Volume 5 ▪ Issue 2 ▪ October 2011

Editor-in-Chief
Dr Wei Wang

INTERNATIONAL JOURNAL OF SECURITY (IJS)

ISSN : 1985-2320

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

VOLUME 5, ISSUE 2, 2011

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-2320

International Journal of Security (IJS) 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.

IJS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

Book: Volume 5, Issue 2, October 2011
Publishing Date: 05 – 10 - 2011
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

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

CSC Publishers, 2011

EDITORIAL PREFACE

This is the second issue of volume fifth of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJS appears in more focused issues. Besides normal publications, IJS 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.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS 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 IJS. 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. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

TABLE OF CONTENTS

Volume 5, Issue 2, October 2011

Pages

A Novel Approach For Image Steganography In Spatial Domain Using Last Two Bits of Pixel Value

Rajkumar Yadav *rajyadav76@rediffmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Ravi Saini *ravisaini1988@rediffmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Gaurav Chawla *chawla.gaurav17@gmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Abstract

In this present study a new method for insertion of message in an image is proposed. We have used last two bits of pixel for insertion and retrieval of message. This method is an improvement over earlier methods like Least Significant Bit (LSB) method [2], 6th and 7th bit method [5] and 6th, 7th and 8th bit method [6]. Our method provides us optimal solution in case of chances of message insertion at a pixel location such that the change at a pixel value does not exceed range from +1 to -1 which is negligible to human eye.

Keywords: LSB Method, Cryptography, Steganography, Pseudo Random Number Generator.

1. INTRODUCTION

Steganography is the art and science of hiding information by embedding data into cover media. The term originated from Greek roots that literally mean “covered writing” [1]. The field of Steganography is very old. Throughout history, many steganography techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing and microdots [2, 3, 4]. Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover. As an example, the cover text:-“I’m feeling really stuffy. Emily’s medicine was not strong enough without another febrifuge.” hides the sentence “Meet me at Nine” if the reader retains the second letter of each word in sequence [11].

Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio in such a way that the human-perceived quality of the unsuspecting medium is not altered [12]. The idea was first described by Simmons in 1983 [7]. More comprehension theory of steganography is given by Anderson [8]. Steganography is different from cryptography which is about concealing the content of message whereas steganography is about concealing the existence of the message itself [9]. Images provide excellent carriers for hiding information and many different techniques have been introduced [10].

The most popular and oldest technique for hiding data in digital image is LSB technique [2]. One of the major disadvantage associated with LSB technique is that intruder can change the LSB of all image pixels. In this way, hidden message can be destroyed but the change in image quality is in the range of +1 to -1 at each pixel position.[5] designed the algorithm which uses 6th and 7th bits of pixel value for message insertion. It removes the disadvantages of LSB techniques but it has also one disadvantage. The disadvantage is that the chance of message insertion at pseudo random location at first chance is only 49%. Batra et *al.* [6] gives an algorithm which uses 6th, 7th and 8th bit for message insertion. This technique increases the chances of message insertion at pseudo random location at the first chance up to 85.93%. Our method uses the last two bits of pixel value and it increases the chances of message insertion at pseudorandom location at first chance up to 100% which is optimal solution.

2. DESCRIPTION OF PROPOSED METHOD

We have used the last two bits of pixel value for insertion and retrieval of message. We can insert 0 at a pixel value if last two bits of pixel value are 00 or 10. If the last two bits of pixel value, are not 00 or 10 by adding or subtracting 1 at that pixel value for insertion of 0. Similarly, we can insert 1 at a pixel value if last two bits of pixel value are 01 or 11. If the last two bits of pixel value are not 01 or 11 then we try to make them 01 or 11 by adding or subtracting 1 at that pixel value for insertion of 1. Now, at the retrieval end, if the last two bits of pixel value are 00 or 10 then 0 is the message bit else 1 is the message bit. The insertion process is shown in figure 2 (a) and retrieval process is shown in figure 2 (b).

The intruder can change the LSB of all the pixel values in our method also as in case with LSB method. But in case of our method if intruder changes LSB's of all pixel values then at some locations the change in pixel values would be +2 or -2 which will be visible to human eye. This situation indicates that something goes wrong in the middle (i.e. between sender and receiver). So, in this age the sender retransmit the stego image once again.

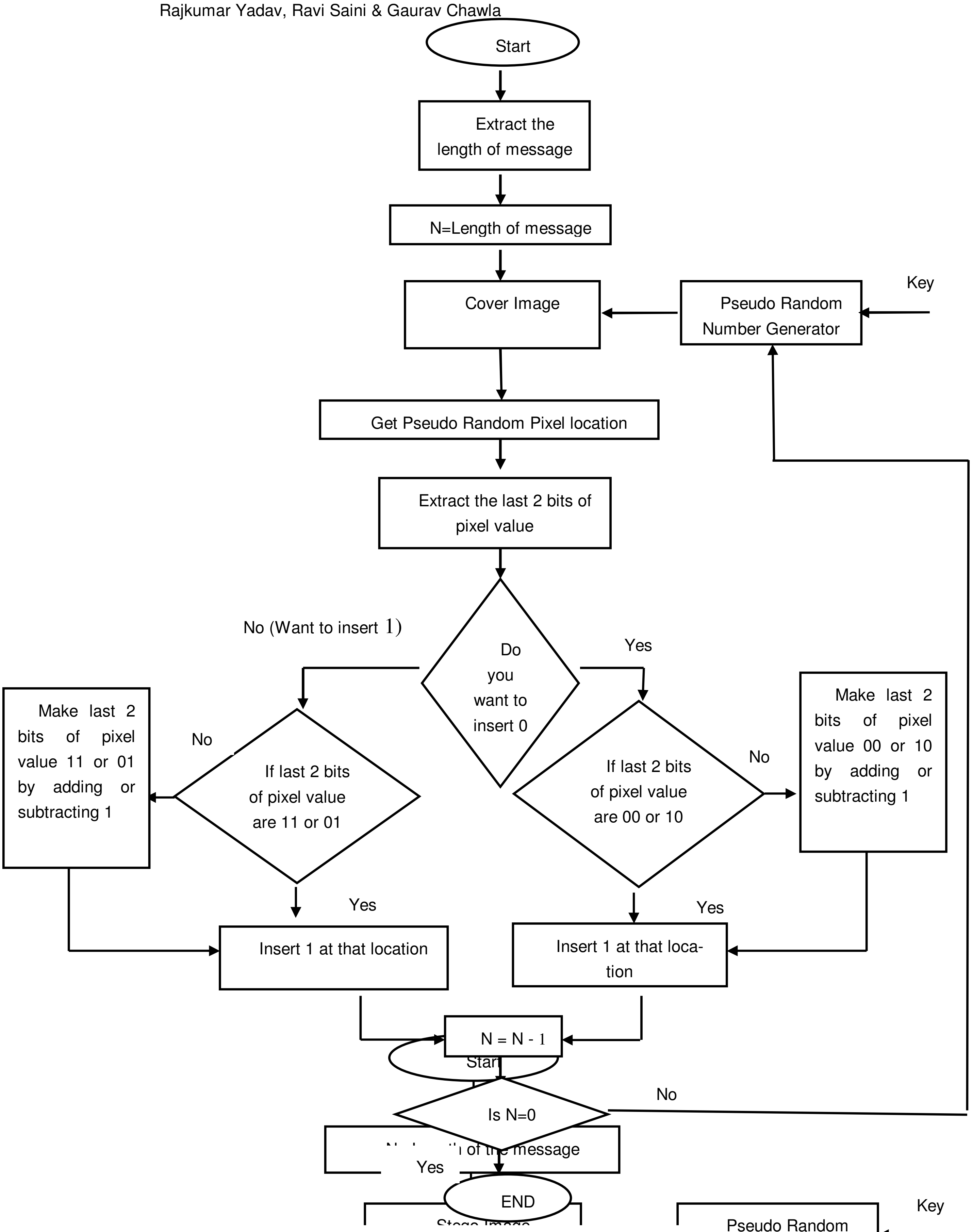
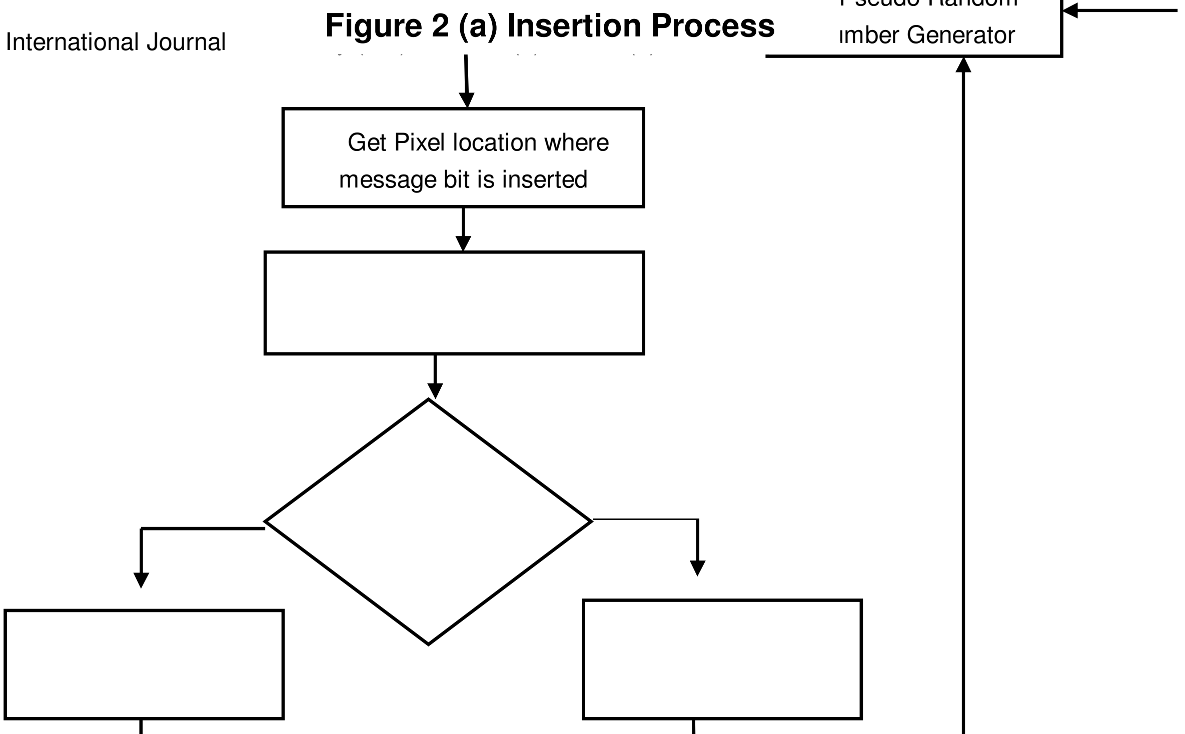

Start
Extract the length of message
N=Length of message
Cover Image
Pseudo Random Number Generator
Key
Get Pseudo Random Pixel location
Extract the last 2 bits of pixel value
Do you want to insert 0
No (Want to insert 1)
Yes
No
If last 2 bits of pixel value are 11 or 01
Make last 2 bits of pixel value 11 or 01 by adding or subtracting 1
If last 2 bits of pixel value are 00 or 10
No
Make last 2 bits of pixel value 00 or 10 by adding or subtracting 1
Yes
Insert 1 at that location
Yes
Insert 1 at that loca-tion
N = N - 1
Start
Is N=0
No
Yes
END

Figure 2 (a) Insertion Process



3. LGORITHMS

3.1. Assumptions

I. Sender and Receiver agree on the cover image in which message is to be hidden.

II. Both sender and receiver agree on the same pseudo-random key to decide the pseudo random locations where message is to be inserted.

