard is light-weighted and can detect upto 96% unknown phishing attacks in real-time. We believe that LinkGuard is not only useful for detectingphishing attacks, but also can shield users from maliciousor unsolicited links in Web pages and Instant messages. Our future work includes further extending the LinkGuard algorithm, so that it can handle CSS (cross site scripting) attacks.

VI. ACKNOWLEDGEMENT

We express our sincere thanks to **SJCET** providing us good lab facilities. A heart full and sincere gratitude to our beloved parents and friend for their tremendous motivation and moral support.

VII. REFERENCES

[1] I. Androutsopoulos, J. Koutsias, K.V. Chandrinos, and C.D. Spyropoulos.An Experimental Comparison of Naive Bayesian and Keyword-Based Anti-Spam Filtering with Encrypted Personal E-mail Message.In *Proc. SIGIR 2000*, 2000.

[2] The Anti-phishing working group. http://www.antiphishing.org/.

[3] Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C.Mitchell. Client-side defense against web-based identity theft. In *Proc.NDSS 2004*, 2004.

[4] Cynthia Dwork, Andrew Goldberg, and Moni Naor. On Memory-BoundFunctions for Fighting Spam. In *Proc. Crypto 2003*, 2003.

[5] EarthLink.ScamBlocker. http://www.earthlink.net/software/free/toolbar/.

[6] David Geer. Security Technologies Go Phishing. *IEEE Computer*,38(6):18–21, 2005.

[7] John Leyden. Trusted search software labels fraud sites 'safe'.http://www.theregister.co.uk/2005/09/27/untrusted search/.

[8] Microsoft. Sender ID Framework. http://www.microsoft.com/ mscorp/safety/technologies/senderid/default.mspx.

[9] Net craft toolbar. http://toolbar.netcraft.com/.

[10] PhishGuard.com. Protect Against Internet Phishing Scams .http://www.phishguard.com/.

[11] Jonathan B. Postel. Simple Mail Transfer Protocol. RFC821http://www.ietf.org/rfc/rfc0821.txt.

[12] Georgina Stanley. Internet Security - Gone phishing.http://www.cyota.com/news.asp?id=114.

[13] Meng Weng Wong. Sender ID SPF. http://www.openspf.org/whitepaper.pdf.

Implementation of new technique to detect occurrence of undesired events in sensitive systems

Parthasarathi.G

Department of Computer science and engineering
Velammal engineering college, Chennai, TN

Abstract- Surveillance in real time needs continuous monitoring of systems by the individual directly or via a camera. This is wastage of human resource which can be used for some other beneficiary purposes. Constant monitoring and recording is used in the existing systems. Instead of recording and saving continuously in memory, This paper proposed system will record and stores that video in separate storage area when a particular selected object is moved .A Background-modeling algorithm is described for segmenting moving objects from the background, which is capable of adapting to dynamic scene conditions, as well as determining shadows of the moving objects. Then the object association between consecutive frames is done. After that activity analysis and object identification is done. In order to recognize the nature of an event occurring in a scene, hidden Markov models can be utilized and to do it object trajectories, which are obtained through a successful track, are written as a sequence of flow vectors that capture the details of instantaneous velocity and location information. Color structure and homogeneous texture parameters of the independently moving objects are extracted and classifiers, such as Support Vector Machine (SVM) and Bayesian plug-in (Mahalanobis distance), are utilized to test the performance of the proposed person identification mechanism.

Keywords- *Moving Object Detection, Object Tracking, Event Recognition, Object Identification, SVM, HMM.*

I. INTRODUCTION:

In recent years, with the latest technological advancements, there has been a lot of increase in the crime rate. One of the main reason o avoid this is we have to provide a good surveillance system. Now-a-days most of the system we provide has a camera and again a person has to monitor it. Old-fashioned security systems were vastly relying on human labor instead of system hardware or software. So it will be better if we have some mechanism to track the undesired motion and trigger the necessary actions. This in urn saves human resources. This mainly consists of hree major jobs. First moving object detection,second Object tracking and last event recognition. Moving object detection is detecting changes in image sequences of the same scene, captured at different times. This is important since Video surveillance is among the important applications, which require reliable detection of changes in the scene. There are several different approaches for such a detection problem. First one is frame differencing, where change mask is computer based on the difference in the frames. The model for the background is simply equal to the previous frame.

if $|I(x,y,t)-I(x,y,t)|<$threshold
$m(x,y,t)=0$
if $|I(x,y,t)-I(x,y,t-1)|<$threshold
$m(x,y,t)=1$
where,
$I(x,y,t)$ is the intensity at pixel location (x,y) at time t.
Threshold is the threshold value.
$m(x,y,t)$ is the change mask obtained after thresholding.
It is quite fast and has adaptation ability to the changes n the scene, it has a relatively low performance in dynamic scene conditions and its results are very sensitive to the threshold value. Second approach is Moving Average Filtering where a fixed initial frame is used as a reference. Instead of using the previous frame, a single frame, which does not include any moving objects, can also be used as a reference.

$m(x,y,t)=0$ if $|I(x,y,t)-Iref|<$threshold
$m(x,y,t)=1$ if $|I(x,y,t)-Iref)|<$threshold
where,

$I(x,y,t)$ is the intensity at pixel location (x,y) at time t.
Threshold is the threshold value .
$m(x,y,t)$ is the change mask obtained after thresholding.
Iref is initial image sequence and its update equation is given by,
$Iref(t)=a*I(x,y,t-1)+(1-a)*Iref(t-1)$
a is learning factor.

This method is also not suitable for multimodal distribution. Since it is highly dependent on threshold.
Third one is hierarchical parzen window which used a window function to compute the change mask.This method overcomes all the disadvantages of the above methods and this will produce good results. Obtaining the correct track information of the moving objects is crucial for subsequent actions, like event modeling and activity recognition. For this purpose, many different types of tracking algorithms have been proposed. Most of these algorithms can be listed under the following 4 different groups: model-based, region-based, contour -based and feature based algorithms. Model-based algorithms track objects by the aim of fitting them into a predetermined model. The models rely upon prior knowledge about the nature of the object and the scene under consideration. An obvious disadvantage of this type of tracking is the need for prior information about all

the objects that might appear in the observed environment. Region-based approaches extract relevant object information like color or texture from regions and track these regions by utilizing such information Unlike other tracking methods, contour-based approaches rely on the contour information of the moving object instead of the whole set of pixels inside the object region. Object boundaries are extracted and updated in successive frames and a simpler representation is achieved in this way.
The performance of such a tracker is quite sensitive to initialization, making it difficult to adapt to an automated surveillance system. Feature-based approaches aim to find and track relevant features of the object like perimeter, area of the object region or more local features, like corners or vertices inside a given region. Event recognition is probably the ultimate purpose of a fully automated surveillance system. Even though it is quite important and useful to recognize an activity, it is not easy to define the type of motion that is interesting and meaningful within surveillance context. So we construct a flow vector consisting of the moving object's position and velocity. Hence every motion consists of a sequence of flow vectors. Any undesired action can be specified by means sequence of flow vector and if that sequence occurred, the required actions are triggered.

II. LITERATURE SURVEY:

In this modern world there are many systems that are existing for motion tracking as well as for the surveillance systems. Most of the system does not track the object perfectly or they are not efficient in many aspects. Some of the systems that are available are able to track the motion properly but they take a lot of resources for processing. Certain systems follow store and track policies, while other systems follow complete storage concepts for tracking with the poor efficiency of the tracking. In the store and track system the entire video is recorded first and after a delay period tracking process will be done, so immediate event recognition will not be present and due to this reason it cannot be implemented in high security surveillance systems. Whereas in the later case the tracking will be done instantly but this takes the usage of more resources, making the system costlier and as the complete recording is done more storage is required. In the proposed system when an abnormal event (detected using this method) is occurred from that point of time the video is stored to a separate storage space.

III. PROPOSED SYSTEM:

A. Moving Object Detection:
Images of the same scene are acquired in time by a static camera and the aim is to detect changes between consecutive frames. Pixels that have a significant difference compared to the previous ones are marked as foreground pixels, whereas other pixels are labeled as background, resulting in a change mask. This is done through the Hierarchical Parzen window-based moving object detection
B. Hierarchical Parzen Window: This approach depends on non parametrically estimating the probability of observing pixel intensity values, based on the sample intensities. An estimate of the pixel intensity can be obtained by,]
$P(x)=(1/n)\sum f(x-xk)$
where
set {x1, x2, …, xN} gives the sample intensity values in the temporal history of a particular pixel in the image and the function.
f(.) is the window function.
Window function gives a measure for the contribution of each sample in the estimate of p(x).
It can be of any function even Gaussian function.It = consists of mainly two stages. At stage 1, we decide whether a pixel is background or foreground using the following calculation. P(x) > threshold, it is taken as background. P(x)<threshold, it is taken as foreground.
At stage 2, by using the sample history of the neighbors of pixel (instead of its own history values), the following probability value is Calculated,
PN (x) =max y=N(x) p(x | B y)
where,
N(x) defines a neighborhood of the pixel x .
By is the sample intensity values in the temporal history of y where y∈ N(x).
PN can be defined as the pixel displacement probability .

Probability
PN can be defined as the pixel displacement probability and it is the maximum probability that the observed value is the part of the background distribution of some point in the neighborhood of x. A similar calculation is performed on foreground pixels by using the history of y instead of x. After thres holding, a pixel can be decided to be a part of a neighboring pixel's background distribution. This approach reduces false alarms due to dynamic scene effects, such as tree branches or a flag waving in the wind

C. Noise Removal using Morphological Operators (Erosion):

Morphological operators work usually on binary images by using a structuring element and a set operator (intersection, union, etc). Structuring element determines the details of the operations to be performed on the input image. Generally, the structuring element is 3×3 in size and has its origin at the center pixel. It is shifted over the image and at each pixel of the image its elements are compared with the ones on the image. If, for each pixel having a value "1" in the structuring element, the corresponding is a foreground pixel, then the input pixel is not changed. However, if any of the surrounding pixels belong to the background, the input pixel is also set to background value. As a result foreground regions shrink and holes inside a region grow.

D. Connected Component Labeling (CCL):

Connected component labeling groups pixels in an image into components based on pixel connectivity. To identify the different objects in an image. Each object is given a label. a)Algorithm:

1. Image is scanned
2. If the pixel under consideration is a foreground pixel (having value 1)
a. If one of the pixels on the left, on the mupper-left, on top or on the upper right is labeled, this label is copied as the label of the current pixel.

b. If two or more of these neighbors has a label, one of the labels is assigned to the current pixel and all of the labels are marked as equal (as being in the same group) and an equivalence table is formed.
c. If none of the neighbors has a label, current pixel is given a new label
3. All pixels on the image are scanned considering the rules defined in Step 2.
4. Classes representing the same group of pixels in the equivalence table are merged and given a single label.
5. Image is scanned once more to replace old labels with the new ones. All isolated groups of pixels are given a distinct label as a result of the algorithm

E. Shadow Removal:

Shadow removal is done in the change mask matrix. This is done using the formula

$Is(x,y) = \alpha I(x,y)$, $\alpha < 1$
where ,
I(x,y) is the intensity value at point (x,y)
Is(x,y) denotes the value after shadow at point (x,y) .
The foreground pixels, having intensity values different from the background, but color values that are close to background values, are labeled as shadow region.

F. Object Tracking:

After the object segmentation is achieved, the problem of establishing a correspondence between object masks in consecutive frames should arise. Indeed, initializing a track, updating it robustly and ending the track are important problems of motion tracking. Hence a method to match the object between two image sequences is necessary. So we use bounding box method and match matrix method for this purpose. After connected component labeling is applied, the bounding boxes and centroids of the moving objects can be easily obtained. The bounding box of the mask of an object in the previous frame is compared to the bounding boxes of the masks in the current frame. A metric, yielding the percentage of the overlapping regions of the boxes, provides a measure for associating the masks in two consecutive frames. Object velocity (distance between centroids of two regions) is recorded at each frame . Occurrence of motion is found using the following algorithm.

If (Box Overlapping (Bi (t), B j(t -1) +v (t -1)) >threshold)
then Oi (t)=Oj (t) // no movement
Else
Oi (t)!=Oj (t) //a significant movement is there.

Where,
Oi (t): Object i at time t (current frame)
Oj (t): Object j at time t-1 (previous frame)
Bi (t): Bounding box of object i at time t
Bj(t-1): Bounding box of object j at time t-1
v j(t -1):Velocity of the object j at time t-1

During each frame sequence ,match matrix field is updated. Match matrix, M, is an mxn matrix denoting the matches between objects in consecutive frames "1" value at position Mij means that object i of the previous frame can be associated with object j of the current frame. Conversely, if the entry has a value of "0", there is no matching between objects i and j.
Where, m is the number of objects in previous frame (at time=t-1) and n is the number of objects in current frame (at time=t).

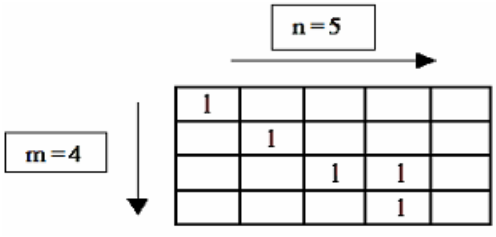


Fig 1 : Match matrix

Observing the arrangement of M, one can see that more than one entry in a row or in a column might obtain a value of 1. In some cases, a row or a column may not have a single match at all. In general seven cases are been observed.

Case1:

- No "1" value in a column means a new object does not match any of the old objects known by the system.
- In this case a new track is initialized for the new object.

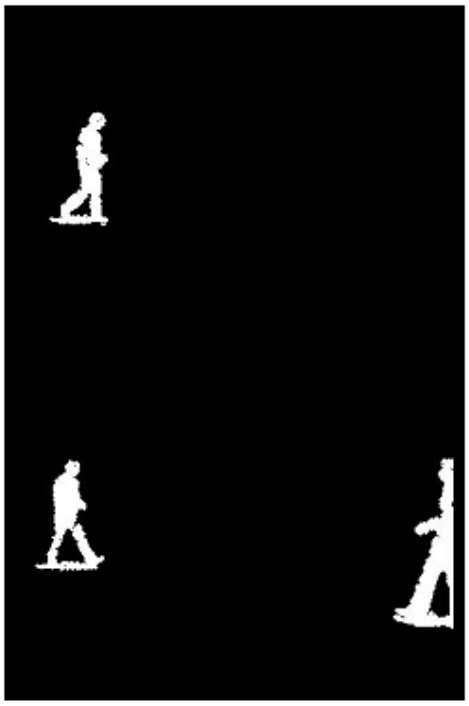


Fig 2 :A new object appeared in the scene.

Case2:

- Single "1" value in a column stands for the situation in which a new object has only a single match. This is the desired tracking result

Fig 3 :Single object moves from frame1 to frame2.

Case3:

- More than a single "1" value in a column means a new object matches with more than one old object.
- This situation can be observed, if isolated objects come together to form a group.

Fig 4 :Two objects in the previous frame merged into single object in frame2.

Case4:

- No "1" value in a row stands for the situation in which a previous object does not have a match in the current frame.
- This situation may occur when the moving target is temporarily blocked by another object in the scene or when the target leaves the scene.

Case 5:

- Single "1" value in a row means a previous object has only a single match in the current frame. This is the same situation described in column single match case.

Case 6:

- More than a single "1" value in a row means a previous object has more than one match among the objects in the current frame.
- The first reason is the splitting of object cparts. The second case is the splitting of group objects that were previously merged

G. EVENT RECOGNITION:

Fig 5: Movement of vehicles in the road.

By now we have formulated a method to track moving objects in the scene which is not our goal. For surveillance system it is not necessary to detect any motion but detection of "abnormal" motion patterns should be the ultimate aim of every robust surveillance system. For ex in one-way road, the undesired motion can be a vehicle moving in a wrong way. So the next step is event reorganization. Once tracking of an object is successfully achieved, its trajectory information is obtained for every point it has visited. This information involves the position of the centroid and object's instantaneous velocity at each point, which are then utilized to construct a flow vector, f:f (x,y,vx,vy)

Initially abnormal sequence of flow vectors is provided. If that sequence is happened, the abnormal event it detected and the necessary event are triggered. If the initially abnorma sequence of flow vectors is unknown we used hidden markov model to compute the initial states. Hidden Markov model (HMM) is a statistical model where the system being modeled is assumed to be a Markov process. When an abnormal sequence is followed, the necessary actions are triggered. The action can be giving a alarm, locking the door, trigger a gunshot etc.

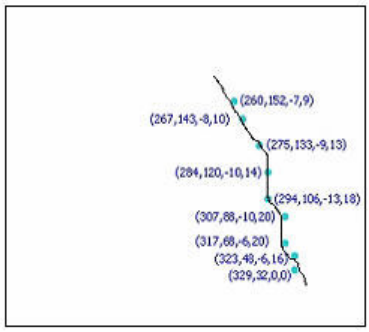


Fig 6: Flow vectors obtained for movement of vehicles in road.

IV. PERFORMANCE ANALYSIS:

Fig 7 : Input image.

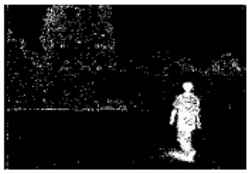


Fig 8: Frame Differencing

Fig 9: Moving Average Filtering

Fig 10: Hierarchical Parzen Windows

CONCLUSION :

There is an increasing demand for personal and public security systems. However, utilizing human resources in such systems builds up the expenses and wastes time and resources. Besides, technological devices are vastly available in this era. All of these factors indicate the inevitable utilization of automated systems. Hence this system is quite useful in many surveillance system and in many real time video tracking.

Table1:Performance Analysis

Method Name	Background separation (%)	Object Identification (%)	Noise level (%)
Frame Differencing	70	80	70
Moving Average Filtering	90	50	35
Hierarchical Parzen Window	98	96	10

VI. REFERENCES:

[1]. VSAM-PAMI Tracking-Learning Patterns of activities using real-time racking.(Artificial Intelligence Laboratory, MIT,USA)

[2]. Digital Image Processing Using Matlab - Gonzalez Woods & Eddins

[3]. Digital Signal and Image Processing Using MATLAB - Gerard Blanchet & Maurice Charbit.

[4]. B. Orten, M. Soysal, A. A. Alatan, "Person Identification in Surveillance Video by Combining MPEG-7 Experts." WIAMIS 2005,Montreux.

[5]. Piccardi,M. "Background subtractiontechniques: a review." Systems, Man and Cybernetics, 2004 IEEE International Conference, Vol 4,2004.

[6]. Cavallaro, A.; Salvador, E.; brahimi, T., " Detecting shadows in image sequences." Visual Media Production, 15-16 March 2004. [7].J. D. Shutler, M. S. Nixon, and C. J. Harris, "Statistical gait recognition via temporal moments." Proc. IEEE Southwest Symp.Image Analysis and Interpretation, 2000.

[8]. A. Elgammal, D. Harwood, and L.S. Davis. "Non-parametric Modelfor Background Subtraction." In Proc. IEEE ICCV'99 FRAME-RATE Workshop, 1999.

[9]. C.R. Wren, A. Azarbayejani, T. Darrell, and A. Pentland, "Pfinder: Real-Time Tracking of the Human Body," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 19, no. 7, pp. 780-785, July 1997.

[10]. L. R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition." Proceedings of the

Lock-Free Producer-Consumer

[1]Ryan Saptarshi Ray & [2]Utpal Kumar Ray

[1&2]Department of Information Technology, Jadavpur University

Abstract— The past few years have marked the start of a historic transition from sequential to parallel computation. The necessity to write parallel programs is increasing as systems are getting more complex while processor speed increases are slowing down. Current parallel programming uses low-level programming constructs like threads and explicit synchronization using locks to coordinate thread execution. Parallel programs written with these constructs are difficult to design, program and debug. Also locks have many drawbacks which make them a suboptimal solution. Software Transactional Memory (STM) is a promising new approach to programming shared-memory parallel processors. It is a concurrency control mechanism that is widely considered to be easier to use by programmers than locking. It allows portions of a program to execute in isolation, without regard to other, concurrently executing tasks. A programmer can reason about the correctness of code within a transaction and need not worry about complex interactions with other, concurrently executing parts of the program. This paper shows the concept of writing code using Software Transactional Memory (STM) and the performance comparison of codes using locks with those using STM.

Keywords- *Parallel Programming; Multiprocessing; Locks; Transactions; Software Transactional Memory*

I. INTRODUCTION

Generally one has the idea that a program will run faster if one buys a next-generation processor. But currently that is not the case. While the next-generation chip will have more CPUs, each individual CPU will be no faster than the previous year's model. If one wants programs to run faster, one must learn to write parallel programs as currently multi-core processors are becoming more and more popular. The past few years have marked the start of a historic transition from sequential to parallel computation. The necessity to write parallel programs is increasing as systems are getting more complex while processor speed increases are slowing down. Parallel Programming means using multiple computing resources like processors for programming so that the time required to perform computations is reduced [**1**].

II. PRODUCER-CONSUMER PROBLEM USING LOCKS

The hardest problem that should be overcome when writing parallel programs is that of synchronization. Multiple threads may need to access the same locations in memory and if careful measures are not taken the result can be disastrous. If two threads try to modify the same variable at the same time, the data can become corrupt . Currently locks are used to solve this problem . Locks ensure that a critical section, which is a block of code that contains variables that may be accessed by multiple threads, can only be accessed by one thread at a time. When a thread tries to enter a critical section, it must first acquire that section's lock. If another thread is already holding the lock, the former thread must wait until the lock-holding thread releases the lock, which it does when it leaves the critical section [**2**].

In the producer-consumer problem there is a buffer of fixed size. In the examples below we have taken the buffer size as 100000000. Then multiple producers and consumers can access the buffer simultaneously to produce and consume elements from the buffer. The problem is to synchronize these accesses properly so that there is no discrepancy in the number of elements in the buffer. Maximum number of elements which can be produced is fixed by the buffer size and when the buffer is empty then no elements can be consumed.

The following code in Code Snippet 1 shows a parallel program using threads and locks which solves the producer-consumer problem:

```
#include <pthread.h>
#include<sys/time.h>
#include<stdio.h>
#include<stdlib.h>

#define MAXNTHREADS 4
#define BUF 100000000

unsigned long count=0, tra;
void *produce( );
void *consume( );
char a[BUF];
pthread_mutex_t
mutex=PTHREAD_MUTEX_INITIALIZER;

int main(int argc, char **argv)
{
   int arg_to_be_passed[MAXNTHREADS];
   struct timeval ini_tv, final_tv;
   pthread_mutex_init(&mutex,NULL);
   int i;
```

```
   pthread_t
tid_produce[MAXNTHREADS],tid_consume[MAX
NTHREADS];
   gettimeofday(&ini_tv,NULL);
    if(MAXNTHREADS==1)
   {
       for(i=0;i<MAXNTHREADS;i++)
       {
          arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_passed[i]);
       }
       for(i=0;i<MAXNTHREADS;i++)
       {
          pthread_join(tid_produce[i],NULL);
       }
   }
    else
   {
      for(i=0;i<MAXNTHREADS/2;i++)
      {
         arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_passed[i]);
       }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
       {
          arg_to_be_passed[i]=i;

pthread_create(&tid_consume[i],NULL,consume,&ar
g_to_be_passed[i]);
       }
       for(i=0;i<MAXNTHREADS/2;i++)
       {
          pthread_join(tid_produce[i],NULL);
       }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
       {
          pthread_join(tid_consume[i],NULL);
        }
   }
    printf("Transactions=%d\n",tra);
   gettimeofday(&final_tv,NULL);
   printf("Total Time Taken=%ld\n",final_tv.tv_sec-
ini_tv.tv_sec);
   exit(0);
}

void *produce(int *num_ptr)
{
   unsigned long j;
   int num, *number_ptr;
   number_ptr=num_ptr;
   num=*number_ptr;

for((j=(((num*BUF)/MAXNTHREADS)));j<(((num+
1)*BUF)/MAXNTHREADS;j++)
{
   if(count==BUF)
   continue;
   pthread_mutex_lock(&mutex);
   tra++;
   a[count ++]='VALUE';
   pthread_mutex_unlock(&mutex);
   }
   pthread_exit(0);
}

void *consume(int *num_ptr1)
{
    unsigned long k;
   int num1, *number_ptr1;
    number_ptr1=num_ptr1;
    num1=*number_ptr1;

for((k=(((num1*BUF)/MAXNTHREADS)));k<(((nu
m1+1)*BUF)/MAXNTHREADS;k++)
{
   if(count<0)
   continue;
   pthread_mutex_lock(&mutex);
   tra++;
   a[count --]='/0';
   pthread_mutex_unlock(&mutex);
   }
   pthread_exit(0);


}
```

Code Snippet 1: Parallel Program using threads and locks for solving producer-consumer problem

In the above program "produce" and "consume" are the two thread processes for adding and removing elements from the buffer respectively. Here the array a is the buffer. The global variable tra keeps track of the number of transactions and the global variable count keeps track of the number of elements in the buffer. The following statements mean that if there is only one thread then elements can only be produced.

```
if(MAXNTHREADS==1)
   {
       for(i=0;i<MAXNTHREADS;i++)
       {
          arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_paqssed[i]);
       }
      for(i=0;i<MAXNTHREADS;i++)
       {
```

```
        pthread_join(&tid_produce[i],NULL);
      }
   }
```

If the number of threads is greater than one then elements can both be produced and consumed. The following statements show the creation of threads and also ensure that even if any thread finishes its execution before other threads finish execution it has to wait till all other threads have finished their executions:

```
else
  {
      for(i=0;i<MAXNTHREADS/2;i++)
      {
        arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_paqssed[i]);
      }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
      {
        arg_to_be_passed[i]=i;

pthread_create(&tid_consume[i],NULL,consume,&ar
g_to_be_passed[i]);
      }
      for(i=0;i<MAXNTHREADS/2;i++)
      {
        pthread_join(&tid_produce[i],NULL);
      }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
      {
        pthread_join(&tid_consume[i],NULL);
      }
    }
```

In the thread “produce” elements are added to the buffer by the following statements. In each position of the buffer we store the string “VALUE” when an element is produced.

```
for((j=(((num*BUF)/MAXNTHREADS)));j<(((num+
1)*BUF)/MAXNTHREADS;j++)
{
  if(count==BUF)
  continue;
  pthread_mutex_lock(&mutex);
  tra++;
  a[count ++]=’VALUE’;
  pthread_mutex_unlock(&mutex);
}
```

In the thread “consume” elements are removed from the buffer by the following statements. In the corresponding position of the buffer where an element is removed we store the string “NULL”.

```
for((k=(((num1*BUF)/MAXNTHREADS)));k<(((nu
m1+1)*BUF)/MAXNTHREADS;k++)
{
  if(count<0)
  continue;
  pthread_mutex_lock(&mutex);
  tra++;
  a[count --]=’/0’;
  pthread_mutex_unlock(&mutex);
}
```

The following statement prints the total number of transactions in the program:

```
printf(“Transactions=%d\n”,tra);
```

The following statement is used to record the time before the threads are created:

```
gettimeofday(&ini_tv,NULL);
```

The following statement is used to record the time when all threads have just finished their executions:

```
gettimeofday(&final_tv,NULL);
```

The total time taken is then calculated and printed using the following statement:

```
printf("Total Time Taken = %ld\n", final_tv.tv_sec -
ini_tv.tv_sec);
```

As can be seen from the above figure, three lock calls are being used in this program. **pthread_mutex_init(&mutex1,NULL)** is used for lock initialization. **pthread_mutex_lock(&mutex1)** means that any thread must acquire the lock on mutex1 to execute the critical section following this function. **pthread_mutex_unlock(&mutex1)** is used for unlocking.

In this program the regions where more than one thread may access the global variables count and tra at the same time are the critical sections. Thus these regions are enclosed within locks. Hence there is no discrepancy among the number of elements in the buffer at any point of time.

III. PRODUCER-CONSUMER PROBLEM USING STM

The synchronization problem can also be solved using STM. If STM is used in a program then we do not have to use locks in the program. Thus the

problems which occur due to the presence of locks in a program do not occur in this type of code. The critical section of the program has to be enclosed within a transaction. Then STM by its internal constructs ensures synchronization in the program.
The following code in Code Snippet 2 shows a parallel program using threads and STM which solves the producer-consumer problem:

```
#include <pthread.h>
#include<sys/time.h>
#include<stdio.h>
#include<stdlib.h>
#include<time.h>
#include<atomic_ops.h>
#include<stm.h>

# define RO
# define RW 0
# define START( id , ro )
{ \
sigjmp_buf  * _ e = stm_getenv ( ) ; \
 stm_tx_attr_t  _a = { id , ro } ; \
sigset_jmp (*_ e , 0 ) ; \
 stm_start ( _e , & a )
 # define COMMIT stm_commit ( ) ; }
# define LOAD( addrofptr ) \
stm_load_ptr ( ( volatile void __) addrofptr )
# define STORE( addrofptr , value ) \
Stm_store_ptr ( ( volatile void __) addrofptr , \
( void _) v a l u e )

#define MAXNTHREADS 4
#define BUF 100000000

unsigned long count=0, tra;
void *produce( );
void *consume( );
char a[BUF];

int main(int argc, char **argv)
{
   stm_init( );
   int arg_to_be_passed[MAXNTHREADS];
   struct timeval ini_tv, final_tv;
   int i;
   pthread_t
tid_produce[MAXNTHREADS],tid_consume[MAX
NTHREADS];
   gettimeofday(&ini_tv,NULL);
   if(MAXNTHREADS==1)
   {
      for(i=0;i<MAXNTHREADS;i++)
      {
         arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_passed[i]);
      }
      for(i=0;i<MAXNTHREADS;i++)
      {
         pthread_join(tid_produce[i],NULL);
      }
   }
   else
   {
       for(i=0;i<MAXNTHREADS/2;i++)
      {
         arg_to_be_passed[i]=i;

pthread_create(&tid_produce[i],NULL,produce,&arg
_to_be_passed[i]);
      }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
      {
         arg_to_be_passed[i]=i;

pthread_create(&tid_consume[i],NULL,consume,&ar
g_to_be_passed[i]);
      }
      for(i=0;i<MAXNTHREADS/2;i++)
      {
          pthread_join(tid_produce[i],NULL);
      }

for(i=MAXNTHREADS/2;i<MAXNTHREADS;i++)
      {
         pthread_join(tid_consume[i],NULL);
      }
   }
   printf("Transactions=%d\n",tra);
   gettimeofday(&final_tv,NULL);
   printf("Total  Time  Taken=%ld\n",final_tv.tv_sec-
ini_tv.tv_sec);
   stm_exit( );
   exit(0);
}


void *produce(int *num_ptr)
{
   unsigned long byte_under_stm1;
   unsigned int byte_under_stm2;
   stm_init_thread( );
   unsigned long j;
   int num, *number_ptr;
   number_ptr=num_ptr;
   num=*number_ptr;

for((j=(((num*BUF)/MAXNTHREADS)));j<(((num+
1)*BUF)/MAXNTHREADS);j++)
   {
      if(count==BUF)
         continue;
      START(0,RW);
      a[count]='VALUE';
  byte_under_stm1=(unsigned long)LOAD(&count);
```

```
      byte_under_stm2=(unsigned int)LOAD(&tra);
      byte_under_stm1++;
      byte_under_stm2++;
      STORE(&count, byte_under_stm1);
      STORE(&tra, byte_under_stm2);
      COMMIT;
   }
   stm_exit_thread( );
   pthread_exit(0);
}

void *consume(int *num_ptr1)
{
    unsigned long byte_under_stm3;
   unsigned int byte_under_stm4;
   stm_init_thread( );
  unsigned long k;
   int num1, *number_ptr1;
    number_ptr1=num_ptr1;
    num1=*number_ptr1;

for((k=(((num1*BUF)/MAXNTHREADS)));k<(((nu
m+1)*BUF)/MAXNTHREADS);k++)
   {
       if(count<0)
          continue;
      START(0,RW);
      a[count]='/0';
      byte_under_stm3=(unsigned
long)LOAD(&count);
      byte_under_stm4=(unsigned int)LOAD(&tra);
       byte_under_stm3--;
      byte_under_stm4++;
      STORE(&count, byte_under_stm3);
      STORE(&tra, byte_under_stm4);
      COMMIT;
   }
   stm_exit_thread( );
   pthread_exit(0);

}
```

Code Snippet 2: Parallel Program using threads and STM for solving producer-consumer problem

The program structure is same as that of the program for producer-consumer problem using threads and locks. The only difference is that STM is being used in this program.

stm_init is used to initialize the TinySTM library at the outset. It is called from the main thread before accessing any other functions of the TinySTM library.

stm_init_thread is used to initialize each thread that will perform transactions. It is called once from each thread that performs transactional operations before the thread calls any other functions of the TinySTM library. In this program it is called from the threads **produce** and **consume**.

stm_exit is the corresponding shutdown function for stm_init. It cleans up the TinySTM library. It is called once from the main thread after all transactional threads have completed execution.

stm_exit_thread is the corresponding shutdown function for stm_init_thread. It cleans up the transactional thread. It is called once from each thread that performs transactional operations upon exit. In this program it cleans up the threads **produce** and **consume**.

