

Volume 5 ▪ Issue 4 ▪ October 2011

INTERNATIONAL JOURNAL OF
COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year



CSC PUBLISHERS
<http://www.cscjournals.org>

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 5, ISSUE 4, 2011

**EDITED BY
DR. NABEEL TAHIR**

ISSN (Online): 1985-1553

International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website <http://www.cscjournals.org>, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers

Computer Science Journals

<http://www.cscjournals.org>

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 5, Issue 4, October 2011

Publishing Date: 05 - 10- 2011

ISSN (Online): 1985 -1553

This work is subjected to copyright. All rights are reserved whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication of parts thereof is permitted only under the provision of the copyright law 1965, in its current version, and permission of use must always be obtained from CSC Publishers.

IJCSS Journal is a part of CSC Publishers

<http://www.cscjournals.org>

© IJCSS Journal

Published in Malaysia

Typesetting: Camera-ready by author, data conversion by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2011

EDITORIAL PREFACE

This is third issue of volume five of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members

International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

ASSOCIATE EDITORS (AEiCs)

Associate Professor. Azween Bin Abdullah

Universiti Teknologi Petronas,
Malaysia

Dr. Padmaraj M. V. nair

Fujitsu's Network Communication division in Richardson
Texas, USA

Dr. Blessing Foluso Adeoye

University of Lagos,
Nigeria

Dr Haralambos Mouratidis

University of east London
Afghanistan

EDITORIAL BOARD MEMBERS (EBMs)

Professor. Abdel-Badeeh M. Salem

Ain Shams University
Egyptian

Professor. Sellappan Palaniappan

Malaysia University of Science and Technology
Malaysia

Professor Mostafa Abd-El-Barr

Kuwait University
Kuwait

Professor. Arun Sharma

Amity University
India

Dr. Alfonso Rodriguez

University of Bio-Bio
Chile

Dr. Debotosh Bhattacharjee

Jadavpur University
India

Dr. Teng li Lynn

University of Hong Kong
Hong Kong

Dr. Chiranjeev Kumar
Indian School of Mines University
India

Dr. Ghossoon M. Waleed
University Malaysia Perlis
Malaysia

Dr. Srinivasan Alavandhar
Caledonian University
Oman

Dr. Deepak Laxmi Narasimha
University of Malaya
Malaysia

TABLE OF CONTENTS

Volume 5, Issue 4, October 2011

Pages

- 394 - 404 Robust Image Watermarking Scheme Based on Wavelet Technique
Aree Ali Mohammed, Haval Mohammed Sidqi
- 405 - 413 A proposed Solution: Data Availability and Error Correction in Cloud Computing
Anil Gupta, Parag Pande, Aaftab Qureshi, Vaibhav Sharma
- 414 - 424 Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation
*Iwasokun gabriel Babatunde, Akinyokun, Oluwole Charles, Alese Boniface kayode,
Olabode Olatunbosun*

Robust Image Watermarking Scheme Based on Wavelet Technique

Aree Ali Mohammed
College of Science, Computer Dept.
University of Sulaimani
Sulaimani, Iraq

aree.ali@univsul.net

Haval Mohammed Sidqi
Institute of Computer Science.
Technical Foundation
Sulaimani, Iraq

havalms@yahoo.com

Abstract

In this paper, an image watermarking scheme based on multi bands wavelet transformation method is proposed. At first, the proposed scheme is tested on the spatial domain (for both a non and semi blind techniques) in order to compare its results with a frequency domain. In the frequency domain, an adaptive scheme is designed and implemented based on the bands selection criteria to embed the watermark. These criteria depend on the number of wavelet passes. In this work three methods are developed to embed the watermark (one band (LL|HH|HL|LH), two bands (LL&HH | LL&HL | LL&LH | HL&LH | HL&HH | LH&HH) and three bands (LL&HL&LH | LL&HH&HL | LL&HH&LH | LH&HH&HL) selection. The analysis results indicate that the performance of the proposed watermarking scheme for the non-blind scheme is much better than semi-blind scheme in terms of similarity of extracted watermark, while the security of semi-blind is relatively high. The results show that in frequency domain when the watermark is added to the two bands (HL and LH) for No. of pass =3 led to good correlation between original and extracted watermark around (similarity = 99%), and leads to reconstructed images of good objective quality (PSNR=24 dB) after JPEG compression attack (QF=25). The disadvantage of the scheme is the involvement of a large number of wavelet bands in the embedding process.

Keywords: Multi-Bands Wavelet, Watermark, Semi Blind Watermark Detection, Robustness, Malicious Attacks.

1. INTRODUCTION

Digital watermarking is a method to hide some information that is integrated with a multimedia object [1]. The object may be any form of multimedia, such as image, audio, video, or text. Watermarking has many different applications [2], such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks [3,4]. Any watermarking technique has to be evaluated to judge its performance. Three factors, as given below, must be considered while evaluating an image watermarking algorithm.

1. Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors;
2. Robustness, i.e. the resistance of the watermark to alterations of the original content such as compression, filtering or cropping;
3. Visibility, i.e. how easily the watermark can be discerned by the user.

Available techniques use different transform domains to embed the watermark inspired by information coding and image compression. The watermarking is performed in the cover (host) image through several domains such as discrete cosine transforms (DCT) [5], discrete wavelet

transforms (DWT) [6], and discrete Fourier transforms (DFT) [7]. The watermarking algorithm proposed in this work uses DWT ideas [8].

In this study a new digital image watermarking scheme is presented which is based on the float 9/7 Tap filter wavelet transform. Before performing wavelet transformation on the host image, some tests are taken in a spatial domain to make a comparison with a frequency domain. On the other hand, in a frequency domain the watermarking scheme is developed for non-blind and semi-blind techniques. In spatial domain, the watermark is directly embedded into the highly sorted pixel's value while in a frequency domain the host image is firstly decomposed by a multi-resolution wavelet transformation and then embedding watermark into either low or high frequencies based on some criteria [10-12].

The proposed scheme has a good robustness under some conventional attacks and geometrical attacks. Also it is robust against jpeg image compression. Figure (1) illustrates the general diagram of the proposed watermarking scheme applied on spatial and frequency domain respectively.

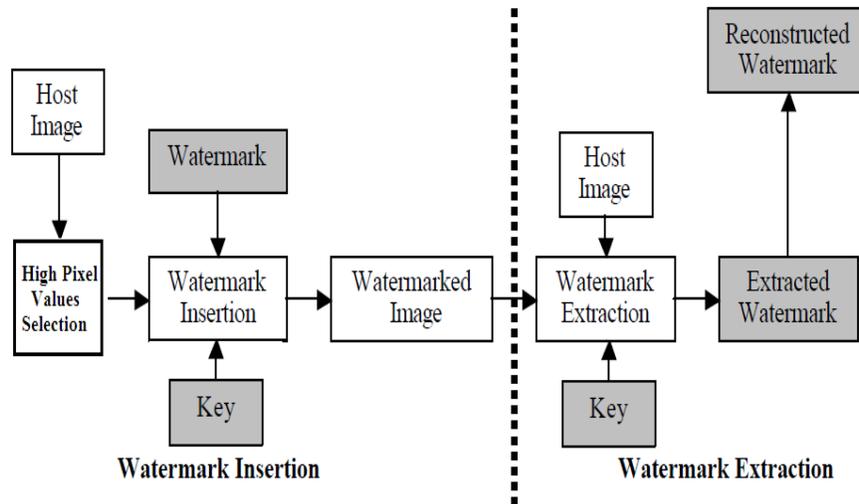


FIGURE 1: General diagram of the watermarking proposed scheme.

This paper will be organized as follows. Section 2 illustrates the proposed watermarking scheme in detail. Section 3 presents experiment results as well as some discussions. Conclusions are given in section 4.

2. PROPOSED WATERMARKING SCHEME

Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm. The following subsections describe the details of the proposed scheme.

2.1 Watermarks Type

The watermarks used in this work are divided into three types:

1. Gray or color image,
2. Logo and
3. Randomly generated sequence of bits

Figure (2) shows some watermark types used in image watermarking scheme.



FIGURE 2: Watermarks type.

2.2 Watermarking Embedding Process

In the proposed approach, the embedded watermark must be invisible to human eyes and enough robust to some image processing operations. Before insertion, the host image color system (RGB) is converted to another color space (YCbCr) and then the histogram of the color values is calculated to find out the high pixel values in the host image. YCbCr is not an absolute color space; it is a way of encoding RGB information. The actual color displayed depends on the actual RGB colorants used to display the signal. Therefore a value expressed as YCbCr is only predictable if standard RGB colorants are used. Since the watermark is added to the luminance, the RGB color space of the image should be converted to YCbCr color space. The Y component is used later to embed the watermark.

In the embedding process the watermark is added not directly to the original pixel values of Y – Luminance component but to the selected pixel values based on histogram calculation of Y component. Figure (3) and (4) presents the flowchart of the embedding process in frequency domain for non and semi blind algorithm. The watermark used (random number, logo and gray or color image) is of size 32*32 pixels or 1024 bytes.

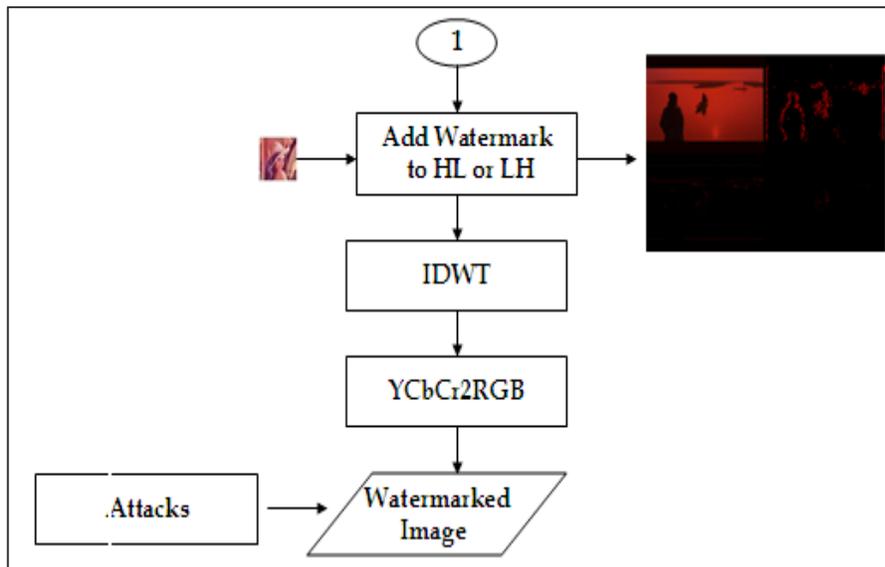
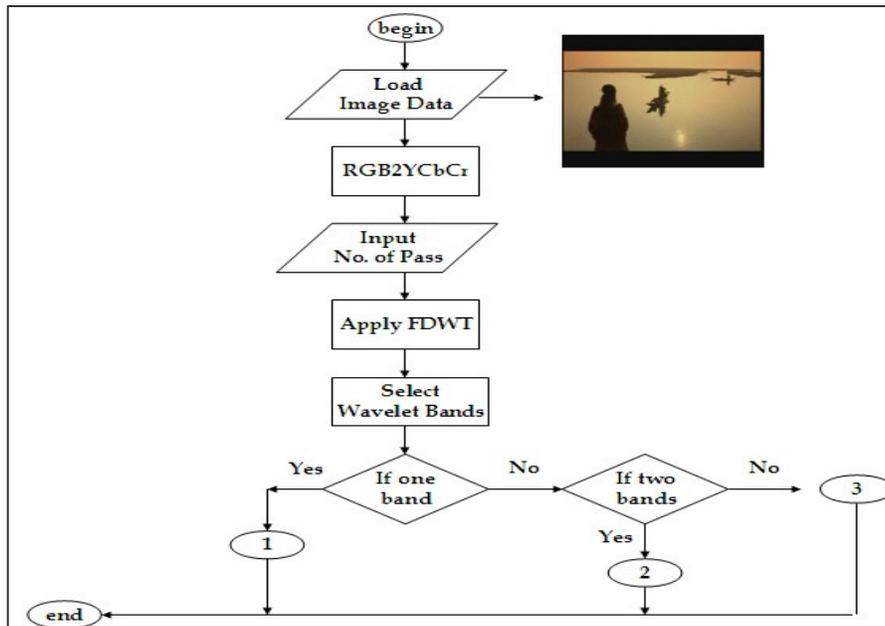
In the frequency domain the watermark is added not directly to the pixel values of the original image but the host image is first transformed into the frequency domain using float 9/7 Tap filter wavelet transform. The transformed image has now a low (approximation) and high (details) frequency regions. In any watermarking scheme developed in the literature, the most important step is the embedding process, which is hiding the information into the specific region of the host signal. In this work, the mid frequencies (HL, LH) depending on the number of pass are selected to embed the majority data of the watermark about (%80) and the rest of the data (%20) is added to the high frequencies (HH). As in the spatial domain the color space of the original image is converted from RGB to the YCbCr system. And then the Y (Luminance) channel which is adequate with a visual system is chosen to add the watermark data.