III. Both sender and receiver either agree on the length of message "OR" the length of the message is hidden with the message itself at some prespecified locations which are known to both sender and receiver.

3.2. Insertion Algorithm

I. Find the pseudo-random location (L) in cover image from secret key to insert the message bit (For detail see [13] and [14]).

II. Extract the last two bits of the selected pixel location (L).

III. If we want to insert 0 then go to step (iv) else go to step (v).

IV. (a) If the last two bits of the selected pixel location (L) is 00 or 10 then insert 0 at location (L) and go to END.
(b) If the last two bits of the selected pixel location (L) is equal to 01 or 11 then make them 00 or 10 by adding or subtracting 1 at pixel location (L). Insert 0 to that location and go to END.

V. (a) If the last two bits of the selected pixel location (L) is 11 or 01 then insert 1 at location (L) and go to END.
(b) If the last two bits of the selected pixel location (L) are equal to 00 or 10 then make them 11 or 01 by adding or subtracting 1 at pixel location (L). Insert 1 to that location and go to END.

VI. END.

3.3. Retrieval Algorithm

I. Generate the pixel location (L) from the same secret key as used for insertion of message.

II. Extract the last two bits of the selected pixel location (L).

III. If last two bits of the selected pixel location (L) is 00 or 10 then 0 is the message bit else 1 is the message bit.

IV. END.

4. CHANGES IN PIXEL VALUE AFTER THE INSERTION OF MESSAGE

Now, we see how various pixel values changes during insertion of message. Table I shows how pixel values changes during insertion of 0 and Table II shows how pixel values changes during insertion of 1.

5. CHANGE IN PIXEL VALUE WHEN INTRUDER CHANGES LSB'S OF ALL PIXEL VALUES

Here, we have considered the case in which intruder changes the least significant bits of pixel values of the cover image with message. Table III shows changes the LSB's of pixel value and 0 is inserted at the pixel value. Table IV shows change in pixel value when intruder changes the LSB's of pixel value and 1 is inserted at the pixel value.

TABLE 1 (Change in Pixel Value after Insertion of 0)

TABLE II (Change in Pixel Value after Insertion of 1)

Decimal Value	Pixel value before inse tion of '1'	Pixel value after inse tion of '1'	Change in Pixel value comment for insertion of
Decimal Value	Pixel value before inse tion of '0'	Pixel value after inse tion of '0'	Change in Pixel value comment for insertion of
0	00000000	00000001	+1, Insert
0	00000000	00000000	NC, Insert
1	00000001	00000001	NC, Insert
1	00000001	00000010	+1, Insert
2	00000010	00000011	+1, Insert
2	00000010	00000010	NC, Insert
3	00000011	00000011	NC, Insert
3	00000011	00000100	+1, Insert
4	00000100	00000011	-1, Insert
4	00000100	00000100	NC, Insert
5	00000101	00000101	NC, Insert
5	00000101	00000100	-1, Insert
6	00000110	00000111	+1, Insert
6	00000110	00000110	NC, Insert
7	00000111	00000111	NC, Insert
7	00000111	00000110	-1, Insert
8	00001000	00001001	+1, Insert
8	00001000	00001000	NC, Insert
9	00001001	00001001	NC, Insert
9	00001001	00001000	-1, Insert
10	00001010	00001001	-1, Insert
10	00001010	00001010	NC, Insert
11	00001011	00001011	NC, Insert
11	00001011	00001100	+1, Insert
12	00001100	00001011	-1, Insert
12	00001100	00001100	NC, Insert
13	00001101	00001101	NC, Insert
13	00001101	00001110	+1, Insert
14	00001110	00001111	+1, Insert
14	00001110	00001110	NC, Insert
15	00001111	00001111	NC, Insert
15	00001111	00001110	-1, Insert
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
127	01111111	01111111	NC, Insert
127	01111111	10000000	+1, Insert
128	10000000	01111111	-1, Insert
128	10000000	10000000	NC, Insert
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
254	11111110	11111111	+1, Insert
254	11111110	11111110	NC, Insert
255	11111111	11111111	NC, Insert
255	11111111	11111110	-1, Insert

TABLE III (Change in Pixel Value after Insertion of 0 with Changed LSB)

Decimal Value	Pixel value befor insertion of '0' (C1)	Pixel value after i sertion of '0'	Pixel value after i sertion of '0' with changed LSB's by ir truder (C2)	Net change i.e C2 - C1
0	00000000	00000000	00000000	NC
1	00000001	00000000	00000000	+2
2	00000010	00000000	00000000	+2
3	00000011	00000000	00000000	+2
4	00000100	00000000	00000000	+2
5	00000101	00000100	00000100	NC
6	00000110	00000100	00000100	+2
7	00000111	00000000	00000000	+2
8	00001000	00000000	00000000	+2
9	00001001	00001000	00001000	NC
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
254	11111110	11111110	11111110	NC
255	11111111	11111111	11111110	-1

TABLE IV (Change in Pixel Value after Insertion of 1 with Changed LSB)

6. RESULTS AND CONCLUSIONS

6.1 The Following Results Obtained From Table I And Table Ii Tells Us How Our Method Is Better Than The Previous Methods.

(i) The message bit will be inserted at the pseudorandom location at first chance = 512/512*100 = 100%.

(ii) Chance when message is inserted, no change in pixel value is required = 256/512*100 = 50%.

6.2 The Comparison Table Of Our Method With 6^{th} & 7^{th} Bit Method And 6^{th}, 7^{th} & 8^{th} Bit Method Is Shown Below:

Method	Message bit Insertion at pseudorandom location at firs chance	No change in Pixel value when message bit is inserte
6th, 7th Bit	50%	50%
6th, 7th & 8th Bit	85.93%	43.18%
7th, 8th Bit	100%	50%

TABLE V (Comparison Table)

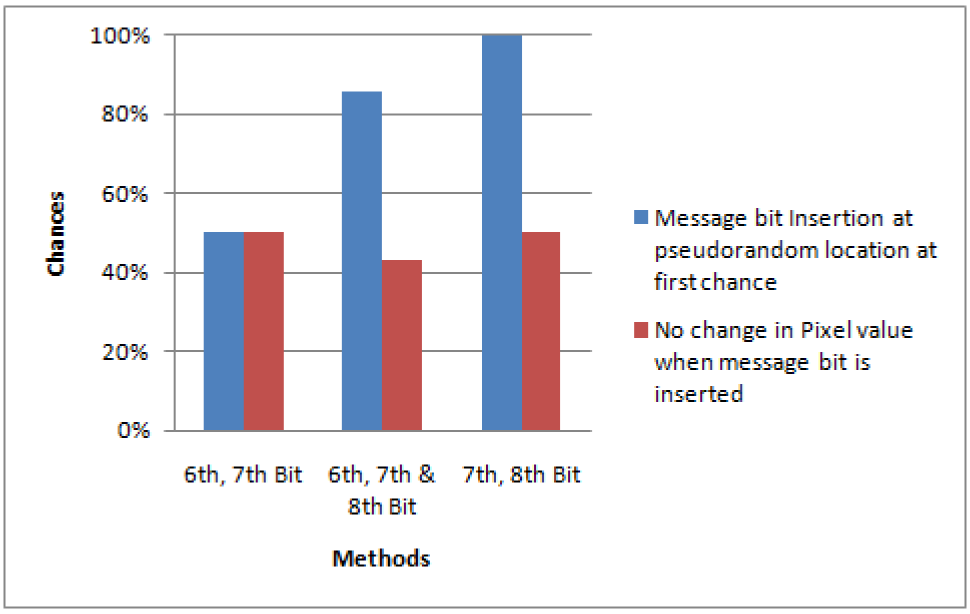


FIGURE 6 (a) Comparison Chart

From Table V and Figure 6 (a), we conclude that our method provides maximum chances of message insertion at a pixel location i.e. 100% which is an improvement over earlier existing methods like 6^{th}, 7^{th} bit method and 6^{th}, 7^{th} & 8^{th} bit method. 6^{th} , 7^{th} bit method provides only

50% chances of message insertion at a pixel value due to which approximately half of the pixel locations cannot be used for insertion of the message. 6th , 7th & 8th bit method increases the chances of message insertion at a pixel value from 49% to 85.93% which is also not a optimal solution. Our method provides optimal solution in case of chances of message insertion which is an improvement over earlier existing methods.

6.3. Table III and Table IV shows that when intruder tries to change the LSB's of all pixel values when message is inserted in the image then the change at some pixel values becomes +2 or -2 which will be visible to human eye. So, in case of our algorithm if intruder tries to distort our message by changing LSB's of all pixel values then it reflects at the receiver end that something has gone wrong in the middle. In this situation, receiver asks to sender to send the message again for retrieval of correct message.

REFERENCES

[1] A. Gutub, M. Fattani, "A Novel Arabic Text Steganography Method using letter Points and Extension", WASET International Conference on Computer Information and System Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[2] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34, February 1998.

[3] D. Kahn, *The Codebreakers,* Macmillian, New York, 1967.

[4] B. Norman, *Secret Warfare*, Acropolis Books, Washington D.C., 1973.

[5] Parvinder Singh, Sudhir Batra and HR Sharma, "Evaluating the Performance of Message Hidden in First and Second Bit Plane," WSEAS Transaction on Information Science and Technology, Vol. 2, No 89, pp 1220-1222, Aug 2005.