START(0,RW) is used to start a transaction. In this program it is used in the threads **produce** and **consume**.

COMMIT is used to close the transaction. In this program it is used in the threads **produce** and **consume**.

byte_under_stm1=(unsigned long)LOAD(&count) stores the value of count in byte_under_stm1. In this program it is used in the thread **produce**.

byte_under_stm2=(unsigned int)LOAD(&tra) stores the value of tra in byte_under_stm2. In this program it is used in the thread **produce**.

byte_under_stm3=(unsigned long)LOAD(&count) stores the value of count in byte_under_stm3. In this program it is used in the thread **consume**.

byte_under_stm4=(unsigned int)LOAD(&tra) stores the value of tra in byte_under_stm4. In this program it is used in the thread **consume**.
STORE(&count, byte_under_stm1) stores the value of byte_under_stm1 in count. In this program it is used in the thread **produce**.

STORE(&tra, byte_under_stm2) stores the value of byte_under_stm2 in tra. In this program it is used in the thread **produce**.

STORE(&count, byte_under_stm3) stores the value of byte_under_stm3 in count. In this program it is used in the thread **consume**.

STORE(&tra, byte_under_stm4) stores the value of byte_under_stm4 in tra. In this program it is used in the thread **consume**.

In this program the regions where more than one thread may access the global variables count and tra at the same time are the critical sections. Thus these regions are enclosed within transactions using

TinySTM which is a type of STM. Hence there is no discrepancy among the number of elements in the buffer at any point of time.

IV. CONCLUSION

STM has been shown in many ways to be a good alternative to using locks for writing parallel programs. STM provides a timetested model for isolating concurrent computations from each other. This model raises the level of abstraction for reasoning about concurrent tasks and helps avoid many parallel programming errors.

This paper has discussed how STM can be used to solve the problem of synchronization in parallel programs. STM has ensured that lock-free parallel programs can be written. This ensures that the problems which occur due to the presence of locks in a program do not occur in this type of code.

Many aspects of the semantics and implementation of STM are still the subject of active research. While it may still take some time to overcome the various drawbacks, the necessity
for better parallel programming solutions will drive the eventual adoption of STM. Once the adoption of STM begins it will have the potential to pick up momentum and make a very large impact on software development in the long run. In the near future STM will become a central pillar of parallel programming.

REFERENCES

[1] Simon Peyton Jones, “Beautiful concurrency”.

[2] Elan Dubrofsky, “A Survey Paper on Transactional Memory”.

[3] Pascal Felber, Christof Fetzer, Torvald Riegel, “Dynamic Performance Tuning of Word-Based Software Transactional Memory”.

[4] http://en.wikipedia.org/wiki/Transactional_memory

[5] James Larus and Christos Kozyrakis. “Transactional Memory”

[6] Pascal Felber, Christof Fetzer, Patrick Marlier, Torvald Riegel, “Time-Based Software Transactional Memory”

[7] Tim Harris, James Larus, Ravi Rajwar, “Transactional Memory”

[8] Mathias Payer, Thomas R. Gross, “Performance Evaluation of Adaptivity in Software Transactional Memory”

[9] Kevin E. Moore, Jayaram Bobba, Michelle J. Moravan, Mark D. Hill, David A. Wood., “LogTM: Log-based Transactional Memory”

[10] Dave Dice , Ori Shalev , Nir Shavit., “Transactional Locking II”

[11] http://tmware.org

[12] Maurice Herlihy, J. Eliot B. Moss, “Transactional Memory: Architectural Support for Lock-Free Data Structures”.

[13] Martin Schindewolf, Albert Cohen, Wolfgang Karl, Andrea Marongiu, Luca Benini, **“**Towards Transactional Memory Support for GCC”.

[14] Virendra J. Marathe, Michael F. Spear, Christopher Heriot, Athul Acharya, David Eisenstat, William N. Scherer III, Michael L. Scott, “Lowering the Overhead of Nonblocking Software Transactional Memory”.

[15] Utku Aydonat, Tarek S. Abdelrahman, Edward S. Rogers Sr., “Serializability of Transactions in Software Transactional Memory”.

[16] Maurice Herlihy, Nir Shavit, “The Art of Multiprocessor Programming”.

[17] Brendan Linn, Chanseok Oh, “G22.2631 project report: software transactional memory”.

[18] http://en.wikipedia.org/wiki/Software_transactional_memory

[19] http://research.microsoft.com/~simonpj/papers/stm/

[20] http://www.haskell.org/haskellwiki/Software_transactional_ memory.

A Review of Speaker Identification System Using Wavelet Transformation Technique

[1]**Jignya Jadav**, [2]**Sneha Sarda &** [3]**Rajesh Prasad**

[1&2]Dept. of Computer Engg. V.I.I.T., Pune – 411048. University of Pune, India
[3]Dept. Of Computer Engg, ZES's DCOER, India.

Abstract – Speaker identification is the field where we try to identify a person based on his spoken words. This paper surveys the working of a speaker identification system. This system makes use of signal processing techniques for feature extraction from speech signal. Our objective is used to study the feature extraction process for a text – independent speaker identification system. In this paper, a study of wavelet transforms technique for feature extraction for a text independent speaker identification system is presented. Wavelet Transforms is a multi-resolution technique which is been used for feature extraction which results in improved feature extraction. A survey about wavelet analysis is been made that would enable us to develop a more efficient speaker identification system.

Keywords – *Biometrics system, Speaker Identification System, Feature Extraction Process, Wavelet Transform, Multi-resolution Analysis.*

I. INTRODUCTION

Speaker recognition is a biometric task that uses a person's voice for recognition purposes. Speaker recognition is based on both, the physical structure of an individual's vocal tract and the behavioural characteristics of an individual. Speaker recognition has mainly two applications: - speaker identification and speaker verification. Speaker identification is the process of determining from which of the registered speakers a given utterance comes. Speaker verification refers to whether or not the speech samples belong to some specific speaker [1].

Speaker identification can be further classified as, text dependent speaker identification and text independent speaker identification. In text-dependent speaker identification, speaker speaks a specific phrase or a word whereas in text-independent speaker identification, speaker can speak anything.

The identification process includes comparing the features of speaker with that of a set of valid speakers already enrolled with the system. The simplified model of speaker identification system is illustrated in figure 1.

The two main modules of speaker identification system are feature extraction and feature matching. The main focus of feature extraction is to convert speech waveform into parametric representation for further analysis which is often referred to as signal processing front end. In feature matching, the features extracted from the input speech are matched with the stored template and recognition is made.

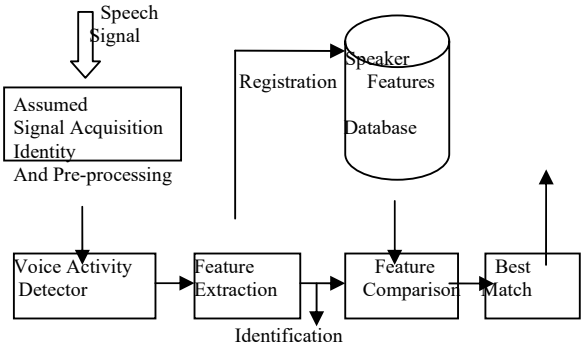


Figure 1: Speaker Identification System

All audio techniques start by converting the raw speech signal into sequences of acoustic feature vector carrying distinct information about the signal [2]. The most commonly used acoustic vectors are Mel Frequency Coefficients (MFCC), Linear Prediction Cepstral Coefficient (LPCC) Coefficient. In MFCC feature representation, the Mel frequency scale is used to get a high resolution in low frequency region, and a low resolution in high frequency region. This kind of processing is good for obtaining stable phonetic information, but not suitable for speaker features that are located in high frequency regions. The speaker individual information, which is non-uniformly distributed in the high frequencies, is equally important for speaker recognition. Based on this fact, multi-resolution capabilities of wavelet transform are used to derive the new features.

The rest of the paper is organized as follows: literature survey is given in section II. Speaker recognition process is described in Section III. Review of wavelet transform is stated in Section IV.

The proposed feature extraction process is described in Section V. Finally Conclusion and Future work are outlined in section VI.

II. BACKGROUND

A considerable amount of work has been carried out in the speaker-recognition field. Researches of several enterprises and universities have come up with various models of speaker-recognition systems. Those institutions include AT&T and its derivatives (Bolt, Beranek, and Newman); Nippon Telegraph and Telephone (Japan); Rutgers University and Texas Instruments (TI); the Dalle Molle Institute for Perceptual Artificial Intelligence (Switzerland); MIT Lincoln Labs; National Tsing Hua University (Taiwan).

In the noise free environment the text-independent speaker identification results in 99.5% of accuracy whereas the identification accuracy level is reduced to 60 % of data set transmitted over telephone channels. Hence influence of noise is one of the major problems in real-time application of speaker identification system.

Researchers in voice and speaker recognition systems has been entered a new stage. The overall researches concern on trials to enhance the accuracy and precession of the developed system techniques, especially in intelligent systems. The use of Digital Signal Processing (DSP) with cooperation of Artificial Intelligence (AI) is common in such researches. But the main inertia in that is to developing the algorithm in trial and error in most cases. This research aims to find the hot spot points in merging specific techniques of DSP with AI. Multi-level decomposition of wavelet transformation is adopted to extract the features of the speaker person.

The field of Speech processing attracted much research during the past few decades. The field matured to a point where many applications, such as Speech Recognition, Speaker Identification/Verification and Language Recognition, are achieving near perfect recognition results under ideal or well controlled conditions. In practical applications these recognizers have to operate under conditions that are very different from the ideal laboratory environments.

The voice biometrics has a main place in computer systems and access controls. Voice and speaker recognition has a role of protecting the user's identity in addition to the computerized data. Such systems have become increasingly difficult. The main concept of security is authentication identifying or verifying.

This field is still under intensive study at which the appropriate feature set that contains the best unique characteristic of each voice need to be investigated in addition to the appropriate classifier for each feature set.

The identity authentication could be done in three ways:

1. Something the user knows. i.e. password
2. Something the user has. i.e. RFID
3. Something the user is. And this is so called Biometrics.

One of the most widely used systems is the speaker recognition technique. Since every human being has a unique feature in his/her voice, it is very easy to differentiate between two people using their respected voices. The concept of speaker recognition, which is different from the speech recognition system, is to verify the individual human speaker against a stored voice data set of patterns, not to recognize what is being said, while speech recognition is determining what is being said. In the area of speaker recognition many traditional techniques have been developed such as Hidden Markov Models, Neural network, Fuzzy logic and Genetic algorithms.

Human voice has two types of information high-level information and low level information. High-level information is values like dialect, an accent (the talking style and the subject manner of context).

Speaker recognition is concerned with the low-level information from the human speaker's voice, like pitch period, frequency, tone, rhythm, spectral magnitude, and bandwidth of an individual speaker's voice. This information from the speech signal is recorded as the individual's features.

III. SPEAKER RECOGNITION PROCESS

The speaker recognition process begins with generating a speech signal by speaking few words or phrases; the spoken production is decoded into speech signal as a vector of values. The speaker recognition system is a combination of the following steps: input speech signal, speech signal processing, comparison and matching phase. First a stored data set is used to be processed, afterwards the manipulation stage, finally features of each speech signal are stored as reference features, for training and validation sets, and to achieve precise recognition rate [4].

The speech feature vectors are used for creating a pattern with respect to each speaker. Moreover, the number of reference models that are needed for effective and efficient speaker recognition application depends upon the type of speech features and also the methods that the system uses for identifying any particular speaker, the speech features those are the same as stored features are extracted from an input voice signal of speaker to be authenticated. Later, the acceptance depends upon the comparison and matching between the stored feature model and the extracted ones from the input signal.

In recognition and identification system, the difference between an input speech signal of the speaker and the rest of the recorded feature set patterns is estimated. The speaker with the minimum difference with the input signal model will be accepted as the same speaker of the input voice waves. A given utterance based on the information restricted in the speech signals is the process of deciding who is speaking [4].

Speaker identification system can be viewed as the task of recognizing who is speaking from a dataset of known voices of speakers. As per figure 1, the functioning of speaker identification system begins with the speech acquisition phase. Speech signal is acquired by the system in the signal acquisition phase and a pre-processing step is performed. Noise is removed from the speech signal in the initial stages. Once the speech signal has been captured, the VAD (Voice Activity Detector) block detects the presence of human voice in the speech signal. Also the part of speech signal that is silent are been detected. After the human voice has been detected, then the feature extraction process takes place. The features extracted from the speech signal are compared and matched with the feature dataset that are already enrolled with the system. The best match is provided as the output.

IV. REVIEW OF WAVELET TRANFORMS FOR FEATURE EXTRACTION

In eighties wavelets came up as the time-frequency revolution in signal processing. In 1989, Mallet proposed the fast Discrete Wavelet Transform (DWT) algorithm to decompose a signal using a set of quadrature mirror decomposition filters, and which have respective band-pass and low-pass properties specific to each mother wavelet. Since this period, wavelets have been applied in a variety of fields including fluid dynamics, engineering, etc [5].

Wavelet transform consists of three main phases; signal transformation, feature extraction and similarity comparison. The wavelet transform is applied to decompose the input speech signal into two different frequency bands named lower frequency approximation coefficients and higher frequency detail coefficients. Wavelet transform provides multi-resolution framework, making it possible to analyze a signal at several levels of resolution.

Discrete wavelet transform decomposes a signal into multilevel successive frequency bands. Signal at various scales and translations provide multi resolution time-frequency representation, as shown in figure 2.

In discrete wavelet decomposition of signal, the output of high band pass filter and low band pass filter can be represented mathematically by equation 1 and 2.

$$Y^{high}[k] = \sum^{n} X[n]g[2k-1] \qquad (1)$$

$$Y^{low}[k] = \sum^{n} X[n]h[2k-1] \qquad (2)$$

Where Y^{high} and Y^{low} are the outputs of the high band pass and low band pass filters respectively. The wavelet analysis is performed by passing the signal into successive high pass and low pass filter. Selection of a suitable wavelet function and the number of levels of decomposition is important.

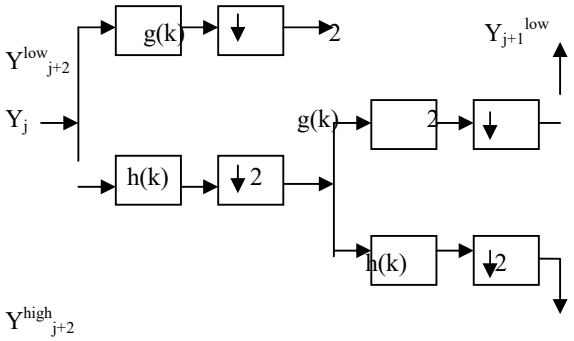


Figure 2: Schematic of Discrete Wavelet decomposition of a signal.

The advantage of using a system using wavelet transform as compared to the other classification techniques is the fast and efficient identification.

Feature extraction is an important factor that affects the performance of identification. In our system discrete wavelet transform (Daubechies4) is used to extract feature from speech signal.

Due to the superposition of various frequency components, the speech signals consist of complex waveform. Time and frequency are the two types of information that are inherent in speech signals. In the time domain of speech signal, the signal amplitude and the sharp variations are generally considered as the most meaningful features. So, the detailed contours clearly give us the idea about complicated signal. In the frequency domain, the dominant frequency channels of speech signal mostly are restricted to the middle frequency region. But different individual speakers might have different responses in all the different frequency regions. Thus the traditional approaches that just consider the fixed frequency channels might tend to lose some useful information during the feature extraction process. So, by using the multi-resolution decomposition approach, the speech signal can be decomposed into various resolution levels. The characteristics of multiple frequency channels and any change in the smoothness of the signal can then be detected to perfectly represent the signals.

V. SPEAKER IDENTIFICATION APPROACHES

A number of studies have been performed in the area of speaker identification system since its conception. Table 1 illustrates a summary of the main research approaches performed till date.

Study	Technique Used	Advantages	Conclusion / Challenges
P. Nghia, Et al [8]	Robust Wavelet – based.	Higher recognition rate than the other techniques.	Recognition rate is quite low.
A. Ahmad, Et al [9]	Vector Quantization Decision Function.	Better improvements in accuracy and brings almost 20% reduce in time processing.	Future work concentrates on Investigation of the effectiveness of hybrid VQ decision /GMM for more robust speaker recognition.
N. Sen, Et al [10]	Robust Text-Independent Speaker Identification	This feature provides better identification accuracy than the MFCC feature.	-
M. Deshpande, Et al [11]	Wavelet Packet Based Decomposition	Improved identification performance compared to other commonly used Mel scale based filter structures using wavelets.	-
N. Sen, Et al [12]	Nyquist Filter Bank for Text-Independent Speaker Identification	Improved time-bandwidth product compared to MFCC function.	-
A. Aladwan, Et al [7]	Speaker Identification Using Neural Networks and Multi-Level Wavelet Decomposition	Enables to represent the meaningful features of the human voice, in low size coefficients data and omitting the whole most of unwanted data in the human voice speech.	Determining the best level to work on future head researches is the job of this paper.

Table 1: Speaker Identification Approaches

VI. CONCLUSION

The above study reveals that the use of wavelet transforms for feature extraction for a text-independent speaker identification system yields better results.

VII. ACKOWLEDGMENT

We would like to express our gratitude towards our advisor & guide Dr. Rajesh Prasad, for his unstinting support. We are indebted to him for his invaluable advice.

VIII. REFERENCES

[1] M.S.Sinith, Anoop Salim, Gowri Sankar K, Sandeep Narayanan K V, Vishnu Soman "A Novel Method for Text-Independent Speaker Identification Using MFCC and GMM", ICALIP 2010, pp. 292-296, Kerela, India.

[2] M. D. Pawar, S. M. Badave "Speaker Identification System Using Wavelet Transformation and Neural Network", International Journal of Computer Applications in Engineering Sciences, Vol 1, July 2011.

[3] Mangesh S. Deshpande and Raghunath S. Holambe "Speaker Identification Using Admissible Wavelet Packet Based Decomposition", International Journal of Information and Communication Engineering, 2010.

[4] Tariq Abu Hilal, Hasan Abu Hilal, Riyad El Shalabi and Khalid Daqrouq "Speaker Verification System Using Discrete Wavelet Transform and Formants Extraction

Based On The Correlation Coefficient", Proceedings of the International MultiConference of the Engineers and Computer Scientists 2011, Vol 2, IMECS 2011, March 16-18, 2011, Hong Kong.

[5] Hannu Olkkonen "DISCRETE WAVELET TRANSFORMS – BIOMEDICAL APPLICATIONS", Copyright © 2011 InTech, Janeza Trdine 9, 51000 Rijeka, Croatia.

[6] CHING-TANG HSIEH, EUGENE LAI AND YOU-CHUANG WANG "Robust Speaker Identification System Based on Wavelet Transform and Gaussian Mixture Model" JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 19, 267-282 (2003).

[7] Aryaf Abdullah Aladwan, Rufaida Muhammad Shamroukh, Ana 'am Abdullah Aladwan, " A Novel Study of Biometric Speaker Identification using Neural Networks and Multi-Level Wavelet Decomposition" World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 2, 68-73, 2012.

[8] Phung Trung Nghia1 Pham Viet Binh1 Nguyen Huu Thai "A Robust Wavelet-based Text-Independent Speaker Identification" International Conference on Computational Intelligence and Multimedia Applications 2007.

[9] Abdul Manan Ahmad, Loh Mun Yee "Vector Quantization Decision Function for Gaussian Mixture Model Based Speaker Identification", 2008 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2008), Swissôtel Le Concorde, Bangkok, Thailand.

[10] Nirmalya Sen, Hemant. A. Patil, T.K Basu "A New Transform for Robust Text-Independent Speaker Identification."

[11] Mangesh S. Deshpande, Raghunath S. Holambe "Speaker Identification Using Admissible Wavelet Packet Based Decomposition" International Journal of Information and Communication Engineering 6:1 2010

[12] Nirmalya Sen, T.K Basu "Temporal Energy and Correlation Features from Nyquist Filter Bank for Text-Independent Speaker Identification" Proceeding of the 2011 IEEE Students' Technology Symposium, 14-16 January, 2011, IIT, Kharagpur.

◈◈◈

Review of Speaker Identification Techniques Using Neural Networks

[1]Ishani Nampurkar, [2]Navandar & [3]Rahul Mandal

[1&2]Dept. of Computer Engg. VIIT, Pune, India
[3]Neville Wadia Institute of Mgmt. Studies & Research, Pune, India

Abstract-In this paper a detailed study of the neural network types used for speaker recognition has been presented. The study is grounded on two standard neural network structures called as classifiers used in the speaker identification and classification performance. The standard neural network types considered are the Multilayered Feed-forward Neural Network and the Radial Basis Function Neural Network.

Keywords—*Feed forward Neural Networks, Neural networks, Radial Basis Functions Neural Networks, Speech recognition.*

I. INTRODUCTION

The fundamental and the most effective means of communication between any two or more people is speech. Speech could be a useful interface to interact with machines. For a considerably long duration research has been done on ways to improve this communication interface. Some noticeable work and inventions in this field include the megaphone, telephone.

In recent times, when genuineness and authentication is a requisite for security, biometric features play a vital role. Speech, being a biometric feature, it can be efficiently used for development in the authentication and security domains. Speaker recognition technology has the inherent capacity to create new services that will make our day to day lives even more secured. Besides, another noteworthy application of the speaker recognition technology is for forensic works. Speaker recognition has been viewed as a challenging research area for the last few decades which still renders a number of unresolved problems such as:

- Exactly the same word is pronounced in different ways by different people because of gender, age, physical variations, speed, emotional state of the speaker and dialect differences.
- A noisy surrounding can add noise to the signal. The speaker himself can add noise by the way he speaks.
- When we speak, there may or may not be a pause between words. This makes it difficult to recognize individual words.
- Other factors involved are the position and direction of the microphone from the speaker, etc.

Neural networks which are a simulation of the human neural system are used for the speech recognition. Neural networks are composed of simple computational elements, called as neurons.

The network function is determined largely by the connections between the neurons. We can train a neural network so that a particular input leads to a specific target output.

II. BACKGROUND

The speech signal carries the necessary information required to identify a speaker. The area of speaker identification is relevant to extracting the identity of the person speaking. The input speech signal is recorded for X speakers first. Then the feature extraction is done by means of LPC coefficients, calculating AMDF, and DFT. The network is trained by applying these features as input parameters. These features are stored in templates for further comparison. The features of the speaker who has to be recognized are extracted and compared with the stored templates.

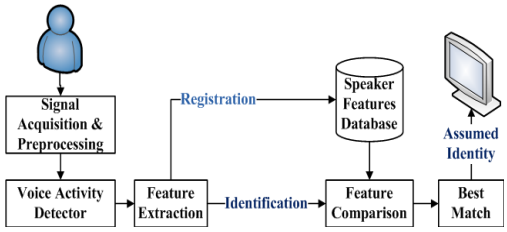


Figure 1: Speaker Identification system [8]

Feature extraction from the speech signal is one of the most important steps in the field of speaker recognition, and it can bring the important parts of the data to front and makes it easier to find the differences.[6] In speaker recognition (especially in noisy environment), all extracted feature vectors have not similar values therefore selecting the feature type and considering suitable weights highly increases the accuracy in speaker identification.[7]Then the trained network equates to the output, the input is the extracted features of the speaker to be recognized.

The network does the weight adjustment and the best match is found to recognize the speaker. The number of epochs required to get the target decides the network performance.

A considerable amount of research and development has been carried out in the field of neural networks used in the pattern recognition process of speaker verification. Note that speech is a pattern. It is clear from the recent researches that artificial neural networks can benefit a large vocabulary, speaker independent, continuous speech recognition system. Initially, most speech recognition systems were based on hidden Markov models (HMMs), a statistical framework that supports both acoustic and temporal modelling. Despite their decent performance, HMMs make a number of suboptimal modelling assumptions that limit their potential effectiveness.Neural networks avoid many of these assumptions, while they can also learn complex functions, generalize effectively, tolerate noise, and support parallelism. While neural networks can readily be applied to acoustic modeling, it is not yet clear how they can be used for temporal modelling. Therefore, a class of systems called NEURAL NETWORK-HMM hybrids has also been explored, in which neural networks perform acoustic modelling, and HMMs perform temporal modelling Robust speech recognition refers to the art of producing graceful performance degradation when training and testing data set conditions differ.[2]

Research and development also continues to focus on increasingly tough problems. A major area to be worked upon is the robustness of speech recognition performance, not only against noise but against any condition that causes a major deterioration in performance. Another key area of research is to emphasize on an opportunity rather than a problem. This research takes benefit of the truth that in many applications there is an enormous quantity of speech data available. It is too cost ineffective to have humans to jot down such large quantities of speech, so the research enlightens on developing new methods of machine learning that can effectively use large quantities of unlabeled data.

Another field of research is to know the human capabilities and to use this knowledge to improve machine recognition performance.

III. IMPLEMENTATION OF NEURAL NETWORKS USED FOR SPEAKER RECOGNITION

Neural Networks use a set of processing elements called as nodes, more or less in analogy with the neurons in the brain. These nodes are interconnected in a network that can then recognize patterns in data. In other words, the network learns from experience similar to the way humans learn. This distinguishes neural networks from traditional computing programs that follow instructions in a fixed sequential order. The learning exhibited by neural networks can be categorized to two sections:

a) Supervised Learning

Supervised learning is that which demands the network to have an external 'teacher' which tells the network how well it is performing. The algorithm adjusts weights using input-output data to match the input output characteristics of a network with the desired characteristics.

b) Unsupervised Learning

If the network 'learns' by itself, the learning is called as unsupervised learning. The network attempts to reflect properties of some given data in its output just by examining the data. This type of learning is also known as self organized learning. Hebbian learning is representative of unsupervised learning algorithm.

The two neural networks studied are the multilayer feed forward neural network and the radial basis function neural network. These can be implemented using the MATLAB Neural Network toolbox.

A. Multilayer Feed Forward Network

The first type of network is a Multilayer Feed Forward Neural Network.

This type of neural network is the most popular neural network and is used worldwide in many different types of applications. The network consists of an input layer, one hidden layer and an output layer. The

Network is trained in batch mode which means that the weights and biases of the network are updated only after the entire training set has been applied to the network. The gradients calculated at each training example are added together to determine the change in the weights and biases. Feed forward neural network with the desired output being the same as the input vector can be explored for capturing the distribution of input feature vectors. These neural network models try to map an input vector onto itself, and hence they are known as auto association or identity mapping networks. A feed forward neural network model is expected to capture the functional relationship between the input and output feature vectors of the given training data. The architecture of a multilayered feed forward neural network is shown below.

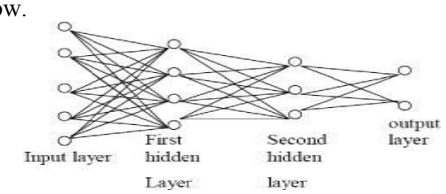


Figure 2: Multilayered Feed Forward Neural Network

The number of layers considered for this network is four. It is known that a neural network with two hidden layers can realize any continuous vector-valued function. The first layer is the input layer with linear units. The second and third layers are hidden layers. The second layer of the network has more units than the input layer, and it can be interpreted as capturing some local features in the input space. The third layer has fewer units than the first layer, and can be interpreted as capturing some global features. The fourth layer is the output layer, and the numbers of units represent the dimension of output feature vector. The activation function for the units at the input layer is linear, and for the units at the hidden layers, it is non-linear. Generalization by the network is influenced by three factors: the size of the training set, the architecture of the neural network, and the complexity of the problem.

Feed forward neural networks are used to capture the features representing the linguistic context, production constraints influencing the duration and intonation patterns of the sequence of syllables. The prediction performance of the neural network models is analysed using objective measures. In this study, we use 25 features, which form a feature vector for representing the linguistic context and production constraints of each syllable. These features represent positional, contextual and phonological information of each syllable. Features representing the positional information are further classified based on the position of a word in the phrase and the position of the syllable in a word and phrase. [5]

It was noticed that the trained network performs pretty well. The performance of the network depends majorly on the quality of the signal pre-processing. This neural network doesn't manage to work properly on input data coming from the spectrogram, but performs very well with MFCCs as input having more than 90% successful classification rate.

B) Radial Basis Function Network

The second type of network used is the Radial Basis Function Neural Network.