2.2.1 Non Blind Technique

In non-blind scheme watermark detection, both the original host information and watermark key are needed to estimate the embedded watermark data. The steps of this scheme are presented as follows (see figure 3):

1. Load original color image (RGB).
2. Convert RGB to YCbCr.
3. Apply forward wavelet transform (9/7 Tap Filter).
4. Select Y band to embed the watermark
 - a. Add to LL, HL, LH and HH separately
 - b. Add to (HL + LH) together
 - c. Add to (HL + LH) and some frequencies of HH
5. Store the position of the original image affected by the watermark.

6. Apply inverse wavelet transform.
7. Convert YCbCr to RGB.
8. Perform some malicious attacks on watermarked image (JPEG and JPEG2000 compression).
9. Find fidelity measure (PSNR) between original and watermarked image before and after attacks.
10. Extract watermark before and after attacks.
11. Determine similarity between embedded (original) and extracted watermark.



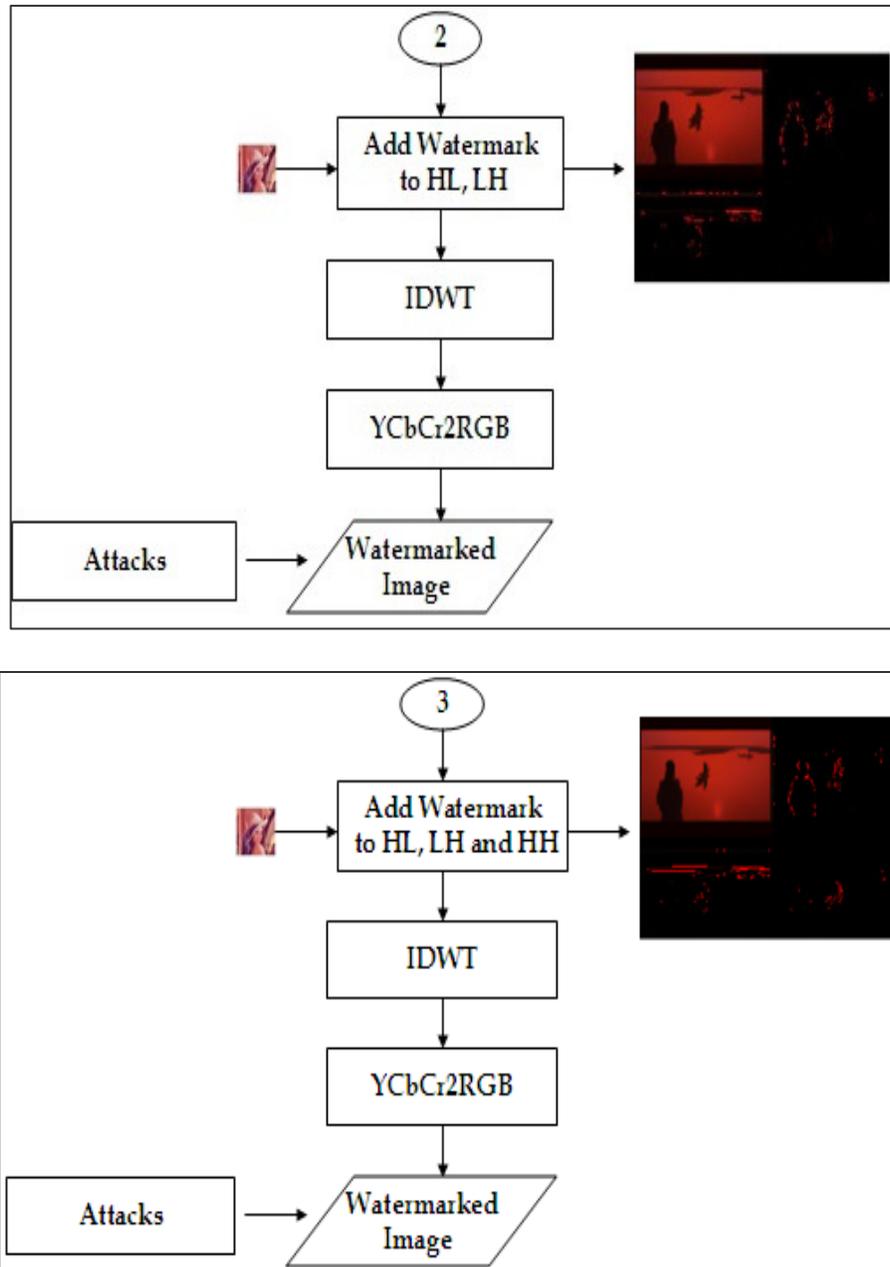


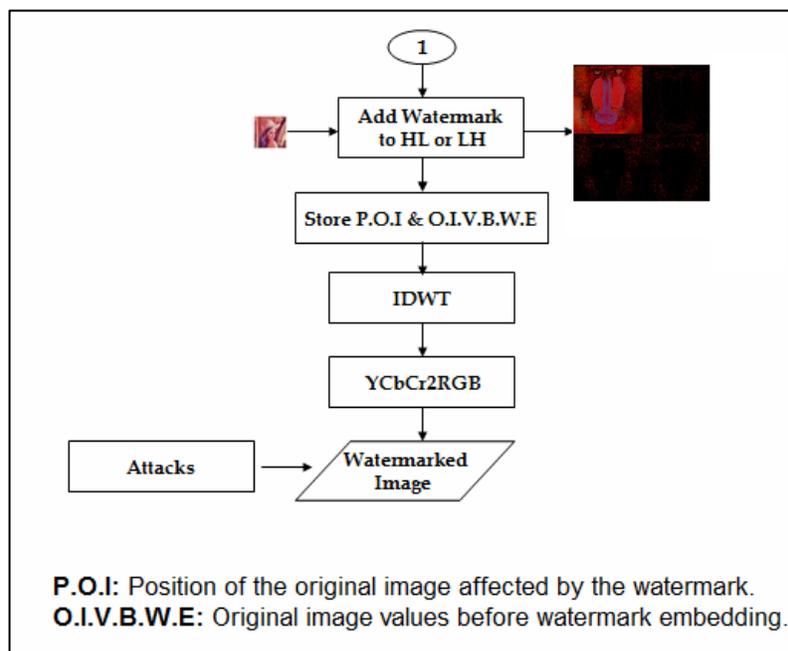
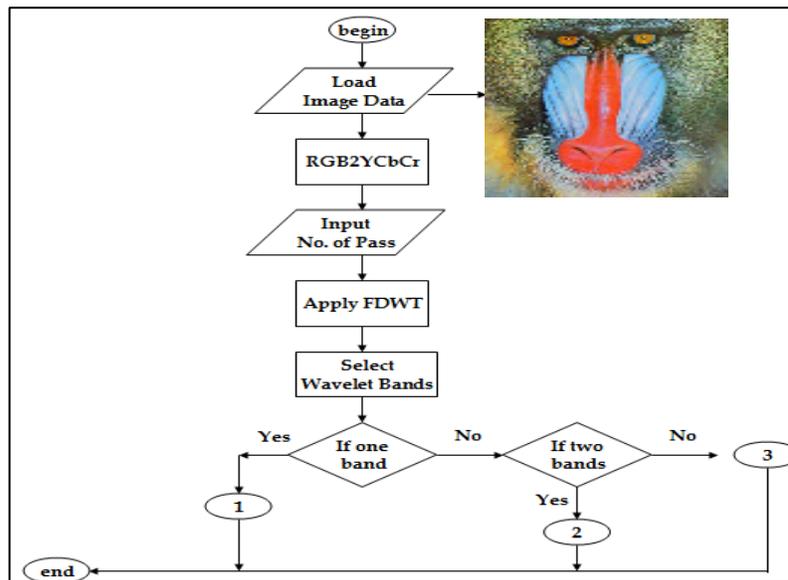
FIGURE 3: Non blind embedding process in frequency domain

2.2.2 Semi Blind Technique

In semi-blind watermark detection, both of the watermark key and watermark position in the original image that affected by the watermark are needed to estimate the embedded watermark data. The steps of this scheme are presented as follows (see figure 4):

1. Load original color image (RGB).
2. Convert RGB to YCbCr.
3. Apply forward wavelet transform (9/7 Tap Filter).
4. Select Y band to embed the watermark
 - a. Add to LL, HL, LH and HH separately

- b. Add to (HL + LH) together
- c. Add to (HL + LH) and some frequencies of HH
5. Store the position of the original image affected by the watermark and the original image values before watermark embedding.
6. Apply inverse wavelet transform.
7. Convert YCbCr to RGB.
8. Perform some malicious attacks on watermarked image (JPEG and JPEG2000 compression).
9. Find fidelity measure (PSNR) between the original and watermarked image before and after attacks.
10. Extract watermark before and after attacks.
11. Determine similarity between embedded (original) and extracted watermark.



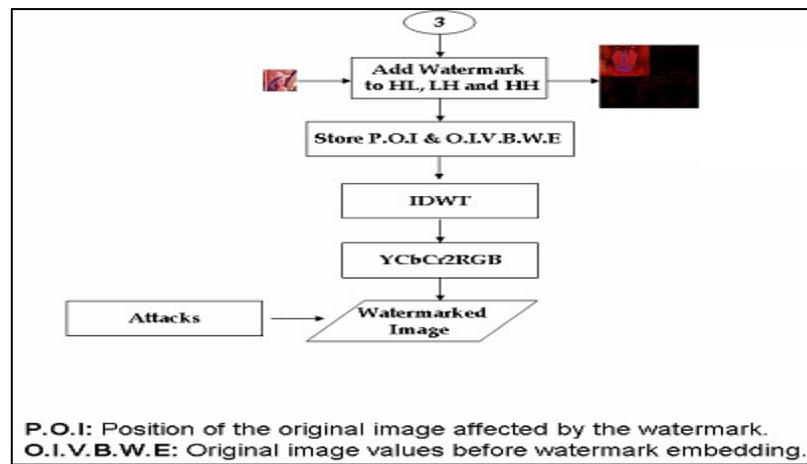
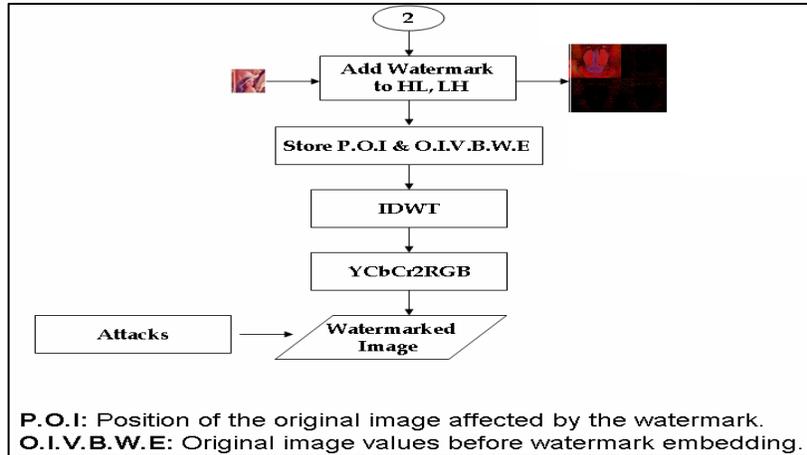


FIGURE 4: Semi blind embedding process in frequency domain

2.3 Watermarking Extracting Process

In figure (5) the flowchart of extraction process for the non-blind scheme is shown.