[6] Sudhir Batra, Rahul Rishi and Raj Kumar, "Insertion of Message in 6th, 7th and 8th bit of pixel values and its retrievals in case intruder changes the least significant bits of image pixels", International Journal of Security and its application, Vol. 4, No. 3, July 2010.

[7] Simmons G. J, "The Prisoners Problem and the Subliminal Channel", Proceedings of crypto '83, Plenum Press, pp 51-67, 1983.

[8] Anderson R. J, "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.

[9] Anderson R. J, Peticolas FAP, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[10] N.F. Johnson and Zoran Duric, S. G. J. *Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1).* Kluwer Academic Publishers, February 15, 2001.

[11] Eugene, T.L., Delp Edward J., "A Review of Data Hiding in Digital Images".

[12] Amirtharajan Rengarajan, Ganesan Vivek, Jithamanyu R, Rayappan John Bosco Balaguru, "An Invisible Communication for Secret Sharing against Transmission Error", Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121, Nov-2010.

[13] 13. E Franz, A Jerichav, S Moller, A Pfitznaun, I Steierand, “Computer Based Stegnography”, Information Hiding, Springer Lecturer Notes in Computer Science, Vol. 1174, pp. 7-21, 1996.

[14] Yeuan-Luen Lee, Ling-Hwei Chen, “A Secure Robust Image Stegnography Nodel,”10th National Conference on Information Security, Hualien, Taiwan, pp 275-284, May 2000.

[15] Stallings.W. Cryptography and network security: Principles and practice. In *Prentice Hall*, 2003.

[16] Chandramouli, R., Memon, N.D., ‘Steganography capacity: A steganalysis perspective’, Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003

[17] S.Craver ,N. Memon , “Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications”, IEEE Trans.,Vol 16,No. 4,pp. 573-586,1998.

[18] W. Bender,D. Gruhl, N.Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol. 35, no. 3-4, pp. 313–335, 1996.

[19] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” Signal Processing, vol. 66, no. 3, pp. 385–403, 1998.

[20] Jing Dong and Tieniu Tan, “Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations”, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, 10190, Beijing, China.

[21] Jessica Fridrich, Miroslav Goljan , Rui Du, “Detecting LSB Steganography in Color and Gray-Scale Images”, IEEE Multimedia, issue 4, vol 8, 2001

[22] Johnson, Neil F., Zoran Duric, S. G. J., Information Hiding: Steganography and Watermarking – Attacks and Countermeasures (Advances in Information Security, Volume I). Kluwer Academic Publishers, February 15, 2001.

[23] RJ Anderson, FAP Petitcolas, “On the Limits of Stegnography”, IEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[24] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2, JUNE 2008.

[25] Parvez M. T. and Gutub A., “RGB Intensity Based Variable-Bits Image Steganography”, APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[26] Pal, S.K., Saxena, P.K., Muttoo, S.K., ‘Image steganography for wire less networks using the handmaid transform’, International Conference on Signal Processing & Communications (SPCOM), 2004

A Spectral Domain Local Feature Extraction Algorithm for Face Recognition

Hafiz Imtiaz *hafiz.imtiaz@live.com*
Bangladesh University of Engineering and Technology
Dhaka-1000, Bangladesh

Shaikh Anowarul Fattah *sfattah@princeton.edu*
Bangladesh University of Engineering and Technology
Dhaka-1000, Bangladesh

Abstract

In this paper, a spectral domain feature extraction algorithm for face recognition is proposed, which efficiently exploits the local spatial variations in a face image. For the purpose of feature extraction, instead of considering the entire face image, an entropy-based local band selection criterion is developed, which selects high-informative horizontal bands from the face image. In order to capture the local variations within these high-informative horizontal bands precisely, a feature selection algorithm based on two-dimensional discrete Fourier transform (2D-DFT) is proposed. Magnitudes corresponding to the dominant 2D-DFT coefficients are selected as features and shown to provide high within-class compactness and high between-class separability. A principal component analysis is performed to further reduce the dimensionality of the feature space. Extensive experimentations have been carried out upon standard face databases and the recognition performance is compared with some of the existing face recognition schemes. It is found that the proposed method offers not only computational savings but also a very high degree of recognition accuracy.

Keywords: Feature Extraction, Classification, Two Dimensional Discrete Fourier Transform, Dominant Spectral Feature, Face Recognition, Modularization.

1. INTRODUCTION

Automatic face recognition has widespread applications in security, authentication, surveillance, and criminal identification. Conventional ID card and password based identification methods, although very popular, are no more reliable as before because of the use of several advanced techniques of forgery and password-hacking. As an alternative, biometric, which is defined as an intrinsic physical or behavioral trait of human beings, is being used for identity access management [1]. The main advantage of biometric features is that these are not prone to theft and loss, and do not rely on the memory of their users. Among physiological biometrics, face is getting more popularity because of its non-intrusiveness and high degree of security. Moreover, unlike iris or finger-print recognition, face recognition do not require high precision equipment and user agreement, when doing image acquisition, which make face recognition even more popular for video surveillance.

Nevertheless, face recognition is a complicated visual task even for humans. The primary difficulty in face recognition arises from the fact that different images of a particular person may vary largely, while images of different persons may not necessarily vary significantly. Moreover, some aspects of the image, such as variations in illumination, pose, position, scale, environment, accessories, and age differences, make the recognition task more complicated. However, despite many relatively successful attempts to implement face recognition systems, a single approach, which is capable of addressing the hurdles, is yet to be developed.

Face recognition methods are based on extracting unique features from face images. In this regard, face recognition approaches can be classified into two main categories: holistic and texture-based [2]-[4]. Holistic or global approaches to face recognition involve encoding the entire facial image in a high-dimensional space [2]. It is assumed that all faces are constrained to particular positions, orientations, and scales. However, texture-based approaches rely on the detection of individual facial characteristics and their geometric relationships prior to performing face recognition [3], [4]. Apart from these approaches, face recognition can also be performed by using different local regions of face images [5], [6]. It is well-known that, although face images are affected due to variations, such as non-uniform illumination, expressions and partial occlusions, facial variations are confined mostly to local regions. It is expected that capturing these localized variations of images would result in a better recognition accuracy [6]. Hence, it is motivating to utilize local variations for feature extraction and thereby develop a scheme of holistic face recognition incorporating the advantageous properties of texture-based approach.

The objective of this paper is to develop a spectral domain face recognition scheme based on dominant spectral features extracted from local zones instead of using the entire face image as a whole. In order to exploit the high-informative areas of a face image, an entropy based horizontal band selection criterion is presented. Such high-informative bands are further divided into some smaller spatial modules to extract local variations in detail. A spectral domain feature extraction algorithm using 2D-DFT is developed, which operates within those local zones to extract dominant spectral features. It is shown that the discriminating capabilities of the proposed features are enhanced because of modularization of the face images. In view of further reducing the computational complexity, principal component analysis is performed on the proposed feature space. Finally, the face recognition task is carried out using a distance based classifier..

2. BRIEF DESCRIPTION OF THE PROPOSED SCHEME

A typical face recognition system consists of some major steps, namely, input face image collection, pre-processing, feature extraction, classification and template storage or database, as illustrated in Fig. 1. The input image can be collected generally from a video camera or still camera or surveillance camera. In the process of capturing images, distortions including rotation, scaling, shift and translation may be present in the face images, which make it difficult to locate at the correct position. Pre-processing removes any un-wanted objects (such as, background) from the collected image. It may also segment the face image for feature extraction. For the purpose of classification, an image database is needed to be prepared consisting template face poses of different persons. The recognition task is based on comparing a test face image with template data. It is obvious that considering images themselves would require extensive computations for the purpose of comparison. Thus, instead of utilizing the raw face images, some characteristic features are extracted for preparing the template. It is to be noted that the recognition accuracy strongly depends upon the quality of the extracted features. Therefore, the main focus of this research is to develop an efficient feature extraction algorithm.

The proposed feature extraction algorithm is based on extracting spatial variations precisely from high informative local zones of the face image instead of utilizing the entire image. In view of this, an entropy based selection criterion is developed to select high informative facial zones. A modularization technique is employed then to segment the high informative zones into several smaller segments. It should be noted that variation of illumination of different face images of the same person may affect their similarity. Therefore, prior to feature extraction, an illumination adjustment step is included in the proposed algorithm. After feature extraction, a classifier compares features extracted from face images of different persons and a database is used to store registered templates and also for verification purpose.

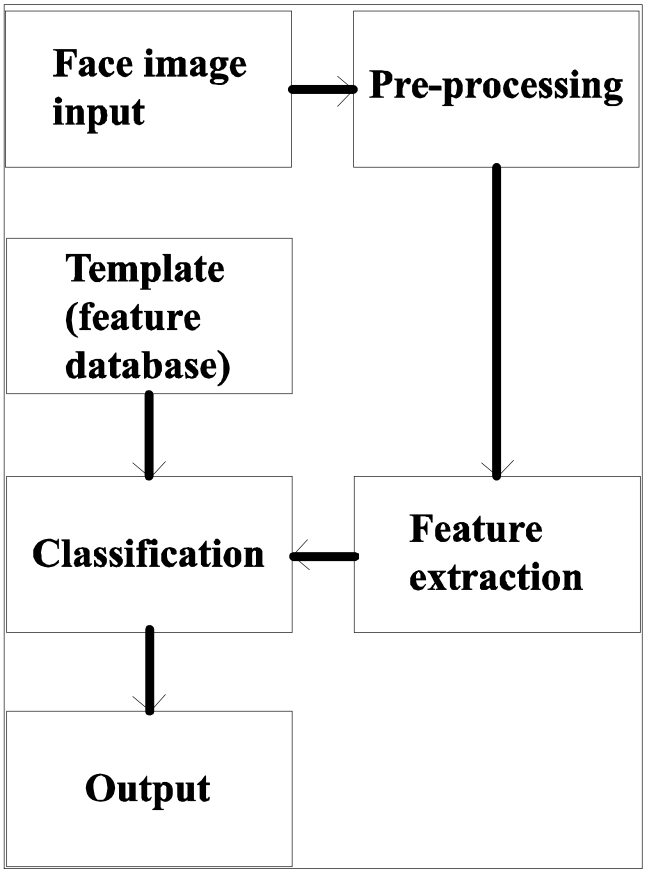


FIGURE 1: Block diagram of the proposed method

3. PROPOSED METHOD

For any type of biometric recognition, the most important task is to extract distinguishing features from the training biometric traits, which directly dictates the recognition accuracy. In comparison to person recognition based on different biometric features, face image based recognition is very challenging even for a human being, as face images of different persons may seem similar whereas face images of a single person may seem different, under different conditions. Thus, obtaining a significant feature space with respect to the spatial variation in a human face image is very crucial. Moreover, a direct subjective correspondence between face image features in the spatial domain and those in the frequency domain is not very apparent. In what follows, we are going to demonstrate the proposed feature extraction algorithm for face recognition, where spatial domain local variation is extracted using frequency domain transform.