This network consists of three layers: an input layer, a hidden layer and an output layer. The main difference of this type of network is that the hidden layer has (Gaussian) mapping functions. Mostly they are used for function approximation, but they can also solve classification problems. Radial means that they are symmetric around their centre, basis functions means that a linear combination of their functions can generate (approximate) an arbitrary function. [1]

When simulating the trained network here also the network is capable of recognizing words that are not in the training set. The performance depends very much on the chosen spread. A too large spread causes a lower performance which means that the network tends to make more classification errors. This type of neural network is practical for large training sets and it performs very well for a small spread. The amount of hidden layer neurons needed increases very fast the more words need to be recognized.

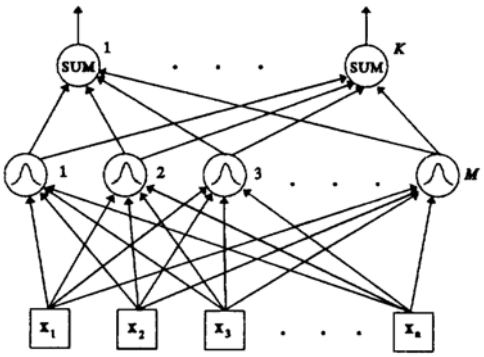


Figure 3: Radial Basis Function Neural Network

Radial basis function networks can be viewed as a feed forward neural network with a single hidden layer. An RBF network with n inputs, M hidden units and K outputs is shown in the figure. Each hidden unit is a non linear function usually Gaussian, with output related to the distance between the input vectors and the centroid of the basis function. The output layer forms a linear combiner which calculates the weighted sum of the outputs of the hidden units. Therefore, the output of an RBF network with a single output unit is given by the equation:

$$R(x) = w_0 + \sum_{i=1}^{M} (w_i \Phi_i)(\|x - c_i\|) \quad (1)$$

Where w_i (w=1...M) are the network weights, x is the input vector, c_i are the function centres and Φ, (|.|) are the non linear functions and w_0 is the bias. If the Gaussian shaped basis functions are used as non linearity the above equation can be written as:

$$R(x) = w_0 + \sum_{i=1}^{M} \left(w_i \exp\left\{ -\frac{1}{2\sigma_i^2} \|x - c_i\|^2 \right\} \right) \quad (2)$$

Where σ_i is the function width which controls the influences of each Gaussian function over a small region, with centroid at c_i. This is a fast learning algorithm. [3]

IV. COMPARISON

After reviewing both the types of neural networks, the following comparisons can be made:

- For function approximation problems, RBF networks are better suggested for surface with regular peaks and valleys, since required and accurate design can be obtained. However, for surfaces without regular peaks and valleys, multilayered feed forward neural networks are suggested as a general model.
- For classification problems, multilayered feed forward neural networks can yield better classification results. They have efficient networks than the RBF networks.
- For trained networks, RBF networks perform more robustly and tolerantly than multi layered feed forward neural networks, when dealing with noised input data set.
- In case of the RBF networks, the parameters in the hidden layer and the parameters in the output layer can be computed separately. This leads to a fast learning algorithm thus being an advantage of the RBF networks in comparison to the multi layered feed forward networks.

V. CONCLUSION

Research and development on speaker recognition methods and techniques has been carried out for more than four decades. Most of the development has emphasized on using speaker verification to control access to information, services, or computer accounts in order to provide security.

Few assumptions on the statistics of input features are made with neural networks. However, in spite of their effectiveness in classifying short-time units such as individual phones and isolated words, neural networks are rarely successful for continuous recognition tasks, largely because of their lack of ability to model temporal dependencies.

Neural networks emerged as an attractive acoustic modelling approach in ASR in the late 1980s. Neural networks make no assumptions about feature statistical properties and have several qualities making them attractive recognition models for speech recognition.

VI. REFERENCES

[1] Wouter Gevaert, Georgi Tsenov andValeri Mladenov, Senior Member, IEEE, "Neural Networks used for Speech Recognition", Journal Of Automatic Control, University Of Belgrade, Vol. 20:1-7, 2010.

[2] Mohamad Adnan Al-Alaoui, Lina Al-Kanj, Jimmy Azar, and Elias Yaacoub, "Speech Recognition using Artificial NeuralNetworks and Hidden Markov Models", IEEE Multidisciplinary Engineering Education Magazine, Vol. 3, 2008.

[3] M.W. Mak, W.G. Allen and G.G. Sexton, "Speaker Identification Using Radial Basis Functions", University of Northumbria at Newcastle, U.K.

[4] K Sreenivasa Rao, "Role of Neural Network Models for Developing Speech Systems", Sadhana Vol. 36 Part 5, Indian Academy of Sciences, October 2011.

[5] Mary L and Yegnanarayana B, "Extraction and representation of prosodic features for language and speaker Recognition", Speech Commun. 50(10): 782–796.

[6] Yanling, Z.Xiaoshi, G.Huixian, L.Na,"A Speaker Recognition Based on VQ" 3rd IEEE Conferences on Industrial Electronics and Applications (ICIEA), PP.1988-1990, June 2008.

[7] Rahul Mandal and Pawan Kumar Jha, "A Comparative Study of Techniques to Implement Text-Independent Speaker Recognition System", International Conference on Emerging Trends in Computer and Electronics Engineering (ICETCEE'2012), 2012 Dubai March 24-25.

[8] F. Bimbot, J.-F. Bonastre, C. Fredouille, G. Gravier, et al., "A Tutorial on Text-Independent Speaker Verification", EURASIP Journal on Applied Signal Processing, Vol. 4, pp. 430 – 451, 2004.

◈◈◈

Simulation and performance analysis evaluation for Multipath Extension of AODV to improve End to End Delay, Route Error Sent, Routing Load and Packet Drop Ratio

[1]Manjhari Jain, [2]Akhilesh Waoo & [3]P. S. Patheja

[1, 2&3]Dept of CSE, BIST, Bhopal, India

Abstract—This paper describes improvement in standard routing protocol AODV for mobile ad-hoc networks. Our mechanism setups multiple optimal paths based on bandwidth and delay. It allows to store multiple optimal paths based on Bandwidth and delay. At time of link failure, it will switch to next available path. To set up multiple paths, we have used the information that we get in the RREQ packet and also send RREP packet to more than one path. It reduces overhead of local route discovery at the time of link failure and because of this End to End Delay and Drop Ratio decreases. The main feature of our mechanism is that it is simple, efficient. We evaluate through simulations the performance of the AODV routing protocol including our scheme and we compare it with HLSMPRA (hot link split multi-path routing algorithm) Algorithm. Indeed, our scheme reduces routing load, End to End Delay, route error sent, and Packet drop ratio. The simulations have been performed using network simulator OPNET-14.0. The network simulator OPNET is discrete event simulation software for network simulations which means it simulates events such as sending, receiving, forwarding and dropping packets.

Keywords: *AODV, Bandwidth, End to End Delay, Optimal path, Opnet, Packet Drop, Routing Load, Route Error sent.*

1. INTRODUCTION

Ad hoc networks are presently enjoying unprecedented research interest, and are expected to provide opportunities for utilization of network applications in new scenarios in which today Internet-based communication paradigms are no longer applicable. In particular, we expect that ad hoc networks will be formed in situations where no infrastructure is available, and for which no predetermined subnet structure is known. Ad hoc networks are typically considered to be composed of mobile wireless devices, with the result that the interconnection pathways between the devices can change rapidly. This characteristic often causes ad hoc networks to be viewed more quite different than traditional networks; however, our experience shows that instead there is a strong commonality which, as we learn to understand it better, will illuminate not only the nature of ad hoc networks but also some fundamental aspects of networking [1].

In a network composed of mobile nodes, changes in the network topology required the frequent rebuilding of routes, so maintaining stable routes may be infeasible. Therefore, MANET is a communication network of a set of mobile nodes, placed together in an ad hoc manner, without any fixed infrastructure that communicate with one another via wireless links. All nodes have routing capabilities and forward data packets for other nodes in multi-hop fashion. Nodes can enter or leave the network at any time, and may be mobile, so that the network topology continuously changes during deployment. The need for exchange of digital information outside the typical wired office or unarranged environment is growing such as a class of students may need to interact during a lecture; business associates serendipitously meeting in an airport may wish to share files; or disaster recovery personnel may need to coordinate relief information after a hurricane or flood. Each of the devices used by these information producers and consumers can be considered a node in a MANET [2].

2. ROUTING IN MANET

"Routing is the process of information exchange from one host to the other host in a network.". Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself [4].

2.1 Different Strategies

Routing protocol for ad-hoc network can be categorized in three strategies.

a) Flat Vs Hierarchical architecture.
b) Pro- active Vs Re- active routing protocol.
c) Hybrid protocols.

2.2 Flat Vs. Hierarchical architecture

Hierarchical network architecture topology consists of multiple layers where top layers are more seen as master of their lower layer nodes. There are cluster of nodes and one gateway node among all clusters has a duty to communicate with the gateway node in other cluster. In this schema there is a clear distribution of

task. Burden of storage of network topology is on gateway nodes, where communicating different control message is dependent on cluster nodes.

But this architecture breaks down when there is single node failure (Gateway node). Gateway nodes become very critical for successful operation of network. Examples include Zone-based Hierarchical Link State (ZHLS) routing protocol. Where in flat architecture there is no layering of responsibility.

2.3 Proactive Vs Reactive routing protocol in MANET

2.3.1 Proactive routing protocol

In this, each node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node needs a route to the destination it runs an appropriate path finding algorithm on the topology information it maintains [4].

Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. Destination Sequenced Distance Vector Routing protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm[5].

Examples of Proactive Routing Protocols are:
a) Global State Routing (GSR).
b) Hierarchical State Routing (HSR).
c) Destination Sequenced Distance Vector Routing (DSDV).

2.3.2 Reactive routing protocol

In this type of routing protocol, each node in a network discovers or maintains a route based on-demand. It floods a control message by global broadcast during discovering a route and when route is discovered then bandwidth is used for data transmission. The main advantage is that this protocol needs less touting information but the disadvantages are that it produces huge control packets due to route discovery during topology changes which occurs frequently in MANETs and it incurs higher latency. [4]

Examples of reactive protocols are:
a) Ad hoc On-demand Distance Vector Routing (AODV).
b) Dynamic Source Routing (DSR).
c) Location Aided Routing (LAR).
d) Temporally Ordered Routing Algorithm (TORA).[5]

2.4 Hybrid routing protocols in MANET

These protocols combine the best features of the above two categories. Nodes with a certain distance from the source node concerned or within a particular geographical region are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes located beyond this zone, an on-demand approach is used. [4]

2. 5 Cost benefits trade-off between proactive and reactive protocols

Advantage: proactive Vs reactive
Proactive protocols: Routes are readily available when there is any requirement to send packet to any other mobile node in the network. Quick response to Application program.

3. AD HOC ON DEMAND DISTANCE VECTOR (AODV)

The information in this section concerning the Ad Hoc on Demand Distance Vector Protocol (AODV) protocol is taken from the RFC [6]. AODV is a reactive protocol, i.e., so the routes are created and maintained only when they are needed. The routing table stores the information about the next hop to the destination and a sequence number which is received from the destination and indicating the freshness of the received information. Also the information about the active neighbors is received throughout the discovery of the destination host. AODV provides on-demand route discovery in MANET [7]. Whenever the nodes need to send data to the destination, if the source node doesn't have routing information in its table, route discovery process begins to find the routes from source to destination. Route discovery begins with broadcasting a route request (RREQ) packet by the source node to its neighbors. RREQ packet comprises broadcast ID, two sequence numbers, and the addresses of source and destination and hop count. The intermediary nodes which receive the RREQ packet could do two steps: If it isn't the destination node then it'll rebroadcast the RREQ packet to its neighbors. Otherwise it'll be the destination node and then it will send a unicast replay message, route replay (RREP), directly to the source from which it was received the RREQ packet. A copied RREQ will be ignored.

The advantages of AODV are that less memory space is required as information of only active routes are maintained, in turn increasing the performance, while the disadvantage is that this protocol is not scalable

and in large networks it does not perform well and does not support asymmetric links.

4. HLSMPRA Algorithm

HLSMPRA algorithm mainly aims at dealing with the degradation of performance in whole networks resulting from rare area congestion in wire transmission network. Firstly, the focus of our work is to keep the routing information in the source node, so as to conduct data transmission in method of alternative path or multi-path intercurrently in source node when congestion happens. Secondly, check congestion regularly, meanwhile record the bandwidth of each link, and then judge whether the link in the state of overload by comparing excess bandwidth.

4.1 HLSMPRA Algorithm Procedures:

(1) Call Dijkstra algorithm, evaluate the shortest path **sp** between source node and destination node, if set **SP** is null set, quit, and otherwise continues.

(2) Search and compare each path in SP, and do statistics
of each link frequency. Range them in order from high to
low.

(3) Check the excess bandwidth of each link in SP regularly.

(4) We can judge from the result which link is heavy load link, and put it into set A; that it's a idle link, put the links which satisfies the condition into set B.

(5) Pick up links from the set A, if k=0 stop and otherwise to continue procedure 6.

(6) Find out the upstream node w of the heavy link, find out w node in idle set, and select the node link of next hop .Get data packet through the path, make the bigger Bandwidth path of surplus link as the first priority links.

(7) After selecting the new path, figure out the surplus bandwidth, and then sort it out and put into corresponding set (set A or set B)

(8) If k=0 stop calling the algorithm; otherwise, to continue to check the heavy load links, and split stream, then jump into the step 4.

5. Proposed System

In the proposed algorithm, multipath is discovered and maintained in advance at the time of route discovery, but instead of considering each and every RREQ at each node it will consider only specified number of request. At destination or intermediate node, RREP is sent to every received RREQ from unique node. Thus more than one path is maintained all with same but optimal paths will be stored in routing table and one of them will be used for data transfer. Other non used optimal paths will be used at time of link breakage.

It has three phases, Route Discovery, Data Sending and Route Maintenance

5.1 Route Discovery

Route discovery is initiated by the source node when it has some data to send and does not have the route table entry for the destination. It broadcasts RREQ packet to its neighbors.

When Intermediate node gets RREQ, it will check for the route table entry, for the destination mentioned in the RREQ packet. If it finds route table entry for the destination, it will generate RREP packet and send it to the source. If it doesn't have the route table entry for that destination it will rebroadcast the RREQ, after updating the route entry for the source.

When RREQ packets come at the destination, it will generate RREP packet for each RREQ packet, and unicast it to the source.

5.2 Data Sending

Data will be sent as soon as the first RREP packet comes to the source data packets will be sent and it will traverse hop by hop.

5.3 Route Maintenance

If a link break is detected, it will check for the unreachable destination and if any, it will broadcast a Route Error (RERR) packet. The entire node getting RRER packet, will re broadcast it if and only if there is at least one unreachable destination.

As we have alternate optimal paths, when a data packet arrives, it will use the next path which is available. i.e. It switch to the next optimal path on route failure and will send the RERR only when it does not have any alternate path for the destination.

5.4 Proposed Algorithm Procedures:

This Algorithm performs following steps:-

1) Estimate the Delay, Bandwidth, availability, mobility of each node.
2) Calculate the validity of each route for available packet forwarding/transmitting for selecting optimal path.
3) Remove the available routes, which is not satisfied the above condition.
4) Randomly select any one route from the available routes, which provides optimal route.

5) Sends the packet using optimal route.

6. SIMULATION ENVIRONMENT

6.1 Simulation Model

Here we give the emphasis for the evaluation of performance of Ad Hoc routing protocol AODV with varying the number of mobile nodes. The simulations have been performed using network simulator OPNET. The network simulator OPNET is discrete event simulation software for network simulations which means it simulates events such as sending, receiving, forwarding and dropping packets. The version of OPNET is 14.0, supports simulation for routing protocols for ad hoc wireless networks such as AODV, TORA, DSDV, and DSR. OPNET is written in C++ programming language and Object Tool Common Language (OTCL). Opnet allows you to model network topologies with nested sub-networking approach. This software allows nodes and protocols to be modeled as classes with all features of object oriented design It facilitates modeling the behavior of individual objects at the “Process Level” and interconnect them to form devices at the "Node Level" So that you can interconnect devices using links to form networks at the "Network Level." You can organize multiple network scenarios into “Projects” to compare designs and Aggregate traffic from LANs or "Cloud" nodes [8].

The OPNET model in its very core consists of C++ codes. These codes are complied and executed just like the C++ program. This enables very detailed control of the model by the user (if the user is proficient in C++).

6.2 Simulation Parameters

We consider a network of nodes placing within a 1000m
X 1000m area. The performance of AODV is evaluated by keeping the network speed and pause time constant and varying the network size (number of mobile nodes).Table 1 shows the simulation parameters used in this evaluation.

OPNET is written in C++ programming language and Object Tool Common Language (OTCL). Opnet allows you to model network topologies with nested sub-networking approach. This software allows nodes and protocols to be modeled as classes with all features of object oriented design It facilitates modeling the behavior of individual objects at the “Process Level” and interconnect them to form devices at the "Node Level" So that you can interconnect devices using links to form networks at the "Network Level." You can organize multiple network scenarios into “Projects” to compare designs and Aggregate traffic from LANs or "Cloud" nodes [8].
The OPNET model in its very core consists of C++ codes. These codes are complied and executed just like the C++ program. This enables very detailed control of the model by the user (if the user is proficient in C++).

6.3 Simulation Parameters

We consider a network of nodes placing within a 1000m
X 1000m area. The performance of AODV is evaluated by keeping the network speed and pause time constant and varying the network size (number of mobile nodes).Table 1 shows the simulation parameters used in this evaluation.

Simulation Parameter	
Simulator	Opnet-14.0
Protocol	AODV
Simulation Duration	30 min
Number of nodes	13
Pause Time	100sec
Average Speed	102.714 events/sec
Addressing Mode	IPv4
Packet Size(bits)	1024
Data Rate(bps)	11mbps
Buffer Size(bits)	256000

Table: 1

6.4 Performance Metrics

While analyzed the AODV protocol, we focused on three
Performance metrics which are End to End Delay, Routing Load, Total route error sent.
The graphs Figure 1 to 4 shows that the overall performance- End to End Delay, normalized routing load, Packet Drop and Total route error sent are improved by using our local route repair method.

End-to-End Delay: A specific packet is transmitting from source to destination and calculates the difference between send times and received times. Delays due to route discovery, queuing, propagation and transfer time are included in the delay metric.

Routing Load: The number of routing packets transmitted per data packet delivered at the destination. Each hop wise transmission of a routing packet is counted as one transmission.
Total Packet Drop: Due some error in transmission, there may be a chance of packet loss in wireless communication. Packet losses may occur because of the mobility of the nodes. Mobility also induces route change in the network which is tolerable but packet

loss is not tolerable for effective communication in wireless network.

Total Route error sent: In routing protocols the nodes generates error packets when the route is interrupted or broken. These packets are diffused to nearby nodes which are affected due to route break. The total number of routing packets transmitted during the simulation.

5. SIMULATION RESULTS & OBESRVATION

In this paper, local retransmission is used to improve the End to End Delay. Improved Delay, Routing Load denotes the efficiency, reliability and effectiveness of proposed routing protocol. Thus, the total route error is reduced to some extent. Though it is expected to produce minimum error sent for the proposed routing Algorithm; Total Delay is an indication of reliability, efficiency, and effectiveness of routing protocol. From Figure 1, the Total Delay shows improved reliability, effectiveness and efficiency, figure 2 shows Routing Load, figure 3 shows total packet Drop and figure 4 shows total route error sent.

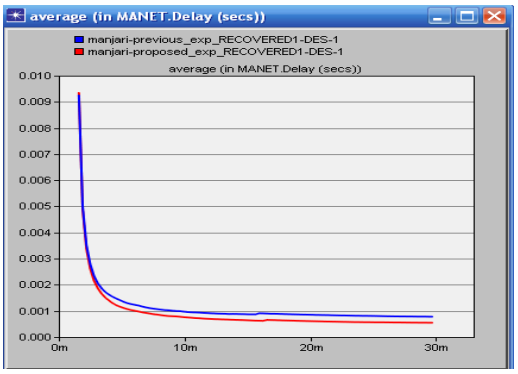


Figure 1: Total Delay

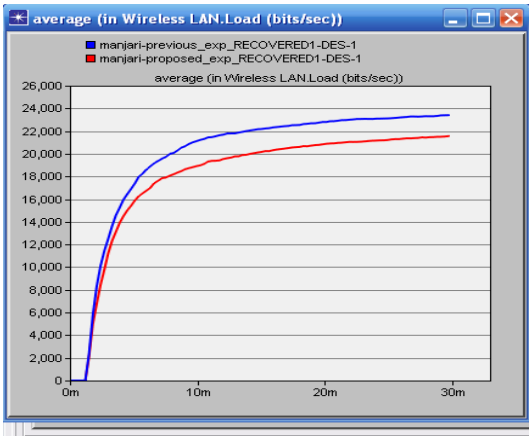


Figure 2: Routing Load

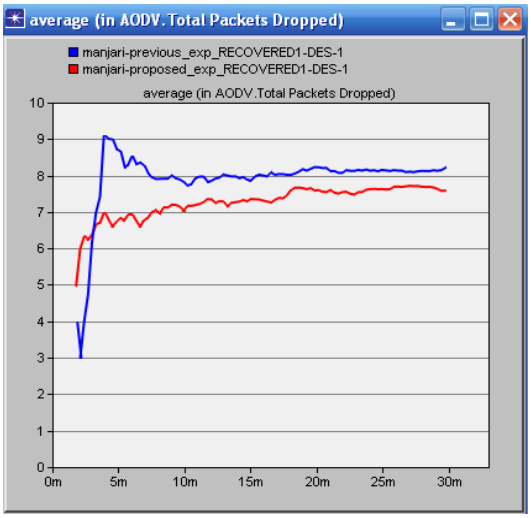


Figure 3: Total Packet Drop

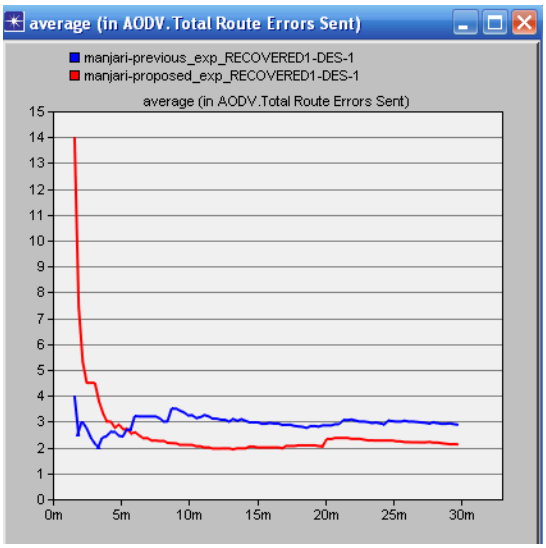


Figure 4: Total route error sent

CONCLUSION

The proposed algorithm will generate slightly higher overhead than that of Previous Algorithm for first time at the time of route discovery. But once route discovery is over, it will be beneficial for route maintenance. And this overhead overcomes the route overhead generated at the time of link failure. The proposed Algorithm reduces the total Delay, Routing Load, Packet Drop, Total route error sent. This algorithm is based on Optimization. The proposed algorithm improves the efficiency, robustness and reliability. The efficiency of proposed Algorithm shown to better than Previous Algorithm.

REFERENCES

[1]. Elizabeth M. Belding-Royer, Charles E. Perkins.Evolution and future directions of the ad hocon-demand distance-vector routing protocol. Ad Hoc Networks 1 (2003) 125–150

[2]. Srinivas Sethi, Siba K.Udgata." The Efficient Ant Routing Protocol for MANET" International Journal on Computer Science and Engineering.07, 2010, 2414-2420.

[3].V. Zangeneh, S. Mohammadi.New Multipath Node-Disjoint Routing Based on AODV Protocol World Academy of Science, Engineering and Technology 76 2011

[4]. Humaira Nishat, Vamsi Krishna, Dr. D.Srinivasa Rao and Shakeel Ahmed. "Performance Evaluation of On Demand Routing Protocols AODV and Modified AODV (R-AODV) in MANETS" International Journal of Distributed and Parallel Systems (IJDPS) January 2011.

[5]. Amit Shrivastava, Aravinth Raj Shanmogavel, Avinash Mistry Nitin Chander, Prashanth Patlolla, Vivek Yadlapalli. Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols.

[6]. C. Perkins, E. Belding-Royer and S. Das "Ad hoc On-Demand Distance Vector (AODV) Routing." RFC 3561, IETF Network Working Group, July 2003.

[7]. Manijeh Keshtgary and Vahide Babaiyan. Performance Evaluation of Reactive, Proactive and Hybrid Routing Protocols in MANET. International Journal on Computer Science and Engineering (IJCSE) February 2012 ISSN : 0975-3397.

[8]. OPnet Tutorial Written by Andrew Kim Last updated: March 7, 2003

[9]. Sujata Agrawal, Dr. M.B. Daigavane, Dr. K.D.Kulat. Performance Evaluation of Routing Protocols for Wireless Adhoc Network E-ISSN 0976-3945

[10].Dr.Scott F. Midkiff, Chair,Dr. LuizA.DaSilva,Dr.Nathaniel J. Davis, IV Dr. Ira Jacobs Dr. Charles P. Koelling Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications.

[11].Xiaoyan Hong, Kaixin Xu and Mario Gerla "Scalable Routing Protocols for Mobile Ad Hoc Networks." Computer Science Department, University of California, Los Angeles, August 2002.

Distributed System for Rendering 3D animations in Blender-3D

[1]Ganesh.V.PATIL & [2]Ganapati.A.PATIL

[1&2]Department of Computer Science and Technology, Shivaji University Kolhapur, Maharashtra, India.

Abstract- Rendering of complex scenes in animation movies require high computational environment to achieve at most photo-realistic effects. The rendering process also requires more computational time and most of the high end computational resources have been utilized for this purpose. Camera views and the ray tracing methods usually require complex rendering process. High end processing resources increases the cost of computing which is normally not affordable to small scale animators. Present work will provide the solutions to this problem by using effective computational grid. We are going to provide the solution to the animators which are using Blender-3D software for animation. We suggest the efficient distributed rendering over a low cost computational grid.

Keywords- *Rendering, Photo-Realistic effects, Blender-3D, grid.*

I. INTRODUCTION

To inculcate imaginary actions in modern movies animation is becoming unavoidable part of modern film industries. Computer animation is a process where a series of still images are assembled and shown sequentially to generate an illusion of a continuous motion effect [1].Computer graphics is a combination of imaging, modelling, Rendering and Animation. The task of rendering involves the combine effect of camera views, light effects and removal of hidden surface area. All these effects are applied to a model so it gives more realistic images after rendering. Method that gives most realistic rendering results is Ray Tracing [14].Ray tracing is further classified into Forward Ray Tracing [14] and Backward Ray Tracing [14]. In ray tracing method each pixel in the projection finds the object visible at that pixel and colored according to the object color.Now a days animation is used in variety of sectors that includes area of Entertainment, Computer Aided Design (CAD)[15], Scientific Visualizations, Training, Education, E-Commerce and Computer Art etc.

Blender-3D software is more popular software for 3D animations. Blender contains tools for modelling, animating rigging [17] and rendering purposes. Animation of 3D models becomes a very time consuming task just because of rendering process. As the animators have to find the balance between quality of scene and the production time they have to perform computations on high power computational farm. As the costing of animation goes on increasing as time and cost of computational set up increases.

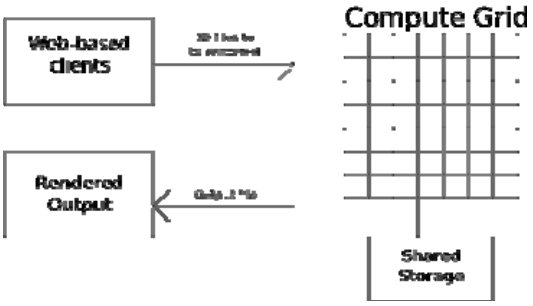


Fig.1. Web based rendering

The idea as shown in fig.1 is to perform web based rendering by using computational grid with shared storage.

A render farm is cluster of interconnected computers which are used for rendering computer generated imagery. There are two types of rendering methods: network rendering and distributed (split-frame) rendering. In network rendering, the images can be rendered in parallel, as each frame can be calculated independently of the others. In that case, the main communication between processors is used for uploading the initial models and textures and downloading the finished images. In distributed (split-frame) rendering, each frame is divided into tiles which are rendered in parallel [1].

The present system will provide fully open source and highly scalable, cost efficient distributed rendering environment. Approach of Hierarchical Master-Worker Configuration will be used. In this system, the Master-Worker will form a hierarchy. A job will get distributed as it goes deeper into the hierarchy, till a point where it need not be further divided. The proposed work tries to implement a grid based, cost-efficient, scalable and flexible solution for rendering 3D animations for Blender3D.

II. RELATED WORK

Many researchers had experimented the task of effective rendering process. Still there are limitations found in those set ups. Here we are listing those rendering farm setups.

DrQueue – is an open source general purpose batch processing solution also used for setting up render farms by the open source community, it works on TCP/ IP connections [4].

FarmerJoe – is a render farm implementation based on TCP/ IP connections to render Blender 3D models. It provides web based interface to schedule the jobs also the functionalities of Bucket based and frame based rendering facilities [5].

Loki Render – is another Blender render farm implementation applied mainly on Linux based systems; it mostly depends on TFTPBoot[16] package to function, and it requires significant knowledge of Networking to set it up [6].

BURP-BOINC – The BURP (Big Ugly Rendering Project), which is based on BOINC (Berkeley Open Infrastructure for Network Computing), is wide area internet based render farm project. The users need to install a component called BONIC on their system to donate their CPUs cycle for it, it is the only Grid based render farm found on the web [7].

Deadline – is a render farm implementation for Windows only applications, it has been developed to be compatible with 3D Max and Blender, etc. [8]

*ResPower[*13] and *Render-IT*[12] are commercial render farms available online. ResPower (USA) is a commercial online render farm with about 730 computing nodes. It charges about USD$213 for rendering 900 frames using *Mental ray*. This job takes about 4.5 minutes while on a single 3.2GHz computer it takes 3 minutes to render only one frame. However, this timing excludes the uploading of the 900 frames and downloading of the rendered images. Render- IT (UK) is a commercial online render farm with about 82 computing nodes.[1]

Besides all these properties all above mentioned rendering farms do not exhibit service orientation & workflow system in which many sub transactions will be executed in a coordinated way leading to many benefits which allow system to take many decisions without conflict. Anthony Chong, Alexei Souring and Levinski in Dec.2006 had a experiment on Grid Based rendering farm and developed a rendering farm for Maya[1] software based rendering. As the Maya is not a open source software and not affordable for small scale animators we are aiming to provide solution with open source Blender-3D [2] software.