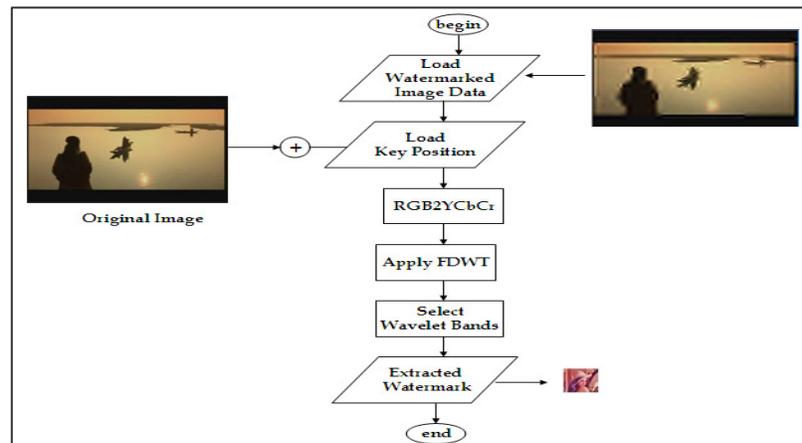


FIGURE 5: Non blind extraction process

In figure (6) the flowchart of extraction process for the semi-blind scheme is shown.

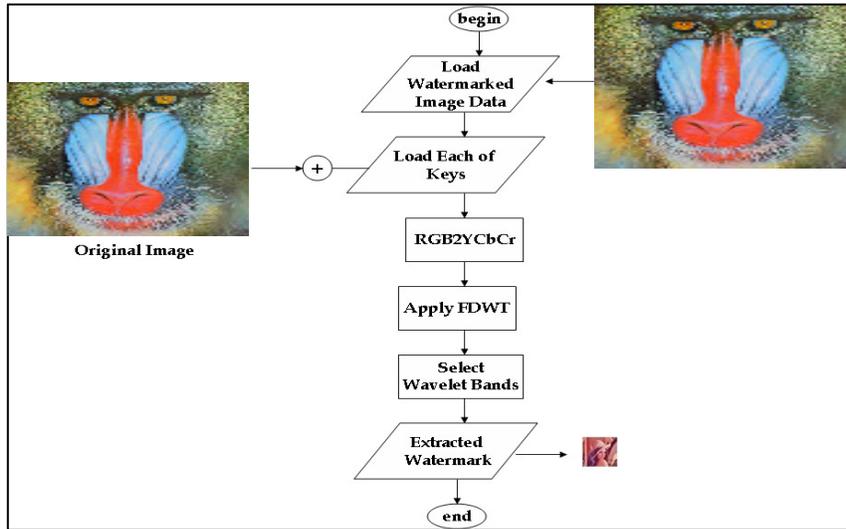


FIGURE 6: Semi blind extraction process

2.4 Watermarking Attacks

Working on attacks is to develop highly robust watermarking schemes and define better benchmarks. In this work, StirMark (benchmarking) program which is writing in C++ language is used to test the robustness of the image watermarking. The robustness tests (embedding, transformation, extraction) fall in (currently) three arbitrary categories:

- Signal processing: these tests typically apply transformation to the image but to not change its size (no resampling required);
- Geometric transformations: these require the use of resampling algorithm as they change the size of the picture.
- Special transforms: they basically include any other test not falling in the previous categories.

Figure (7) illustrates the attacks diagram on watermarked images in both spatial and frequency domain.

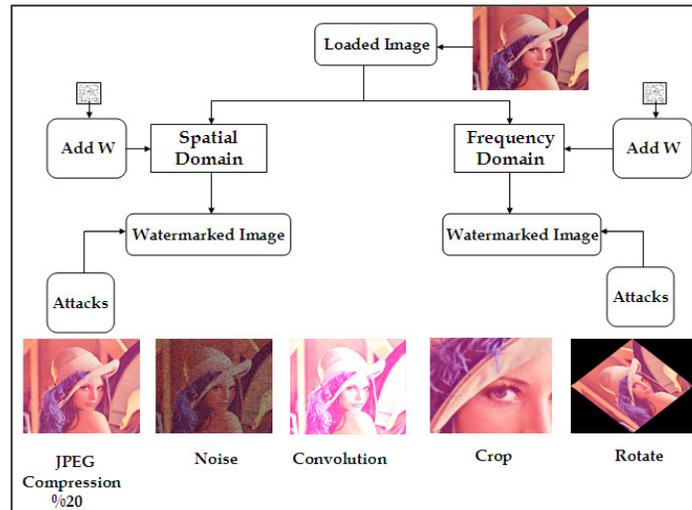


FIGURE 7: Watermarking Attacks type

3. EXPERIMENTS AND RESULTS

To show the efficiency of the proposed schemes in the frequency domain (non-blind and semi-blind), the schemes are tested with the optimal parameters (scaling factor =0.1, No. pass=3, No. band=2 (HL-LH)) on the gray Lena image (512 X 512) with a logo watermark (see Figure 8).



FIGURE 8: Left: original image, Mid: watermarked image, Right: watermark

Figures (9), (10) show the similarity values between numbers of pass under JPEG compression when the quality factor = 50 for (Non and Semi Blind) schemes respectively.

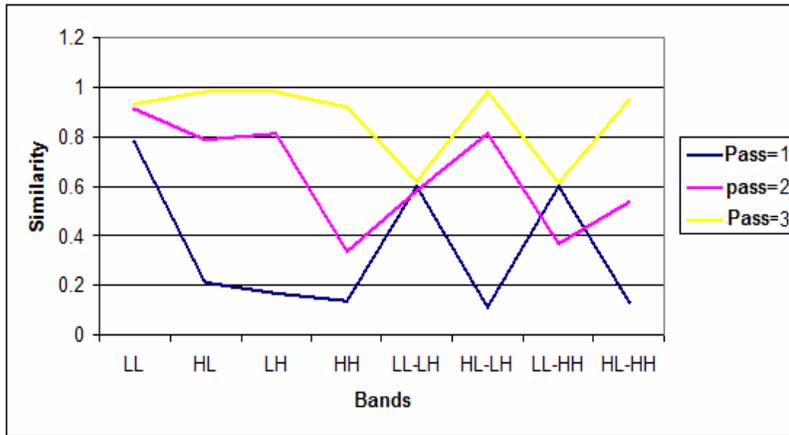


FIGURE 9: Similarity values between numbers of passes under JPEG compression (Non-Blind)

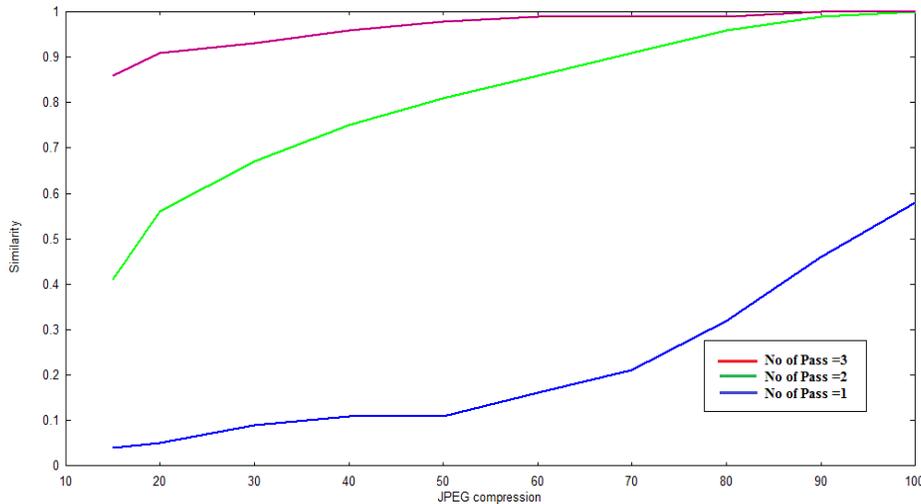


FIGURE 10: Similarity values between numbers of passes under JPEG compression (Semi-Blind)

Table (1) shows that even with low quality factor to 25, the proposed scheme can detect the existence of the watermark. Table (2) presents the comparison results between the current method and other recent publication, which is published in IEEE community [9]. The presented results below are obtained when the proposed scheme is tested for non-blind image watermarking. It also shows the imperceptibility (invisibility) of the watermarked image before the attack, for example the fidelity measure PSNR = 38 dB.

Quality Factor	80	70	50	40	25
Extracted Watermark					
Similarity	1	1	1	1	0.99

TABLE 1: Results against JPEG compression

Different attacks	Similarity		
	Lien[06]	Peng Liu[09]	Our scheme
JPEG (QF=25)	0.63	0.801	0.99
JPEG (QF=40)	0.79	0.828	1
JPEG (QF=50)	0.89	0.916	1
Median Filter 3*3	0.79	0.89	0.98

TABLE 2: Comparison of the proposed scheme with other schemes

4. CONCLUSIONS

The experimental results have shown that the proposed watermark in a frequency domain is invisible to human eyes and very robust to various attacks, such as image compression, image filtering, geometric transformations and noises. In frequency domain, the non-blind watermarking scheme is more robust than semi-blind scheme. For the same used parameters (No. of pass=3, No. of bands=2 HL, LH and scaling factor=0.1), the similarity between the original and the extracted watermark after median filter attack (WinSize=3*3) equals 96% and 92% respectively. The test results led to better performance when the watermark is embedded in the HL and LH bands with a three level of decomposition (i.e., No. of pass=3) in both non and semi-blind schemes.

Simulation results show that the number of wavelet pass affects the embedded watermark values. For the No. of pass=1, the PSNR of the extracted watermark after JPEG attack (CF=25) is equal to 4 dB but for three passes PSNR=24 dB.

Simulation results show that the selection of bands to embed the watermark is very important (in our case best bands are HL and LH). Optimal involved parameters give a new contribution results compared to the recent research publications (see Table 2).

5. REFERENCES

- [1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, 1999.
- [2] BARNETT, R. 1999. Digital watermarking: Application, techniques, and challenges. IEE Electron. Comm. Engin. J., 173–183. BENDER, W., BUTERA, W., GRUHL, D., HWANG, R., PAIZ, F. J., AND POGREB, S. 2000. Applications for data hiding. IBM Syst. J. 39, 3 and 4, 547–568.
- [3] VOLOSHYNOVSKIY, S., PEREIRA, S., PUN, T., EGGERS, J., AND SU, J. 2001. Attacks on digital watermarks: Classification, estimation based attacks and benchmarks. IEEE Comm. Mag. 39, 9, 118–126.
- [4] P. Dong, G. Jovan, "Digital Watermarking Robust to Geometric Distortions" IEEE Transaction on Image Processing, vol. 14, no. 12, pp. 2140-2150, 2005.
- [5] J.R. Hernandez, M. Amado, and F. Perez- Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure," IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.
- [6] Chuanmu Li Haiming Song, 2009, A novel watermarking scheme for image authentication in DWT domain. IEEE on Security and Identification in Communication. pp. 160-162.
- [7] P. Premaratne, "A novel watermark embedding and detection scheme for images in DFT domain", Proceedings of IEE 7th International Conference on Image Processing & Applications, Vol.2, 1999, pp.780-783.
- [8] P. Meerwald, C. Koidl and A. Uhl, "Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization", IEEE Transaction on Multimedia, vol. 11, no. 5, pp. 1037-1041, 2009.
- [9] L. Peng and D. Zhizhong, "A blind image watermarking scheme based on wavelet tree quantization", IEEE 2nd International Symposium on Electronic Commerce and Security, ISBN: 978-0-7695-3643-9, 2009.
- [10] A. Hanaa, M. hadhoud, and A. Shaalan, "A Blind Spread Spectrum Wavelet Based Image Watermarking Algorithm" International Conference on Computer Engineering & Systems, pp. 251-256, 2009.
- [11] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", (Second Edition), Morgan Kaufmann Publisher, ISBN-10: 0123725852, 2007.
- [12] Y. Zhang, "Digital Watermarking "Digital Watermarking Technology: A Review", International Conference on Future Computer and Communication, pp. 250-252, 2009.