3.1 Entropy Based Horizontal Band Selection

The information content of different regions of a human face image varies widely [7]. It can be shown that, if an image of a face were divided into certain segments, not all the segments would contain the same amount of information. It is expected that a close neighborhood of eyes, nose and lips contains more information than that possessed by the other regions of a human face image. It is obvious that a region with high information content would be the region of interest for the purpose of feature extraction. However, identification of these regions is not a trivial task. Estimating the amount of information from a given image can be used to identify those significant zones. In this paper, in order to determine the information content in a given area of a face image, an entropy based measure of intensity variation is defined as [8]

$$H = -\sum_{k=1}^{m} p_k log_2 p_k, \tag{1}$$

where the probabilities $\{p_k\}_1^m$ are obtained based on the intensity distribution of the pixels of a segment of an image. It is to be mentioned that the information in a face image exhibits variations more prominently in the vertical direction than that in the horizontal direction [9]. Thus, the face image is proposed to be divided into several horizontal bands and the entropy of each band is to be computed. It has been observed from our experiments that variation in entropy is closely related to variation in the face geometry. Fig. 2(b) shows the entropy values obtained in different horizontal bands of a person for several sample face poses. One of the poses of the person is shown in Fig. 2(a). As expected, it is observed from the figure that the neighborhood of eyes, nose and lips contains more information than that possessed by the other regions. Moreover, it is found that the locus of entropies obtained from different horizontal bands can trace the spatial structure of a face image. Hence, for feature extraction in the proposed method, spatial horizontal bands of face images are chosen corresponding to their entropy content.

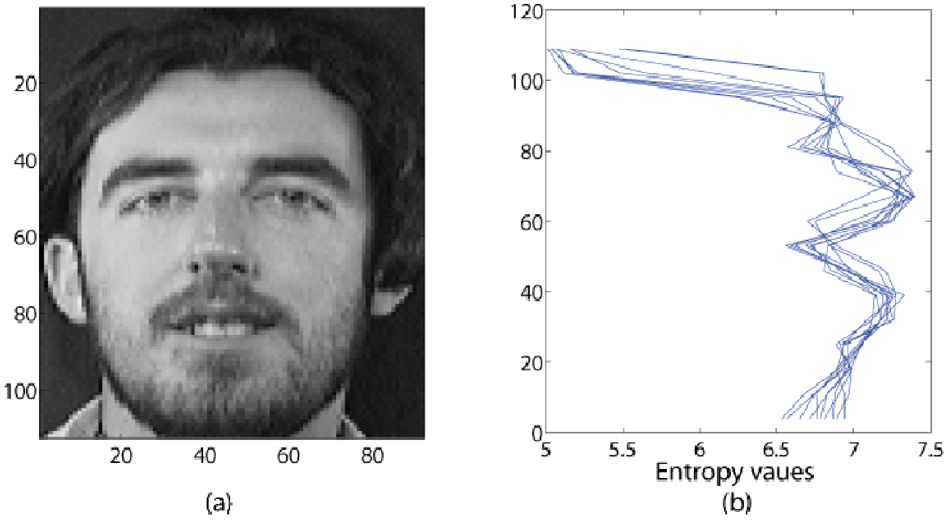


FIGURE 2: (a) Sample face image of a person and (b) entropy values in different horizontal bands of several face poses

3.2 Spectral Feature Extraction and Illumination Adjustment

For biometric recognition, feature extraction can be carried out using mainly two approaches, namely, the spatial domain approach and the spectral domain approach [10]. The spatial domain approach utilizes the spatial data directly from the face image or employs some statistical measure of the spatial data. On the other hand, spectral domain approaches employ some kind of transform over the face images for feature extraction. In case of spectral domain feature extraction, pixel-by-pixel comparison between face images in the spatial domain is not necessary. Phenomena, such as rotation, scale and illumination, are more severe in the spatial domain than in spectral domain. Hence, in what follows, we intend to develop a feature extraction algorithm based on spectral domain transformation. We have employed an efficient feature extraction scheme using Fourier transform, which offers an ease of implementation in practical applications. For a function $f(x,y)$ with two-dimensional variation, the 2D Fourier transform is given by [11]

$$\mathcal{F}(\omega_x,\omega_y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-j2\pi(\omega_x x+\omega_y y)}dxdy, \tag{2}$$

where ω_x and ω_y represent frequencies in the two-dimensional space.
It is intuitive that images of a particular person captured under different lighting conditions may vary significantly, which can affect the face recognition accuracy. In order to overcome the effect of lighting variation in the proposed method, illumination adjustment is performed prior to feature extraction. Given two images of a single person having different intensity distributions due to variation in illumination conditions, our objective is to provide with similar feature vectors for these two images irrespective of the different illumination condition. Since in the proposed method, feature extraction is performed in the Fourier domain, it is of our interest to analyze the effect of variation in illumination on the DFT-based feature extraction.

In Fig. 3, two face images of the same person are shown, where the second image (shown in Fig. 3(b) is made brighter than the first one by changing the average illumination level. 2D-DFT is performed upon each image, first without any illumination adjustment and then after performing illumination adjustment. Considering all the 2D-DFT coefficients to form the feature vectors for these two images, a measure of similarity can be obtained by using correlation. In Figs. 4 and 5, the cross-correlation values of the 2D-DFT coefficients obtained by using the two images without and with illumination adjustment are shown, respectively. It is evident from these two figures that the latter case exhibits more similarity between the DFT coefficients indicating that the features belong to the same person. The similarity measure in terms of Euclidean distances between the 2D-DFT coefficients of the two images for the aforementioned two cases are also calculated. It is found that there exists a huge separation in terms of Euclidean distance when no illumination adjustment is performed, whereas the distance completely diminishes when illumination adjustment is performed, as expected, which clearly indicates that a better similarity between extracted feature vectors.

3.3 Proposed Dominant Spectral Feature

It has already been mentioned that, in the proposed algorithm, instead of taking the DFT coefficients of the entire image, the coefficients obtained form each modules of the high-informative horizontal band of a face image are considered to form the feature vector of that image. However, if all of these coefficients were used, it would definitely result in a feature vector with a very large dimension. One advantage of working in the frequency domain is that a few DFT coefficients with higher magnitudes would be sufficient to represent an image or a portion of an image. Hence, in view of reducing the feature dimension, we propose to utilize the magnitudes and 2D-frequencies corresponding to the dominant DFT coefficients as spectral features.

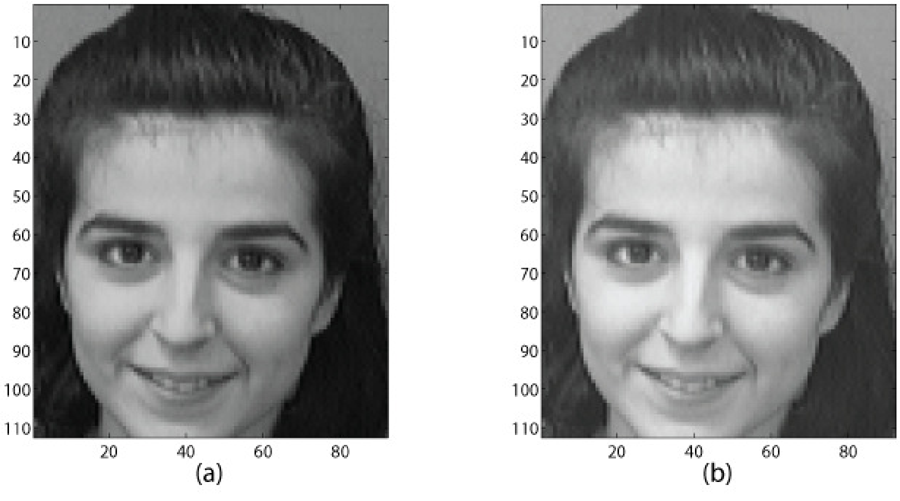


FIGURE 3: Two face images of the same person under different illumination

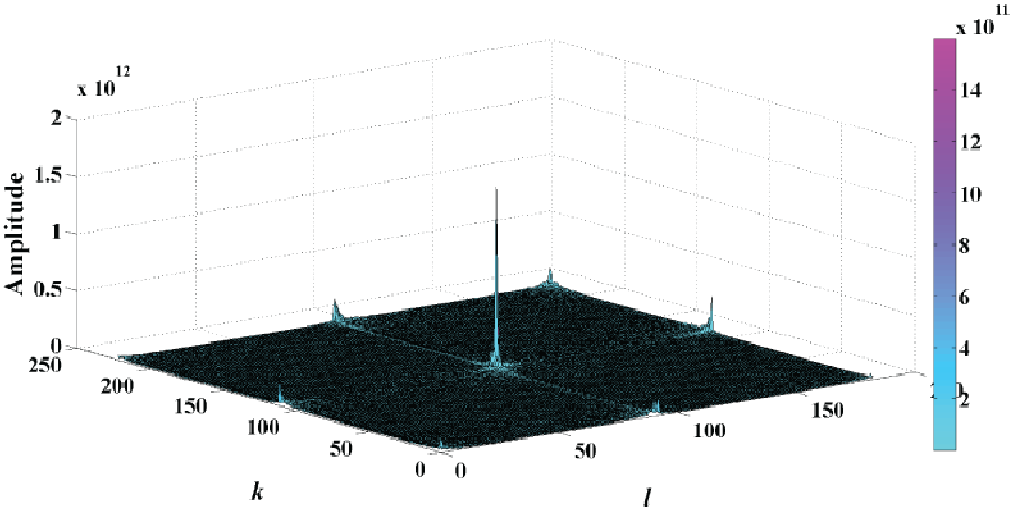


FIGURE 4: Correlation of the 2D-DFT coefficients of the sample images: no illumination adjustment