TABLE 1

COMPARISON OF EXISTING RENDERING FARMS WITH PRAPOSED ONE.

RF	PI	JM	GB	RS	OS	FM	SG	FA	SA
DQ	Y	Y	N	N	Y	Y	Y	Y	N
FJ	Y	Y	N	N	Y	Y	Y	Y	N
LR	N	Y	N	N	Y	Y	Y	Y	N
BB	Y	N	Y	Y	N	Y	N	Y	N
DD	N	Y	N	-	N	N	N	Y	N
RP	Y	Y	N	Y	N	N	N	Y	N
RC	Y	Y	N	Y	N	N	N	Y	N

TABLE 2

FEATURE KEYS

RF-Rendering Farm, DQ-DrQueue, FJ-Farmer Joe, LR-Loki Render, BB-Burp-BONIC, DD- Deadline, RP-ResPower, RC- Render-core,	JM-Job Monitoring, GB-Grid Based, RS-Registry Support, OS-Open Source, SG-Script Generator, FA-Fully Automatic, SA-Service Oriented.

Proposed system will have following features,

1. Job Monitoring
2. Grid based Rendering
3. Registry Support
4. Open Source Software
5. Service Oriented Architecture
6. Script Generation.

We are going to adopt the best things from all the existing set ups made for distributed rendering process. As we can see in Table 2. none of them provides a service-oriented architecture. Only a few of them supports animation. Only Burp supports Grid-based computation.

III. NEED OF THE WORK

Systems proposed by DrQueue and Farmer Joe do not support rendering animations. Both systems support only rendering still images and are not robust since they do not maintain registry for crash recovery.

None of them supports service-oriented architecture. Hence they are not flexible in their deployment. The output of all the existing systems is images. The computation power required for these types of works is very high, so there is a need to distribute the same 3D animation work by using Blender software and also to achieve best price performance ratio. The proposed system is based on service oriented architecture hence it can be deployed on both small scale and enterprise level. This system supports animation and maintains a registry for crash recovery. The system also has an encoder which converts the still images to required video formats.

IV. ARCHITECTURE OF PROPOSED WORK

Figure.2 shows the architecture of proposed system in which many of the problems which are in the existing system described above will be overcome.

A. DETAILS OF ARCHITECTURE

1. Central Manager

The central manager will manage all the other components. It will take the input Blender file and stores it in the Shared Mass Storage. It will also maintain a database of all the jobs completed, jobs in progress, their completion percentages, the queue and other statistical information.

2. Job Registry

An overall database will be maintained by the render farm management system where the users can store and manage the jobs to be rendered and those already rendered by the

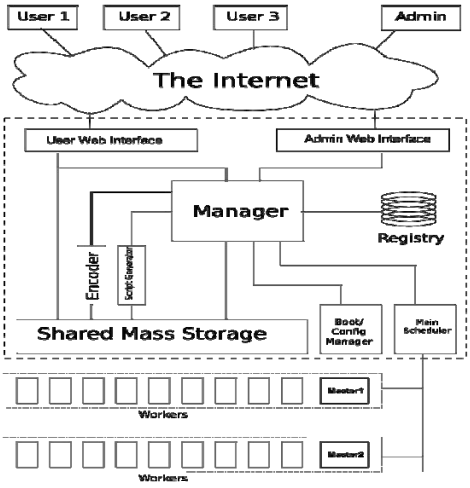


Fig.2.Architecture of proposed work

Grid environment. The registry will maintain the job information such as the Job id, job name, description, number of frames to render, number of sub jobs to create from original animation, whether the job is rendered or not, rendered result path.

3. Script Generator

Script Generator will be the application specific converter which will convert the .blend Blender file to a series of XML files. A XML file will represent a single frame of an animation sequence. A XML file will contain all the details necessary to render a particular frame. These XML files will be fed into the worker nodes for rendering.

4. Shared Mass Storage

The Shared Mass Storage will be a shared storage facility which will contain all the frames to be rendered. The worker nodes will fetch the data from this shared storage. It will be also used to store the finished, rendered images.

5.Boot / Configuration Manager

The Boot/Configuration manager will have PXE compliant DHCP server which can PXEBoot the workers. It will store the image of the worker operating system, which is copied to all the workers when they are booted. It will also have scripts which configures the newly added workers. These scripts will include assigning new host-name to the worker, updating their hosts file, setting the masters IP and other configuration.

6.Main Scheduler

The main scheduler's job will be to monitor all of its child sub-systems and assign jobs to them. Job assignment will be based on the current CPU load average, memory usage.

7.User interface

To make user interface simpler we will have to introduce a web-based system, where user can submit their jobs, monitor the progress of the rendering in real-time. It will also provide an interface for retrieving the rendered images. The user interface can also be a Blender plug-in which when used automatically submits the job online and it will display the results inside the Blender.

There will be a web-based administration interface, using which the administrator can monitor the entire system

The objectives of the proposed work are:

1. *TO DEVELOP SCRIPT GENERATOR*
   a. The scripts generator will convert the .blend file into renderer operable XML files which will be later distributed across the system.
   b. The YaFaRay [3] renderer operates on the XML files only, hence the .blend needs to be converted to the XML files.
   c. The current YaFaRay[3] converter is implemented as a plug-in to Blender3D and it overwrites the same XML file for every frame generated, since it does not allow to export animations to XML files

d. Hence we need to develop a standalone version of the same which supports exporting animations to a set of different XML files.

e. This plug-in will be developed in Python since Blender supports Python.
f. Every XML file will be independent and will describe the entire scene for that particular frame.

2. TO DESIGN SCHEDULING ALGORITHM

a. The master will be notified about the CPU utilization of the worker nodes. The master will keep track of the CPU utilization of the worker nodes.
b. The master will have an in-memory database of its immediate worker nodes
c. The master will maintains a sorted list of its immediate worker nodes based on the work load on each of its immediate worker node.
d. It will use this sorted list to allocate the job from the job queue.

3. MAINTAINING THE REGISTRY AND SHARED MASS STORAGE

A) Maintaining the registry.

TABLE 3.Registry structure

JobID	ClientID	LocBlend	LocXML	Progress

The above table shows the registry structure that will be maintained for monitoring progress of each job.

B) SHARED MASS STORAGE

a. The shared mass storage will be implemented local to the master node.
b. The XML file transfers will be managed by the NFS (Network File System).

4. USER AND ADMIN WEB-INTERFACES

a. The web-interface will provide facility for user registration
b. Job submission
c. Job progress monitoring
d. Later retrieval of the output.

5. FUNDAMENTAL CONFIGURATIONS

A) BOOT & CONFIGURATION MANAGER

DHCP server allots the IP address for the new worker nodes and the address of the TFTP server. TFTP server will provide the worker OS images during boot. Scripts will configure the newly booted worker nodes.

B) SLAVE CONFIGURATION

The slave will have the YaFaRay pre-installed on the TinyCoreLinux [18] image. It will have the program to calculate the CPU utilization and memory usage and notify its master about the same. It will have boot scripts that will configure it immediately after the boot.UDP packets will be used to transfer the monitoring packets between the worker and the master nodes, since UDP has less overhead than TCP. Reliable TCP connections will be used to transfer the control information between the worker nodes and the master node.

6. TO PLUG DEVELOPED SOFTWARE IN BLENDER3D

A plug-in can be implemented inside the Blender Environment which will provide the facility of automatic submission of jobs to our system. The output of the rendering shall be shown within the Blender Environment.

7. PERFORMANCE AND COST COMPARISON

1. The performance will be compared with the existing systems which are used in the animation industry.
2. The cost will be compared the high-end machines used in the modern animation industry.

TABLE. 4.Examples of servers used in modern animation industries.

Company	Server	Price
Intel	Pentium Xeon	Rs. 2,50,000
Intel	Quad Core	Rs. 2,00,000

Various animation industries like DreamWorks, which produced award winning films like Shrek series uses 500 of such high machines each with 4GB memory and terabytes of storage. It takes around three months of 24x7 rendering to produce films like these.

In such a way the proposed system will provide a solution to highly computational rendering task in an efficient and economic manner. Later the system will be compared with the latest distributed systems which are used in modern animation industries and check the improvement in performance ratio.

V. CONCLUSION

In this way idea of distributed rendering farm has been put forward. The basic objective of this work will be to provide the time efficient and cost effective solution to 3D animation rendering process. Our idea of grid based rendering farm will be the alternative way to use high end computational resources.

The experimentation on many of the modules in current work is going on and we are achieving the expected results.

REFERENCES

[1] Anthony Chong, Alexei Sourin and Konstantin Levinski. "Grid-based Computer Animation Rendering "

[2] M. Z. Patoli, M. Gkion, A. Al-Barakati, W. Zhang, P. Newbury and M. White"An Open Source Grid Based Render Farm for Blender 3D"

[3] The Blender Foundation, http://www.blender.org

[4] DrQueue, the open source distributed render queue http://drqueue.org/cwebsite/

[5] Farmerjoe distributed rendering system for Blender http://blender.formworks.co.nz/?p=1

[6] Loki Render, Queue manager, http://sourceforge.net/projects/loki-render/

[7] BURP-BOINC – Big Ugly Rendering Project http://burp.boinc.dk/

[8] Deadline Render farm, The hassle-free administration and rendering toolkit for Windows based render farms. http://www.franticfilms.com/software/products/deadline/overview/

[9] Ffmpeg encoders, http://ffmpeg.mplayerhq.hu/

[10] M.Z.Patoli, A.Al-Barakati, M.Gkion, W.Zhang, P. Newburry, N. Belof, and M.White, "A Service-Orientation Approach for a Digital Library System focused on Portable Antiquities and Shared Heritage", Vast 2007, 26 to 29 November 2007, submitted to The 8th International Symposium on Virtual Reality, Archaeology and Cultural Heritage (2007).

[11] E. Wes Bethel, Greg Humphreys ,Brian Paul Tungsten Graphics J. Dean Brederson "Sort-First, Distributed Memory Parallel Visualization and Rendering" IEEE Symposium on Parallel and Large-Data Visualization and Graphics (PVG'03)0-7695-2091-X/03 $ 17.00 © 2003IEEE

[12] RENDER-IT. http://www.render-it.co.uk

[13] RESPOWER. http://www.respower.com

[14] Ray Tracing http://en.wikipedia.org/wiki/Ray_tracing_%28graphics%29

[15] CAD en.wikipedia.org/wiki/Computer-aided_design

[16] TFTP Boot http://www.thegeekstuff.com/2010/07/tftpboot-service.

[17] Riggininghttp://en.wikipedia.org/wiki/Skeletal_animation

[18] TinyCoreLinux http://distro.ibiblio.org/tinycorelinux/welcome.html

◈◈◈

Grid Location Service for Optimal Performance in MANETs

[1]Gogineni Krishna Chaitanya, [2]Lakshmi Chetana & [3]P.Narasimham

[1]SRI SAI ADITYA Institute of Science & Technology
[2&3]DVR & Dr.HS MIC College of Technology

Abstract: For achieving optimum performance over dynamic topologies like MANETs either topology based routing algorithms or position based routing algorithms were used. Location updates are essential for the latter's perspective. Each node needs to refresh and maintain its location information at random intervals with respect to a neighborhood update (NU) and a certain distributed location server update(LSU) in the network. Location inaccuracies raise the application costs leading to alternative node mobility models. The location update decisions on NU and LSU can be independently carried out without loss of optimality using a Markov Decision Process (MDP) model. For practicality the location update problem is implemented using a low-complexity learning algorithm (LSPI) that achieves a near optimal solution. Using a single location server update (LSU) in the network is unlikely to scale to a large number of mobile nodes; it cannot allow multiple network partitions to function normally in their own partition; and nodes near to each other gain no advantages—they must contact a potentially distant location server in order to communicate locally. We propose to use a distributed Grid location service (GLS) that is designed to address these problems. GLS is fault-tolerant; and is not dependent on specially designated nodes. GLS supports large number of nodes.

Keywords: *Grid Location Service(GLS), Markov Chain Process(MDP),Neighborhood Update(NU),Location Server Update(LSU).*

I. INTRODUCTION

Mobile Ad hoc NETworks (MANET) are a set of autonomous wireless mobile nodes that do not require a pre-established infrastructure. Each node in the network acts both as a router and an end system. For message forwarding in MANET various routing algorithms have been proposed to take care of frequent topological changes. Some algorithms use information about the physical location (position) of the participating nodes. These algorithms are known as position based routing algorithms for which location updates are essential. Position based routing algorithms assume that each node knows its physical location that can be obtained using Global Positioning System (GPS).

In a MANET, since the locations of nodes are not fixed. There are two basic location update operations at a node to maintain its up-to-date location information in the network. One operation is to update its location information within a neighboring region, where the neighboring region is not necessarily restricted to one hop neighboring nodes. We call this operation neighborhood update (NU), which is usually implemented by local broadcasting/flooding of location information messages. The other operation is to update the node's location information at one or multiple distributed location servers. The positions of the location servers could be fixed or unfixed. We call this operation location server update (LSU), which is usually implemented by unicast or multicast of the location information message via multihop routing in MANETs.

It is obvious that there is a tradeoff between the operation costs of location updates and the performance losses of the target application in the presence of the location errors (i.e., application costs). On one hand, if the operations of NU and LSU are too frequent, the power and communication bandwidth of nodes are wasted for those unnecessary updates. On the other hand, if the frequency of the operations of NU and/or LSU is not sufficient, the location error will degrade the performance of the application that relies on the location information of nodes.

Using a single location server update has a number of problems. The centralized server is a single point of failure; it is unlikely to scale to a large number of mobile nodes; it also causes overhead to the centralized server and its neighboring nodes that need to relay location update to the server and it cannot allow multiple network partitions to each function normally in their partition. Nodes near to each other gain no advantages—they must contact a potentially distant location server in order to communicate locally.

Therefore in order to minimize the overall Costs and overhead of location update, an efficient location update schemes are needed for maintaining up to date information in the location servers. It should replicate location information in order to minimize database servers' failures and network partitioning. Distribution of location information should involve minimum resources of the network in updating and retrieving of the information.

In this paper, we proposed to use a distributed location service called grid location Service scheme analytically using Markov chain model. Grid location service uses geographical forwarding to take advantage of the similarity between physical and network proximity. A source must know the geographical positions of any destination to which it wishes to send, and must label packets for that destination with its position. In the model, a distance based triggering strategy is used to trigger a location update for moving nodes in the network. Further, the model also considers selective queries for destination search to compute the average total cost that includes the update cost and query cost. To study the impact of varying the threshold distances on these update schemes, we have used different threshold distances.

II. GRID LOCATION SERVICE

The main idea of GLS is that every node maintains its current location in a number of location servers distributed throughout the network which address various problems of single location service update. GLS uses geographical forwarding to take advantage of the similarity between physical and network proximity. GLS arranges that different nodes tend to have different sets of location servers. These location servers are not specially designated. Each node acts as a location server on behalf of some other nodes. The location servers for a node are relatively dense near the node but sparse father from node. This ensures that anyone near a destination can use a nearby location server to find the destination, while also limiting the number of location servers for each node.

GLS is fault-tolerant and scales to large number of nodes because there is no dependence on specially designed nodes. Here, Nodes can move in any direction within the given network area. While a node is moving, it can trigger a location update using an appropriate triggering strategy. In this model, we have used a distance based triggering strategy. In this strategy, a node triggers a location update when it crosses a given threshold distance, i.e., it crosses the boundary of a sub area defined as the network width times twice of the threshold distance around the current location of the node in north and south directions. Therefore this location update strategy ensures that a node is located within a sub area that is twice of the threshold distance from the last updating location of the node.

Figure 1, shows the system for grid location service update scheme. When a node has moved from position *A* to position *B*, the node updates all its location servers with ID greater and closest to the ID of the node located in different squares of all order-squares. For destination query, a source node sends a destination request query for location servers available in the squares of 1st order square, 2nd order square, 3rd order square, and sth order square of the source node. The search for destination continues using the location information obtained from the location servers in sub area 0. If the search fails, the destination search is continued in the sub areas 1, 2, and *d* with respect to destination based on the threshold distance considered.

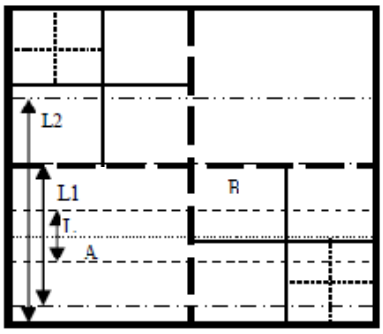


Figure 1. Structure of GLS model.

In grid location service update scheme, when a moving node crosses the threshold distance *d*, it sends location update messages to all location servers located in different order squares from 1st order square up to sth order square. In this case, we have considered $s = 4$. Therefore, the update cost of the location servers in the four order squares for grid location service model is the sum of location update cost in each order square from one to four. The location update cost in the 1st order square is the number of transmissions in terms of hop count needed to cover the 1st order square with circles of radius equal to transmission range. The update cost between the source and any one of the remaining order squares is the sum of the cost of updating three location servers and the search cost to identify the location servers in that order square.

III. MARKOV CHAIN MODEL

In this work, we have used a random walk mobility model. In this model, a moving node travels to one of its neighboring sub areas with probability *q* or stays at the current sub area with probability $1 - q$. We have formed a discrete-time Markov chain model to capture the mobility and query arrival patterns of a moving node in two-dimensional network. Figure 2 shows the state diagram of Markov chain model when the threshold distance for triggering a location update is *d*. The state of the Markov chain *i* ($i = 0, 1, 2 \ldots d$) is defined as the distance between the current location

of the moving node and its last updating location from where the node has updated its location servers.

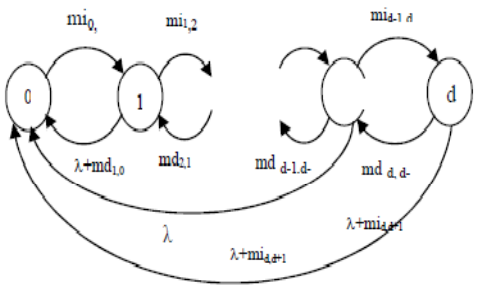


Figure 2. State diagram of Markov chain model.

The transition probability $mi_{i,i+1}$ represents the probability at which the distance of the moving node from its last updating location increases in north or south directions. The transition probability $md_{i,i-1}$ represents the probability at which the distance of the moving node from its last updating location decreases in north or south directions. The request query arrival probability is denoted by λ . transitions from a given state to one of its neighboring states represent movements of the node away from its current sub area. A state transition to state 0 represents either the arrival of request query or the triggering of location update when the threshold distance *d* is reached.

We use the steady state probabilities calculated in section three to determine the cost of both location updates and query requests for a given threshold distance *d*. We assume that the cost for updating location servers of a moving node is *U*. We consider that the network is a random graph with fixed transmission range. The mean hop count is the average distance between any pair of nodes or the average path length.

IV. PERFORMANCE

we present numerical results for home agent, quorum based, and GLS update schemes obtained by using some selected values for input parameters. In home agent update scheme, we have considered that the side of a square representing home region of a node is 264 meters. Further, in quorum based update scheme, we have considered that the size of the update column is almost equal to that of the home region of the home agent update scheme. Further, the thickness of the column to be updated and the thickness of row to be searched are assumed equal. Also, for GLS update scheme, we have taken the side of the 1st order square to be equal to 250 meters.

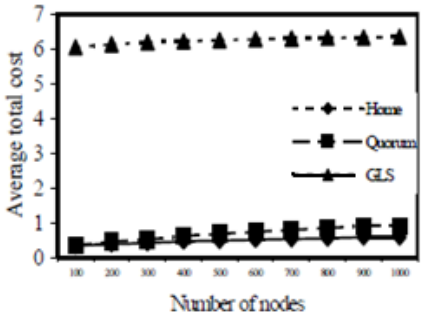


Figure 3. Analytical results for density.

we have compared the location update schemes under investigation based on the analytical results for density based approach. This comparison is done for threshold distance L0 corresponding to one sub area only in the network. Figure 3, shows the analytical results of home agent, quorum based and grid location service update schemes for density approach. It is clear that grid location service update scheme has the maximum average total cost and home agent update scheme has minimum average total cost.

V. RELATED WORK

Most existing ad hoc routing systems distribute either topology information or queries to all nodes in the network. Some, such as DSDV, are *proactive*; they continuously maintain route entries for all destinations. Other techniques are *reactive*, and construct routes to destinations as they are required. This includes systems such as DSR, AODV, and TORA. Broch et al. and Johansson et al. Each provide overviews of these ad hoc routing techniques, along with comparative measurements using small (30–50 node) simulations. Grid's main contribution compared to these works is increased scalability.

More closely related to Grid are protocols that use geographic positions. Finn's Cartesian routing addresses each node with a geographic location as well as a unique identifier. Packets are routed by sending them to the neighbor closest to the packet's ultimate destination. Dead ends are handled by scoped flooding. However, Finn gives no detailed explanation of how node locations are found or how mobility is handled. More recent work on geographic approaches to routing includes the DREAM and LAR systems. Both systems route packets geographically, in a manner similar to Finn's Cartesian system. They differ in how a node acquires the geographic position of a destination. DREAM nodes proactively flood position updates over the whole network, allowing other nodes to build complete position databases. LAR nodes reactively flood position queries over the

entire network when they wish to find the position of a destination. Because they both involve global flooding, neither system seems suited to large networks.

The Landmark system actively maintains a hierarchy to provide routing in a changing network. Nodes in a Landmark network have unique permanent IDs that are not directly useful for routing. Each node also has a changeable Landmark address, which consists of a list of IDs of nodes along the path from a well-known root to the node's current location. A Landmark address can be used directly for routing, since it is similar to a source route. The Landmark system provides a location service that maps IDs to current addresses. Each node **X** sends updates containing its current Landmark address to a node that acts as its address server, chosen by hashing **X**'s ID to produce a Landmark address _ If a node **Y** exists with that address, **Y** acts as **X**'s location server. Otherwise the node with Landmark address closest to A is used. Anyone looking for **X** can use the same algorithm to find **X**'s location server, which can be queried to find **X**'s current Landmark address. This combination of location servers and addresses that encode routing information is similar to the architecture described in this paper. Grid, however, avoids building hierarchies, as they are vulnerable to the movement of nodes near the top of the hierarchy.

VI. CONCLUSION

Wireless technology has the potential to dramatically simplify the deployment of data networks. For the most part this potential has not been fulfilled: most wireless networks use costly wired infrastructure for all but the final hop. Ad hoc networks can fulfill this potential because they are easy to deploy: they require no infrastructure and configure themselves automatically. But previous ad hoc techniques, do not usually scale well to large networks.

In this paper, we have presented a distributed location server called grid location service using markov chain model which address problems of single location service update. Markov chain model was developed to describe the behavior of mobility and query arrival patterns of mobile nodes in grid location service update schemes. We have used distance based triggering strategy to update location servers of a moving node. The average total cost is calculated for different threshold distances corresponding to sub areas in the network. The analytical results show that as the threshold distance increases, the average total cost decreases.

VII. REFERENCES

[1] M. Mauve, J. Widmer, and H. Hannes, "A Survey on Position- Based Routing in Mobile Ad Hoc Networks," Proc. IEEE Network, pp. 30-39, Nov./Dec. 2001.

[2] Y.C. Tseng, S.L. Wu, W.H. Liao, and C.M. Chao, "Location Awareness in Ad Hoc Wireless Mobile Networks," Proc. IEEE Computer, pp. 46-52, June 2001.

[3] S.J. Barnes, "Location-Based Services: The State of the Art," e-Service J., vol. 2, no. 3, pp. 59-70, 2003.

[4] Giordano S., Stojmenovic I., and Blazevic L., Position *Based Routing Algorithms for Ad Hoc Networks: A Taxonomy*, Kluwer Academic Puplisher, 2001.

[5] Hekmat R. and Mieghem P., "Degree Distribution and Hop Count in Wireless Ad Hoc Networks," *in Proceedings of* IEEE *International Conference on Networks (ICON' 2003)*, Sydney Australia, pp. 603-609, 2003.

[6] Ho J. and Ian A., "Mobile User Location Update and Paging under Delay Constraints," *Computer Journal of Wireless Networks*, vol. 1, no. 4, pp. 413-425, 1995.

[7] Brad Karp and H. T. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. In *Proc. ACM/IEEE MobiCom*, August 2000.

[8] I. Stojmenovic, "Location Updates for Efficient Routing in Ad Hoc Networks," Handbook of Wireless Networks and Mobile Computing, pp. 451-471, Wiley, 2002.

[9] T. Park and K.G. Shin, "Optimal Tradeoffs for Location-Based Routing in Large-Scale Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 13, no. 2, pp. 398-410, Apr. 2005.

[10] R.C. Shah, A. Wolisz, and J.M. Rabaey, "On the Performance of Geographic Routing in the Presence of Localization Errors," Proc. IEEE Int'l Conf. Comm. (ICC '05), pp. 2979-2985, May 2005.

[11] S. Giordano and M. Hamdi, "Mobility Management: The Virtual Home Region," ICA technical report, EPFL, Mar. 2000.

[12] I. Stojmenovic, "Home Agent Based Location Update and Destination Search Schemes in Ad Hoc Wireless Networks," Technical Report TR-99-10, Comp. Science, SITE Univ. Ottawa, Sept. 1999.

Gogineni Krishna Chaitanya received M.C.A degree from Acharya Nagajuna University Guntur, India in 2009. Currently. His research interests include cooperative communications in Mobile Adhoc Networks and Neural networks.

R.Srinivas currently working on his reasearch on distributed data bases . His research interests include in Mobile Adhoc Networks and Distributed data bases.

◈◈◈

User Authentication Using Biometrics Pattern

[1]Raunak Khatri, [2]Hitesh Sachdev & [3]Rajesh S Prasad

[1, 2] Department of Computer Engineering, VIIT Pune India
[3]Department of Computer Engineering, DCOER, Pune

Abstract- Information Security is an important aspect only due to the Progress in the field of Information Technology. We outline the position of biometrics in the current field of computer security. Authentication plays an important role in order to deal with security. This paper presents a review on the biometric authentication techniques and some future possibilities in this field. In biometrics, a human being needs to be identified based on some characteristic physiological parameters. The purpose of such schemes is to ensure that the rendered services are accessed only by a rightful user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. The position of biometrics in the current field of Security has been depicted in this work. We also propose classification of biometric systems that would allow us to compare the biometrics systems reasonably.

Keywords: *Classification, biometrics, authentication, security, evaluation.*

1. INTRODUCTION

Since the beginning of modernization, identifying fellow beings has been important to the human society. Consequently, person identification is a crucial part of the infrastructure needed for diverse business sectors such as access control, finance, health care, transportation, entertainment, security, law enforcement, government, and communication.

Authentication means whether a user should be allowed access to a particular system or resource. It is a serious area of security research and practice. User id passwords are most commonly used for authentication, but in today's world many other methods are also available, such as biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise main concerns such as acceptability and lack of flexibility and smart cards usually need a Personal Identification Number (PIN) because cards can fall in the hand of imposters. As a result, passwords are still dominant and are expected to continue to remain so for some time. Password and PINs which are traditional measures need more advanced safeguards against unauthorized access to computer resources and information. (Coming)

Automatic means are very important even for trustworthy person's recognition, because our civilization has become electronically connected to form one big global community. Surrogate representations of identity such as passwords and cards no longer that reliable.

There are five important characteristics of biometric identifiers. They are as follows:-

1. Uniqueness
2. Universality
3. Acceptability
4. Permanence
5. Collectability

There are two different authentication methods in biometrics.

1) Verification: Is he/she the person who claims he/she is? Works with id biometrics. Thus it is based on a combination of modes.
2) Identification: Who is this person? Uses only the biometrics and searches the entire database

So here we are only dealing with a binary-decision scheme where we either approve or disapprove a person. Four components of simple biometric systems are as follows:

1) Sensor modules: This module procures biometric user data. Example- fingerprint sensor or retina scanner. [7]

2) Feature extraction modules: This unit is mainly responsible for taking out the feature values of a biometric traits. If hand geometry is used as a biometric trait then feature values would include width of fingers at several locations, length of the palm, thickness of the palm, width of the palm, length of fingers etc. [7]

3) Matching modules: The matching modules compare all the biometrics features with all the other features that present in the database. [7]

4) Decision-making modules: The user's identity is either established or a claimed identity is approved or disapproved. This is done based on the results of the matching modules.