A proposed Solution: Data Availability and Error Correction in Cloud Computing

Anil Gupta

Maharaja Ranjit Singh College,
Hemkunt Campus, Khandwa Road,
Indore-452001, MP, India

anil_sg@yahoo.com

Parag Pande

Shri Satya Sai Institute of Science and Technology,
Sehore M.P, India

parag.pande@yahoo.com

Aaftab Qureshi

Shri Satya Sai Institute of Science and Technology,
Sehore, M.P, India

aaftab_toc@yahoo.com

Vaibhav Sharma

Maharaja Ranjit Singh College,
Hemkunt Campus, Khandwa Road,
Indore-452001, MP, India

vaibhav.sharma_09@yahoo.com

Abstract

Cloud Computing is the hottest technology in the market these days, used to make storage of huge amounts of data and information easier for organizations. Maintaining servers to store all the information is quite expensive for individual and organizations. Cloud computing allows to store and maintain data on remote servers that are managed by Cloud Service Providers (CSP) like Yahoo and Google. This data can then be accessed through out the globe. But as more and more information of individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. In this paper we discussed security issues and requirements in the Cloud and possible solutions of some the problems. We develop an architecture model for cloud computing to solve the data availability and error correction problem.

Keywords: Cloud Computing, Security Issues, Cloud Security, Cloud Architecture.

1. INTRODUCTION

One of the identifying characters of cloud computing is that computing is delivered via the Internet as services. Computing and IT resources are encapsulated as services, hiding all the details of implementation, deployment, maintenance and administration [1]. Computing will be shifted from on-premise systems to remote systems and users are connected to their data via the Internet. Individual organizations will lose their control of their data to some extent, as the data is stored over the Internet and is likely leased from cloud operators. With cloud computing, deployment of IT systems and data storage is changed from on-premises user-owned IT infrastructures to off-premises third-party IT infrastructures. Having the whole IT systems and data on infrastructures with limited controls creates an obstacle for migrating traditional IT systems and data into clouds, as users have the following security concerns:

Limited control over the data may incur security issues.

As the data is on the single cloud, data availability becomes a great challenge.

Having the whole IT system and data on a single cloud may give the cloud operator excessive power for controlling and modifying users' data.

In this paper we try to specify security issues and requirements in the Cloud and possible solutions of some the problems. We develop an architecture model for cloud computing to solve the data availability and error correction problem.

Our paper is organized as follows: Section 2 identifies the security issues and requirement that users must be aware when adopting cloud computing. Section 3 surveys the related work. Section 4 summarizes the RAID models to address the security concerns. Section 5 explains our proposed architecture for cloud computing with features provided by the models. Section 6 concludes the paper.

2. SECURITY ISSUES AND REQUIREMENT

Security concerns [2,3] have been raised due to the new computing model introduced by cloud computing, which is characterized by off-premises computing, lost control of IT infrastructure, service-oriented computing, and virtualization, and so on. Security concerns from users can be briefly summarized as follows:

- **System failure and Data availability:** When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider,
Requirement: If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider.
- **Data error:** Client data should be error free on the cloud. As the data is stored on the cloud whereas the client is at other side. If the correct storage strategy is not used data might not be stored correctly on the storage server of the Cloud.
Requirement: Very essential requirement for the client on the cloud.
- **Data Migratibility:** Users that adopt cloud computing may subject to the risk that their data cannot be migrated to other clouds.
Requirement: Without the capability of migrating data to other clouds, users may be forced to stay with a cloud if they have considerable dependence on the data.
- **Data confidentiality and integrity:** Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control [25, 19].
Requirement: They may not be able to prevent unauthorized disclosure or malicious modification of their data.
- **Long-term viability:** Ideally, cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event.
Requirement: How you would get your data back and if it would be in a format that you could import into a replacement application in such an event.
- **Data location:** When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in.
Requirement: Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.
- **Data segregation:** Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
Requirement: For data security and privacy.
- **Data Recovery:** Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.
Requirement: otherwise clients will losses their all data. Provider has "the ability to do a complete restoration, and how long it will take."

- **Data security:** Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the European Union. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS).
Requirement: For data security and privacy.
- **Data privacy:** The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy.
Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

These concerns have been identified in several earlier works [12, 19]. Armbrust et al. [19] considered these concerns as the top most obstacles to growth of cloud computing.

3. RELATED WORK

Extensive research efforts have been put into cloud computing and its related technologies, resulting in several well acknowledged cloud computing theories and technologies, including MapReduce [4] and its implementation Apache Hadoop [5], Microsoft Dryad [6], Condor DAGman [7], Eucalyptus [26], Nimbus [8], Reservoir [27], and CARMEN [9].

Various security related issues and concerns in cloud computing have been identified and are studied, including data privacy [10, 11, 12], data protection [13], access control [14, 15, 12], availability [16], authentication [17], scalability [18].

Armbrust et al. [19] identified ten obstacles to growth of cloud computing. The top three obstacles are actually very close to the concerns identified in Section 2.

Research in security patterns has established a structural way and a proven practice for secure system designs and implementations. They provide guidelines as well as knowledge that are proven and standardized [20, 21, 22, 23].

Domain security is a method developed by Qinetiq to develop architectural models for applications based on security requirements [24]. The architectures generated by the Domain Security method focus on the software engineering aspect of systems to implement, instead of security protocols, cryptographic operations and so on.

4. RAID MODELS

RAID 1: RAID 1 creates an exact copy (or mirror) of a set of data on two or more disks. As shown in figure 1. This is useful when performance read or data availability (reliability) is more important than data storage capacity. Such an array can only be as big as the smallest member disk. A classic RAID 1 mirrored pair contains two disks, which increases availability (reliability) over a single disk. Since each member contains a complete copy of the data, and can be addressed independently, ordinary wear-and-tear reliability is raised by the power of the number of self-contained copies.

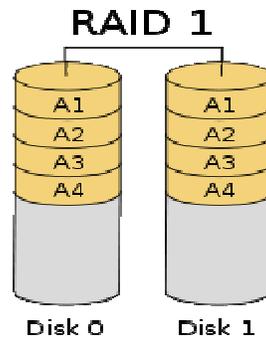


FIGURE 1: RAID 1 Model

RAID 5: RAID 5 uses block-level striping with parity data distributed across all member disks. As shown in figure 2. RAID 5 has achieved popularity because of its low cost of redundancy. This can be seen by comparing the number of drives needed to achieve a given capacity. For an array of n drives, with S_{\min} being the size of the smallest disk in the array, In RAID 5 storage capacity is $S_{\min} \times (n - 1)$.

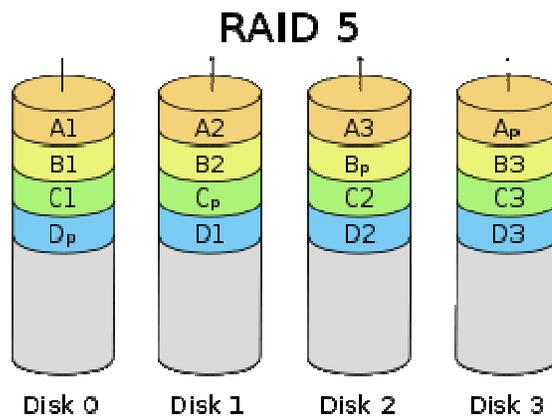


FIGURE 2: RAID 5 Model

Parity Calculation

A concurrent series of blocks (one on each of the disks in an array) is collectively called a stripe. If another block or some portion of that block is written on that same stripe, the parity block or some portion of that block is recalculated and rewritten. For any write operation it requires:

- Read the old data block
- Read the old parity block
- Compare the old data block with the write request. For each bit that has flipped (changed from 0 to 1, or from 1 to 0) in the data block, flip the corresponding bit in the parity block
- Write the new data block
- Write the new parity block

The disk used for the parity block is staggered from one stripe to the next; hence the term distributed parity blocks. RAID 5 write operations are expensive in terms of disk operations and traffic between the disks and the controller.

The parity blocks are not read on data reads, since this would add unnecessary overhead and would diminish performance. The parity blocks are read, however, when a read of blocks in the stripe fails due

to failure of any one of the disks, and the parity block in the stripe are used to reconstruct the errant sector. The CRC error is thus hidden from the main computer. Likewise, should a disk fail in the array, the parity blocks from the surviving disks are combined mathematically with the data blocks from the surviving disks to reconstruct the data from the failed drive on-the-fly.

This is sometimes called Interim Data Recovery Mode. The computer knows only that a disk drive has failed, so that the operating system can notify the administrator that a drive needs replacement; applications running on the computer are unaware of the failure. Reading and writing to the drive array continues seamlessly, though with some performance degradation.

5. PROPOSED MODEL

We are proposing a model for cloud, based on RAID architecture. In our proposed model we are using RAID 1 and RAID 5 level. This configuration can sustain the failure of all disks in either of the arrays, plus up to one additional disk from the other array before suffering data loss, i.e., by using this architecture at the data storage servers in the Cloud, we can handle the problem of Fault tolerance, data availability and Data recovery.

We combine both RAID 1 and RAID 5 for our proposed architecture. These combine architecture known as RAID 51 architecture. A **RAID 1** creates an exact copy (or **mirror**) of a set of data on two or more disks. This is useful for data availability (reliability). A **RAID 5** uses block level striping with parity data distributed across all member disks. This is very important for data correction.

RAID 51: RAID 51 architecture is an array that consists of two RAID 5's that are mirrors of each other. In this configuration reads and writes are balanced across both RAID 5s. In this architecture, there are two set of RAID 5 model that are mirror of each other. As well as they don't have any idea that their mirror image is also exist. Mirroring provides guarantee of data availability and since they are not aware about the mirroring, if any one try to change the data can easily be traceable. Similarly, the RAID 1 has no idea that its underlying disks are RAID 5's. As we are using RAID 5 under the RAID 1 architecture, we get the data correction facility also. Because A RAID 5 uses block level striping with parity data distributed across all member disks. As shown in figure 3.