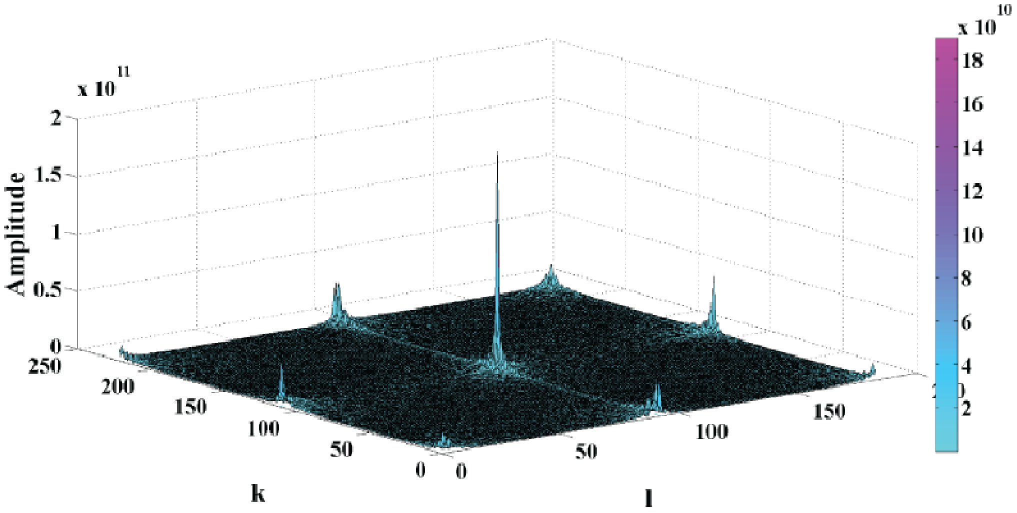


FIGURE 5: Correlation of the 2D-DFT coefficients of the sample: illumination adjusted

The 2D-DFT coefficient corresponding to the maximum magnitude is treated as the dominant coefficient ($D1$). Considering the magnitudes of the 2D-DFT coefficients in descending order, magnitude values other than the dominant one may also be treated as possible candidates for desired features. In accordance with their magnitude values, these dominant magnitudes are termed as second-dominant $(D2)$, third-dominant $(D3)$, and so on. If the magnitude variations along all the segments for the case of different dominant magnitudes remain similar, it would be very difficult to select one of those dominant magnitudes as a desired feature.

In order to demonstrate the characteristics of the dominant magnitudes in different modules, sample face images of two different persons are shown in Fig. 6. In Fig. 7, four dominant magnitudes $(D1, D2, D3, and D4)$ obtained from all the modules of the image of Person 1, appeared in Fig. 6(a), are shown. The face image is divided into 16 modules. It is found that different dominant magnitudes obtained from the spatial modules exhibit completely different characteristics. However, the magnitude value for the first dominant $(D1)$ is found reasonably higher than other dominant magnitudes. An analogous behavior, as shown in Fig. 7, is obtained for Person 2 of Fig. 6(b). It is evident from Fig. 7 that $D1$ is the most significant among all the dominant magnitudes and thus, it is sufficient to consider only $D1$ as a desired feature, which also offers an advantage of reduced feature dimension. Computing $D1$ in each segment of the high-informative horizontal bands of a face image, the proposed feature vector is obtained.

It should be noted that, for a high-informative horizontal band of dimension $N \times N$ with M number of modules (of dimension $n \times n$), considering only $D1$ will reduce the length of feature vector from $M \times n \times n$ to M, an order of n^2 reduction.

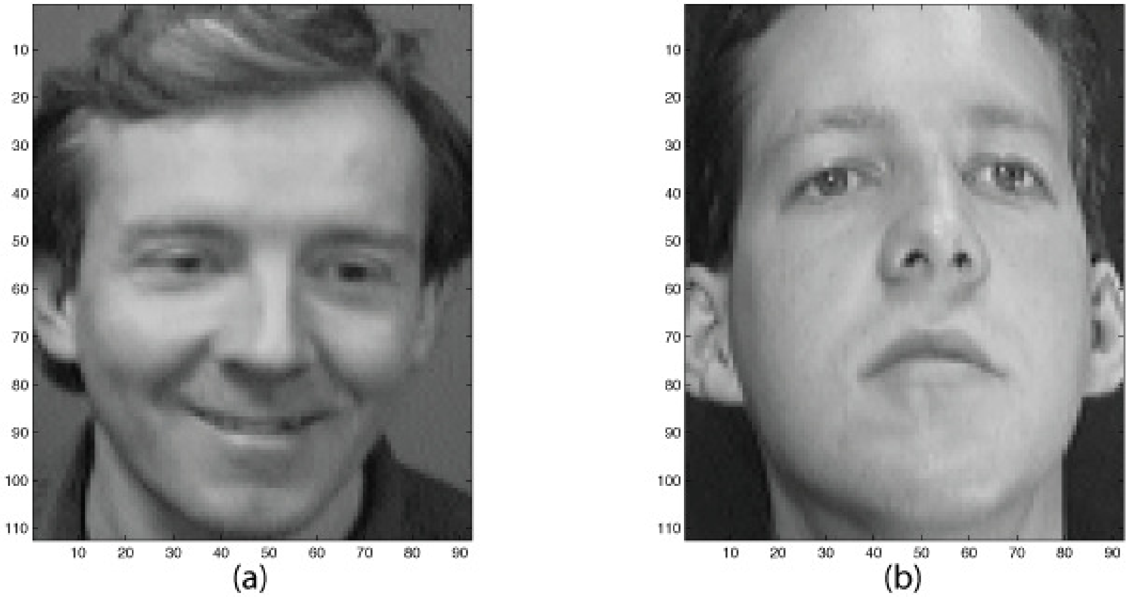


FIGURE 6: Sample face images of two persons

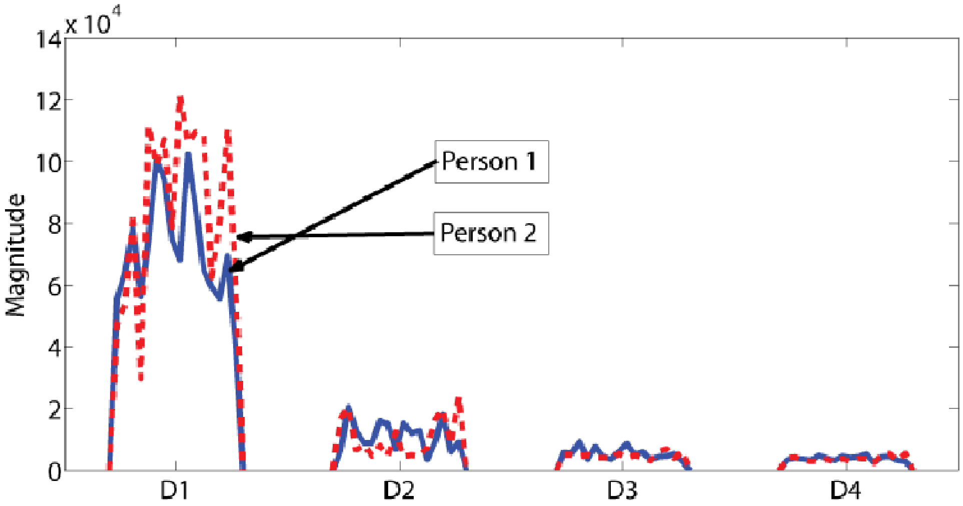


FIGURE 7: Proposed dominant magnitude-features

In order to investigate the effect of division of horizontal bands into smaller segments on the characteristics of dominant magnitude features, Fig. 8 is presented, where the dominant magnitudes obtained from a single high-informative horizontal band of the different poses of the same two persons shown in Fig. 6 are shown. It is observed from the figure that the dominant feature magnitudes for different poses of a particular person are significantly scattered resulting in poor within-class compactness. Moreover, the dominant feature magnitudes of two different persons are substantially overlapped resulting in poor between-class separation.

It is observed that a significant variation may occur in the poses of a single person taken under different conditions. In view of demonstrating the effect of such variations on the proposed dominant features, we consider ten sample poses for each of the two persons as appeared in Fig. 6. In Fig. 9, the proposed dominant features obtained from different modules of the high-informative horizontal bands of all the face poses of two different persons are shown. For each person, the centroid of the proposed feature vectors is also shown in the figure (in thick continuous lines). It is to be noted that the feature centroids of the two different persons are well-separated. It is also observed that a low degree of scattering exists among the features around their corresponding centroids. Hence, the dominant features extracted locally within a high-informative horizontal band of a face image offer not only a high degree of between-class separability but also satisfactory within-class compactness.

3.4 Reduction of Feature Dimension

Principal component analysis (PCA) is an efficient orthogonal linear transform to reduce the feature dimension [12]. In the proposed method, considering the magnitudes of the dominant DCT coefficients as features results in a feature space with large dimension. Thus, implementation of PCA on the derived feature space could efficiently reduce the feature dimension without losing much information. Hence, PCA is employed to reduce the dimension of the proposed feature space.

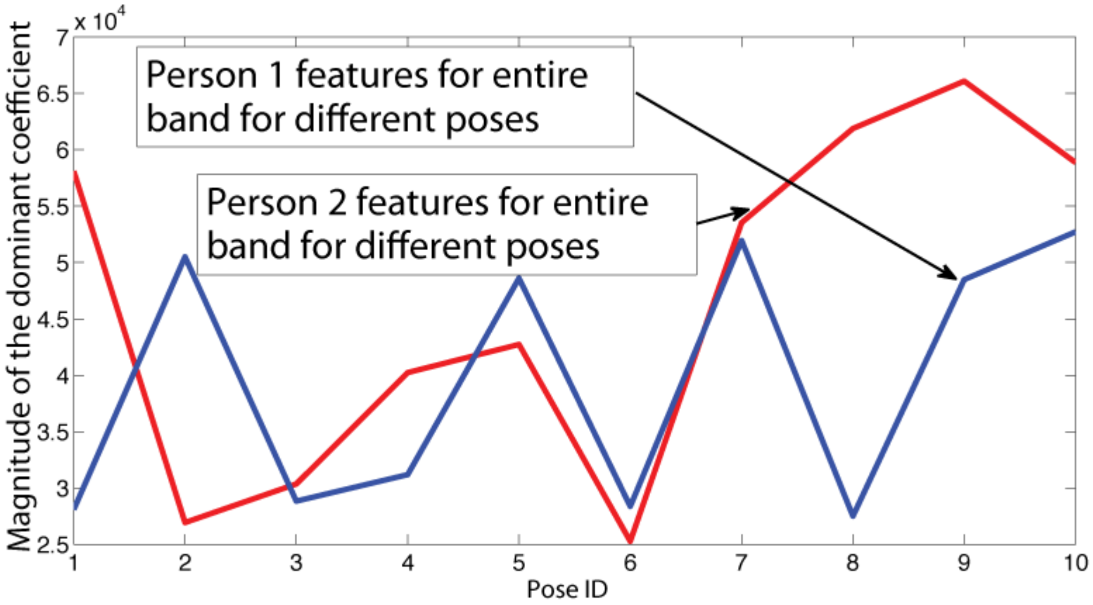


FIGURE 8: Variation of dominant magnitude features with poses using entire horizontal band