There are mainly two different methods of authentication: Natural properties of an individual, i.e. physiological features such as fingerprints, iris, retina, face geometry, voice, etc. artificial measures, either physical objects held solely by the user (e.g. magnetic card, key, badge, token, etc.), and/or personal private information known only to the authentic user (e.g. password, the name of his/her mother, spouses, etc.) [7]

2. METHODOLOGY

A biometric system is fundamentally a pattern recognition system that works by attaining biometric data from an individual, taking out a feature set from the attained data, and equating this feature set against the template set in the database. Depending on the application background, biometric system can operate in any of the modes either verification mode or identification mode.[1]

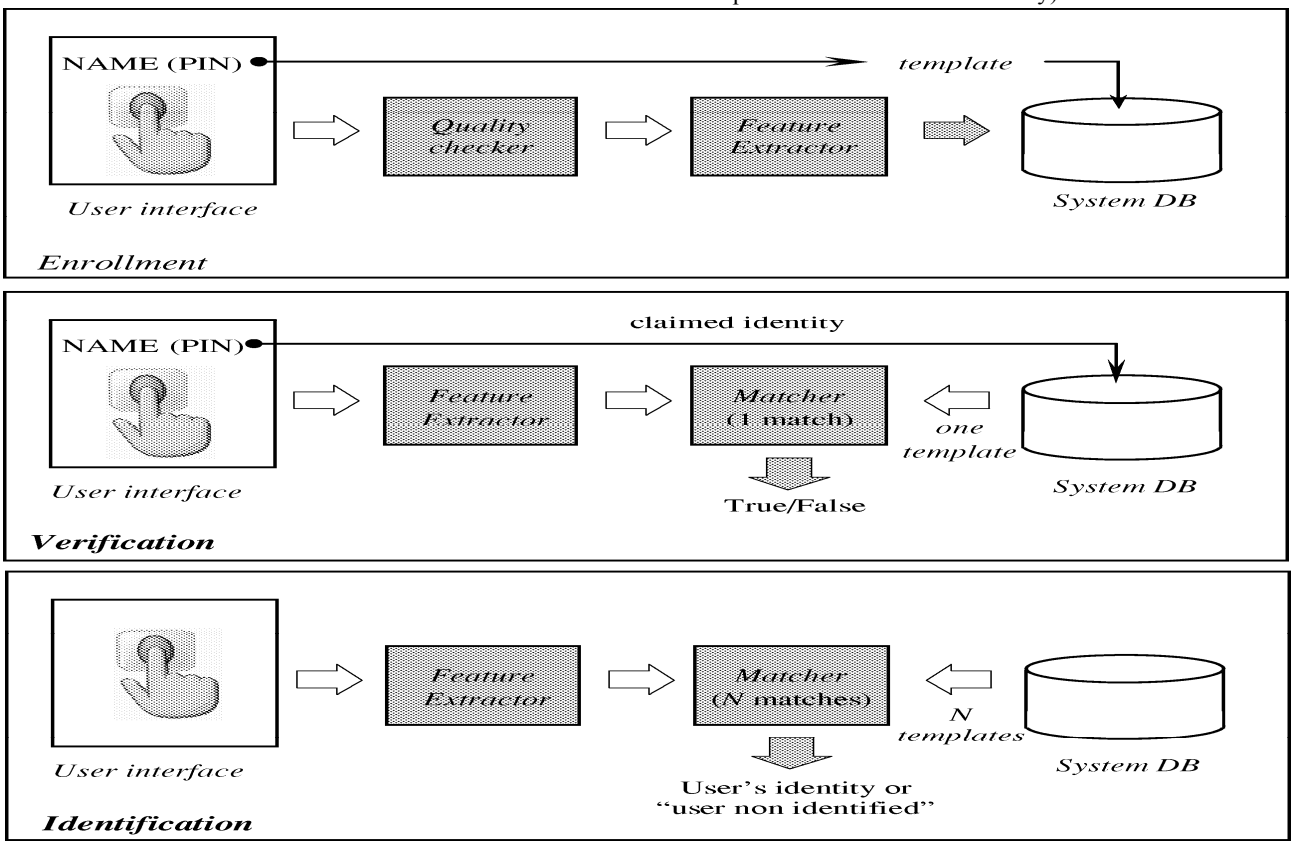
• First, in the verification mode, the system authorizes an individual's identity by relating the taken biometric data with her/his own biometric template(s) reserved in the system database. [1]

Fig. 1. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules

of a biometric system, i.e., sensor, feature extraction, matcher, and system database.[1]

In this kind of system, a person who wishes to be recognized claims an identity, generally via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "*Does this biometric data belong to Bob?*"). Identity authentication is normally used for *positive recognition*, in which the target is to avoid many peoples using the similar identity. [1]

•Second, in the identification mode, in this the system try to match all the templates of the users present in the database to recognize an individual. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The negative recognition helps in preventing a single person from using multiple identities. For convenience identification may also be used in positive recognition (the user is not required to claim an identity). Traditional



The block diagrams of a verification system and an identification system are shown in Fig. 1; user enrollment, which is common to both of the tasks, is also graphically illustrated. [1]

Some of the biometric authentication methods are briefly described:

2.1 Signature

There are many stages to be executed to perform identification & verification. After preprocessing all signatures from the database by converting them to a portable bitmap (PBM) format, their boundaries are extracted to facilitate the extraction of features using MDF. With neural based classifiers, identification and verification experiments are been performed.

2.1.1 Signature Database

Experiments have been performed with the "Grupo de Procesado Digital de Senales" (GPDS) signature database. The results provided in this research used a total of 2106 signatures. From those 2106 signatures, we used 39 sets of signatures (i.e. from 39 different persons) and, for each set, 24 samples of genuine and 30 samples of forgeries.

Although the full GPDS database includes 140 signature sets, only a component (39 sets) of that was made available at the time of the experimentation. [2]

2.1.2 Boundary Extraction

Boundary of every signature must take prior to the feature extraction process. The binary image of every signature which is given is preprocessed and the contour is also extracted, providing the first stage in the method of reducing the amount of data describing each pattern. [2]

2.1.3 The tri Surface Feature

The surface area of two different signatures could be the same. So for increasing the accuracy of the feature telling the surface area of the signature, the feature called 'tri Surface' was implemented, in this the signature was separated into three equal parts, vertically. The surface area feature is basically the surface covered by the signature, and it also includes the holes contained in it. The total number of black pixels present in the surface was counted, and the proportion of the signature's surface over the total surface of the image was calculated. This same process was used for all the three equal parts of the signature, giving three values between 0 and 1.

2.1.4 The Length Feature

The length feature represents the length of the signature, after scaling all the signatures from the database to the same height. In order to obtain a value between 0 and 1, the minimum and the maximum signature lengths were respectively considered as 0 and 1. The remaining signature lengths were then converted to values between this minimum and maximum range. [2]

2.2 keystroke

It's a biometric system based on keystroke timings which is used to monitors an individual session on a computer system with the help of the keystroke information being generated during the session. Following steps are to taken keystroke model: -

2.2.1 *Data Collection*

When a new individual enter to the system for authentication, he / **s**he is asked to register. They collect as much keystroke data of the individual of the system in one day or even as much as a week on the computer to be monitored. Then the collected data is preprocessed and stored in the database. A program is to be built that will capture and log keystroke timings from an authorized user of a computer system over a couple of days. Then this data used to build a profile of a user and to build a repository of training data features.

2.2.2. *Feature Extraction*

The abstraction of typical features from the data and the minimization of the dimensionality of the resulting design vectors is often denoted to as the preprocessing and feature abstraction problem. For example, we may choose to use only a selected number of dimensions from the input, either because these features are enough to recognize the discrete or because the addition of other extra features maximizes the computational complexity of the problem or produces no real benefit.

2.2.3 Pattern Classification

Identification and classification involves the determination of prime decision measures. After the observed data from designs to be known have been stated in the form of measurement vectors in the design space, we want to decide to which design class these data belong. Reference template is constructed by using some possible abstraction techniques, which calculate person typing characteristic. During verification process the same techniques are used. Different techniques give the different quality description of typing rhythm, what influent success of verification. During recognition, when database of user's reference template is large, some clustering methods can be used, such as typing speed for decrease in amount of templates used for verification.

2.3 Voice

The speech recognition though seems to be simple concept, but actually it is very difficult and it is firmly fixed in mathematics. From the almost infinite

variety of tonal inflections, accentuations, pronunciations and volume when comparing one speaker with another speaker, the complexity arises. Problems also arise when words that sound the same but have different spelling. Further complicating the process is the variety of equipment used to record the speech at the front end of converting the speech to text. Complexity is added because of the equipment include noise introduced from improper microphones and differences in sampling rates when converting the analog voice signal to a digital signal.

The basic likelihood of speech recognition exploits a statistical model called the Hidden Markov Model (HMM) to compute overall probability of matching speech. The HMM utilizes small sections of speech, called frames, with each segment having a related probability density function. This probability model is discussed in the next section titled "Basic Mathematics of Speech Recognition".

2.3.1 Basic Mathematics of Speech Recognition

Because of these complexities in speech recognition, when considering continuous speech instead of discrete speech and when considering very large vocabularies necessary to interpret every-day conversational language, mathematical models form a very important research tool of the system developers.

The speech signal is basically a non-stationary random process. Any process in which the joint probability distribution function (pdf) of random variable or vectors at an instant of time t is equal to the time at t + Δt is known as stationary random process. The signals are stationary but only for short period of time, and in these short periods of time, normally mentioned to as frames, the signal is stationary, the joint pdf is considered to remain untouched. This permits the calculation of features such as autocorrelation, covariance, and mean amplitude or frequency of the samples belonging to the frame with the help of that pdf.

In the HMM based speech recognition system, there are many different ways through which several frames of speech are analyzed through maximum probability path being the one taken to signify the word. Although the next exclamation of the similar word may or may not exactly match a set of features, when considering a threshold probability, whether there is not an exact match in terms of all the features that are compared, but the words should match. In other words we can say that, each path may be represented by a combination of different feature vectors or polynomials containing features of some words with the HMM analyzing which word or path most likely represents the spoken word. One can refer to "Statistical Methods for Speech Recognition" by Frederick Jelinek, for more detailed description of the Hidden Markov Model for speech recognition. [3]

At the most basic level, the mathematical formulation of combining phonemes into words and strings of words can be described in the following statistical terms.

Let X represent a sequence of symbols taken from some alphabet. Each symbol might represent a unique phoneme. This sequence represents the intermediate form which has been translated from the waveforms by the translation device. In essence it is the acoustic evidence provided by the translation device. Let W represent a string of spoken words, each belonging to a known vocabulary. The speech recognition problem can then be stated as finding the maximum probability that the translated text, $W\sim$, is the same as the spoken words W given the evidence X

$$W\sim = \max(w)P(W|X)$$ [3]

2.4 GAIT

Recognizing individuals by the way they walk is done by Gait biometrics, this is a particularly challenging research area. The potential for particular identification is supported by a rich fiction, including medical and psychological studies. The main reason that make gait attractive for identification purpose is that the completely unobtrusiveness lacking any subject cooperation or contact for data acquisition. Gait recognition techniques at the state of the art can be divided into 3D and 2D approaches. In the first group, identification relies on parameters extracted from the 3D limb movement. These methods use a large number of digital cameras and after a camera calibration process the 3D reconstruction is achieved. On the other hand, the 2D gait biometric approaches extract explicit features describing gait by means of human body models or silhouette shape. A rich variety of data has been collected for evaluation of 2D gait biometrics. The widely used and compared databases on gait recognition include: the Human ID Gait Challenge; CASIA; and the University of Southampton data. The majority of methods and databases found in the literature use a single camera positioned with a specific view of the subject's walking direction. (Generally capturing the walk from the lateral view) and a large number of papers describing gait recognition have been published.

In surveillance scenarios, the system should operate in an unrestrained environment where the subject walks freely and maybe there is no information regarding the camera. Recently there has been development in methods which can recognize subjects walking in intersecting camera views, by using the new method which uses viewpoint invariant recognition. The gait feature derived from different viewpoint into the side-view plane a new

reconstruction technique has been employed to correct and standardize it, and exploit such data for recognition. Initial evaluation of the method shows that a recognition rate of 73.6% is still achievable with an experiment carried out on a large gait data set with over 2000 video sequences consisting of different viewpoints. Additionally, further experiments applied on CCTV footage has shown the potential of using gait to track people identities across different non-intersecting un-calibrated camera views based on gait analysis. This is an important step in translating gait biometrics into single view scenarios where calibration information cannot be recovered such as in surveillance and forensic applications. [4]

2.5 Fingerprint

A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges". The traditional method uses the ink to get the finger print onto a piece of paper. This paper is then scanned using a scanner. Live finger print readers are used in modern approach .These are based on optical, thermal, silicon or ultrasonic principles. It is the oldest of all the biometric techniques. Optical finger print reader is the most common at present. They are based on reflection changes at the spots where finger papilar lines touch the reader surface. All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the pressure. Some of the readers are fitted out with the processing and memory chips as well.

The size of optical finger is around 10*10*15. It is difficult to minimize them much more as the reader has to comprise the source on light reflection surface and light sensor. Optical Silicon Fingerprint Sensor is based on the capacitance of finger. On a silicon chip, dc-capacitive finger print sensor consists of rectangular arrays of capacitors. One plate of the capacitors contains a tiny area of metallization on the chips surfaces on placing finger against the surfaces of a chip and the other is the finger, the ridges of finger print are close to the nearby pixels and have high capacitance to them. The valleys are more distant from the pixels nearest to them and therefore have lower capacitance.[6]

Ultrasound finger print is un-common. It uses ultrasound to monitor the figure surfaces, the user places the finger on a piece of glass and the ultrasonic sensor moves and reads whole finger print. This process takes 1 or 2 seconds.

Finger print matching techniques can be placed into two categories. One of them is Minutiae based and the other one is Correlation based. Minutiae based techniques find the minutiae points first and then map their relation placement on the finger. Correlation based techniques require the precise location of a registration point and are affected by image translation and rotation. [6]

2.6 IRIS Technology

The iris of the eye is used in this recognition method. Iris patterns are different of every individual and it is obtained with the help of video based image acquisition system.

Each iris structure is featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings.

The iris pattern is taken by a special gray scale camera at a distance of 10- 40 cm from the camera. When gray scale image of the eye is found then the software tries to trace the iris within the image. The software creates a net of curves covering the iris when the iris is found. Based on the darkness of the points along the lines the software creates the iris code.

Here, two influences have to take into account. First, the overall darkness of image is influenced by the lighting condition so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture darkness. Secondly, the size of the pupil changes so the size of the iris also get change. Before computing the iris code, a proper transformation must be done.[6]

In decision process, the matching software takes two iris codes and compute the hamming distance based on the number of different bits. The hamming distances score (within the range 0 means the same iris codes), which is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast (it is the fact only counting the number of bits in the exclusive OR of two iris codes). We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced. Depending on the result decision is taken [6]

3. APPLICATIONS

Physical characteristics are much more problematic to copy as compare to passwords, hardware sensors, substantial memory capacity, due to all this systems are costly, this is the reason that Biometric authentication is very reliable. Biometric based authentication applications include workstation and network access, single sign-on, application logon,

Biometric	EER	FRR	FAR	Explanation
Keystrokes	1.8%	0.1%	7%	during 6 months period
Voice	6%	10%	2%	text dependent and multilingual
finger print	2%	2%	2%	rotation and exaggerated skin distortion
Iris	0.01%	0.99%	0.94%	indoor environment

data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures.

4. EVALUATION OF BIOMETRIC TECHNIQUES

With the biometrics authentication departments like investing and other financial transactions, retail sales, health and social services are getting benefits.

For big scale enterprise network confirmation/authentication environments, for the protection of all types of digital content etc, biometric technologies plays a very important role. It can be used alone or combined with other technologies such as PIN, encryption keys and digital signatures, biometrics is expected to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is used in various schools, colleges in India for many different purposes.

There are many more applications of biometrics authentication like for verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and users' authentication in a variety of social services.[6]

5. REFERENCES

[1]. Anil K. Jain" An Introduction to Biometric Recognition" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004

[2]. Stéphane Armand, Michael Blumenstein and Vallipuram Muthukkumarasamy " Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural-based Classification"

[3]. JOHN E. STRANGE "Voice Authentication A Study of Polynomial Representation of Speech Signals"

[4]. Michela Goffredo, John N. Carter and Mark S. Nixon "Front-view Gait Recognition"

[5]. Hugh Wimberly, Lorie M. Liebrock "Using Fingerprint Authentication to Reduce System Security: An Empirical Study" 1081-6011/11 2011 IEEEDOI 10.1109/SP.2011.35

[6]. Debnath Bhattacharyya Rahul Ranjan Farkhod Alisherov A. and Minkyu Choi "Biometric Authentication: A Review" International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009

[7]. Igor B¨ohm and Florian Testor "Biometric Systems"

◈◈◈

Ranking for Web Databases Based on Veracity Using Truth Finder

[1]S. Hemanth Chowdary, [2]Vijaykumar Mantri & [3]G Hari Charan Sharma

[1&2]Dept of Information Technology, Dr. B V Raju Inst of Technology, Narsapur, Hyderabad, India
[3]Dept of Computer Science, TRR Engineering College, Patancheru, Hyderabad, India

Abstract− In the current epoch, the World Wide Web has turn out to be the most influential resource of information for us. But, the unswerving information that is accessible on the web is very less and diverse websites provide dissimilar information which may direct to conflicts, by such kind of conflicts the user may not get the required unswerving information. In our, proposed framework, we projected a system which is used for finding the true facts about the websites and ranking those websites based on the true facts and also deals with the predicament of authenticity. This is extremely prevailing when compared to the existing systems. This also provides compact protection against malwares, attacks and unendorsed information and provides the reliable information to the users.

Keywords− *veracity, true facts, web mining, truth finder.*

I. INTRODUCTION

Information quality is task dependent user might consider the quality of a piece of information appropriate for one task but not sufficient for another task. Information quality is quality attribute concerned user might consider the quality of the same piece of information appropriate for both tasks. Which quality dimensions are relevant and which levels of quality are [4] required for each dimension is determined by the specific task at hand and the subjective preferences of the information consumer. Earlier researchers generated compelling list of web attributes that engender trust worthiness for example one commonly cited study has identified six features of web sites that enhance consumer perceptions of the markets trust worthiness. The world-wide web has become a necessary part of important information source for most people everyday people retrieve all kinds of information from the web for example when online shopping people find product specifications from web site like ShopZilla.com looking for interesting [1] DVD they get information and review on web sites such as NetFlix.com or IMDB.com. Web services are the new industrial standard for distributed computing and are considered, for the first time, a real opportunity to achieve universal interoperability. The trustworthiness problem of the Web has been realized by today's Internet users. According to a survey on the credibility of websites conducted by Princeton Survey Research in 2005 [3], 54 percent of Internet users trust news websites at least most of time, while this ratio is only 26 percent for websites that offer products for sale and is merely 12 percent for blogs. There have been many studies on ranking web pages according to authority (or popularity) based on hyperlinks. The most influential studies are Authority-Hub analysis [7], and Page Rank [10], which lead to Google.com. In this paper, we propose a new problem called the Veracity problem, which is formulated as follows: Given a large amount of conflicting information about many objects, which is provided by multiple websites (or other types of information providers) We use the word "fact" to represent something that is claimed as a fact by some website, and such a fact can be either true or false.

II. RELATED WORK

The quality of information on the Web has always been a major concern for Internet users [3]. There have been studies on what factors of data quality are important for users [10] and on machine learning approaches for distinguishing high-quality and low-quality web pages [9], where the quality is defined by human preference. It is also shown that information quality measures can help improve the effectiveness of Web search [2]. Unfortunately, the popularity of web pages does not necessarily lead to accuracy of information. TRUTHFINDER studies the interaction between websites and the facts they provide and infers the trustworthiness of websites and confidence of facts from each other. An analogy can be made between this problem and Authority-Hub analysis, by considering websites as hubs (both of them indicate others' authority weights) and facts as authorities. However, these two problems are very different, and Authority-Hub analysis cannot be applied to our problem. In Authority-Hub analysis, a hub's weight is computed by summing up the weights of authorities linked to it. TRUTHFINDER uses iterative methods to compute the website trustworthiness and fact confidence, which is

widely used in many link analysis approaches [5], [6], [7],[10], [1]. This iterative procedure has been proven to be successful in many applications, and thus, we adopt it in TRUTHFINDER.

III. EXISTING SYSTEM

The working mechanism of the existing system is as follows, in the existing system only the query process is made through the search engine, there are many web pages with the conflicting information which are called conflicting web pages. The following figure 1 shows the process of ranking the web pages:

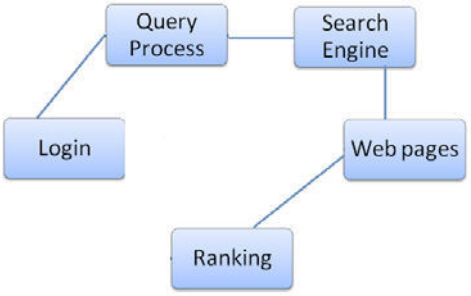


Figure 1 Normal Process of Ranking Web Pages

When the user searches the web pages, there leads to many conflicting information which confuses the user and the user may not get the accurate information which he exactly required, ranking such kind of web pages may also results in the conflicts. So there are many problems regarding ranking the web pages. In our proposed frame work we introduced the truth finder in reducing the conflicts in the web pages and produce the trustworthy web pages.

IV. PROPOSED FRAMEWORK

Diverse facts about the same object may be contradictory For example if we consider the search for Apple, the information may be conflict because, the Apple may be fruit or the same Apple which the user is referring is related to Apple computer. So, if the user wants the Apple as Apple computers and wants the computer related information and if the search is made for Apple fruit, the information which the user gets may lead to conflicts. So, to reduce the conflict information we introduced a framework based on the veracity and the trustworthiness of the web page by using truth finder.

The proposed framework for the ranking the web pages by using the truth finder is as shown below:

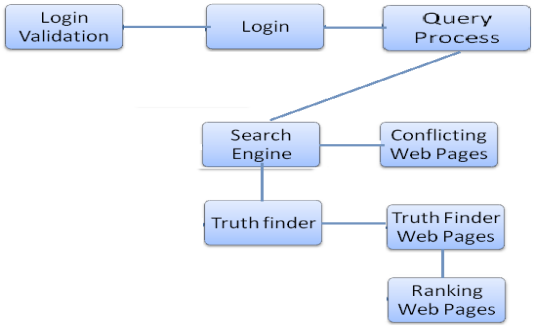


Figure 2 Framework for ranking web pages using truth finder

The input of TRUTHFINDER is a large number of facts are provided by many websites, the goal of TRUTHFINDER is to identify the true fact among them. Conflicting facts on the web such as different sets of authors for a book, many web sites some of which are more trustworthy than some others. A fact is likely to be true if it is provided by trustworthy websites.

In the framework first we have to know the two important basic definitions A) The confidence of facts and B) The trustworthiness of websites.

Confidence of facts: The confidence of a fact f(denoted by s(f)) is the probability of f being correct, according to the best of our knowledge.

Trustworthiness of websites: The trust-worthiness of a website w(denoted by t(w)) is the expected confidence of the facts provided by w.

For website w, we compute its trustworthiness t(w) by calculating the average confidence of facts provided by w:

$$t(w) = \frac{\sum_{f \in F(w)} s(f)}{|F(w)|}$$

Where F(w) is the set of facts provided by w.

The trustworthiness score of a website can be defined by using logarithmic as: $T(w) = -\ln(1 - t(w))$ T(w) is between and zero and $+\infty$, and a larger T(w) indicates higher trustworthiness.

By observing the real data we have four heuristics based on the data. The heuristics are as follows:

1. Usually there is only one true fact for a property of an object.
2. This true fact appears to be the same or similar on different websites.
3. The false facts on different websites are less likely to be the same or similar
4. In a certain domain, a website that provides mostly true facts for many objects will likely provide true facts for other objects.

There are trustworthy websites such as Wikipedia and untrustworthy websites such as blogs and some small websites. We believe that a website has some consistency in the quality of its information in a certain domain.

Different parameters used are as shown in the following table:

TABLE 1 NOTATIONS USED IN THE PAPER

Name	Description
w	Web site
t(w)	Trustworthiness of web site
T(w)	The trustworthiness score of website
f	Fact
s(f)	Confidence of fact
∂	Maximum difference between two iterations

ALGORITHM

Input: The set of websites W, the set of facts, and links between them.

Output: The ranked website with trustworthiness and fact confidence.

Calculate the matrix A & B

1. For each website belongs to set of websites i.e., (w ∈ W) Calculate the trustworthiness of website Calculate the trustworthiness score of website.
2. Repeat Compare the adjusted confidence score with the confidence score of the other website
3. Compute the confidence using adjusted confidence score.
4. Compute the trustworthiness score of website from trustworthiness.
5. Calculate the same until the cosine similarity of trustworthiness and temporary trustworthiness is greater than the max difference between the two iterations.
6. Compute the rank of the trustworthy websites using the similarity function between the websites.

V. RESULT ANALYSIS

Analyzing the results of Dataset contains the authors of many books provided by many online bookstores it contains 1265 computer science books published by Addison Wesley, McGraw Hill, Morgan Kaufmann, or Prentice Hall. For each book we use ISBN to search on www.abebooks.com,which returns the book information on different online bookstores that sell this book. The dataset contains 894 bookstores, and 34031 listings (i.e., bookstore selling a book). On average each book has5.4 different sets of authors. Truth Finder performs iterative computation to find out the set of authors for each book. In order to test its accuracy, we randomly select 100 books and manually find out their authors. Compare the set of authors found by Truth Finder with the standard fact to compute the accuracy. For a certain book, suppose the standard fact contains P authors, Truth Finder indicates there are Q authors, among which R authors belong to the standard fact. The accuracy of Truth Finder is defined as R max (P,Q). Sometimes, Truth Finder provides partially correct facts.

VI. CONCLUSION

Our proposed system formulate the Veracity problem, which aims at resolving conflicting facts from multiple web sites, and finding the true facts among them and this approach that utilizes the inter-dependency between web site trustworthiness and fact confidence to find trustable web sites and true facts and ranking the web sites based these true facts which is used for retrieving the reliable information from the web.

REFERENCES

[1] Anonymous, Net users distrust corporate privacy policies-study, available at : http://www.newsbytes.com/cgi-bin/udt/im..Ble?client.id newsbytesandstory.id – 174596.

[2] Brown, G., Kananga, T., Carey, M., Kumar, A., Tanniru, M., & Zhao, J. L., Services Science: Services Innovation Research and Education, Proceedings of the IEEE International Conference on Services Computing, July 11–15, Orlando, Florida, 2005.

[3] Princeton Survey Research Associates International, "Leap of faith: Using the Internet Despite the Dangers," Results of a Nat'l Survey of Internet Users for Consumer Reports WebWatch,Oct. 2005.

[4] G. Jeh and J. Widom, "SimRank: A Measure of Structural-Context Similarity,"Proc. ACM SIGKDD '02,July 2002.

[5] M. Kleinberg, "Authoritative Sources in a Hyperlinked Environ-ment,"J. ACM,vol. 46, no. 5, pp. 604-632, 1999.

[6] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank Citation Ranking: Bringing Order to the Web," technical report, Stanford Digital Library Technologies Project, 1998.

[7] A. Borodin, G.O. Roberts, J.S. Rosenthal, and P. Tsaparas, "Link Analysis Ranking: Algorithms, Theory, and Experiments,"ACM Trans. Internet Technology,vol. 5, no. 1, pp. 231-297, 2005.

[8] Sigmoid Function from Wolfram MathWorld, http://mathworld.wolfram.com/SigmoidFunction.html, 2008.

[9] X. Yin, J. Han, and P.S. Yu, "LinkClus: Efficient Clustering via Heterogeneous Semantic Links,"Proc. 32nd Int'l Conf. Very Large Data Bases (VLDB '06),Sept. 2006

[10] X. Zhu and S. Gauch, "Incorporating Quality Metrics in Centralized/Distributed Information Retrieval on the World Wide Web,"Proc. ACM SIGIR '00,July 2000.

◈◈◈

Approaches in Handwritten Numeral Recognition

[1]Kiran J. Gabra & [2]Shalaka U. Dixit

[1&2]Department of Computer Engineering
Vishwakarma Institute of Information Technology, India

Abstract- A profound groundwork has been done in the field of Handwritten Numeral Recognition (HNR) over the past three or four decades leaving a perceptible impact on applications. The paper explores the new trends in Handwritten Numeral Recognition (HNR) and enlists the challenges with the appropriate possible solutions. The handwritten digits are not always of the same size, thickness and orientation. This leads to various problems such as complex pattern spaces, low amount of data per dimension and poor signal to noise ratio. The concept of commotion from writing habits leads to obstacles ranging from the dissimilarity of the methods' application to the intrinsic complexity of the problem. Therefore for the efficacious implementation of the applications in this field, thorough knowledge of the behavior and the robustness in matching a particular context is required.

Keywords- *Handwritten Numeral Recognition, Pattern spaces, Data per dimension, Signal to noise ratio.*

.

I. INTRODUCTION

Much attention has been given to the fiend of recognition of digits, which is a subfield of character recognition, since the initial years of research in character recognition. The solutions of this subfield are considered to be simple and robust. Work of many researches proposing solution to this problem even today can be found in literature.

In the fields of document analysis and recognition of numeral strings, numeral recognition has been an important subject of research. It is used in wide range of applications such as, ZIP codes, bank checks, tax forms, and census forms. Recognizing the numeral strings of variable lengths and in different styles proves to be a major challenge. One of the dominant obstruction in a handwriting numeral string recognition system is segmentation. It can be found in different stratums, such as, segmenting the information of interest from the document, segmenting phrases into words, and words into characters.

TABLE 1

EVOLUTION OF VARIOUS RECOGNITION STRATEGIES.

Strategy	Year	Remark
Template Matching Operations	1988	Determines the degree of similarity between two vectors in feature space.
Hidden Markov Model (HMM)	1989	Efficient algorithms to automatically train the models without any need of labeling presegmented data.
Fuzzy Set Reasoning Technique	1993	Employs fuzzy set elements to describe the similarities between the features of the characters. It gives more realistic results and its probability cannot be calculated.
The k-Nearest Neighbor Method	1995	Posterior probability is estimated from the frequency of nearest neighbors of unknown partners.
Support Vector Machine (SVM)	1995	Based on the statistical learning theory and quadratic programming optimization.
Neural Networks	1995	A computing structure consisting of a massively parallel interconnection of adaptative "neural" processors. It is able to be trained

		automatically, good performance with noisy data, efficient tool for learning large databases.
The Polynomial Discriminant Classifier	1996	Assigns a pattern to a class with the maximum discriminant value which is computed by a polynomial in the components of a feature vector.
The Bayesian classifier	2001	Assigns a pattern to a class with the maximum a posteriori probability. Class prototypes are used in the training stage to estimate the class conditional probability density function for a feature vector.

This paper aims to highlight the various handwritten numeral recognition system developed till date. Table I describes the evolution of recognition strategies over the past few years.

II. RECOGNITION APPROACHES

A. TEMPLATE MATCHING

Template matching[1] is a technique in digital image processing for finding small parts of an image which match a template image. Template matching operations determine the degree of similarity between two vectors (groups of pixels, shapes, curvatures, etc) in the feature space. Matching techniques can be grouped into three classes: direct matching, deformable templates and elastic matching and relaxation matching. A basic method of template matching uses a convolution mask (template), tailored to a specific feature of the search image, which we want to detect. This technique can be easily performed on grey images or edge images. The convolution output will be highest at places where the image structure matches the mask structure, where large image values get multiplied by large mask values.

B. HIDDEN MARKOV MODEL

Hidden Markov Model (HMM), as described by Rabiner[2], is a doubly stochastic process, with an underlying stochastic process that is not observable (hence the word hidden), but can be observed through another stochastic process that produces the sequence of observations. HMM can be discrete or continuous depending upon the nature of the observations. Hidden Markov models are especially known for their application in temporal pattern recognition such as speech, handwriting, gesture recognition, part-of-speech tagging, musical score following, partial discharges and bioinformatics. These probabilistic models offer many enticing properties for modeling numerals. One of the most salient properties is the existence of efficient algorithms to automatically train the models without any need of labeling pre-segmented data. Britto[3] have effectively used HMMs in handwritten numeral recognition. The two basic approaches for handwriting recognition using HMM are Model-Discriminant HMM and Path-Discriminant HMM. In the former, a model is constructed for each class (numeral string unit or digit) in the training phase. In the latter, a single HMM is constructed for the whole language or context.