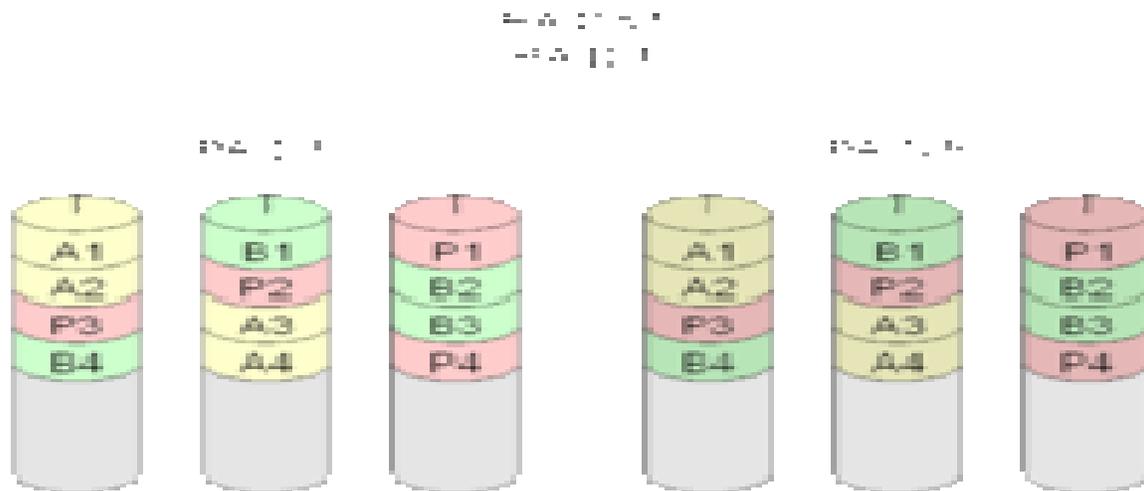


FIGURE 3: RAID 5+1 Model

Though RAID solves our problems but it suffer from poor performance when faced many write operations which are smaller than the capacity of a single stripe. This is because parity must be updated on each write, requiring read-modify-write sequences for both the data block and the parity block.

We can use RAID 6 in place of RAID 5 also. It extends RAID 5 by adding an additional parity block; thus it uses block-level striping with two parity blocks distributed across all member disks. RAID 6 does not have a performance penalty for read operations, but it does have a performance penalty on write operations because of the overhead associated with parity calculations. Performance varies greatly depending on how RAID 6 is implemented in the storage architecture.

Parity Calculation

Two different syndromes need to be computed in order to allow the loss of any two drives. One of them, P can be the simple XOR of the data across the stripes, as with RAID 5. A second, independent syndrome is more complicated and requires the assistance of field theory.

To deal with this, the Galois field $GF(m)$ is introduced with $m = 2^k$, where $GF(m) \cong F_2[x]/(p(x))$ for a suitable irreducible polynomial $p(x)$ of degree k . A chunk of data can be written as $d_{k-1}d_{k-2}...d_0$ in base 2 where each d_i is either 0 or 1. This is chosen to correspond with the element $d_{k-1}x^{k-1} + d_{k-2}x^{k-2} + ... + d_1x + d_0$ in the Galois field. Let $D_0, \dots, D_{n-1} \in GF(m)$ correspond to the stripes of data across hard drives encoded as field elements in this manner (in practice they would probably be broken into byte-sized chunks). If g is some generator of the field and \oplus denotes addition in the field while concatenation denotes multiplication, then **P** and **Q** may be computed as follows (n denotes the number of data disks):

$$\mathbf{P} = \bigoplus_i D_i = \mathbf{D}_0 \oplus \mathbf{D}_1 \oplus \mathbf{D}_2 \oplus \dots \oplus \mathbf{D}_{n-1}$$

$$\mathbf{Q} = \bigoplus_i g^i D_i = g^0 \mathbf{D}_0 \oplus g^1 \mathbf{D}_1 \oplus g^2 \mathbf{D}_2 \oplus \dots \oplus g^{n-1} \mathbf{D}_{n-1}$$

where \oplus is a bitwise XOR operator and g^i is the action of a linear feedback shift register on a chunk of data. Thus, in the above formula, the calculation of P is just the XOR of each stripe. This is because addition in any characteristic two finite fields reduces to the XOR operation. The computation of Q is the XOR of a shifted version of each stripe.

Mathematically, the generator is an element of the field such that g^i is different for each nonnegative i satisfying $i < n$.

If one data drive is lost, the data can be recomputed from P just like with RAID 5. If two data drives are lost or the drive containing P is lost the data can be recovered from P and Q using a more complex process. Working out the details is not hard with field theory. Suppose that D_i and D_j are the lost values with $i \neq j$. Using the other values of D , constants A and B may be found so that $D_i \oplus D_j = A$ and $g^i D_i \oplus g^j D_j = B$. Multiplying both sides of the latter equation by g^{n-i} and adding to the former equation yields $(g^{n-i+j} \oplus 1)D_j = g^{n-i}B \oplus A$ and thus a solution for D_j which may be used to compute D_i .

The computation of Q is CPU intensive compared to the simplicity of P. Thus, a RAID 6 implemented in software will have a more significant effect on system performance.

6. CONCLUSION

Cloud Computing is the cost, time and performance effective. Some basic Security issues are the key concern in the Cloud Computing use and in the implementation for the Client as well as for Vendors.

Security concern of the Cloud infrastructure relies on trusted computing and cryptography. Organizational data must be protected in a manner consistent with policies. No standard contract exists that the cover the security related issues. Having a list of common outsourcing provisions, such as privacy and security standards, regulatory and compliance issues, service level requirements and penalties, change management processes, continuity of service provisions, and termination rights, provides a useful starting point. The migration to a cloud computing environment is in many ways an exercise in risk management.

A RAID 1 model can be an effective protection against physical disk failure; it does not provide protection against data corruption due to viruses, accidental file changes or deletions, or any other data-specific changes. By design, any such changes will be instantly mirrored to every drive in the array segment. A virus, for example, that damages data on one drive in a RAID 1 array will damage the same data on all other drives in the array at the same time. For this reason system using RAID 1 to protect against physical drive failure should also have a traditional data backup process in place to allow data restoration to previous points in time. It would seem self-evident that any system critical enough to require disk redundancy also needs the protection of reliable data backups.

The risks must be carefully balanced against the available safeguards and expected benefits, with the understanding that accountability for security concern remains with the organization. Too many controls can be inefficient and ineffective, if the benefits outweigh the costs and associated risks. An appropriate balance between the strength of controls and the relative risk associated with particular programs and operations must be ensured.

7. REFERENCES

- [1] Anil Gupta, Aaftab Qureshi, Parag Pande, "Cloud Computing Characteristics and Service Models: our own interpretation".
- [2] Kresimir Popovic, et al., "Cloud "Computing issues and challenges" MIPRO 2010 May 24-28 Opatija, Croatia, pp 344-349.
- [3] Gansen Zhao, et al., "Deployment Models: Towards Eliminating Security Concerns from Cloud Computing" IEEE 2010, pp 189-195.
- [4] J. Dean and S. Ghemawat. "Mapreduce: simplified data processing on large clusters". *Commun. ACM*, 51(1):107–113, 2008.
- [5] Apache Hadoop, 2009. <http://hadoop.apache.org/>.
- [6] M. Isard, M. Buidu, Y. Yu, A. Birrell, and D. Fetterly. "Dryad: distributed data-parallel programs from sequential building blocks". In EuroSys '07: Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems 2007, pages 59–72, New York, NY, USA, 2007. ACM.
- [7] Condor DAGman, 2009. <http://www.cs.wisc.edu/condor/dagman/>. [18] D. Nurmi, R. Wolski, C. Grzegorzcyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov. "The eucalyptus open-source cloud-computing system". In Proceedings of Cloud Computing and Its Applications, October 2008.
- [8] Nimbus. "Introduction to nimbus", 2009. <http://workspace.globus.org/clouds/nimbus.html>. [3] S. Beco, A. Maraschini, and F. Pacini. "Cloud computing and RESERVOIR project". NUOVO CIMENTO DELLA SOCIETA ITALIANA DI FISICA C-COLLOQUIA ON PHYSICS, 32(2), Mar-Apr 2009.
- [9] CARMEN, 2009. <http://www.carmen.org.uk/>.

- [10] Å. A. Nyre and M. G. Jaatun. "Privacy in a semantic cloud: What's trust got to do with it?". In *The First International Conference on Cloud Computing*, pages 107–118, 2009.
- [11] S. Pearson, Y. Shen, and M. Mowbray. "A privacy manager for cloud computing". In *The First international Conference on Cloud Computing*, pages 90–106, 2009.
- [12] L. Kaufman. "Data security in the world of cloud computing". *IEEE SECURITY & PRIVACY*, 7(4), July- August 2009.
- [13] S. Creese, P. Hopkins, S. Pearson, and Y. Shen. "Data protection-aware design for cloud services". In *The First International Conference on Cloud Computing*, pages 119–130, 2009.
- [14] L. Hu, S. Ying, X. Jia, and K. Zhao. "Towards an approach of semantic access control for cloud computing". In *The First International Conference on Cloud Computing*, pages 145–156, 2009.
- [15] D. Chen, X. Huang, and X. Ren. "Access control of cloud service based on ucon". In *The First International Conference on Cloud Computing*, pages 559–564, 2009.
- [16] T. Uemura, T. Dohi, and N. Kaio. "Availability analysis of a scalable intrusion tolerant architecture with two detection modes". In *The First International Conference on Cloud Computing*, pages 178–189, 2009.
- [17] L. Yan, C. Rong, and G. Zhao. "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography". In *The First International Conference on Cloud Computing*, pages 167–177, 2009.
- [18] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. ping Ye, and N. Tang. "Cloud computing: A statistics aspect of users". In *The First International Conference on Cloud Computing*, pages 347–358. Springer, 2009.
- [19] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "Above the clouds: A Berkeley view of cloud computing". Technical Report UCB/EECS- 2009-28, EECS Department, University of California, Berkeley, Feb 2009.
- [20] M. Schumacher, E. Fernandez, D. Hybertson, and F. Buschmann. *SECURITY PATTERNS: INTEGRATING SECURITY AND SYSTEMS ENGINEERING*. John Wiley & Sons, 2005.
- [21] T. Heyman, K. Yskout, R. Scandariato, and W. Joosen. "An analysis of the security patterns andscape". In *SESS '07: Proceedings of the Third International Workshop on Software Engineering for Secure Systems*, page 3, Washington, DC, USA, 2007. IEEE Computer Society.
- [22] E. B. Fernandez, J. Wu, M. M. Larrondo-Petrie, and Y. Shao. On building secure scada systems using security patterns. In *CSIRW '09: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research*, pages 1–4, New York, NY, USA, 2009. ACM.
- [23] B. Blakley and C. Heath. *SECURITY DESIGN PATTERNS*, 2004. The Open Group Security Forum.
- [24] K. J. Hughes. "Domain Based Security: enabling security at the level of applications and business processes", 2002. www.qinetiq.com.
- [25] A. Singh, M. Srivatsa, and L. Liu. "Search-as-a-Service: Outsourced Search over Outsourced Storage". *ACM TRANSACTIONS ON THE WEB*, 3(4), September 2009.

- [26] D. Nurmi, R. Wolski, C. Grzegorzczak, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov. "The eucalyptus open-source cloud-computing system". In Proceedings of Cloud Computing and Its Applications, October 2008.
- [27] S. Beco, A. Maraschini, and F. Pacini. "Cloud computing and RESERVOIR project". NUOVO CIMENTO DELLA SOCIETA ITALIANA DI FISICA C-COLLOQUIA ON PHYSICS, 32(2), Mar-Apr 2009.
- [28] Wikipedia" www.wikipedia.org".

Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation

Iwasokun Gabriel Babatunde

*Department of Computer Science,
Federal University of Technology,
Akure, Ondo State, Nigeria*

maxtunde@yahoo.com

Akinyokun, Oluwole Charles

*Department of Computer Science,
Federal University of Technology,
Akure, Ondo State, Nigeria*

akinwole2003@yahoo.co.uk

Alese Boniface Kayode

*Department of Computer Science,
Federal University of Technology,
Akure, Ondo State, Nigeria*

kaalfad@yahoo.com

Olabode Olatunbosun

*Department of Computer Science,
Federal University of Technology,
Akure, Ondo State, Nigeria*

olabode_olatubosun@yahoo.co.uk

Abstract

Fingerprint is a very vital index in the field of security. Series of Automatic Fingerprint Identification Systems (AFIS) have been developed for human identification. These systems compare each of the features of a template fingerprint image with each of the features in the feature sets in the reference database to determine whether the template and each of the reference images are from the same source. Comparison is done on the basis of preset parameters such as feature type, location, orientation and so on. Getting the features used for the construction of a reference database from the images involve the implementation of a sound fingerprint feature detection, validation and extraction algorithm. In this paper, the process of detecting and extracting true and false feature points in a fingerprint image is discussed. Attention is also given to the elimination of the false feature points through the process of validation. Some of the existing fingerprint feature extraction and validation algorithms were firstly modified and the resulting algorithms were implemented. The implementation was carried out in an environment characterized by Window Vista Home Basic as platform and Matrix Laboratory (MatLab) as frontend engine. Fingerprints images of different qualities obtained from the manual (ink and paper) and electronic (fingerprint scanner) methods were used to test the adequacy of the resulting algorithms. The results obtained show that with the modified algorithm, valid and true minutiae points were extracted from the images with greater speed and accuracy.