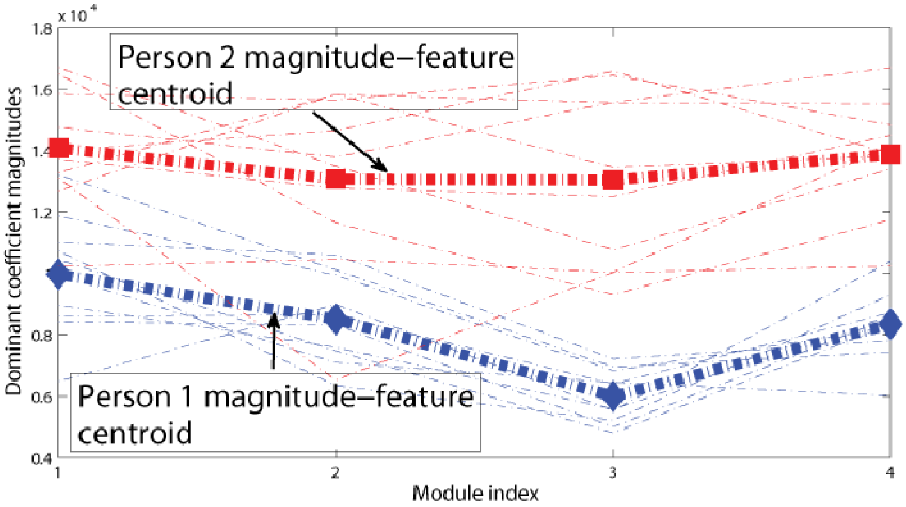


FIGURE 9: Variation of magnitude features with vertical segments of horizontal bands for several poses

3.5 Distance Based Face Recognition

In the proposed method, for the purpose of recognition using the extracted dominant features, a distance-based similarity measure is utilized. The recognition task is carried out based on the distances of the feature vectors of the training face images from the feature vector of the test image. Given the m-dimensional feature vector for the k-th pose of the j-th person be $\{\gamma_{jk}(1),\gamma_{jk}(2),\ldots,\gamma_{jk}(m)\}$ and a test face image f with a feature vector $\{v_f(1),v_f(2),\ldots,v_f(m)\}$, a similarity measure between the test image f of the unknown person and the sample images of the j-th person, namely *average sum-squares distance,* Δ, is defined as

$$\Delta_j^f = \frac{1}{q}\sum_{k=1}^{q}\sum_{i=1}^{m}|\gamma_{jk}(i) - v_f(i)|^2, \tag{3}$$

where a particular class represents a person with q number of poses. Therefore, according to (3), given the test face image f, the unknown person is classified as the person j among the p number of classes when

$$\Delta_j^f \le \Delta_g^f, \forall j \neq g and \forall g \varepsilon \{1,2,\ldots,p\} \tag{4}$$

4. EXPERIMENTAL RESULTS

Extensive simulations are carried out in order to demonstrate the performance of the proposed feature extraction algorithm for face recognition. In this regard, different well-known face databases have been considered, which consist a range of different face images varying in facial expressions, lighting effects and presence/absence of accessories. The performance of the proposed method in terms of recognition accuracy is obtained and compared with that of some recent methods [13, 14].

4.1 Face Databases

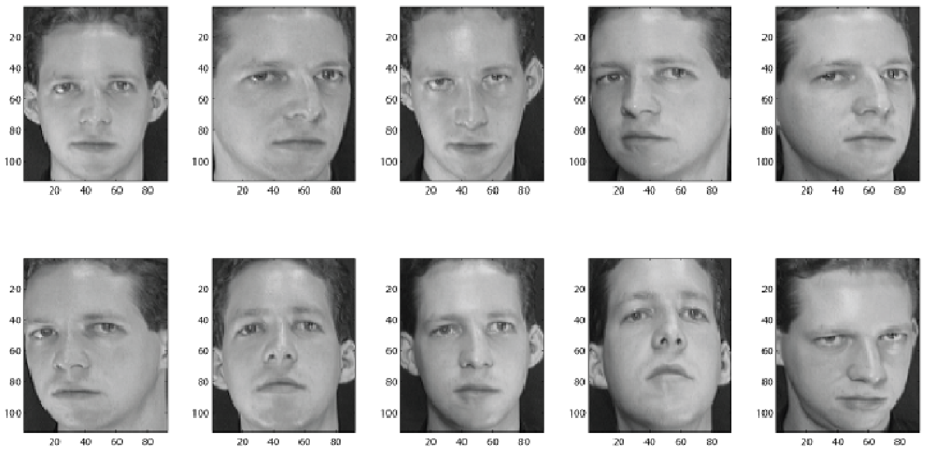


FIGURE 10: Sample poses of a person from the ORL database

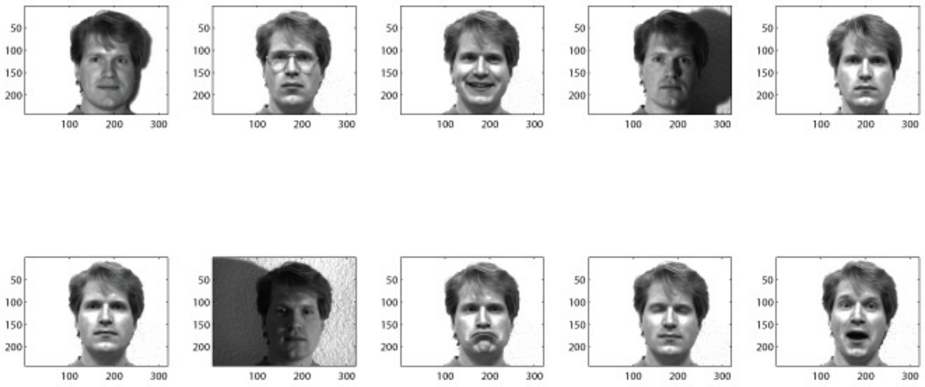


FIGURE 11: Sample poses of a person from the Yale database

In this section, the performance of the proposed face recognition scheme has been presented for two standard face databases, namely, the ORL database (available at http://www.cl.cam.ac.uk/Research/DTG/attarchive/pub/data/) and the Yale database (available at http://cvc.yale.edu/projects/yalefaces/yalefaces.html). In Figs. 10 and 11, sample face images of different poses of two different persons taken from the ORL and the Yale databases, respectively, are shown. The ORL database contains a total of 400 images of 40 persons, each person having 10 different poses. Little variation of illumination, slightly different facial expressions and details are present in the face images. The Yale database, on the other hand, consists a total of 165 images of 15 persons, each person having 11 different poses. The poses exhibit large variations in illumination (such as central lighting, left lighting and right lighting, dark condition), facial expressions (such as wink, sad, happy, surprised, sleepy and normal) and other accessories (such as with glasses and without glass).

4.2 Performance Comparison

In the proposed method, dominant spectral features (magnitudes and frequencies) obtained from all the modules of high-informative horizontal bands of a face image are used to form the feature vector of that image and feature dimension reduction is performed using PCA. The recognition task is carried out using a simple Euclidean distance based classifier as described in Section 3.5. The experiments were performed following the leave-one-out cross validation rule.

For simulation purposes, N number of horizontal bands are selected based on the entropy measure described in Section 3.1 and divided further into small modules. Module height is the same as that of the horizontal band and module width is chosen based on the face image width. In our simulations, $N = 2$ for the ORL database and $N = 3$ for the Yale database are chosen and the module sizes are chosen as 28×23 pixels and 27×20 pixels, respectively.

In order to show the effectiveness of the proposed local dominant feature extraction scheme, where each modules within the high-informative horizontal bands are considered separately, the recognition task is also carried out by considering the entire horizontal bands as a whole using the same feature extraction algorithm. We refer to the later scheme as *Proposed Scheme Without Modularization* (PSWOM) method. For the purpose of comparison, recognition accuracies obtained using the proposed method (*Proposed Scheme With Modularization* or PSWM) along with those obtained by the PSWOM method, and methods reported in [13] and [14] are listed in Table 1. Here, in case of the ORL database, the recognition accuracy for the method in [14] is denoted as not available (N/A). It is evident from the table that the recognition accuracy of the proposed method is comparatively higher than those obtained by the other methods for both the databases. It indicates the robustness of the proposed method against partial occlusions, expressions and nonlinear lighting variations. It is to be noted that the recognition accuracy is drastically reduced for the PSWOM method, where unlike the proposed method, feature extraction is carried out without dividing the horizontal bands into modules.

Method	Yale Database	ORL Database
PSWM	99.20%	99.65%
PSWOM	87.27%	65.75%
Method [13]	98.18%	99.00%
Method [14]	97.70%	N/A

TABLE 1: Comparison of recognition accuracies.

5. CONCLUSIONS

A spectral feature extraction algorithm based on 2D-DFT is proposed for face recognition. Instead of using the whole face image for feature extraction, first, certain high-informative horizontal bands within the image are selected using the proposed entropy based measure. In order to capture spatial information of face images locally, modularization of the horizontal bands is performed. The dominant spectral features are then extracted from the smaller modules within those horizontal bands using 2D-DFT. It has been found that the proposed feature extraction scheme offers an advantage of precise capturing of local variations in the face images, which plays an important role in discriminating different faces. Moreover, it utilizes a very low dimensional feature space, which ensures lower computational burden. For the task of classification, an Euclidean distance based classifier has been employed and it is found that, because of the quality of the extracted features, such a simple classifier can provide a very satisfactory recognition performance and there is no need to employ any complicated classifier. From our extensive simulations on different standard face databases, it has been found that the proposed method provides high recognition accuracy even for images affected due to partial occlusions, expressions and nonlinear lighting variations.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude towards the authorities of the Department of Electrical and Electronic Engineering and Bangladesh University of Engineering and Technology (BUET) for providing constant support throughout this research work.

6. REFERENCES

[1] A. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4 – 20, 2004.

[2] C.Villegas-Quezada and J. Climent, “Holistic face recognition using multivariate approximation, genetic algorithms and adaboost classifier: Preliminary results,” World Academy of Science, Engineering and Technology, vol. 44, pp. 802–806, 2008.