C. FUZZY SET REASONING TECHNIQUE

Fuzzy set reasoning is a technique that incorporates fuzzy set elements to describe the alikeness between the features of the numerals. In the fuzzy model based numeral recognition[4], the features extracted from a numeral are used to form the fuzzy sets. The interactive fuzzy model includes the criterion function which is a part of the consequent part of the fuzzy rule. The fuzzy measure theory is directed by the interaction among the input fuzzy sets. The criterion function is used to study model parameters and the test function which is a component of the criterion function matches the unknown numeral with the reference numerals in the knowledge base. Fuzzy set elements give more realistic results when there is not a prior knowledge about the data, and therefore, the probabilities cannot be calculated. The literature reports different approaches based on this technique such as fuzzy graphs, fuzzy rules, and linguistic fuzzy.

D. THE k-NEAREST NEIGHBOUR METHOD

In pattern recognition, the *k*-nearest neighbor algorithm (*k*-NN) is a method for classifying objects based on closest training examples in the feature space. The k-Nearest-Neighbor (k-NN) rule is a popular non-parametric recognition method, where a posterior probability is estimated from the frequency of nearest neighbors of the unknown pattern. Persuasive recognition results for handwriting recognition have been reported using this approach[5]. The downside of this method is the high computational cost when the classification is presided

over. To overstep such a predicament some researchers have proposed faster k-NN methods. A comparison of fast nearest neighbor classifiers for handwriting recognition is given in[6].

E. SUPPORT VECTOR MACHINE

Support Vector Machine (SVM) is based on the statistical learning theory and quadratic programming optimization. The basic SVM takes a set of input data and predicts, for each given input, which of two possible classes forms the input, making it a non-probabilistic binary linear classifier. An SVM is basically a binary classifier and multiple SVMs can be combined to form a system for multi-class classification. In the past few years, SVM has received increasing attention in the community of machine learning due to its excellent generalization performance. More recently, some SVM classification systems have been developed for handwriting digit recognition, and some promising results have been reported in[7].

F. NEURAL NETWORKS

Work on artificial neural networks, commonly referred to as *neural networks*, has been motivated right from its inception by the recognition that the brain computes in an entirely different way from the conventional digital computer. The struggle to understand the brain owes much to the pioneering work of Ramón y Cajál (1911), who introduced the idea of neurons as structural constituents of the brain. A Neural Network (NN) is elucidated as a computing structure consisting of a parallel interconnection of adaptative “neural” processors. The ability of neural network to be trained automatically from examples and its possible parallel implementation make it propitious. Along with this neural networks give good performance and serve as a efficient tool for learning large databases. Prominent results in the field of handwritten numeral recognition have been observed with the use of NNs. The most widely studied and used neural network is the Multi-Layer Perceptron (MLP)[8]. Other architectures include Convolutional Network (CN), Self-Organized Maps (SOM), Radial Basis Function (RBF), Space Displacement Neural Network (SDNN), Time Delay Neural Network (TDNN), Quantum Neural Network (QNN) and Hopfield Neural Network (HNN).

G. THE POLYNOMIAL DISCRIMINANT CLASSIFIER

The polynomial discriminant classifier assigns a pattern to a class with the maximum discriminant value which is computed by a polynomial in the components of a feature vector. The class models are implicitly represented by the coeficients in the Polynomial[9].

H. THE BAYESIAN CLASSIFIER

A naive Bayes classifier is a simple probabilistic classifier based on applying Bayes' theorem with strong (naive) independence assumptions. In simple terms, a naive Bayes classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature, given the class variable. A more descriptive term for the underlying probability model would be "independent feature model". Depending on the precise nature of the probability model, naive Bayes classifiers can be trained very efficiently in a supervised learning setting. In many practical applications, parameter estimation for naive Bayes models uses the method of maximum likelihood; in other words, one can work with the naive Bayes model without believing in Bayesian probability or using any Bayesian methods. The Bayesian classifier assigns a pattern to a class with the maximum a posterior probability. Class prototypes are used in the training stage to estimate the class conditional probability density function for a feature vector [10]. In spite of their naive design and apparently oversimplified assumptions, naive Bayes classifiers have worked quite well in many complex real-world situations.

III. METHODOLOGY

The general Methodology adopted in the handwritten numeral recognition system is given in Figure1. The data acquired from various samples forms the database. The raw data is subjected to a number of preliminary processing steps, few of which include binarization, size normalization, etc. In Feature Extraction stage each character is represented as a feature vector, which becomes its identity. The output of previous stage is then applied to the classifier, which generates the final recognized output.

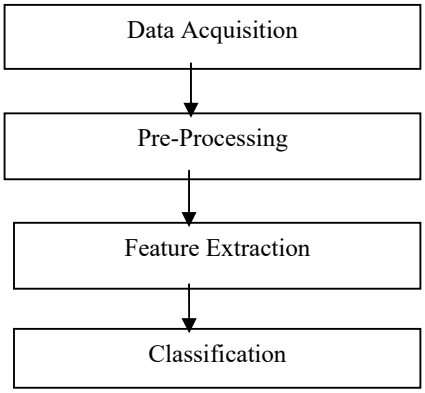


Fig.1 Block diagram of Handwritten Numeral Character Recognition

IV. CONCLUSION

Authors have surveyed majority of approaches in the field of handwritten numeral recognition with respect to aspects such as feasibility, efficiency and accuracy. The authors would wish to extend this study further with some questions, such as is it possible to incorporate both the methodologies that is off-line and on-line in a single system? Is it possible to design a transparent or crystal clear system?

V. REFERENCES

[1] R. Brunelli, *Template Matching Techniques in Computer Vision: Theory and Practice*, Wiley, ISBN 978-0-470-51706-2, 2009 *([1] TM book).*

[2] L. R. Rabiner (1989). A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. *Proceedings of the IEEE*, Vol. 77, No. 2, pp.257-286.

[3] Britto Jr., R. Sabourin, F. Bortolozzi, and C. Y. Suen (2001). A two-stage hmm based system for recognizing handwritten numeral strings. In *Proc. 6th International Conference on Document Analysis and Recognition*, Seattle-USA, September, pp. 396-400.

[4] O.V. Ramana Murthy, M.Hanmandlu, Interactive Fuzzy Model Based Recognition of Handwritten Characters.

[5] Guillevic and C. Y. Suen (1998). HMM-KNN word recognition engine for bank cheque processing. In *Proc. of 14th International Conference on Pattern Recognition*, Brisbane- Australia, August, pp 1526-1529.

[6] L. Mico, J. Oncina (1999). Comparison of fast nearest neighbour classifier for handwritten character recogniton. *Pattern Recognition Letters*, 19(3-4):351-356.

[7] L. S. Oliveira, R. Sabourin (2004). Support Vector Machines for Handwritten Numerical String Recognition, 9th *International Workshop on Frontiers in Handwriting Recognition*, October 26-29, Kokubunji, Tokyo, Japan, pp 39-44.

[8] M. Bishop (1995). *Neural Networks for Pattern Recognition*. Oxford Univ. Press, Oxford- U.K.

[9] J. Schurmann (1996). *Pattern Classification* - A unified view of statistical and neural approaches. Wiley interscience.

[10] R. O. Duda, P. E. Hart, D. G. Stork (2001). *Pattern Classification*. John Wiley and Sons, second edition edition.

[11] Jayashree R. Prasad,Dr. U.V.Kulkarni (2010).Trends in Handwriting Recognition, *Third International Conference on Emerging Trends in Engineering and Technology*. 978-0-7695-4246-1/10.

[12] Flávio Bortolozzi, Alceu de Souza Britto Jr., Luiz S. Oliveira and Marisa Morita. Recent Advances in Handwriting Recognition. *Document Analysis, Editors: Umapada Pal, Swapan K. Parui, Bidyut B. Chaudhuri, pp.1-30.*

Improving Regression Test Coverage Using Parse Tree

[1]G. M. Malik Basha & [2]P. RadikaRaju,

[1&2] Dept. of Computer Science and Engineering, JNTUCEA, Anantapur, india, ,

Abstract:-In this project we investigate on efficient dataflow and slicing techniques to further reduce the instrumentation so that we can get even greater savings in the time for the regression testing. Dynamic Slicingalgorithms can greatly reduce the debugging effort by focusing the attention of the useon a relevant subset of program statements. In this projectthe design and evaluation of three precise dynamic slicingalgorithms called the full preprocessing (FP), no preprocessing (NP) and limited preprocessing (LP) algorithms.The algorithms differ in the relative timing of constructing the dynamic data dependence graph and its traversalfor computing requested dynamic slices. Theseexperimentsshow that the LP algorithm is a fast and practical preciseslicing algorithm. In fact we show that while precise slicescan be orders of magnitude smaller than imprecise dynamicslices, for small number of slicing requests, the LP algorithm is faster than an imprecise dynamic slicing algorithmproposedByAgarwalandHorgan [1and2].

Index Terms:-*Introduction, Regression Testing, Imprecise Algorithm, Full Preprocessing, No Preprocessing, Limited preprocessingAlgorithms.*

1. INTRODUCTION

The technique used for debugging and understanding[3]a program is named program slicing. it works as follows. For any given program P, a slicing criterion is provided by the programmer of the form (l, V), where ‘ l ‘is a control location in the program and ‘ V ’ is a set of program variables referenced at l. The purpose of slicing is to find out the statements in P which can affect the values of V at l via control and/or data flow. So, if during program execution the values of V at l were unexpected”, the corresponding slice can be inspected toexplain the reason for the unexpected values. There are two types of slicing techniques they are Static slicing and Dynamic Slicing.

Static Slicing andDynamic Slicing

For the slicing criterion. Static slicing techniques typically operate on a program dependence graph(PDG).The nodes of the PDG are simple statements/ conditions and the edges correspondtodata/control dependencies [Horwitz et al. 1990].For agiven input of a program P dynamic slices are often smaller than the staticslice of the ProgramP. Dynamic slicing with respect to an input I on the otherhand, often proceeds bycollecting the execution trace corresponding to I. The dynamic data andcontroldependencies between thestatement occurrences inexecution trace can be precomputed or computed on objects and pointers in programs, static slices may bevery large. On the other side, dynamic slices capture the closure of dynamic data and control dependencies. Hence they are much more precise, and more helpful for narrowing the attention of the programmer.The slicing criterion for particular input may affect the dynamic slices of the program fragments,they naturally support the taskof debugging via running of selected test inputs.

Dynamic slicing techniquewas proposed for debugging [Korel and Laski 1988Agrawal and Horgan 1990], subsequently it has been used for pro demand during slicing [Zhang et al. 2005].Static data dependence computations are often conservative due to the presence of gram comprehension in many other innovative ways. In particular, dynamic slices or their variants which also involve computing the closure of dependencies by trace traversal have been used for studying causes of program performance degradation [Zilles and Sohi 2000], identifying isomorphic instructions in terms of their runtime behaviors [Sazeides 2003] and analyzing spurious counter-example traces producedby software model checking [Majumdar and Jhala[2005]. Even in the context of debugging, dynamic slices have been used in unconventional ways e.g. [Akgul et al. 2004] studies reverse execution along a dynamic slice. Thus, dynamic slicing formsthe core of many tasks in program development and it is useful to develop efficientmethods for computing dynamic slices.

In this paper, an infrastructure for dynamic slicing of Java programs has been provided. Our method operates on bytecode traces, we work at the bytecode level since slice computation may involve looking inside library methods and the source code of libraries may not always be available. First, the bytecode stream corresponding to an execution trace of a Java program for a given input is collected. The tracecollection is done by modifying a virtual machine; we have used the Kaffe Virtual Machine in our experiments. We then perform a backward traversal of the bytecodetrace to compute dynamic data and control dependencies on thefly. The slice is updated as these dependencies are encountered during

trace traversal. Computing the dynamic data dependencies on bytecode traces is complicated due to Java's stack based architecture. The main problem is that partial results of a computation are often stored in the Java Virtual Machine's operand stack. This results in implicit data dependencies between bytecodes involving data transfer via the operand stack. For this reason, our backwards dynamic slicing performs a "reverse" stack simulation while traversing the bytecode trace from the end. These methods of dynamic slicing typically involve traversal of the execution trace. This traversal may be used to precompute a dynamic dependence graph or the dynamic dependencies can be computed on demand during trace traversal. Thus, the representation of execution traces is important for dynamic slicing. In the case for backwards dynamic slicing where the trace is traversed from the end .The traces tend to be huge. The work of [Zhang et al. 2005] reports experiences in dynamic slicing programs like gccandperl where the execution trace runs into several hundred million instructions. Itmight be inefficient to perform postmortem analysis over such huge traces. Consequently, it is useful to develop a compact representation for execution traces whichcapture both control flow and memory reference information. During program executioncompact trace should be generated on-the-fly. Our method proceeds by on the fly construction of a compact byte code trace during program execution. The compactness of our trace representation is owing to several factors. First, bytecodes which do not correspond to memory access (i.e.data transfer to and from the heap) or control transfer are not stored in the trace. Operands used by these bytecodes are fixed and can be discovered from Java class files. Secondly, the sequence of addresses used by each memory reference bytecodeor control transfer bytecode is stored separately. Since these sequences typically have high repetition of patterns, we exploit such repetition to save space. We modify a well-known lossless data compression algorithm called SEQUITUR [Nevill- Manning and Witten 1997] for this purpose. This algorithm identifies repeated patterns in the sequence on-the-fly and stores them hierarchically.this algorithm
followed during the execution and each point where data is referenced through pointers we know the address from data is accessed.

2. REGRESSION TESTING

IEEE (Institute of Electrical and Electronics Engineers) defines regression testing as follows: "Regression testing is selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements." [IEEE].During software development projects, there are several design changes that typically result from added new features and error correction work. Customers want new features in the latest releases, but still expect the older features to remain in place. This is where regression testing plays a role. In order to prevent quality from degrading, the new versions of software are retested using a combination of existing test cases. To accomplish this time consuming task effectively, test selection techniques and test automation are recommended.

3. PRECISE DYNAMIC SLICING ALGORITHM

In precise dynamic slicing algorithmbwe execute the program once and produce the execution trace that is processed to construct dynamic datadependence graphwhich in turn is traversed to compute the dynamic slices. The execution trace captures the complete runtime information of the programs execution used by the dynamic slicing algorithm. There is sufficient information To compute the precise dynamic slices. The information that the trace holds the full control flow trace and memory reference trace. Thus we can Know the complete path

3.1 Full Preprocessing Algorithm

The main aim of developing full preprocessing slicing algorithm is to achieve dynamic data dependence graph representation that would not only allow for computation of precise dynamic slices. It supports computation of dynamic slices for variables and memory address at any point of execution. This property is not supported by the precise dynamic slicing algorithm of Agrawal and Horgan [1]. Here we consider the statement level control flowgraph representation of the program and add it to the edges corresponding to the data dependences extracted from the execution trace. The execution instances of the statements involved in the dynamic data dependence are explicitly indicated on the dynamic data dependence edges thus allowing the above goal to be met. it is equally easy to compute a dynamic slice atany earlier execution point.

3.2. No Preprocessing Algorithm

The Full preprocessing algorithm first carries out all preprocessing and then starts slicing. For large program with long execution run it is possible that the dynamic dependence graph requires too much space to store and too much space to build. The experiment shows that too often run out off memorysince the graphs are too large. For this reasons we propose precise dynamic slicing algorithm that do not perform any preprocessing.To avoid prior preprocessing we can use demand driven analysis of the trace to

recover dynamic dependences when a slice computation begins we traverse the trace backwards to recover the dynamic dependences required for the slice computation. If we need to the dynamic lices for the variable vat the end of the program, we traverse it in backward until the definition of the variable v is found and include the defining statement in the dynamic slice. If v is defined in terms of other variable w, we resume the traversal of the trace starting from the point where the traversal had stopped upon finding the definition of v and so on.

3.3 Limited Preprocessing

While the NP algorithm described above addresses the space problem of the FP algorithm, this comes at the cost of increased time for slice computations. The time required to traverse a long execution trace is a significant part of the cost of slicing. While the FP algorithm traverses the trace only once for all slicing requests, the NP algorithm often traverses the same part of the trace multiple times, each time recovering different relevant dependences for different slicing request.With the above discussion we can say that No Preprocessing algorithm does too little preprocessing leading to high slicing cost while Full Preprocessing perform too much preprocessing leading to the space problems. next we propose an algorithm that strikes the balance between the preprocessing and slicing cost. In this precise algorithm first we carry out limited preprocessing of the execution trace augmenting the trace with summary information that allows faster traversal of the augmented tracefor this we use demand driven analysis to compute the slice using the augmented trace. This algorithm is called as limited preprocessing algorithm (LP).In LP algorithm the trace is divided into fixed size trace blocks .At the end of each traceblock we store a summary of all downwards exposed definitions of variables names and memory addresses. During the backward traversal for slicing , when looking for variable names and the memory addresses, we firs tlok at their presence in the summary downward exposed definitions. If the definition is found then we traverse the trace block to locate the definition.otherwise using the size information we skip away to start of the trace block.

4. CONCLUSION

In this paper we have shown the design of a dynamic slicing can greatly improve its practicality. We designed and studied three different precise dynamic slicing algorithms: FP, NP, and LP. We made the use of demand driven analysis (with and without caching) and trace augmentation (with trace block summaries) to achieve practical implementations of precise dynamic slicing. We demon-strated that the precise LP algorithm which first performs limited preprocessing to augment the trace and then usesdemand driven analysis performs the best. In comparison to with other algorithms LP runs faster for small number of slices.In conclusion this paper we shows that imprecise dynamic slicing algorithms are too imprecise and therefore not a better option, a carefully designed precise dynamic slicing algorithm such as the *LP* algorithm is practical as it provides precise dynamic slices at reasonable space and time costs.

5. REFERENCES

[1]. H. Agrawal and J. Horgan, “Dynamic Program Slicing,” ACMSIGPLAN Conference on Programming Language Design And Implementation (PLDI), pages 246-256, 1990.

[2]. H. Agrawal, R. DeMillo, and E. Spafford, “Debugging with Dynamic Slicing and Backtracking,” Software Practice and Experience SP&E), Vol. 23, No. 6, pages 589-616, 1993.

[3]. Weiser, M. 1984. Program slicing. IEEE Transactions on Software Engineering 10, 4, 352-357.

[4]. B. Korel and J. W. Laski. Dynamic program slicing. Information Processing Letters, 29(3):155–163, 1988.

[5]. C. G. Nevill Manning and I. H. witten. Linear time, Incremental hierarchy inferences for compressionIn Data Compression Conference(DCC), pages 3–11, 1997.

[6]. J. Zhao. Dependence analysis of Java bytecode. In IEEE Annual International Computer Software and Applications Conference, pages 486–491, 2000.

[7]. Akgul, T. , Mooney, V. , and Pande, S. 2004. A fast assembly level reverse execution method via dynamic slicing. In International Conference on Software Engineering (ICSE). IEEE Computer Society, Edinburgh, Scotland, UK, 522–531.

[8]. Sazeides, Y. 2003. Instruction isomorphism in program execution. Journal of Instruction-Level Parallelism 5.

[9]. Zhang, X. , Gupta, R. , and Zhang, Y. 2005. Cost and precision tradeoffs of dynamic data slicing algorithms. ACM Transactions on Programming Languages and Systems (TOPLAS) 27, 631–661.

[10]. Majumdar, R. and Jhala, R. 2005. Path slicing. In Intl. Conf. on Programming Language Design and Implementation (PLDI).ACM, Chicago, IL, USA.

◈◈◈

Energy efficient cluster based routing mechanism forWireless sensor networks

[1]Swami Naik J, [2]M.Jagadeeshwara Reddy, & [3]Indira Priyadarshini Y

[1,2&3]CSE Department, G. PullaReddy Engineering College (autonomous), Kurnool

Abstract- The Wireless sensor networks is one of the premier research are from past few decades, so the need to maintain energy efficient routing between from the nodes to base station, proper data aggregation and scalability is the important concern.In hierarchical routing LEACH is one of the energy efficient clustering protocol, but only the problem is size of the clusters are not same either they may be small or large ,which causes to reduce the network lifetime. The other protocol FZ-LEACH addresses the LEACH problem by selecting some random cluster heads, but not energy efficient. In this paper, we propose a new protocolenhanced far-zone cluster based routing protocol with optimized algorithm(FZ-CRP), form's cluster heads and zone heads based on the intra communication cost and energy. If the node's energy is the less than or equal to average minimum reach ability power then that node is said to be in far zone , far zone node transmits the data to base station via far zone, cluster heads.The performance of the proposed is better when we compare with existed scenarios.

Keywords**:** *wireless sensor network, clusterhead, cluster formation, network life time and energy consumption, leach protocol.*

I.INTRODUCTION

Sensor networks have emerged as a promising tool for monitoring (and possibly actuating) the physical worlds, utilizing self-organizing networks of battery-powered wireless sensors that can sense, process and communicate[1]. In sensor networks, energy is a critical resource, while applications exhibit a limited set of characteristics. Wireless sensor network is a large network consists of several nodes called sensor nodes which transmits the data to/from a fixed wired station called base station (BS),serves as a gateway in the network. The applications of wireless sensor network include military field, structural health, environment etc.,[2,3,4].

The main objective is to achieve energy efficiency with limited resource. Hence the node does not communicate with another node where the energylevel at the initial state and while transmission state are equal. In order to overcome this draw back a new protocol is designed by considering the improved version of energy factor.

The FZCRP is a hierarchical based routing protocol, which enforces the structure of a network to use energy efficiency, extend the lifetime, and scalability.in this protocol clusters are created and a head node is assigned to them, which acts as a leader for the remaining nodes in each and every cluster, it has the responsibilities like collection and aggregating the data from the respective cluster and transmitting the aggregated data to the base station[5]. This data aggregation in each and every cluster greatly reduces the energy utilization in the network where the messages are to be send to the base station. This paper presents an extension to the protocol FZCRP[6] based on different power levels for wireless sensor network. The proposed protocol FZCRP maintains the energy consumption during the transmissions in order to increase the lifetime of a sensor node.

The remaining part of the paper is arranged s follows.an overview of related work is given by section 2, section 3 describes the implementation of (FZCRP) far-zone cluster based routing protocol .Simulation and analysis results are discussed in section 4.in section 5,the paper conclusion work and the future scope is presented.

II. RELATED WORK

Low-Energy Adaptive Clustering Hierarchy (LEACH) [7] is a clustering based protocol to collect data from wireless network. In the network, hundreds and thousands of wireless sensors are dispersed that collects and transmit data. In the network cluster heads are elected among the sensor nodes in order to transmit the data collected to the base station.in the network the sensor node being in expensive and simple their power level is low and cannot be replaced by the another node, because of this each sensor in the cluster must take its turn as being a cluster head to make the protocol energy efficient.

Once the cluster head is selected the remaining non cluster heads decides its cluster for this round which requires minimum communication energy based on the received signal strength of the advertisement from each cluster head which is shown in the following fig.The cluster head node in leach uses TDMA schedule in order to transmit the data among the nodes which are present in cluster, it also uses CDMA schedule to transmit the data from one cluster head to another cluster head to reach the data to sink node it uses single hop routing, where it is not applicable in larger networks.

The leach protocol has some deficiencies such as,

1. The initial state and transition state of cluster head uses same energy level.

2. Some large clusters and small clusters may exist in the network at the same time.
3. In this protocol the selection of cluster head is done frequently which changes the network layer and increases the cost of energy.

In leach protocol the cluster head which is far away from the base station requires large amount of energy to transmit the data to base station. Multi hop leach protocol is used to solve this problem by simply changing the transmission mode between cluster head and base station from single hop to multi hop, chooses the best possible path between cluster head and base station by using the other cluster heads as relay stations to send the data to base station.

In leach protocol the cluster heads are not uniformly distributed so, leach-c an improved version of leach is used .this protocol uses the centralised clustering algorithm and a steady state phase that is used by leach.InLEACH – C[8] the node sends their current location information and residual energy level to sink, which calculate the average node energy and finds which node energy is below the average.

In LEACH protocol the cluster head is responsible for receiving data from cluster members, data and then send it to the base station. If base station may be far away from cluster head, the cluster head dies then the data collected by the cluster head will never reach to the base station and therefore the cluster will become useless.

V-LEACH[9] protocol solves this problem by introducing the vice-cluster head acts as a cluster head while the real cluster head dies and start working as cluster head and the cluster head data will reach to the base station. There is no need to elect the new cluster head, so it will save the energy and enhance the network life time.

III. FZ-LEACH PROTOCOL

In this section we present an improvement in pre-existing, well known clustering protocol LEACH, proposed by Heilzemen *et al.* [5]. One major drawback of this protocol is that size of the cluster is not limited; clusters in LEACH may be very small or very large in size. In large clusters sensornodes deplete energy faster because of the transmission distance. Here we propose a solution to this problem by introducing the concept of Far-Zone. The working of algorithm can be divided into two phases.

A. Cluster-head Selection and Cluster Formation Algorithm

In the proposed algorithm, cluster head selection and cluster formation is done in same manner as LEACH. The operation of FZ-LEACH is generally divided into two phases, the set-up phase and the steady-state phase. In the set-up phase, cluster heads are selected and clusters are organized. Inthe steady-state phase, the actual data is transmitted to the sink station. In the proposed FZ-LEACH algorithm, few nodes are randomly selected as CHs. This role is rotated to all nodes to balance the energy dissipation of the sensor nodes in thenetworks. Cluster head formation and creation for the algorithm is shown in the figure 1.

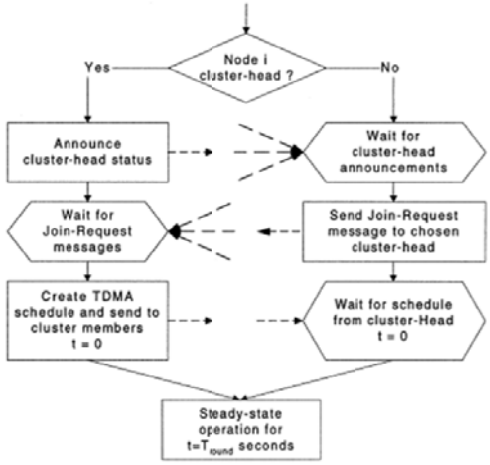


Fig.1. Cluster head selection and formation in proposed FZ-CRP

During the set-up phase, when clusters are being created, each node decides whether or not to become a cluster head for the current round. This decision is based on a predeterminedfraction of nodes and the threshold T(s) given by following equation.

$$T(n) = \frac{P}{1 - P \times (r \bmod P^{-1})} \quad \forall n \in G$$

$$T(n) = 0 \quad \forall n \in G$$

Where n is a random number between 0 and 1
P is the cluster-head probabilty and
G is the set of nodes that weren't cluster-heads the previous rounds

where*popt*is the predetermined percentage of cluster heads (e.g., *popt*= 0.05), r is the current round, and G is the set of nodes that have not been cluster heads in the last 1/ *popt* rounds. Using this threshold, each node will be a cluster headat some round within 1/ *popt*rounds. After 1/ *popt*rounds, all nodes are once again eligible to become cluster heads. In FZLEACH, the optimal number of cluster heads is estimated to be about 5% of the total number of nodes.

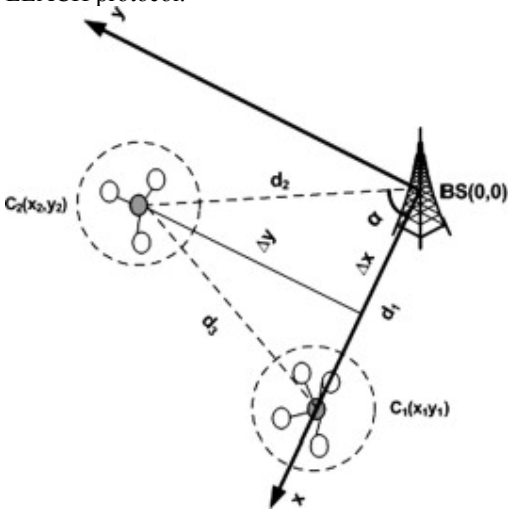
Each node that has elected itself cluster head for the current round broadcasts an advertisement message to the restof the nodes in the network. All the non-cluster head nodes, after receiving this advertisement message, decide on thecluster to which they will belong for this round. This decisionis based on the received signal strength of the advertisement messages. In this way cluster formation is done in FZLEACH.

After cluster head receives all the messages from the nodes that would like to be included in the cluster and based on the number of nodes in the cluster, the cluster head creates a TDMA schedule and assigns each node a time slot when it can

transmit.

B. Far-Zone Formation Algorithm

Most of the percentage of nodes energy is consumed in long distance transmissions. One of the solutions to efficiently utilize the energy in LEACH protocol is formation of Far- Zone in large clusters formed by LEACH protocol.



Once the cluster head formation is complete, proposed algorithm searches for eligible clusters to form Far-Zone. For formation of Far-Zone each node of the cluster sends its power level to CH.

V. SIMULATION AND ANALYSIS

This section compares the performance of proposed algorithm with LEACH protocol. The performance evaluation includes two parts: network lifetime and energy consumption. The sensors are simulated to deploy over a square sized area of l00m x l00m with variable communication range.

Simulation is performed using ns-2 [10], a discrete event network simulator. We have compared the performance of FZLEACH with LEACH. The basic parameters used are listed inTable-I.

TABLE I. SIMULATION PARAMETERS

Parameter	**Value**
Number of nodes	100
Network grid	100 100 m
Base station position	50 X 175 m
*fs*ε	10 pJ/bit/m2
mp ε	0.0013 pJ/bit/m4
elect E	50 nJ/bit
Size of data packet	500 bits
Initial energy of normal nodes	1 J

Figure 5: illustrates the performance comparison of LEACH,FZLEACHandFZCRP in terms of energy dissipation. As shown in Figure 5, energy consumption of FZ-LEACH is less than LEACH protocol in all cases thus it is energy-efficient and has optimum performance with comparing to LEACH.The reason is clear that the sensor nodes within the Far-Zone have not to transmit for long distances that save a significant amount of energy.

Figure 5.Energy dissipation analysis.

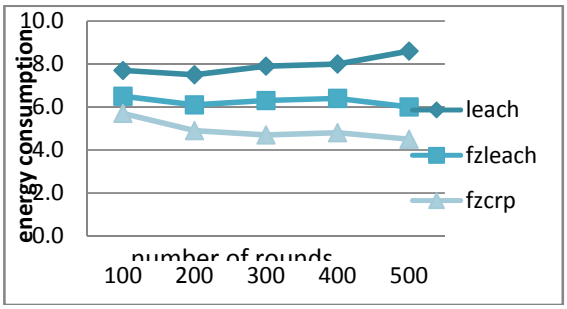


Figure 5.Energy dissipation analysis.

Figure 6 illustrates the performance of our algorithm comparing to LEACH,FZLEACH algorithm in terms of network lifetime. As it is clear from Figure 6 that sensor network performs longer with FZCRP in comparison to,LEACH,FZ- LEACH. This is due to energy saving in transmission by the sensor nodes in Far- Zone.