Keyword: AFIS, Pattern Recognition, Pattern Matching, Fingerprint, Post Processing, Minutiae Extraction.

1. INTRODUCTION

Fingerprint is an essential index in the enforcement of security and maintenance of a reliable identification of any individual. Fingerprint is currently being used as variables of security during voting, operation of bank accounts among others. It is equally used for controlling access to highly secured places like offices, equipment rooms, control centers and so on. The following reasons had been adduced for the wide use and acceptability of fingerprint for the enforcement of security [1-4]:

- a. Fingerprints have a wide variation since no two people have identical prints.
- b. Unlike in other biometrics, fingerprints exhibit high degree of consistency and they do not change in relative appearance.
- c. Fingerprint is left each time the finger contacts a surface.

Other reasons for the much larger market of personal authentication using fingerprints are:

- a. Availability of small and inexpensive fingerprint capture devices
- b. Availability of fast computing hardware
- c. High recognition rate devices that meet the needs of many applications
- d. The explosive growth of network and Internet transactions
- e. The heightened awareness of the need for ease-of-use as an essential component of reliable security.

2.0 FINGERPRINT FEATURES

The main ingredients of any fingerprint that are useful during pattern recognition and matching tasks are the features it possesses. The features are defined by type, position, orientation and so on and they exhibit uniqueness from fingerprint to fingerprint. Fingerprint features are classified into two categories; namely local and global features [5]. The local features are the tiny, unique characteristics of fingerprint ridges that are used for identification. They are found in the local area only and are invariant with respect to global transformation [6]. Two or more impressions of same finger may have identical features but still differ because they have minutia points that are different [7]. In Figure 1, ridge patterns (a) and (b) are two different impressions of the same finger (person). The same minutia point is read as bifurcation in (a) while it appears as a ridge ending in (b).

Global features are characterized by the attributes that capture the global spatial relationships of a fingerprint. The following are the common fingerprint global features [7-9]:

2.1 Basic Ridge Patterns:

The ridge patterns are the patterns formed from the dark areas of the finger tip epidermis produced when a finger is pressed against a smooth surface. The valleys are the bright areas. Ridges and valleys run in parallel as shown in Figure 2.

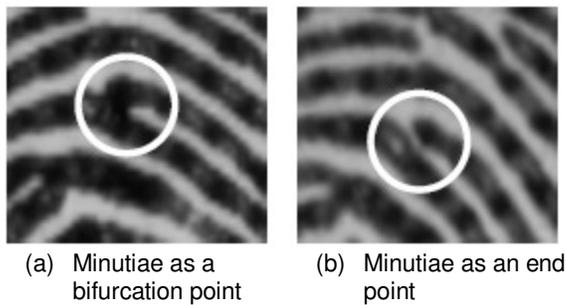


FIGURE 1: The same minutiae extracted from two different impressions.

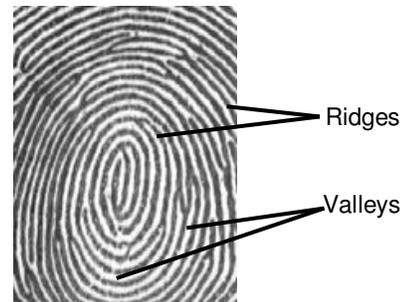


FIGURE 2: Ridges and valleys on a fingerprint image

The ridges form pattern of left loop, right loop, whorl, arch and tented arch as shown in Figure 3. In the loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered. In the right loop pattern, the ridges enter from the right side while the ridges enter from the left side in the left loop. In a whorl pattern, the ridges are usually circular while in the arch pattern, the ridges enter from one side, make a rise in the center and exit generally on the opposite side.

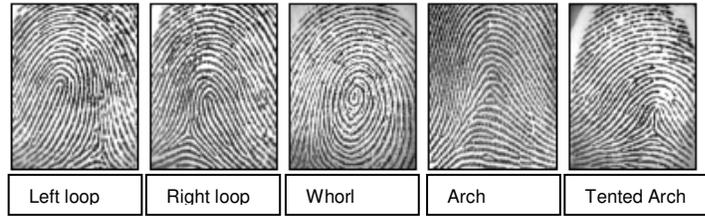


FIGURE 3: Basic types of fingerprint pattern

2.2 Pattern Area

The pattern area is the part of the fingerprint where the global features are found. Fingerprints can be read and classified based on the information in this area. The following are the information available in the pattern area of a fingerprint [2-4]:

- a. **Type Lines and Ridge Count:** Type Lines are the two innermost ridges that start parallel, diverge, and surround or tend to surround the pattern area. When there is a definite break in a type line, the ridge immediately outside that line is considered to be its continuation. The Ridge Count is most commonly the number of ridges between the Delta and the Core. To establish the ridge count, an imaginary line is drawn from the Delta to the Core and each ridge that touches this line is counted. The ridge count between the core and delta shown in Figure 4 is the number of ridges crossed by the imaginary lines drawn across the ridges.

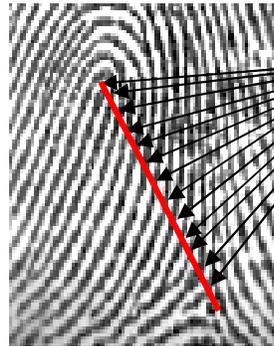


FIGURE 4: The ridge count between Delta and Core

Ridges and line intersections

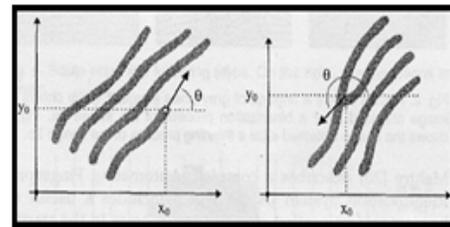


FIGURE 5: Minutia point orientation

- b. **Position:** The position of the minutia point refers to its x, y location, either in an absolute sense or relative to fixed points like the Delta and Core points.
- c. **Type:** Different types of minutiae are found in the fingerprint pattern area. They include termination, bifurcation, lake, independent ridge, point or island, spur, cross over and so on.
- d. **Spatial Frequency:** Spatial frequency refers to how far apart the ridges are in the neighborhood of the minutia point. It is measured by the average distance apart of the ridges.
- e. **Orientation:** The minutia orientation is defined by its direction. The orientations of the ridge ending and bifurcation of Figure 5 are marked as α and β respectively.
- f. **Curvature:** The curvature refers to the rate of change of ridge orientation. The curvature, c of one of the two ridge endings of Figure 6 is obtained from the absolute difference between α_2 of Figure 6(b) and α_1 of Figure 6(a). It is the displacement angle resulting from the change in orientation of the ridge pattern.
- g. **Core and Delta Areas:** The core area is located at the approximate center of the finger impression as shown in Figure 7 and it is used as a reference point for reading and classifying the print. The Delta area is the region in the ridge pattern where there is triangulation or a dividing of the ridges as shown in Figure 7. It is also the point of the first bifurcation, abrupt ridge ending, meeting point of two ridges, dot, fragmentary ridge, or any point upon a ridge at or nearest to the center of divergence of two type lines, located at or directly in front of their point of divergence. It is a definite fixed point used to facilitate ridge counting and tracing.

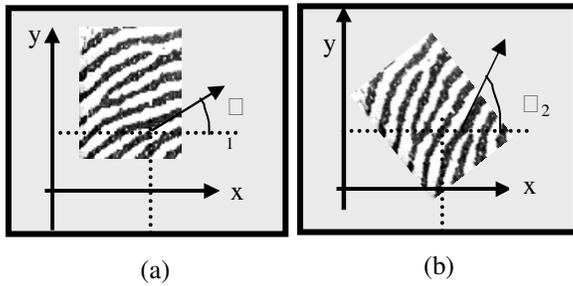


FIGURE 6: Change in ridge orientation



FIGURE 7: The Delta and Core structure of fingerprint

3. DETECTION AND EXTRACTION OF FINGERPRINT FEATURES

The sequence of activities connected to the detection and extraction of features from any fingerprint is illustrated in Figure 8.

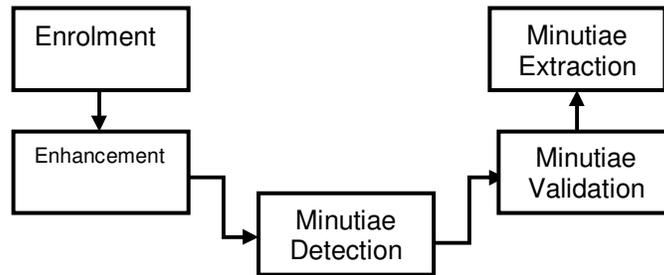


FIGURE 8: Sequence of activities connected to fingerprint feature extraction

Manual or electronic method could be adopted for the enrolment of fingerprint images [5]. In [10-11], several image enhancement algorithms were discussed and implemented. Features were also detected, validated and extracted from the thinned images obtained as the final results of the enhancement stage. A Crossing Number (CN) method for feature detection and extraction from the thinned image had been implemented in [12-13]. In the CN method, the extraction of the features is done through the scanning of the 3 x 3 neighborhood of each ridge pixel in the thinned image. The CN value is then calculated from half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood as shown in Equation 1.

$$CN = 0.5 \sum_{i=1}^8 |P_i - P_{i+1}|, \quad P_9 = P_1 \quad (1)$$

Using the CN properties shown in Table 1, the ridge pixel is classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, a CN of 2 corresponds to a continuing ridge point and a CN of three corresponds to a bifurcation.

CN	Property
0	Isolated point
1	Ridge end point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

TABLE 1: Properties of the Crossing Number.

Similar to the Crossing number approach was the method proposed in [14-15]. These authors devised a method that uses a 3 x 3 window to examine the local neighborhood of each ridge pixel in a skeleton image. A pixel is classified as a ridge ending if it has only one neighboring ridge pixel in the window, and classified as a bifurcation if it has three neighboring ridge pixels. False minutiae may be introduced into the image due to factors such as noisy images, and image artifacts created by the thinning process [12]. Hence, after the detection of minutiae, it is important that a post-processing method is employed to validate them. Some examples of false minutiae structures are illustrated in Figure 9. The false structure include the spur, hole, triangle and spike structures [16]. From inspection, it is revealed that the spur structure generates false ridge endings, while both the hole and triangle structures generate false bifurcations. The spike structure on its own generates a false bifurcation and a false ridge ending point.

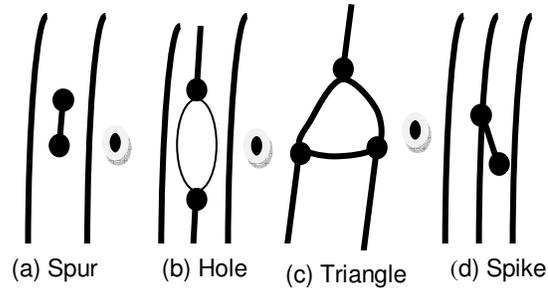


FIGURE 9: Examples of typical false minutiae structures.