[3] L. L. Shen and L. Bai, “Gabor feature based face recognition using kernal methods,” in Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition, vol. 6, 2004, pp. 386–389.

[4] M. Zhou and H. Wei, “Face verification using gabor wavelets and adaboost,”in Proc. Int. Conf. Pattern Recognition, vol. 1, 2006, pp. 404–407.

[5] C. BenAbdelkader and P. Griffin, “A local region-based approach to gender classification from face images,” in Proc. IEEE Comp. Society Conf. Computer Vision and Pattern Recognition, vol. 3, 2005, pp. 52–57.

[6] R. Gottumukkal and V. K. Asari, “An improved face recognition technique based on modular PCA approach,” Pattern Recognition Lett., vol. 25, pp. 429–436, 2004.

[7] S. Alirezaee, H. Aghaeinia, K. Faez, and F. Askari, “An efficient algorithm for face localization,” Int. Journal of Information Technology, vol. 12, pp. 30–36, 2006.

[8] E. Loutas, I. Pitas, and C. Nikou, “Probabilistic multiple face detection and tracking using entropy measures,” IEEE Trans. Circuits and Systems for Video Technology, vol. 14, pp. 128–135, 2004.

[9] S. C. Dakin and R. J. Watt, “Biological ‘bar codes’ in human faces,” World Academy of Science, Engineering and Technology, vol. 9, pp. 1–10, 2009.

[10] X. Zhang and Y. Gao, “Face recognition across pose: A review,” Pattern Recogn., vol. 42, pp. 2876–2896, 2009.

[11] R. C. Gonzalez and R. E. Woods, Digital Image Processing. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1992.

[12] I. Jolloffe, “Principal component analysis,” Springer-Verlag, Berlin, 1986.

[13] F. M. deS. Matos, L.V. Batista, and J.v.d. Poel, “Face recognition using DCT coefficients selection,” in Proc. ACM symp. Applied computing, 2008, pp. 1753–1757.

[14] X.Y. Jing and D. Zhang, “A face and palm print recognition approach based on discriminant DCT feature extraction,” IEEE Trans. Systems, Man, and Cybernetics, vol. 34, pp. 2405–2415, 2004.

Smart Card Security; Technology and Adoption

Hamed Taherdoost *hamed.taherdoost@gmail.com*
Department of Computer Science
Islamic Azad University, Semnan Branch
Semnan, Iran

Shamsul Sahibuddin *shamsul@utm.my*
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

Neda Jalaliyoon *neda.jalaliyoon@yahoo.com*
Department of Management
Islamic Azad University, Semnan Branch
Semnan, Iran

Abstract

Newly, smart card technology are being used in a number of ways around the world, on the other hand, security has become significant in information technology, especially in those application involving data sharing and transactions through the internet. Furthermore, researches in information technology acceptance have identified the security as one of the factor that can influence on smart card adoption. This research is chiefly to study the security principals of smart card and assess the security aspects' affect on smart card technology adoption. In order to achieve this purpose, a survey was conducted among the 640 university students to measure the acceptance of smart card technology from security aspects.

Keywords: Smart Card, Security, Adoption/Acceptance, Satisfaction, Privacy, Non-repudiation, Authentication, Integrity, Verification, Information Technology

1. INTRODUCTION

Smart card is called 'smart' because it contains a computer chip. Indeed, smart card is often referred to as 'chip card' or 'integrated circuit card'. The smart card looks like a credit card but acts like a computer [19]. Without realizing it, smart cards have become a very important part of human's life. Smart cards are secure devices that enable positive user identification and they are multi-functional, cost effective devices that can be easily adapted for both physical and logical access. Logical access control concerns such familiar principles as password checking or the more sophisticated cryptographic mechanisms for authentication such as windows logon, virtual private network (VPN) access, network authentication, biometric storage and others. Physical access control relates to ID badges and building access control. Importantly, smart cards technology includes a wide range of applications and additional physical forms, than just plastic cards.

However smart card are currently used in many other applications such as health and services cards, banking (such as auto-teller machine cards), network authentication, telephone (calling) cards, identification (including government identity cards, employee ID badges and membership cards), telecommunication (mobile phone subscriber identification and administration), transport ticketing and tolling, electronic passports, and physical access control if having a look at the Iranian wallet, you will find; notes, coins, driving license, library card, paper identity card and other cards. As a result of accepting smart card technology, all these documents could be replaced by one card and it can be used for all.

It is important to note that consumer acceptance and confidence are crucial for any further development of smart card technology as the underlying issues [15][4]. Several researches developed theories and models to describe and analyze user acceptance and each of these models determines different factors to explain user acceptance. According to [20][11], security can effect on user satisfaction and consequently on user acceptance of smart card technology. In other words, in order to increase the level of smart card usage and user adoption, the emphasis on factors that can influence on user acceptance should be raised. Therefore, the smart card security principals were studied and additionally, a survey was broadcasted to measure the importance of security in smart card adoption.

2. SECURITY OF SMART CARDS

Smart cards are mostly used in security applications. Smart cards offer much higher security compared to basic printed cards, and even magnetic stripe cards. Smart cards are often used to prove identity, control access to protected areas, or guarantee payments. The reason for high security in smart cards is due to the fact that the users of the system are given access to the smart card. The security element is put into the hands of the users, and is therefore open to attacks from hackers, clever outsiders, malicious insiders, or even dedicated and well funded enemies. The memory technology used in smart cards has an influence on security, both in the card and in the overall system. Some memory technologies have characteristics that make them particularly secure or insecure. Smart cards also include other security measures such as holograms, security overlays, guilloche printing, micro-printing, optically variable printing.

2.1 Smart Card Security Features

Some components that play a role in smart card security:

- Human-readable security features
- Security features of the smart card chip
- Security features of the operating system
- Security features of the network

Human Readable Security Features of Smart Cards

Smart card includes human readable security identifiers. Smartcard falsification is prevented by features. The data in the card do not protected by this features, but abuse of the card as badge identification are prevented by features [8]. See Table 1.

TABLE 1: Smart card human readable security features

Feature	Description
Photo lamination	The smart card is issued with passport sized photograph. This photo is laminated on the smartcard.
Signature strip	Credit card have very familiar feature. For singing smart card indelible ink is used.
Hologram	During production of card the hologram is bonded to card. Hologram can be separated from card only with destroying the substrate.
Micro Printing	It is ultra-fine printing that the naked eyes see it as a line. This print completely appears under the magnification.
Embossing	The number that is pressed on the card. For increasing the security some companies presses the card number over the hologram.
Security Patterns	They are expensive process and known as a guilloche. This print is very fine interwoven line onto the card substrate.
Laser Graver	With using laser, company burn images into the card substrate only when the smart card is issued to the cardholder the burning can be done then the burning is personal.

Security Features of the Smart Card Chip

Testing the microcircuit, during the production, is the necessary act for the smart card chip. After testing the chip, it is converted to a mode. Accessing the internal chip circuit is impossible for this mode. For example outside can't access the memory directly. To prevent attacks execution of some project is necessary. For example with interchange the conductor; deduce the function is impossible for firms. The connections between on-chip elements are encrypted. There are circuits in smart card which can detect external tampering. The circuit detects too high and too low supply, too high or too low external clock frequency and too low an operation temperature.

Security Features of the Card Operating System

Access to smart card files can be protected with a Personal Identification Number (PIN) or with cryptographic keys. PIN protected card access, with fine-grained access controls to data objects so that different areas of memory can be subject to different security rules. Likewise, functions in the card – including those realized using card applications downloaded into multi-programmable smartcards can also be PIN enabled, to help safeguard lost and stolen smartcards against potential abuse.

When a pin isn't entered correctly then after number of attempts, which is setting by issuer of smartcard, the smart card is deactivated. Some issuer of card can reset the smartcard when it is inactive. It depends on designing of smart card [6].

Security Features of the Network

The system design should take into account the accessibility of data in transit and protect it accordingly or design the transport protocol such that tampering will not affect the overall system security. Some actions can physically secure the card terminal. For example, building card terminal into a wall then some equipment such as motorized smart card reader with shutter guaranties the security of card. Placing the smart card reader and communications link in a secured environment can physically protect them.

2.2 Security Principles

There are several reasons one requires security in a smart card system. The principles being enforced are namely; Privacy, Non-repudiation, Authentication, Integrity, Verification.

Smart cards use different encryption algorithms to implement these principles. In some cases a single mechanism can provide a number of security services. For example, a digital signature can provide data integrity with source authentication and non - repudiation. Most of this security needs require key management, which provides the policies and procedures required for establishing secured information exchange, and public key infrastructure (PKI) plays a big role. PKI includes data encryption to ensure confidentiality, digital certificates to provide authentication, and digital signatures to prove the transaction was completed by the originator without intervention or error [7]. In the following sections, we will describe the mechanisms use in smart cards to enforce these principles:

Privacy

The act of ensuring the nondisclosure of data between two parties from third party is privacy. More research on privacy and security is needed before such a card comes into being, since the more personal and varied the information stored on an individual's smart card, the greater the potential for privacy loss when that card is accessed. But even in their current incarnation, smart cards support an impressive variety of applications, and are expected to support more as they become smaller, cheaper and more powerful [18].

Symmetrical cryptography and asymmetrical cryptography are used to assure privacy. Depend on the application of cards, different processes are needed. In spite of many physical resources, implement of multiple algorithms is impossible. Single, standard, algorithm will be used. For symmetric key cryptography this will almost certainly mean DES (FIPS 46-3, [13]) or maybe triple-DES (ANSI X9.17 [3]) and for asymmetric cryptography the typical algorithm of choice will be RSA [17]. In the future there might be moves towards using the AES (FIPS 196, [14]) as a replacement for DES, but this is not likely any time soon.

- Symmetrical Cryptography: For encrypting plain text into enciphered text and decrypting enciphered text back into plain text the symmetrical cryptography uses single key. To encrypt and decrypt the message the same key is used by symmetrical therefore symmetrical cryptography is termed symmetrical. DES is utilizable on smart card software and it is fast algorithm (FIPS 46-3, [13]). The defect of Symmetrical encryption is the both partners need to recognize the key. For securely transferring keys to cardholders, writing a des key at card personalization time is the typical manner. If it is not possible the asymmetrical cryptography, that is explained blow, must be used.

- Asymmetrical Cryptography: In 1976, the idea of splitting the encryption/decryption key instead of sharing a common key was first proposed in an article by W. Diffie and M.E. Hellman entitled “New Directions in Cryptography”. This idea has since become known as asymmetrical cryptography. Asymmetrical cryptography uses two keys: one to encrypt the plain text and another to decrypt the enciphered text. The keys are mathematically related. Only messages encrypted with one key can be decrypted with the other key. The best-known asymmetrical cryptographic algorithm is RSA [17].