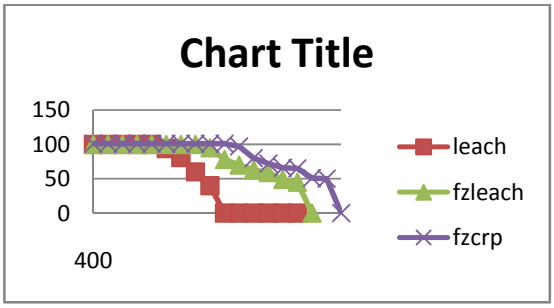


Figure 6. Network lifetime analysis.

VI. CONCLUSION

In this paper we have proposed an improvement in LEACH protocol to overcome the shortcoming in this well-known and widely used protocol for clustering in wireless sensor networks. We have proposed FZ-LEACH algorithm, which is based on the original protocol and considers a Far-Zone inside a large cluster. Simulation results prove the improvement in the performance in the original LEACH protocol in terms of energy dissipation rate and network lifetime. It is found that FZ-LEACH protocol saves around 30% energy of sensor network in comparison to LEACH.

VII. REFERENCES:

[1] Holger Karl and Andreas Willig. "Protocols and Architecture for Wireless sensor networks," Wiley, 2005. ISBN:0470095105.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey".

[3] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A Survey on Sensor Networks," IEEE Communications Magazine, Aug. 2002.

[4] M. Tubaishat, S. Madria, " Sensor Networks: An verview",IEEE Potentials, Volume 22, Issue 2,pages 20 -23, April2003.

[5] SHANG Fengjun, "A Distributed Clustering Algorithm for ireless Sensor Networks," Wuhan University Journal of Natural Sciences 2008, Vol.13 No.4, 385-390.

[6] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks," IEEE Transactions on Mobile Computing, Vol. 3, No. 4, 2004, pp. 366–379.

[7] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energyefficient Communication Protocol for Wireless Sensor Networks," *Proceeding of the Hawaii International Conference on System Sciences*, Hawaii, January 2000, pp. 1-10.

[8] W.B. Heinzelman, A.P. Chandrakasan and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670.

[9] M. BaniYassein, A. Al-zou'bi, Y. Khamayseh and W. Mardini, "Improvement on LEACH Protocol of Wireless Sensor Network (VLEACH)," International Journal of Digital Content Technology and its Applications, Vol. 3, No. 2, June 2009, pp. 132-136.

[10] VINT Project. The ucb/lbnl/vint network simulator-ns. http://www.isi.edu/nsnam/ns.

SECTION –II

ARTIFICIAL INTELLIGENCE & SOFT COMPUTING

Emulation

Ashish Jaggi

IMS CD&R, University of Pune, Ahmednagar Maharastra,

Abstract–The Recreation of current hardware of the technical environment required to view and use digital objects from earlier times or of different type. Emulation is the process of bringing digital objects back to life in their original environment on top of a different computer environment. This process is carried out by an emulator. It is a program that runs on one computer and thereby virtually recreates a different computer. Emulators are based on powerful yet portable object oriented languages like C++, Java. In Layman's language we can say that Emulation is the art to mimic one's ability by a totally different entity. For example: our mobile handset was designed for making calls but it also contains a clock, personal manager, dictionary, conversion table, etc. Due to this we don't need to carry these things.

Index Terms– *computer environment, Emulator, mimics.*

I. WHAT IS AN EMULATOR?

A program which maps and executes instructions intended for architecture to the host machine's architecture. This allows omeone to run software on a machine in which it was not intended to run on. Emulation refers to the ability of a computer program or electronic device to imitate another program or device. Many printers, for example, are designed to emulate Hewlett-Packard LaserJet printers because so much software is written for HP printers. By emulating an HP printer, a printer can work with any software written for a real HP printer. Emulation "tricks" the running software into believing that a device is really some other device. A hardware emulator is an emulator which takes the form of a hardware device. Examples include the DOS-compatible card installed in some old-world Macintoshes like Centris 610 or Performa 630 that allowed them to run PC rograms and FPGA-based hardware emulators. In a theoretical sense, the Church-Turing thesis implies that any operating environment can be emulated within any other. However, in practice, it can be quite difficult, particularly when the exact behavior of the system to be emulated is not documented and has to be deduced through reverse engineering. It also says nothing about timing constraints; if the emulator does not perform as quickly as the original hardware, the emulated software may run much more slowly than it would have on the original hardware, possibly triggering time interrupts to alter performance.

II. STRUCTURE OF AN EMULATOR

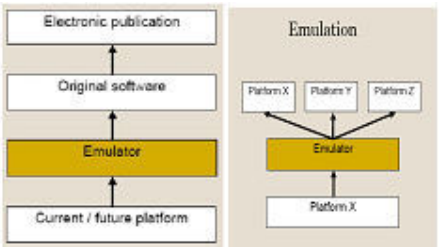


Fig1: Structure of Emulator & multiple platform Demo

Typically, an emulator is divided into modules that correspond roughly to the emulated computer's subsystems. Most often, an emulator will be composed of the following modules:

A. *CPU emulator or CPU simulator (the two terms are mostly interchangeable in this case).*

B. Memory subsystem module Various I/O devices emulators.

C. Buses are often not emulated, either for reasons of performance or simplicity, and virtual peripherals communicate directly with the CPU or the memory subsystem.

III. SPEED HIERARCHY

The word "emulator" was coined in 1957 at IBM, as an optional feature in the IBM 709 to execute legacy IBM 704 programs on the IBM 709. Registers and most 704 instructions were emulated in 709 hardware. Complex 704 instructions such as floating

point trap and input-output routines were emulated in 709 software. In 1963, IBM constructed emulators for development of the NPL (360) product line, for the "new combination of software, microcode, and hardware". It has recently become common to use the word "emulate" in the context of software. However, before 1980, "emulation" referred only to hardware emulation, while "simulation" referred to software emulation. In contrast, a simulator could be a program which runs on a PC, so that old Atari games can be run on it. Purists continue to insist on this distinction, but currently the term "emulation" often means the complete imitation of a machine executing binary code.

IV. WHY USE EMULATION

A. Emulators maintain the original look, feel, and behavior of the digital object, which is just as important as the digital data itself.

B. Despite the original cost of developing an emulator, it may prove to be the more cost efficient solution over time.

C. Reduces labor hours, because rather than continuing an ongoing task of continual data migration for every digital object, once the library of past and present operating systems and application software is established in an emulator, these same technologies are used for every document using those platforms.

D. Many emulators have already been developed and released under GNU General Public License through the open source environment, allowing for wide scale collaboration.

Because of its primary use of digital formats, new media artrelies heavily on emulation as a preservation strategy.

Artists such as Cory Archangel specialize in resurrecting obsolete technologies in their artwork and recognize the importance of a decentralized and deinstitutionalized process for the preservation of digital culture. In many cases, the goal of emulation in new media art is to preserve a digital medium so that it can be saved indefinitely and reproduced without error, so that there is no reliance on hardware those ages and becomes obsolete. The paradox is that the emulation and the emulator have tobe made to work on future computers.

V. COMPUTER EMULATION

A. An emulator in computer sciences duplicates (provides an emulation of) the functions of one system using a different.

B. System, so that the second system behaves like (and appears to be) the first system. This focus on exact reproduction.

C. External behavior is in contrast to some other forms.

D. Computer simulation, which can concern an abstract model of the system being simulated. E. In a theoretical sense, the Church-Turing thesis implies that any operating environment can be mulated within any other.

However, in practice, it can be quite difficult, particularly when the exact behavior of the system to be emulated is notdocumented and has to be deduced through reverse engineering. It also says nothing about timing constraints; if the emulator does not perform as quickly as the original hardware, the emulated software may run much more slowly than it would have on the original hardware, possibly triggering time interrupts to alter performance.

VI. CONSOLE EMULATION

Console emulators are programs that allow a computer or modern console to emulate a video game console. They are most often used to play older video games on personal computers and modern video game consoles, but they are also used to translate games into other languages, to modify existing games, and in the development process of homebrewed demos and new games for older systems. Developers of software for embedded systems or video game consoles often design their software on especially accurate emulators called simulators before trying it on the real hardware. This is so that software can be produced and tested before the final hardware exists in large quantities. So that it can be tested without taking the time to copy the program to be debugged at a low level without introducing the side effects of a debugger. In many cases, the simulator is actually produced by the company providing the hardware, which theoretically increases its accuracy.

VII. STRUCTURE OF EMULATION

Typically, an emulator is divided into modules that correspond roughly to the emulated computer's subsystems. Most often, an emulator will be composed of the following modules:

A. A CPU emulator or CPU simulator (the two terms are mostly interchangeable in this case)

B. A memory subsystem module

C. Various I/O devices emulators

Buses are often not emulated, either for reasons of performance or simplicity, and virtual peripherals communicate directly with the CPU or the memory subsystem.

Memory subsystem

It is possible for the memory subsystem emulation to be reduced to simply an array of elements each sized like an emulated word; however, this model falls very quickly as soon as any location in the computer's logical memory does not match physical memory. This clearly is the case whenever the emulated hardware allows for advanced memory management (in which case, the MMU logic can be embedded in the memory emulator, made a module of its own, or sometimes integrated into the CPU simulator). Even if the emulated computer does not feature an MMU, though, there are usually other factors that break the equivalence between logical and physical memory: many (if not most) architecture offer memory-mapped I/O; even those that do not almost invariably have a block of logical memory mapped to ROM, which means that the memory-array module must be discarded if the read-only nature ofROM is to be emulated. Features such as bank switching or segmentation may also complicate memory emulation. As a result, most emulators implement at least two procedures for writing to and reading from logical memory, and it is these procedures' duty to map every access to the correct location of the correct object. On a base-limit addressing system where memory from address 0 to address ROMSIZE-1 is read-only memory, while the rest is RAM, something along the line of the following procedures would be typical

```
void WriteMemory(word Address, word Value) {
    word RealAddress;
    RealAddress = Address + BaseRegister;
    if ((RealAddress < LimitRegister) &&
        (RealAddress > ROMSIZE)) {
        Memory[RealAddress] = Value;
    } else {
        RaiseInterrupt(INT_SEGFAULT);
    }
}
word ReadMemory(word Address) {
    word RealAddress;
    RealAddress=Address+BaseRegister;
    if (RealAddress < LimitRegister) {
        return Memory[RealAddress];
    } else {
        RaiseInterrupt(INT_SEGFAULT);
        return NULL;
    }
}
```

Fig2: Sample of a Code to generate a Ghost RAM for an Emulator.

CPU simulator

The CPU simulator is often the most complicated part of an emulator. Many emulators are written using "pre-packaged"
CPU simulators, in order to concentrate on good and efficient emulation of a specific machine. The simplest form of a CPU simulator is an interpreter, which follows the execution flow of the emulated program code and, for every machine code instruction encountered, executes operations on the host processor that are semantically equivalent to the original instructions. This is made possible by assigning a variable to each register and flag of the simulated CPU. The logic of the
simulated CPU can then more or less be directly translated into software algorithms, creating a software re-implementation that basically mirrors the original hardware implementation.
The following example illustrates how CPU simulation can be accomplished by an interpreter. In this case, interrupts are checked-for before every instruction executed, though this behavior is rare in real emulators for performance reasons.

```
void Execute(void) {
    if (Interrupt != INT_NONE) {
        SuperUser = TRUE;
        WriteMemory(++StackPointer,
ProgramCounter);
        ProgramCounter = InterruptPointer;
    }
    switch (ReadMemory(ProgramCounter++)) {
        /*
         *    Handling    of    every    valid
instruction
         * goes here...
         */
        default:
        Interrupt = INT_ILLEGAL;
    }
}
```

Fig3: Sample of a Code to generate a Ghost CPU for an Emulator.

Interpreters are very popular as computer simulators, as they are much simpler to implement than more

time-efficient alternative solutions, and their speed is more than adequate for emulating computers of more than roughly a decade ago on modern machines. However, the speed penalty inherent in interpretation can be a problem when emulating computers whose processor
speed is on the same order of magnitude as the host machine. Until not many years ago, emulation in such situations was considered completely impractical by many. What allowed breaking through this restriction were the advances in dynamic recompilation techniques. Simple a priori translation of emulated program code into code runnable on the host architecture is usually impossible because of several reasons:

A. Code may be modified while in RAM, even if it is modified only by the emulated operating system when loading the code (for example from disk)

B. There may not be a way to reliably distinguish data (which should not be translated) from executable code.

Various forms of dynamic recompilation, including the popular Just In Time compiler (JIT) technique, try to circumvent these problems by waiting until the processor control flow jumps into a location containing un-translated code, and only then ("just in time") translates a block of the code into host code that can be executed. The translated code is kept in a code cache, and the original code is not lost or affected; this way, even data segments can be (meaninglessly) translated by the recompiler, resulting in no more than a waste of translation time. Speed may not be desirable as some older games were not designed with the speed of faster computers in mind. A game designed for a 30 MHz PC with a level timer of 300 game seconds might only give the player 30 seconds on a 300 MHz PC. Other programs, such as some DOS programs, may not even run on faster computers. Particularly when emulating computers which were "closed-box", in which changes to the core of the system were not typical, software may use techniques that depend on specific characteristics of the computer it ran on (i.e. its CPU's speed) and thus precise control of the speed of emulation is important for such applications to be properly emulated. I/O Most emulators do not, as mentioned earlier, emulate the main system bus; each I/O device is thus often treated as a special case, and no consistent interface for virtual peripherals is provided. This can result in a performance advantage, since each I/O module can be tailored to the characteristics of the
emulated device; designs based on a standard, unified I/O API can, however, rival such simpler models, if well thought-out, and they have the additional advantage of "automatically" providing a plug-in service through which third-party virtual devices can be used within the emulator. A unified I/O API may not necessarily mirror the structure of the real hardware bus: bus design is limited by several electric constraints and a need for hardware concurrency management that can mostly be ignored in a software implementation. Even in emulators that treat each device as a special case, there is usually a common basic infrastructure for:

A. Managing interrupts, by means of a procedure that sets flags readable by the CPU simulator whenever an interrupt is raised, allowing the virtual CPU to "poll for (virtual) interrupts"
B. Writing to and reading from physical memory, by means of two procedures similar to the ones dealing with logical memory (although, contrary to the latter, the former can often be left out, and direct references to the memory array be employed instead).

VIII. CONCLUSION

A. Most emulators are built on the principle of reverse engineering. Reverse engineering entails mimicking the behavior of an existing code. B. Base without directly copying it. Sometimes in the process of reverse engineering, code on the original platform is decompiled.

C. Disassembled into an intermediate form so its behavior can be determined. The disassembly or de compilation of code for such study could.

D. Be interpreted as creating a derivative work, it is generally carried out by two different people under a "clean room" technique: one.

E. Person writes the specification and the other later codes the result, so that the coder has not seen the original code.

REFERENCES

[1] Marc Boulé and Zeljko Zilic, "Generating Hardware Assertion Checkers: For Hardware Verification, Emulation, Post-Fabrication Debugging and On-Line Monitoring".
[2] Wikipedia.com
[3] Emulasylum.com
[4] Coolrom.com
[5] Pearpc.com

◈◈◈

Personal Authentication by Fusion of PCA and FFT Coefficients of Iris

[1]Prashanth C R, [2]K B Raja, [3]Venugopal K R, & [4]L M Patnaik

[1]Department of Electronics and Communication Engineering,
Vemana Institute of Technology, Bangalore, India
[2, 3] Department of Computer Science and Engineering University,
Visvesvaraya College of Engineering , Bangalore, India
[4]Honorary Professor, Indian Institute of Science, Bangalore India

Abstract—Iris based Biometric systems are more efficient compared to the systems based on other Biometric traits. In this paper, Personal Authentication by Fusion of PCA and FFT Coefficients of Iris (PAFPFCI) is proposed. The CASIA Iris database is considered for the performance analysis. The pre-processing step includes resizing, binarization, cropping and splitting the Iris image into left half and right half. The Fast Fourier Transform (FFT) is applied on the left portion of the Iris to generate absolute value of FFT coefficients. The Principal Component Analysis (PCA) is applied on right portion of Iris to generate Eigen vectors. The FFT and PCA coefficients are fused using arithmetic addition to generate final feature vector set. The test Iris features are compared with the database feature set using Euclidean Distance to identify persons. It is observed that the performance parameters such as FRR, FAR and TSR values are better in the case of proposed algorithm compared to the existing algorithms.

Keywords- *Iris Recognition; PCA; FFT; TSR; Euclidean Distance;*

I. INTRODUCTION

Identity checking through traditional methods is carried out by identity cards, pin codes, smart cards, passwords etc., but these are transferable and stolen. A better way of individual identification is based on human biological features, which leads to biometric identification. The biometric authentication includes physiological and behavioral traits. The physiological traits are parts of the human body and are almost constant through out the life time. They include iris, retina, face, finger print, DNA etc. The behavioral traits such as voice, signature, key stroke dynamics and gait, depend on mood and circumstances. The physiological and behavioral biometric features shall posses the following desirable characteristics: *Universality, Distinctiveness, Permanence, Collectability*, and *Acceptability.*

The biometric system can be utilized in two contexts: verification and identification. Verification is a one-to-one match in which the biometric system tries to verify a person's identity by comparing the distance between test sample and the corresponding sample in the database, with a predefined threshold. If the computed distance is smaller than the predefined threshold, the subject is accepted as being genuine, else the subject is rejected. Identification is a one-to-many match in which the system compares the test sample with all the samples in the database and chooses the sample with the minimum computed distance i e., greatest similarity as the identified result. If the test sample and the selected database sample are from the same subject, it is a correct match. The term

authentication is often used as a synonym for verification. Among all the biometric techniques, Iris Recognition has drawn a lot of interest in Pattern Recognition and Machine Learning research area because of the advantages viz., (i) The Iris formation starts in the third month of gestation period and is largely complete by the eighth month. (ii) The human Iris might be as distinct as the Finger Prints for the different individuals. (iii) The forming of Iris depends on the initial environment of the Embryo and hence the Iris Texture Pattern does not correlate with genetic determination. (iv) The left and the right Irises of the same person are unique. (v) It is impossible to modify the Iris structure by surgery. (vi) The Iris Recognition is non-invasive.

Iris lies between the sclera and the pupil of human eye. Iris is an internal organ and is well protected by the eye-lid when compared to other physiological characteristics. Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high-resolution images of the irides of an individual's eyes. Iris scanning is less intrusive of the eye related biometrics, requires camera with Infra-red illumination and without physical contact of a person. Iris recognition efficacy is rarely impeded by glasses or contact lenses.

An Iris pattern contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. The striated trabecular mesh work of elastic pectinate ligament creates the predominant texture under visible light whereas in the near infrared wavelengths stromal features dominate the Iris pattern [1].

The accuracy, efficiency, robustness, applicability and universality can be improved by biometric fusion. The spatial domain features can be fused to spatial domain feature or transform domain feature to

generate final feature vector. Researchers have shown that the use of biometric fusion provides better authentication performance. The different levels of fusion are: (i) fusion at the feature extraction level, (ii) fusion at the matching score level, (iii) fusion at decision level [2].

Iris Biometric systems are widely used in many applications such as access control to secure facilities, verification of financial transactions, welfare fraud protection, law enforcement, and immigration status checking when entering a country [3].

Contribution: In this paper, Personal Authentication by Fusion of PCA and FFT Coefficients of Iris is proposed. Resizing, binarization, cropping and splitting are performed for pre-processing an Iris image. FFT and PCA are applied on the left and right sides of the pre-processed Iris image respectively. The extracted features are fused by using an arithmetic addition operator. Finally, matching between the test image and database image is done by using Euclidian Distance.

Organization: The paper is organized as follows. Section I gives a brief introduction to biometrics and Iris recognition. In Section II, related works are discussed. In Section III, the proposed PAFPFCI model is discussed. In Section IV, the algorithm presented. The performance analysis is given in Chapter V and conclusion in Chapter VI.

II. LITERATURE SURVEY

The existing techniques are described for individual recognition using the Iris recognition system in this section.

Daugman [4] proposed a phase based Iris recognition system where localization is done using the Integro- differential operator. The phase information is extracted using quadrature 2-D Gabor wavelets and Iris recognition is done by test of statistical independence, involving many degrees of freedom. Xiaomei Liu et al., [5] proposed an Iris recognition system with high accuracy. Focus was mainly on variation of performance of the system with image quality and the amount of user cooperation required in real time environment. Karen Hollingsworth et al., [6] proposed techniques to increase recognition rates using fragile bit masking, signal-level fusion of iris images, and detecting local distortions in Iris texture. Fragile bit masking eliminates the effects of inconsistencies in Iris code that arise from the quantization of the complex filter response in a canonical Iris biometrics algorithm.

Wildes [7] proposed a system based on texture analysis. Isolation of an Iris is done by simple filtering and histogram operations. Localization is done through edge detection and Hough transform. Emine Krichen et al., [8] proposed a method that relied on use of packets of wavelets for the production of an Iris code. A hybrid method is used for Iris segmentation. Hough transform is used to locate the outer boundary and Integro-differential operator is used to detect the inner boundary of an Iris. Sateesh Kumar et al., [9] proposed Iris recognition using Empirical Mode Decomposition (EMD) and Fast Fourier Transform (FFT). The eye image is pre-processed, using Circular Hough Transform and Daugman's Rubber Sheet model. The EMD and FFT are applied on the pre-processed image for features extraction. Raju Dehankar et al., [10] explained edge detection technique for Iris using Haar wavelet. Anuradha Shrivas and Preeti Tuli [11] proposed Iris recognition algorithm based on Hough transform for localization and removal of occlusions. The outer boundary of Iris is obtained by circular summation of intensity. The localized Iris image transformed from Cartesian to polar coordinate system. Corners in the transformed Iris image are detected using covariance matrix of change in intensity along rows and columns. All the detected are corners are features.

III. PROPOSED PAFPFCI MODEL

Figure 1 shows the block diagram of the proposed model. The Iris image is read from the database. Pre-processing is performed to get the desired part of the Iris and exclude the unwanted information. The required feature is extracted using FFT and PCA. The matching between the database image and test image are done using the Euclidean Distance.

A. Iris database

The CASIA Iris database version 1.0 is used as input to the system. The database consists of Iris images from 108 persons. Each person has 7 Iris images. There are total of 756 Iris images. The database is created using 50 peoples' Iris images and 58 peoples' are out of database. The 6 Iris images per person out of 7 images per person are retained in the database and remaining one is used as test image. This classification is done for the computation of FRR, TSR and EER. The FAR computation is done using the out of database images only.

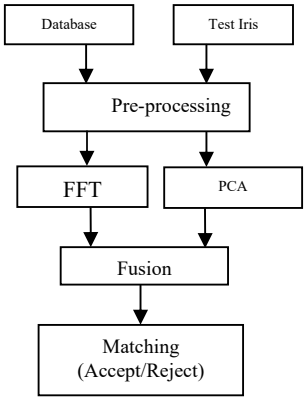


Figure 1. The proposed PAFPFCI model.

B. Pre-processing:

The CASIA database eye image is as shown in Figure 2. The image is resized to 100*300. The eye

image is binarized to locate pupil. It is observed that the intensity values of the pixels in pupil are between 0 and 70. The intensity values of pixels less than or equal to 70 are assigned '0' and the intensity values more than 70 are assigned '1' in binarization. The binarized image is shown in Figure 3, in which the pupil is located. The part of the image above and below the pupil is cropped off to obtain the eye image of size 70*300 as shown in Figure 4. The 35 pixels to the left and the right of the pupil are considered and cropped. The final pre-processed Iris image parts are shown in Figures 5 and 6. The left and right portions of image are of size 70*35 (rows*columns).

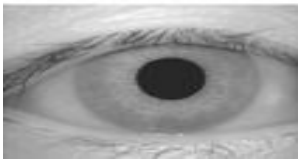


Figure 2. The eye image.

Figure 3. The binarized image.

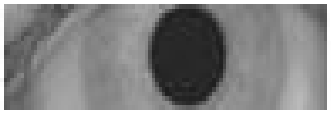


Figure 4. Horizontally segmented portion of the eye.

Figure 5. Left half of Iris image.

Figure 6. Right half of the Iris Image.

C. Feature Extraction

The Principal Component Analysis (PCA) is applied on the right part and the Fast Fourier Transform (FFT) is applied on the left part of the preprocessed Iris image to generate features.

1) Principal Component Analysis

PCA involves the calculation of the Eigen value decomposition of a data covariance matrix or singular value decomposition of a data matrix, usually after mean centring of the data for each attribute. The results of a PCA are usually discussed in terms of component scores and loadings. PCA is the simplest of the true eigenvector based multivariate analyses. Often, its operation can be thought of as revealing the internal structure of the data in a way which best explains the variance in the data.

PCA using the covariance method: The main aim of PCA is to convert a given data set X of dimension M to an alternative data set Y of smaller dimension L by finding the matrix Y, where Y is the Karhunen–Loève Transform (KLT) of matrix X and given by the Equation 1.

$$Y = KLT \{X\} \quad \text{———————} (1)$$

The data set: Consider a data set of observations of M variables, which need to be reduced so that each observation can be described with only L variables, $L < M$. The data is arranged as a set of N data vectors $X_1, X_2 \ldots X_N$ with each X_n representing a single grouped observation of the M variables. $X_1, X_2 \ldots X_N$ are taken as column vectors, each of which has M rows. The column vectors are placed into a single matrix X of dimension $M \times N$.

The empirical mean: The empirical mean along each dimension $m=1, 2, 3 \ldots M$ is found. The calculated mean values are placed into an empirical mean vector u of dimensions $M \times 1$ and this is given by the Equation 2.

$$u[m] = \frac{1}{N} \sum_{n=1}^{N} X[m, n] \quad \text{———} (2)$$

The deviations from the mean: Mean subtraction is an integral part of the solution for finding a principal component as it minimizes the mean square error of the approximation of the data. When mean subtraction is not performed, the first principal component will correspond to the mean of the data. Hence it is absolutely necessary to perform mean subtraction (or "mean centering"), so that it ensures that the first principal component describes the direction of maximum variance, which can be used for the deciphering. Therefore the centering of data is performed by subtracting the empirical mean vector u from each column of the data matrix X. The mean-subtracted data is stored in the $M \times N$ matrix B, as given by the Equation 3.

$$B = X - uh \quad \text{———————} (3)$$

Where h denotes a 1 x N row vector of all 1's, which is given in the form of Equation 4.

$$h[n] = 1, \quad n = 1 \ldots N \quad \text{———————} (4)$$

The covariance matrix: The $M \times M$ empirical covariance matrix C is found by using the formula in Equation 5.

$$C = \mathrm{E}[B \otimes B] = \mathrm{E}[B \cdot B^*] = \frac{1}{N} \sum B \cdot B^* \quad \text{———} \quad \text{——} (5)$$

where

E denotes the expected value operator,

$\otimes$ denotes the outer product operator, and

* denotes the conjugate transpose operator.

The Eigen vectors and Eigen values of the covariance matrix: The matrix *V* of eigenvectors which diagonalizes the covariance matrix *C* is calculated using the Equation 6.

$$V^{-1}CV = D \quad \text{——————} (6)$$

D is the diagonal matrix which has the Eigen values of C. The Matrix D will take the form of an M × M diagonal matrix given by Equation 7.

$$D[p,q] = \lambda_m, \qquad p = q = m \quad \text{——————} (7)$$

The Equation 8 is the m^{th} Eigen value of the covariance matrix C, and

$$D[p,q] = 0 \quad \text{for} \quad p \neq q \quad \text{----------} (8)$$

Matrix V, is also of dimensions M × M, containing M column vectors, each of length M, which represent the M eigenvectors of the covariance matrix C. The Eigen values and eigenvectors so obtained are ordered and paired. Thus the *m*th Eigen value corresponds to the *m*th eigenvector.

The PCA is directly applied to the right half of the pre-processed image. The right half of the pre-processed Iris image of size 70*35 yields PCA coefficients matrix of the size 35*35. This coefficient matrix is converted to a 1D matrix, which is of the size 1*1225, of which the first 252 are selected as they contain sufficient information needed for recognition. The rest are discarded but the amount of information lost is insignificant.

2) Fast Fourier Transform:

The Fast Fourier Transform (FFT) is one of the faster methods for calculating the DFT. While it produces the same result as the other approaches, it is incredibly more efficient, often reducing the computation time by hundred times. The DFT is calculated using the formula given in Equation 9.

$$X(k,l) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} x(m,n) e^{-\frac{j2\pi km}{N}} e^{-\frac{j2\pi ln}{N}},$$

$$0 \le k, l \le N-1 \quad \text{———} (9)$$

Where *N* is the total no of samples, *X(k)* are the DFT coefficients.

Fast Fourier Transform is used for feature extraction of the left half of the pre-processed image.

The left half of the Iris image matrix of size 70*35 is converted into a one dimensional matrix of the size 1*2450 and results in 2450 Fourier coefficients. The first 252 coefficients are selected on the basis of observation as they yield the best results.

3) Fusion

The FFT and the PCA coefficients obtained form the basis of feature vector and fused to get final feature vector. The final feature vector is formed by arithmetic addition of the FFT and the PCA coefficients element by element. The final feature vector is given in Equation 10.

$$Final\ Feature\ Vector = \{Feature_{FFT} + Feature_{PCA}\} \quad \text{-- (10)}$$

D. Template Matching:

Euclidean distance is used as a classifier for matching. The Euclidean distance is also called as Pythagorean distance. The minimum Euclidean distance gives the similarity between the unknown Iris images that is being tested and the ones in the database. The Euclidean distance is selected as it gives us the best result.

In Cartesian co-ordinates, if $p = (p_1, p_2 \ldots p_n)$ and $q = (q_1, q_2 \ldots q_n)$ are two points in Euclidean Space, then the distance from p to q is given by Equation 11.

$$d(p,q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \ldots + (q_n - p_n)^2} \quad \text{— (11)}$$

Here $p = (p_1, p_2 \ldots p_n)$ are the matrix elements of the person whose being compared (tested) and $q = (q_1, q_2 \ldots q_n)$ are the matrix elements of the person who is in the database and with whom the comparison is being done.

IV. ALGORITHM

Problem Definition: Efficient Iris Recognition system using fusion of FFT and PCA features to authenticate a person. The objectives are to:

i. increase the TSR

ii. reduce FAR and FRR

Table I shows the algorithm for the proposed PAFPFCI system, which verifies the authenticity of a given test Iris. The Iris is preprocessed to obtain left and right portions of Iris. The FFT and PCA are applied to left and right portions of Iris to extract transform and spatial domain features. Euclidian Distance is used for comparison.