A novel approach to the validation of minutiae is the post-processing algorithm proposed in [17]. This algorithm operates on the skeleton image. However, rather than employing a different set of heuristics each time to eliminate a specific type of false minutiae, this approach incorporates the validation of different types of minutiae into a single algorithm. It tests the validity of each minutiae point by scanning the skeleton image and examining its local neighborhood. The algorithm is able to cancel out false minutiae based on the configuration of the ridge pixels connected to the minutiae point. In this research, the Crossing Number (CN) method for a pixel P is slightly modified with a view to speed up its operation. The modified version is presented as follows:

$$CN = \sum_{j=0}^7 |P_{j+2} - P_{j+1}|, \quad P_9 = P_1 \quad (2)$$

The eight neighbouring pixels of P are scanned in clockwise direction as follows:

P ₂	P ₃	P ₄
P ₁	P	P ₅
P ₈	P ₇	P ₆

With this modification, a ridge pixel with CN count of 2 corresponds to ridge ending and CN count of 6 corresponds to bifurcation as illustrated in Figure 10.

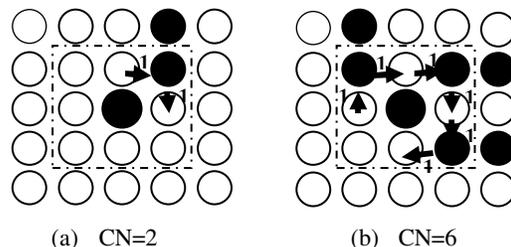


FIGURE 10: CN values for ridge ending and bifurcation point

Towards the validation of the minutiae points, a minutiae validation algorithm proposed in [17] was also modified before its implementation. The modified algorithm tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the point. The first step in the modified algorithm is the creation of an image M of size $W \times W$ centered on the candidate minutia point in the skeleton image. The central pixel of M is labeled with a value of -1. The rest of the pixels in M are initialized to values of zero, as shown in Figure 11(a) and Figure 11(d).

The subsequent steps of the algorithm depend on whether the candidate minutiae point is a ridge ending or a bifurcation.

- i. For a candidate bifurcation point:
 - Examine its 3×3 neighborhood in a clockwise direction. For the three pixels that are connected with the bifurcation point, label them with the value of 1. An example of this initial labeling process is shown in Figure 11(b).
 - Label with 1 the three ridge pixels that are connected to these three connected pixels. Example of this labeling process is shown in Figure 11(c).
 - Count in a clockwise direction, the number of transitions from 0 to 1 (T_{01}) along the border of image M . If $T_{01} = 3$, then extract the candidate minutiae point as a true bifurcation.
- ii. For a candidate ridge ending point:
 - Label with a value of 1 all the pixels contained in M , which are in the 3×3 neighborhood of the ridge ending point (Figure 11(e)).
 - Count in a clockwise direction, the number of 0 to 1 transitions (T_{01}) along the border of image M . If $T_{01} = 1$, then extract the candidate minutiae point as a true ridge ending.

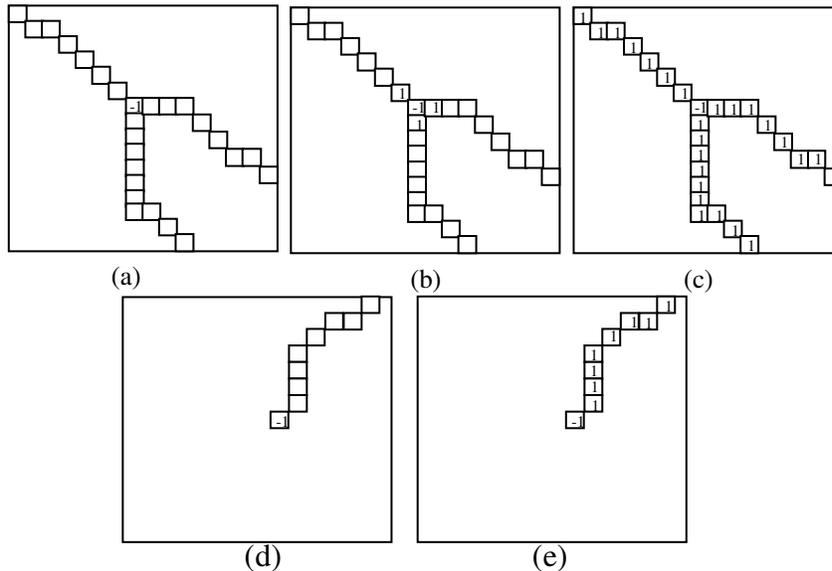


FIGURE 11: Example of validating a candidate bifurcation point $T_{01}=3$ and ridge ending point. $T_{01} =$

1.

4. EXPERIMENTAL RESULTS

The fingerprint minutiae extraction experiment was carried out in an environment characterized by Window Vista Home Basic Operating System as platform and Matlab (Matrix Laboratory) as frontend engine on a Pentium IV Personal computer with 1.87GB processor and 1024MB RAM. The essence of the experimental stage is to ascertain that the modified CN and the post-processing algorithms perform well and better in accuracy and speed over their original versions in the detection and extraction of features from fingerprint images. Shown in Figures 12(a) and 12(b) are the results of using the modified CN method to extract minutiae from a medium quality fingerprint image obtained using a manual fingerprinting method. Figures 12 (c) and 12(d) show

the results for the fingerprint image obtained from the electronic method. From the experimental plots of the extracted minutiae points on the thin images shown in Figure 12(a) and 12(c), it is deduced that both the true and false ridge pixels corresponding to a CN value of two and six have been detected from the images. Ridge endings are denoted by six pointed stars (hexagrams), and bifurcations are denoted by diamonds. The experimental plot presented in Figure 12(b) and 12(d) depict the extracted false and true minutiae points superimposed on the original image.

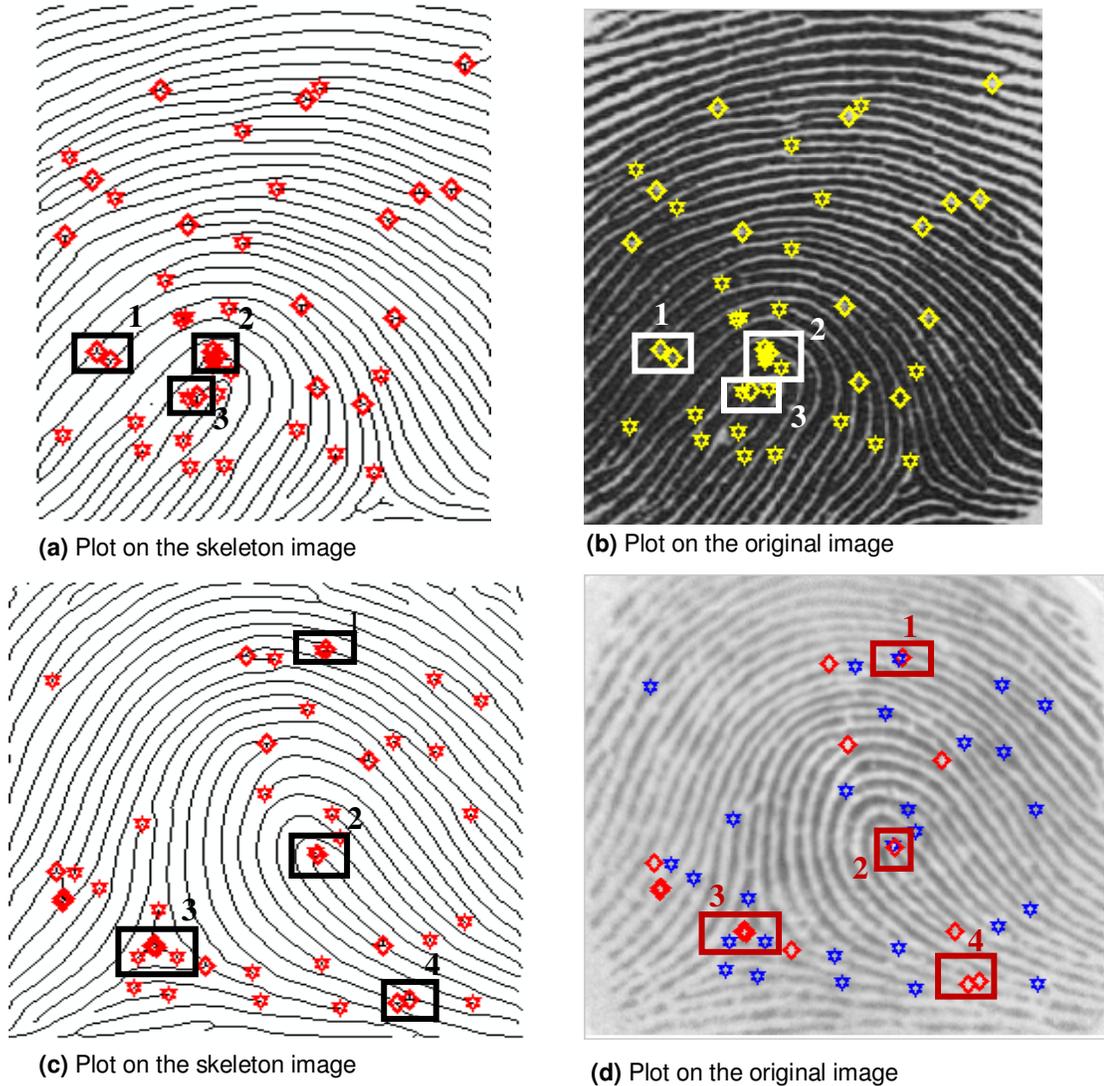


FIGURE 12: Results of performing minutiae extraction on a fingerprint image obtained by manual and electronic methods.

Visual inspection of the plots on the images indicates that the majority of the marked minutiae points from the thin images correspond to valid minutiae points in the original images. In all the plots, false minutiae point sets are covered by large boxes with appropriate labels.

Enlarged views of the false minutiae points shown in Figures 12 (a) and 12(b) are presented in Figure 13. Figure 13(a) depicts a false minutia point called a cross-over structure, which corresponds to the box labeled 1 and Figure 13(b) depicts a false minutiae point comprising of both the hole and the spike structures, which correspond to the box labeled 2. It can be seen that the cross-over structure shown in Figure 13(a) generates two false bifurcation points while the hole and spike structures shown in Figure 13(b) generate two false bifurcation points and a false

end point. Similarly, the spike structure shown in Figure 13(c) generates two false endpoints. However, in the original image shown in Figure 12(b), these minutiae points do not exist.

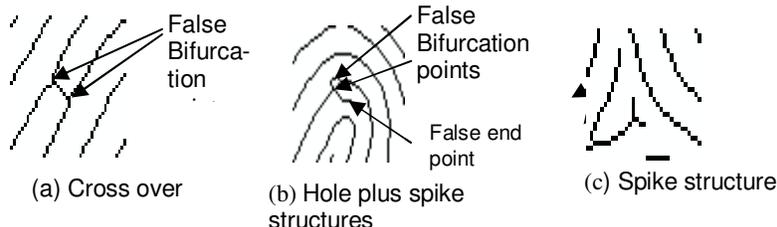


FIGURE 13: Enlarged view of the false minutiae from Figure 12(a).

The modified post-processing algorithm was implemented to eliminate the false minutiae that were extracted using the modified CN method. The experimental plots of the result of the post-processing experiment on the images shown in Figure 12 are presented in Figure 14. It is revealed in Figure 14(a) and 14(c) that all the false minutiae points on the skeleton images have been eliminated at the post-processing stage. The results shown in Figure 14 were obtained with image window of size 25 x 25 centered on the candidate minutia point. When window size is smaller than this value, the algorithm could not eliminate some false minutiae points. Shown in Figure 15(a) and Figure 15(b) are the false minutiae points not eliminated due to small window size of 21. This is due to fact that the entire local neighborhood around the candidate minutiae points could not be captured. This forced the number of 0 to 1 transition to 3 for bifurcation as illustrated in Figure 11(c). The number of 0 to 1 transition is also forced to 1 for the ridge ending as illustrated in Figure 11(e). Similarly with a higher window size, the algorithm eliminated some valid minutiae points. Shown in Figure 15(c) is the valid minutia point that is eliminated due to oversize window of 27. This is explaining the fact that the window extended beyond the local neighbourhood of the candidate minutia point and hence the number of 0 to 1 transition round the border is forced to 0.