TABLE I. PROPOSED PAFPFCI ALGORITHM

Input : Iris image database, Test Iris images
Output : Match/ Mismatch

1. CASIA Iris database is considered.
2. Iris images are pre-processed to obtain left and right portion nearer to the pupil of Iris.
3. FFT is applied on left portion of Iris to generate transform domain features.
4. PCA is applied on right portion of Iris to generate spatial domain features.
5. Fusion of FFT and PCA features using arithmetic addition to generate final feature set.
6. Repeat step 2 to 5 for Test Iris images.
7. Compare Test image features with database features using Euclidean Distance.

V. PERFORMANCE ANALYSIS

The proposed PAFPFCI model is tested on the CASIA Iris image database–version 1.0, which are the most widely used database containing 756 grey-scale Eye images with 108 unique Eyes or classes and 7 different images of each unique Eye. The algorithm is simulated on MATLAB version 7.8. For the performance analysis, the 6 Iris images of first 50 persons are considered to create database. The remaining one Iris image from these 50 persons is considered for finding FRR and TSR. The 7 images of 58 persons are out of database and used for finding the FAR. Seven samples of a human eye in CASIA Iris database are as shown in Figure 7.

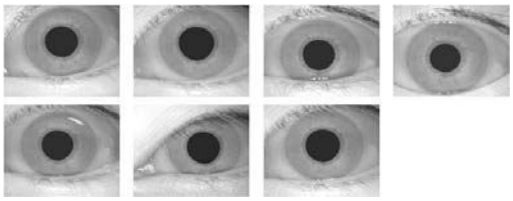


Figure 7. Samples Iris images of CASIA Iris database

The performance parameters to test the proposed PAFPFCI algorithm are:

1) False Acceptance Rate (FAR) is the measure of imposters accepted. It is defined as the ratio of number of persons accepted from out of database to the total number of persons out of database.

2) False Rejection Rate (FRR) is the measure of genuine Iris images rejected. It is defined as the ratio of number of genuine persons rejected to the total number of persons in the database.

3) Equal Error Rate (EER) indicates that the proportion of the false acceptances is equal to the proportions of false rejections. The lower the EER value, the higher the accuracy of the biometric system.

4) True Success Rate or Correct Recognition Rate (TSR or CRR) is the rate at which the system recognizes all the persons in the database as particular individuals correctly. It is the measure of correctness of the system. It is the ratio of number of persons correctly matched to the total number of persons in the database.

Table II shows the performance parameters of the PAFPFCI system, when FFT, PCA and fusion of FFT-PCA are considered separately. It is observed that the values of TSR and FAR increase, whereas FRR decreases with increasing threshold, when PCA is used for feature extraction. The TSR in the case of PCA is around 6% with high values of FAR and FRR. In the case of FFT, the value of TSR is around 96% with FRR value of 0.04 and FAR value of 0.71 at the threshold value of 90. In the case of proposed PAFPFCI algorithm, the TSR is 100% for threshold value of 80, which is an improved TSR value compared to individual PCA and FFT techniques.

The efficiency of the PAFPFCI model is compared with that of existing methods namely, Xianchao Qui et al., [12], Boles and Boashash [13], Martin-Roche et al., [14], Li Ma et al., [15] and Zhongliang Luo [16]. From the Table III, it can be seen that the PAFPFCI model has a better efficiency than the existing ones.

TABLE II. PERFORMANCE ANALYSIS BY APPLYING PCA, FFT AND PROPOSED PAFPFCI

Threshold	PCA			FFT			Proposed PAFPFCI method		
	TSR (%)	FRR	FAR	TSR (%)	FRR	FAR	TSR (%)	FRR	FAR
10	0	1.0000	0.0000	0	1.0000	0.0000	0	1.0000	0.0000
20	0	1.0000	0.1207	0	1.0000	0.0000	0	1.0000	0.0000
30	6	0.9400	1.0000	2	0.9800	0.0000	4	0.9600	0.0517
40	6	0.9400	1.0000	14	0.8600	0.0345	34	0.6600	0.1207
50	6	0.9400	1.0000	26	0.7400	0.0517	64	0.3600	0.3276
60	6	0.9400	1.0000	56	0.4400	0.1552	84	0.1600	0.5172
70	6	0.9400	1.0000	70	0.3000	0.3276	96	0.0400	0.7069
80	6	0.9400	1.0000	88	0.1200	0.4655	100	0.0000	0.8448
90	6	0.9400	1.0000	96	0.0400	0.7069	100	0.0000	0.9310
100	6	0.9400	1.0000	96	0.0400	0.7931	100	0.0000	1.0000
110	6	0.9400	1.0000	96	0.0400	0.9138	100	0.0000	1.0000

TABLE III. COMPARISON OF PAFPFCI WITH OTHOER SYSTEMS

Method	Efficiency (%)
Xianchao Qui et al.,[12]	91.02
Boles and Boashash [13]	92.62
Martin- Roche et al., [14]	93.6
Li Ma et al.,[15]	98.06
Zhongliang Luo [16]	95.9
Proposed PAFPFCI model	100.00

VI. CONCLUSION

The proposed PAFPFCI system is tested on CASIA Iris database version 1.0. In this method binarization technique is applied at the pre-processing stage, to obtain left and right portions of Iris. The PCA and FFT are applied on right and left portion of the preprocessed Iris respectively to generate the corresponding features. The PCA and FFT coefficients are combined using arithmetic addition to obtain final feature vector. Euclidean Distance is used to compare the test features with the database feature set. Finally it is noted that the performance parameters are enhanced in the case of proposed PAFPFCI system than the existing systems. Histogram and/or Edge Detection can be applied in the preprocessing stage to further improve the system performance. The Dual Tree Complex Wavelet Transform (DTCWT) can be used to generate the features.

REFERENCES

[1] Kresimir Delac and Mislav Grgic, "A Survey of Biometric Recognition Methods," *International Symposium on Electronics in Marine*, pp. 184 -193, 2004.

[2] Arun Ross and Anil Jain, "Information Fusion in Biometrics," Pattern recognition Letters, Vol. 24, pp. 2115-2125, 2003.

[3] J Daugman, "High Confidence Visual Recognition by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, No.11, pp.1148-1161, 1993.

[4] J Daugman, "How Iris recognition works," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 14, No. 1, pp. 21-30, 2004.

[5] Xiaomei Liu, Bowyer K W and Patrick J Flynn, "Experimental Evaluation of Iris Recognition," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 158-165, 2005.

[6] Karen Hollingsworth, Sarah Baker, Sarah Ring, Kevin W Bowyer and Patrick J Flynn, "Recent Research Results in Iris Biometrics," *Proceedings of the SPIE*, Vol. 7306, pp. 73061Y- 73061Y-10, 2009.

[7] R P Wildes, "Iris Recognition: An Emerging Biometric Technology," *IEEE Proceedings*, Vol. 85, pp. 1348-1363, 1997.

[8] Emine Krichen, M Anouar Mellakh, Sonia Garcia-Salicetti and Bernadette Dorizzi, "Iris Identification using Wavelet Packets," *International Conference on Pattern Recognition*, Vol. 4, pp. 335- 338, 2004.

[9] Sateesh Kumar H C, Abhilash S K and Raja K B, Venugopal K R and L M Patnaik, " Iris Recognition using Fusion of EMD and FFT," *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 607-613, 2011.

[10] Raju K Dehankar, Seema C Bhivgade and S I Parihsr, "Wavelet Based Comparison of Edge Detection Technique for Iris Recognition" *International Journal of Engineering Research and development*, vol. 1, no. 9, pp. 30-33, 2012.

[11] Anuradha shrivas and Preeti Tuli, "Analysis of Iris Images for Iris recognition System" *International Journal of Computer Applications*, Vol. 46, No. 13, pp. 22-25, 2012.

[12] Xianchao Qui, Zhenan Sun and Tieniu Tan, "Learning Appearance Primitives of Iris images for Ethnic Classification," *International Conference on Image Processing*, pp. 405-408, 2007.

[13] W W Boles and B Boashash, "A Human Identification Technique using Images of the Iris and Wavelet Transform," *IEEE Transactions on Signal Processing*, Vol. 46, No. 4, pp. 1185-1187, 1998.

[14] Martin-Roche D, Sanchez-Avila C and Sanchez-Reillo R, "Iris Recognition for Biometric Identification using Dyadic Wavelet Transform Zero-Crossing," *IEEE International Conference on Security Technology*, pp. 272-277, 2001.

[15] Li Ma, Tieniu Tan, Yunhong Wang and Dexin Zhang, "Personal Identification based on Iris Texture Analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 25, No.12, pp. 1519 - 1533, 2003.

[16] Zhongliang Luo, "Iris Feature Extraction and Recognition based on Contourlet Wavelet Transform," *International Workshop on Information and Electronics Engineering*, pp. 3578-3582, 2012.

Dual Transformation based Face Recognition using Matching Level Fusion

[1]Ramachandra A C , [2]Vineetha M , [3]K B Raja, [4]Venugopal K R , [5]L M Patnaik

[1] Department of Electronics and Communication, Alpha College of Engineering, Bangalore.
[2,3] Department of Electronics and Communication, University Visveswaraya College of Engineering, Bangalore, Karnataka.
[4]University Visveswaraya College of Engineering, Bangalore, Karnataka, India.
[5] Honorary Professor, Indian Institute of Science, Bangalore, Karnataka, India.

Abstract--The identification of a person based on biological features are efficient compared with traditional knowledge based identification system. In this paper we propose Dual Transformation based Face Recognition using Matching Level Fusion (DTFRML). The Singular Value Decomposition (SVD) is applied on face images of database and test images to derive coefficients and resized to a matrix size of 64x 64 to form SVD features of each image. The test image SVD features are compared with database images using ED to compute EER and TSR. The test and database face images are considered again and resized to a size of 64x 64. The kekre Transforms (KT) is applied on resized images to obtain features using KT. The test image KT features are compared with KT features of database using ED to compute EER and TSR. The values of EER and TSR obtained from SVD and KT are fused using log function to obtain better EER and TSR values.

Keywords-- *Biometrics, SVD, KT, Total Success Rate.*

I. INTRODUCTION

The traditional authentication systems are based on memory of a person to remember PIN and discrete cards such as smart card, ID card etc., the advantage of traditional method is simple and low cost, the disadvantage of traditional system is remembering lengthy passwords by a person is difficult and discrete cards may be lost or stolen. The modern or upcoming authentication techniques based on biological features are more efficient and robust compared with existing traditionaltechniques because they cannot be duplicated. The biological features based recognition technology is by using computer, sensors and biometric principles with inherent physiological and behavioral characteristics of a person. The physiological features such as fingerprint, iris, face, palm print etc., are constant throughout life, the behavioral characteristics such as signature, voice, Gait, keystroke etc., these features are not constant, as they depend on circumstances. The biometric system works in two different modes viz. (i) verification mode: it is one to one appraisal to authenticate a person (ii) identification mode: It is one to may appraisal of a trail set with database to identify a person. The system consists of registration, processing and comparison section. The images registered are normalized by color converting, cropping and resizing. The features of a normalized image are extracted by using the spatial domain, transformed domain or combinations of both in the processing section. The extracted features are used to identify a person by comparing features by using classifiers such as Euclidian Distance (ED), Hamming Distance, Random Forest, Neural Network, Support Vector Machine etc .in comparison section. Biometric System are extensively used in applications such as Banking, Airport checking for personal authentication, Home security applications, Electronic Voting Machine, Military force to authenticate refugee, Corporate office for employee authentication, Entry to high security zones like parliamentary houses, Defense Establishments, Legal Documentations like land and business etc.,

Contribution: In this paper DTFRML algorithm is proposed to identify a person. The features of test set and database are obtained using SVD, the obtained features are compared using Euclidian Distance to compute EER and TSR. The database and test set images are resized and KT is applied to extract features. The Equal Error Rate (EER) and Total Success Rate (TSR) of SVD and KT are fused using log functions to get better EER and TSR.

Organization: This paper is organized into following sections. Section II is an overview of related work. The proposed model is described in Section III. Matching is discussed in Section IV, the algorithm for proposed system is given in section V. Performance Analysis of the system is presented in Section VI and Conclusions are contained in Section VII.

II. RELATED WORK

Reza Moradi et al., [1] proposed face recognition method which exploit edge-based features of faces. The performance is independent from the scenario of face recognition. Difficult scenarios of face

recognition are including pose variation, illumination conditions, scale variability, images taken years apart, glasses, moustaches, beards, and low quality image. William Robson et al., [2] employed a set of feature descriptors for face identification using partial least squares to perform multichannel feature weighting, tree-based discriminative structure to reduce the time required to evaluate probe samples. Narasimhan et al., [3] introduced a technique Active Appearance Model (AAM) which is a statistical model for modeling where the face is identified based on their feature points even though if there are many external factors to which they are very sensitive. It is accurate in alignment and effective for handling face deformation. Then the face is projected in 3D for higher efficacy.Ahmad et al., [4] presented two architectures for two dimensional Haar Wavelet Transform (HWT) of transform block in face recognition systems. The proposed architectures comprise 2-D HWT with transpose-based computation and Dynamic Partial Reconfiguration. Xiaoyuan Jing et al., [5] defined two feature extraction approaches, Local Uncorrelated Discriminant Transform (LUDT) and Weighted Global Uncorrelated Discriminant Transform for face recognition (WGUDT). They iteratively calculate the optimal discriminant vectors that maximize the Fisher criterion under the corresponding statistical uncorrelated constraints. Zhengya Xu et.al., [6] presented a feature-based approach for fast face recognition, shape-based automatic reference control point and feature extraction technique are used for face representation, whereby the difference between two faces is measured by a set of extracted features and 3-D features from a set of 2-D images are used for face template registration.

III. PROPOSED MODEL

The block diagram of Dual Transformation based Face Recognition using Matching Level Fusion (DTFRML) is shown in Figure 1

A. Face database

Olivetti Research Laboratory (ORL) [7] face database contains four hundred images of size 112 x 92, it has forty persons with ten images for each person. The images are taken in different poses, expressions and scales with constant lighting conditions. Figure 2 shows the samples of ORL face images of a person with different pose.

Figure 2: Samples of ORL face images

Yale [8] face database includes variation of pose, expression, Illumination, scale and blurring, it has one hundred and sixty five images of size 320 x243 of fifteen persons with ten images for each person. Figure 3 shows the samples of Yale face images of a person with different poses.

Figure 3: Samples of Yale face database

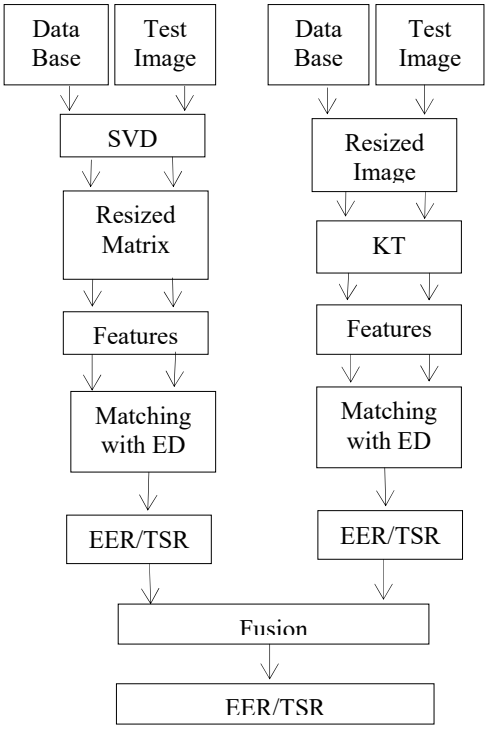


Figure 1: Block diagram of DTFRML model

Japanese Female Facial Expression (JAFFE) [9] ace database consists of seventy images of size 256 x 256 from ten persons with seven images for each person. The images were taken in seven different emotional facial expressions. Out of ten subjects present eight were considered for gallery. Figure 4 shows the samples of JAFFE face images of a person with different poses.

Figure 4: Samples of JAFFE database

Combined [10] face database consists of two thousand, two hundred and eighty images of size 280x320. It is from one hundred and twenty persons with nineteen images for each person. The images were taken in seven different emotional facial expressions. Figure 5 shows the samples of combined face images of a person with different poses.

Figure 5: Samples of Combined database

B. Preprocessing:

The images in the database and test image are processed before extracting the features. It involves, Color to gray scale image conversion and the gray scale image with intensity values between 0 and 255 is obtained from color image to reduce processing time.

C. Feature Extraction:

The features of each face image are extracted using SVD [11] and KT [12][13][14]. The features of SVD and KT are fused using logarithmic transformations to obtain better results compared to individual techniques.

1) Singular Value Decomposition:

The Feature Vectors are extracted using SVD, by considering image of size *m x n* matrix *I.* This image can be compressed and stored by *n x n* matrix *M* and elements are non-negative. The amount of storage is reduced from n^2 to *n*. The obtained matrix has Singular Value Decomposition given by Equation (1)

$$M=USV^* \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where,

U is m x m real or complex unitary matrix,

$$U= I\, I^*$$

I^* is transpose of *I*

S is *m x n* diagonal matrix with non-negative real numbers on the diagonal, and

*V** is Conjugate transpose of *V*, *n x n* real or complex unitary matrix.

$$V=I^*I$$

Expanded version of *M* is given in Equation (2)

$$M=u_1s_1v_1{}^*+. .u_rs_rv_r{}^*+u_{r+1}s_{r+1}v_{r+1}{}^*. . + u_ns_n\, v_n{}^* \quad \ldots\ldots.. \quad (2)$$

The nearest matrix of rank *r* is obtained by taking,

$$s_{r+1} \ldots . + s_n = 0 \ , r << n$$

The rank of *r* considered to be approximately sixteen percent of *n*, still the image is close to original image. The Equation (2) is reduced by considering rank *r* is given in Equation (3)

$$M=u_1 \ s_1 \ v_1{}^* +. \ . \ . \ . \ u_r \ s_r \ v_r{}^* \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

From equation 3, dimension of *M* is reduced from *n* to *r*.

For example if SVD is applied on ORL image of size 112 x 92 with r = 15 the image is compressed to 3075 pixels by keeping image size same instead of original 10304 pixel using Equation (4)

Number of Pixels = r x m + r x n + r …….... (4)

2) Kekre Transform:

The traditional transforms should have the matrix of size equal to the integer power of two, whereas Kekre's transform matrix can be of any size *NxN,* the diagonal and the upper elements of Kekre's transform matrix are unity, while the lower diagonal part except the elements just below diagonal is zero. Generalized

$$K_{NxN} = \begin{bmatrix} 1 & 1 & 1 & \ldots\ldots\ldots & 1 & 1 \\ -N+1 & 1 & 1 & \ldots\ldots\ldots & 1 & 1 \\ 0 & -N+2 & 1 & \ldots\ldots\ldots & 1 & 1 \\ . & . & . & \ldots\ldots\ldots & . & . \\ . & . & . & \ldots\ldots\ldots & . & . \\ . & . & . & & . & . \\ 0 & 0 & 0 & \ldots\ldots\ldots & 1 & 1 \\ 0 & 0 & 0 & \ldots\ldots\ldots & -N+(N-1) & 1 \\ . & & & & & \end{bmatrix}$$

NxN Kekre's transform matrix can be given in determinant.

The elements Kxy are generating using the relation given in Equation 5.

$$K_{xy} = \begin{cases} 1 & : x \le y \\ -N+(x+1) & : x = y+1 \\ 0 & : x > y+1 \end{cases}$$

…… (5)

Where x, y are rows and columns

The image is resized to 64x64 and taken as *f*, the featurevector *F* is calculated by Equation 6

$$[F] = [K]\,[f]\,[K]^* \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

[K]* is the transpose of KT

IV. MATCHING:

A primitive type of matching is finding similarity between the database image and a test image. Euclidean Distance (ED) is one such matching technique which is used to verify whether the test image is present in database or not. If p_i and q_i are two points in a 2D plane

Where i =1and 2

Then the Euclidean distance is given by the Equation 7

$$D(p,q) = \sqrt{((p_1 - q_1)^2 + (p_2 - q_2)^2)} \quad \ldots\ldots\ldots\ldots\ldots (7)$$

A. *Matching with SVD:*

The feature vectors for the images are calculated using SVD. The database is created using different available face database such as ORL, YALE, JAFFE, COMBINED, The test image is one of the images of a person from database and the ED value is compared with the predefined threshold value to compute FRR and TSR. The values of FAR is computed for test image considered from out of database by calculating ED with the images present in database. EER is noted by taking equal values of FAR and FRR.

B. *Matching with KT:*

The feature vectors for the images are computed using KT. The database is created using different available database such as ORL, YALE, JAFFE, COMBINED. The test image is one of the images of a person from database and the ED value is compared with the predefined thresh hold value to compute FRR and TSR. The value of FAR is computed for test image from out of database by calculating ED with the images present in database. EER is noted by taking equal values of FAR and FRR.

C. *Fusion of SVD and KT Parameters:*

The effectiveness of face recognition system is evaluated by FRR, FAR, EER and TSR. The values of FRR, FAR, EER and TSR are computed using SVD and KT. the EER and TSR values of SVD and KT are fused using Equation 8 and 9 respectively to obtain better performance compared to individual techniques.

F_{EER} = abs $(1/\log_2 (SVD) - 1/\log_2 (KT))$ ……..…. (8)

F_{TSR} = 1- abs $(1/\log_2 (SVD) - 1/\log_2 (KT))$ …….. (9)

V. ALGORITHM:

Problem definition: Dual Transformation based Face Recognition using Matching Level Fusion (DTFRML) used to identify a person.

The objectives are

(i) To increase the recognition rate (TSR).
(ii) To decrease Equal Error Rate (EER).

Algorithm of proposed face recognition system is as given in Table 1.

VI. PERFORMANCE ANALYSIS:

The values of EER and TSR for different combination of persons in the data base for ORL face data base are tabulated in Table 2. The value of EER increases and the value of TSR decrease as number of persons in database increases for both SVD and KT techniques. The values of EER decreases and TSR increases as number of person decreases in the out of database for both SVD and KT. It is observed that the values of EER and TSR are better in the case of proposed fused (DTFRML) algorithm compare to individual SVD and KT algorithms.

Table 1: Algorithm of DTFRML.

INPUT: Database Face images, Test Face images
OUTPUT: Matched /Non-matched Test image

1. Color image is converted into gray scale image.
2. SVD is applied on images in database.
3. Coefficients obtained are resized to 64 x 64 and forms features.
4. Steps 2 and 3 are repeated for test image to derive SVD features.
5. Test set features are compared with database images using ED to Compute FRR, FAR, EER and TSR.
6. The original Face Image is resized to 64 x 64.
7. KT is applied on images in database.
8. KT Coefficients are considered as features.
9. Steps 6 to 8 are repeated for test face image to obtain KT features.
10. Test image features are compared with database images using Euclidean Distance (ED) to Compute FRR, FAR, EER and TSR.
11. Results of step 5 and step 10 are fused using Equations
    $F_{EER=}$ abs $(1/\log_{2(SVD)} - 1/\log_{2(KT)})$ ---------(1)
    $F_{TSR=}$ 1- abs $(1/\log_{2(SVD)} - 1/\log_{2(KT)})$------(2)
12. Performance parameters are computed to Match/Non-Match.

Table 2: Comparison of EER and TSR for ORL.

PIDB: PODB	EER			% TSR		
	SVD	KT	DTFRML	SVD	KT	DTFRML
20:100	0.1	0.1	0	90.0	90.0	100
40:80	0.05	0.08	0.0431	95.0	92.5	99.91
60:60	0.05	0.06	0.0150	95.0	93.33	99.94
80:40	0.06	0.08	0.0281	92.5	92.5	100
100:20	0.05	0.08	0.0431	93.0	92.0	99.96

The values of EER and TSR for different combination of persons in the data base for YALE face data base are tabulated in Table 3. The value of EER increases and the value of TSR decrease as number of persons in database increases for both SVD and KT techniques. The values of EER decreases and TSR increases as number of person decreases in the out of database for both SVD and KT. It is observed that the values of EER and TSR are better in the case of proposed fused (DTFRML) algorithm compare to individual SVD and KT algorithms.

Table 3: Comparison of EER and TSR for YALE.

PIDB: PODB	EER			% TSR		
	SVD	KT	DTFRML	SVD	KT	DTFRML
4:10	0.25	0.25	0	75.0	75.0	100
6:8	0.33	0.26	0.1107	66.66	50.0	98.79
8:6	0.50	0.50	0	50.0	37.5	98.59
10:4	0.40	0.30	0.1808	60.0	50.0	99.21

The values of EER and TSR for different combination of persons in the data base for JAFFE face data base are tabulated in Table 4. The value of EER zero and TSR is 100% as number of persons in database increases and number of person decreases in the out of database for both SVD and KT techniques. It is observed that the values of EER and TSR are same in the case of proposed fused (DTFRML) algorithm compare to individual SVD and KT algorithms.

Table 4: Comparison of EER and TSR for JAFFE.

PIDB: PODB	EER			% TSR		
	SVD	KT	DTFRML	SVD	KT	DTFRML
4:6	0	0	0	100	100	100
6:4	0	0	0	100	100	100
8:2	0	0	0	100	100	100

The values of EER and TSR for different combination of persons in the data base for COMBINED face data base are tabulated in Table 5. The value of EER increases and the value of TSR decrease as number of persons in database increases for both SVD and KT techniques. The values of EER decreases and TSR increases as number of person decreases in the out of database for both SVD and KT. It is observed that the values of EER and TSR are better in the case of proposed fused (DTFRML) algorithm compare to individual SVD and KT algorithms.

Table 5: Comparison of EER and TSR for COMBINED.

PIDB: PODB	EER			% TSR		
	SVD	KT	DTFRML	SVD	KT	DTFRML
10:30	0.07	0.13	0.0791	90	80	99.59
20:20	0.1	0.2	0.1296	85	80	99.78
30:10	0.14	0.17	0.0386	86.66	80	99.72
35:05	0.18	0.2	0.0265	77.14	77.14	100

The values of Percentage Recognition Rate for existing Enhanced SVD Based Face Recognition (SVDFR) [15] and proposed (DTFRML) are compared in Table 6. It is observed that the Percentage Recognition Rate is better in the case of proposed algorithm compared to existing algorithm for ORL and YALE face data bases.

Table 6: Comparison of Recognition Rate.

Method	Recognition Rate	
	ORL	YALE
SVDFR[15]	72	90.30
DTFRML	100	99.21

VII. CONCLUSION:

The face recognition is a Physiological biometric trait to identify a person efficiently. In this paper DTFRML algorithm is proposed. The SVD Coefficients are generated from face images and resized to Coefficient Matrix of 64X64 dimensions to form features. The EER and TSR are computed by comparing a SVD feature of test image with database image features using ED. The KT Co-efficient are obtained from test and database resized images to form features. The EER and TSR values are computed from test and database features using ED. The EER and TSR values derived from SVD and KT are fused based on logarithmic transformation to obtain better EER and TSR. It is observed that performance parameter values of EER, TSR are better in the case of proposed algorithm compared with existing algorithms. In future the algorithm can be tested by fusing features at feature level.

REFERENCE

[1] Reza Moradi Rad, Abdolrahaman Attar and Reza Ebrahimi Atani, "A Robust Face Recognition Method Using Edge-Based Features," IEEE Symposium on Computers & Informatics, pp. 185- 188, 2012.

[2] William Robson Schwartz, Huimin Guo, Jonghyun Choi and Larry S. Davis, "Face Identification Using Large Feature Sets," IEEE Transactions on Image Processing, vol. 21, no. 4, 2012.

[3] Narasimhan Renga Raajan, Mohankumar Vishnu Priya, S Suganya, D Parthiban, A lenifer Philomina, Mohan RamKumar and Balakrishnan Monisha, "High Level Imaging for Face Recognition towards More Accurate Detection," IEEE-International Conference on Advances in Engineering, Science And Management, pp. 648- 651, 2012

[4] A Ahmad, A Amira, P Nichol and B Krill, "Dynamic Partial Reconfiguration of 2-D Haar Wavelet Transform For Face Recognition Systems," Fifteenth IEEE International Symposium on Consumer Electronics, pp 9-13, 2011.

[5] Xiaoyuan Jing, Sheng Li, David Zhang and Jingyu Yang, "Face Recognition Based on Local Uncorrelated and Weighted Global Uncorrelated Discriminant Transforms," Eighteen IEEE International Conference on Image Processing, pp 3049-3052, 2011.

[6] Zhengya Xu, Hong Ren Wu, Xinghuo Yu, Kathryn Horadam, and Bin Qi, " Robust Shape-Feature-Vector-Based Face cognition System," IEEE Transactions on Instrumentation and Measurement, vol. 60, no. 12, pp 3781-3791, 2011.

[7] Ferdinando Samaria and Andy Harter, "Parameterization of a Stochastic Model for Human Face Identification," Proceedings of Workshop on Applications of Computer Vision, December 1994.

[8] P. N. Bellhumer, J. Hespanha, and D. Kriegman, "Eigen faces vs. fisher faces Recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Face Recognition, vol.17 No.7 pp711--720, 1997.

[9] Michael J Lyons, Shigeru Akamatsu, Miyuki Kamachi and Jiro Gyoba, "Coding Facial Expressions with Gabor Wavelets," Proceedings on Third IEEE International Conference on Automatic Face and Gesture Recognition, pp. 200-205, 1998.

[10] J J J Lien, T Kanade, J F Cohn and C C Li, "Automated facial expression recognition," Proceedings of the Third IEEE International Conference on Automatic Face and Gesture Recognition, pp. 390-395, 1998.

[11] Neil Muller Lourenc¸o Magaia and B. M. Herbst, "Singular Value Decomposition, Eigenfaces, and 3D Reconstructions," Society for Industrial and Applied Mathematics, vol. 46, no. 3, pp. 518–545, 2004.

[12] H. B. Kekre, Tanuja K, Sarode and Meena S. Ugale, "Performance Comparison of Image Classifier Using DCT, Walsh, Haar and Kekre's Transform," International Journal of Computer Science and Information Security, vol. 9, No. 7, 2011.

[13] H. B. Kekre, Archana Athawale and Dipali Sadavarti, "Algorithm to enerate Kekre's Wavelet Transform from Kekre's Transform," International Journal of Engineering Science and Technology, vol. 2, pp. 756-767, 2010.

[14] H. B. Kekre and Kavita Sonawane , "Query based Image Retrieval using Kekre's, DCT and Hybrid wavelet Transform over First and Second Moment," International Journal of Computer Applications, Vol 32, no.4, pp 13- 18, 2011.

[15] Muhammad Sharif, Saad Anis, Mudassar Raza and Sajjad Mohsin, "Enhanced SVD Based Face Recognition," Journal of Applied Computer Science and Mathematics, vol. 12, no. 6, pp. 49-53, 2012.