In the original algorithm implemented in [12-13], scanning around the candidate minutia point was done in counter-clockwise direction to obtain the CN value. However, in the current study, the CN value was obtained by scanning the pixels around the candidate point in clockwise direction. In the two cases, both true and false minutiae were accurately extracted from the images. It is therefore established that during minutia extraction, emphasis is placed on the CN value rather than the direction of scanning. An implementation of the original CN algorithm over one hundred and seventeen (117) different fingerprint images obtained from FVC2004 fingerprint database DB3 set A took a mean time of 1.93 seconds to extract an average of forty two (42) true and false minutiae points from images. This task takes a mean time of 1.79 seconds with the modified CN algorithm under the same operational environment. This implies that the modified CN algorithm operates 7.25% faster than its original version with this set of images. This is attributed to lesser calculation involved in the modified version.

A window of size 23 x 23 around the candidate minutia point was reported to be most effective in eliminating the false minutiae by the original post-processing algorithm proposed in [17] and implemented in [12]. However, in the modified post-processing algorithm implemented in this research, a window size of 25 x 25 proved to be most effective. The higher window size led to increased reliability as the modified algorithm placed premium on elimination of false minutiae even at the expense of some valid minutiae points.

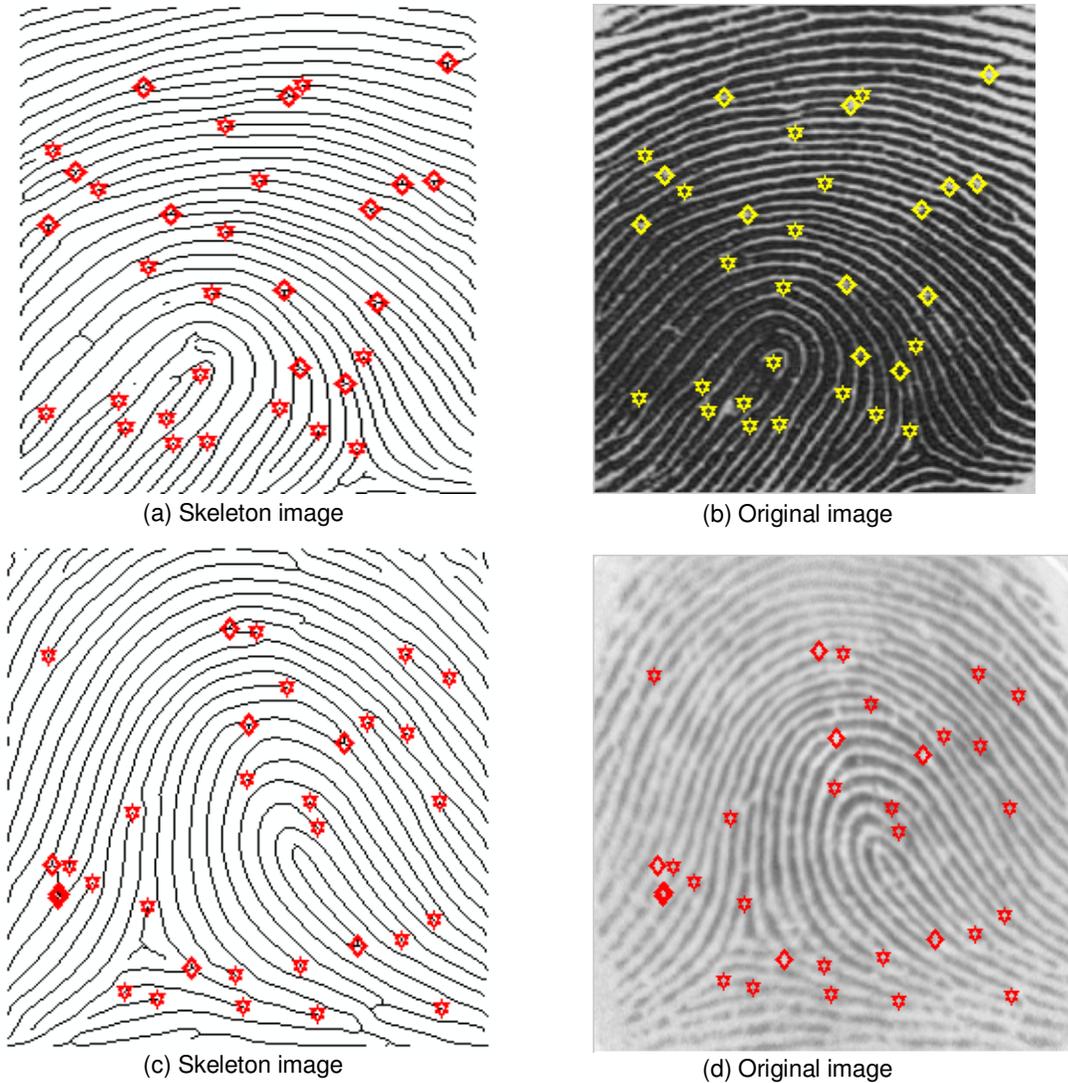


FIGURE 14: Results of minutiae post-processing experiment

5. CONCLUSION

This paper presents the results of the verification and modification of the minutiae detection and extraction method proposed and implemented in some concluded research works. The CN method proposed and implemented in [12-13] had been modified by varying the order and reducing the level of computation. The post-processing algorithm proposed in [17] was modified by labeling all the three connecting ridges to the candidate bifurcation point with 1 thereby raising the 0 to 1 transition to 3. The modified algorithms were implemented with images obtained from the manual (ink and paper) method as well as the electronic (fingerprint scanner) method. In the manner of the original algorithm, the modified CN algorithm extracted both the false and true minutiae points from the fingerprint images. However, greater speed and accuracy is recorded with the modified algorithms. Results also show that with suitable window size, the modified post-processing algorithm extracted all the true minutiae points from the images and ignored all the false minutiae points.

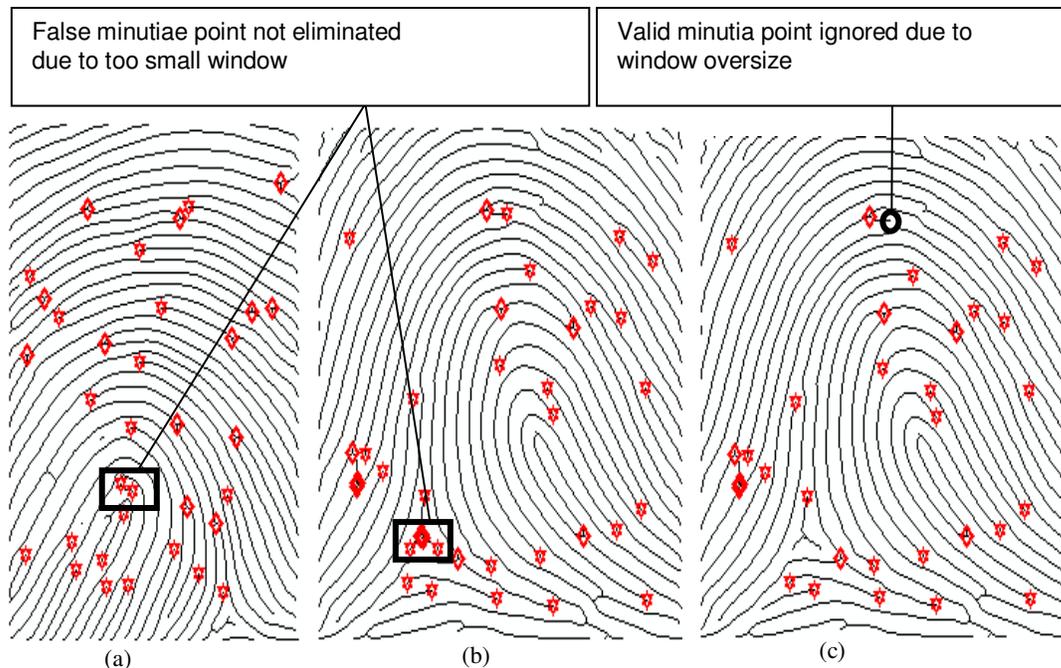


FIGURE 15: Experimental plots for too small and too large neighbourhood

6. REFERENCES

- [1] C. Roberts). 'Biometrics' (<http://www.ccip.govt.nz/newsroom/information-notes/2005/biometrics.pdf>. Accessed 23rd May, 2009
- [2] M. Cherry and E. Imwinkelried. "A Cautionary Note About Fingerprint Analysis and Reliance on Digital Technology", Public Defense Backup Center REPOR Volume XXI Number 3 T, 2006, pp7-9
- [3] M. J. Palmiotto. 'Criminal Investigation'. Chicago: Nelson Hal, 1994, pp234-239
- [4] D. Salter. 'Fingerprint – An Emerging Technology', Engineering Technology, New Mexico State University. 2006
- [5] O. C. Akinyokun and E. O. Adegbeyeni. 'Scientific Evaluation of the Process of Scanning and Forensic Analysis of Fingerprints on Ballot Papers', Proceedings of Academy of Legal, Ethical and Regulatory Issues, Vol. 13, Numbers 1, New Orleans, 2009:
- [6] L. Hong, Y. Wan and A. K. Jain. 'Fingerprint image enhancement: Algorithm and performance evaluation'. IEEE Transactions on Pattern Analysis and Machine Intelligence 20, 8, 2001, pp 777–789.
- [7] J. Tsai-Yang and V Govindaraju. 'A minutia-based partial fingerprint recognition system', Center for Unified Biometrics and Sensors, University at Buffalo, State University of New York, Amherst, NY USA 14228, 2004
- [8] D. Stoney. 'Measurement of fingerprint individuality'. Advances in Fingerprint Technology, 2nd Ed. By Henry C Lee, R. E Gaensslen, CRC Press, 2001

- [9] E. O. Adegbeyeni and O. C. Akinyokun. 'Techno Legal Issues of Scanning and Forensic Analysis of Ballot Papers Fingerprints'. Federal University of Technology, Akure, Nigeria, 2008.
- [10] J. Tsai-Yang and V. Govindaraju. 'A minutia-based partial fingerprint recognition system'. Pattern Recognition. Vol. 38, 10, 2006, pp. 1672-1684.
- [11] L. Hong, Y. Wan and A. Jain. 'Fingerprint image enhancement: Algorithm and performance evaluation'; Pattern Recognition and Image Processing Laboratory, Department of Computer Science, Michigan State University, 2006, pp1-30
- [12] T. Raymond. 'Fingerprint Image Enhancement and Minutiae Extraction', PhD Thesis Submitted to School of Computer Science and Software Engineering, University of Western Australia, 2003, pp21-56.
- [13] N. Sara, D. Sergie and V. Gregory 'User Interface Design of the Interactive Fingerprint Recognition (INFIR) System', 2004
- [14] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. "An identity authentication system using fingerprints". Proc. IEEE, 85(9), 1997, 1365–1388.
- [15] N. Ratha, S. Chen and A. K. Jain 'Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images', Pattern Recognition, Vol. 28, No. 11, 1995, pp 1657-1672.
- [16] Q. Xiao and H. Raafat. 'Pattern Recognition', 24,10, 1991, pp985-992
- [17] M. Tico and P. Kuosmanen. 'An algorithm for fingerprint image postprocessing', Proceedings of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, vol. 2, 2000, pp. 1735–1739.

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 6 - **Issue:** 1 - February 2012

i. Paper Submission: November 30, 2011

ii. Author Notification: January 01, 2012

iii. Issue Publication: January / February 2012

CONTACT INFORMATION

Computer Science Journals Sdn Bhd

B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2011
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org