The credit card companies use asymmetrical cryptography for authentication purpose. It uses rarely to perform the data encryption .also the symmetrical cryptography is used to this aim. For send the des key securely from one partner to another the asymmetrical encryptions is often used. If the Des key is known by both partners transmission of data is symmetrically encrypted. This act improves the performance.

Integrity

Errors and tampering in electronic communications are too many. Cryptographic techniques confirm the correctness of message that transmitted from the original to the recipient this is known as data integrity. In fact Integrity assures that only those authorized can access or modify the information. A data integrity service guarantees the correctness of content of message which we sent [21].

Message Authentication Code: For generate the value one-way cryptographic algorithm is used therefore Mac is unique to that message because it is an 8_byte value generated for a message. A one way cryptographic algorithm cannot be reversed and guaranty the enciphered text always unique then we can say it is special. DES using a key calculates the Mac in smart cards. Both the smartcard and smart card reader share it.

Before the message being sent, the Mac is attached to the end of plain text message. When message is received, the Mac value is calculated and compared by recipient. The Mac changed in an unforeseen way if even one character in the message is changed. The Mac is the assurance for recipient that massage hasn't been tampered. This is necessary that Mac or one of these examples protect the messages which transmitted between smartcard and smart card reader.

Non-Repudiation

Non-repudiation confirms that the origin of data is exchanged in transaction. Certain transaction, that is performed, never could be denied by party. A certain message that sent form a sender could never be denied by receiver. And receiver never can deny this message. Non-repudiation of the transaction is ensured by cryptography.

Digital Signature: For understanding better of this feature we need to plan one example: Bob sent message, which is encrypted, to Alice. For encrypting message, Bob uses Alice's public key, and Alice uses her private key to decrypt the message. With this property Alice can check that bob actually send the message. This is basis for digital signatures [8].

Authentication

Authentication is the process which specifying identity of person. In fact it specifies that someone or something is who or what it is claims to be. For example, before Bob accepts a message from Alice, he wants to be assured that Alice is the owner of key. This needs a process by the name of authentication.

Certificates: Authority issuing the certificate guaranty certificates that the holder of certificate is who she/he pretends to be. If digitally signed message, that include copy of the holders public key and information about certificate holder, is a certificate. Then a person who receiving message assure that key is reliable because the issuing authority signed it.

Verification

Confirming the identity of cardholder is the useful act before using a card. If two parties want to start business they must be assured of identify of another party. For recognizing other parties visual and verbal clues can help us. Encryption technology is used to verify that another person is who to pretend to be.

- PIN Codes: PIN consists of four or five digit numbers this number attaches to smart card. Cardholder memorizes this number. PIN is saved safely. Until accessing from the external world is allowed, data and functions on the smartcard can be protected. This time will took only after the correct pin code is available because of the applications of smart card are too many therefore People are needed to remember more and more pin numbers remember 15_20 different pin codes are difficult for all people and it could causes that somebody write the pin number on the card. It eliminated the benefit of having PIN in the first place that is why recent emphasis on security measures have paid attention to biometric as means of identifying a person.
- Biometrics: Biometric is the technology of measuring personal features. Users are reluctant to memorize passwords and pin numbers. This reluctance is one of the driving forces behind the development of biometric. Also many people can share pin numbers then it is not uniquely but biometrics can specify the real person because it is unique. Some of the biological features that can be measured are:
    - ✓ Signature
    - ✓ Fingerprint
    - ✓ Voiceprint
    - ✓ Hand geometry
    - ✓ Eye retina
    - ✓ Facial recognition

As you can see in Table 2, there is a comparison between several factors of the various traditional and biometric identification methods.

- Mutual Authentication: When smart card put into smartcard reader, they verify to identify each other automatically [8]. For example Bob sends a number to Alice. Alice needs to use DES key to encrypt the number then Alice returns back the enciphered text to Bob. Enciphered text is decrypted by Bob and Bob compares this number with the number that he sent. If they be the same then Bob understands that the same key is shared by Alice [6].

TABLE 2: Compare several factors of the various traditional and biometric identification methods (Source: The IBM Smart Card Development Group)

	Acceptance	Cost of Enrollment	Rejects	Substitution	File Size (Bytes)	Relative Device Cost
PIN	50%	Low	1%	0.1%	1-8	Very cheap
Static Signature	20-90%	Low	5%	1%	1000-2000	Cheap
Static/Ext Signature	20-90%	Low	5%	0.1%	1000-2000	Cheap
Dynamic Signature	20-70%	Medium	1-20%	0.01%	40-1000	Medium
Fingerprint	0-100%	Medium	1-10%	0.1%	300-800	Medium to Expensive
Hand Pattern	0-90%	Medium	5%	1%	10-30	Medium to Expensive
Voice Pattern	100%	Low	10%	1%	100-1000	Cheap
Retinal Pattern	0-10%	High	1%	0.1%	80-1000	Very Expensive

3. PROPOSED MODEL

Based on related literatures review, three main constructs are established in this research, namely Security, Satisfaction and Adoption. Figure 1 shows a research model. But, in this study the focus is on the evaluating measurement models for security construct.

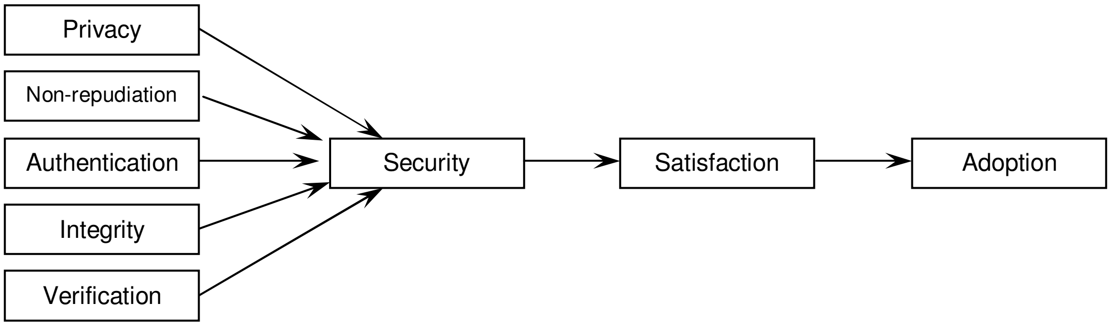


FIGURE 1: Research Model

3.1 Security Dimension

Some studies have reported that users' concern about security has increased and it has been known as one of the most significant factors for technology acceptance. In this study security is defined as "the degree to which a person feels that security is important to them and believes that using smart card is secure" [22]. It has been suggested by [23] that the increase in system security strength would protect the overall quality of the system perceived by users. By protecting the integrity, availability and confidentiality of the content in the system, security controls could help to protect the overall content quality of the system [23].

Content quality is a major determinant of overall information system quality [12], which has a positive effect on individual's perceived ease of use of information systems. Furthermore, [1] found that users' understanding of security issues and awareness of security threats greatly affect their perception of the usefulness of security mechanisms and the overall secured system.

There are several reasons one requires security in a smart card system. The principles being enforced are:

- Privacy: The act of ensuring the nondisclosure of data between two parties from third party.
- Non-repudiation: To confirm the origin of data is exchanged in transaction. Certain transaction, that is performed, never could be denied by party.
- Authentication: The process which specifying identity of person .In fact it specifies that someone or something is who or what it is claims to be.
- Integrity: The correctness of message that transmitted from the original to the recipient.
- Verification: Confirming the identity of cardholder is the useful act before using a card.

3.2 Satisfaction Dimension

Satisfaction of the computer system will have a direct effect on usage [9]. Bailey and Pearson defined satisfaction as ‘‘in a given situation, is the sum of one’s feelings or attitudes towards a variety of factors affecting that situation’’. The measure of computer satisfaction was developed from the comprehensive tool reported by [5].

4. METHODOLOGY

This study collected data samples by conducting online survey aiming at universities’ students as smart card users. Universities’ students were selected because students are usually among the most informed group of people in the society and aware of use of information technology [2]. six hundred and fourty samples were collected. The first section of the instrument assessed demographic characteristics. The second and third parts include twenty five-point Likert scale items ranging from strongly disagree to strongly agree. The questionnaire consists of thirteen measurement items in security section and six measurement items in satisfaction and adoption part. All the nineteen items (security, satisfaction and adoption measures) were used to run factor analysis by SPSS 16.0 for Windows. The value of Cronbach’s alpha (α) is above the 0.7 level and thus satisfies the reliability requirement.

5. RESULTS

Table 3 summarizes the demographic profile and descriptive statistic of the respondents.

TABLE 3: Demographic profile of the respondents

Demographic Variables	**Frequency (N)**	**Percentage (%)**
Gender		
Female	342	53.4
Male	298	46.6
Age		
20 and under	188	29.3
20-25	377	58.9
26-30	60	9.4
More than 30	15	2.4
Education		
Diploma	102	15.9
Bachelor Degree	511	79.9
Master Degree	21	3.3
PhD Degree	6	0.9

In the research model, a further satisfaction factor is security. As it is mentioned earlier, security itself has five principals which are privacy, integrity, non-repudiation, verification and authentication. Therefore, in order to measure the level of security in smart card technology and its importance for user acceptance of smart card technology, it is also needed to investigate these five aspects. Thus, in the survey, there are five items to measure the users’ opinion and their expectation about security of smart card technology and some items regarding to the security principals. Table 4 shows the percentage and frequency of the responses. First of all, once respondents were asked whether they trust on the smart card security or not, more than 84% of them cited their agreement while only 7% disagree or strongly disagree with it.

Moreover, in the next question, more than 77% of participants either agree or strongly agree that they are not concern about the security of smart cards whereas just 11% are concerned about it. Again, almost the same percentage recorded for smart card trustworthiness. On the other point of view, 92% of participants agree or strongly agree that security is important when using smart card. And finally, more than three quarters (80.4%) agree or strongly agree that smart card system is secure though 3.6% disagree.

As shown in Table 4, more than three quarters (80.3%) agree or strongly agree that in the smart card the message will be transmitted correctly from the original to the recipient. Additionally, another related question regarding the data integrity in the smart card system was posed and nearly three quarters (73.6%) either agree or strongly agree rather than (8.2%) disagree or strongly disagree that smart card prevents accidental loss of data and data decay. In terms of non-repudiation, more 77% of respondents agree or strongly agree that in smart card if a certain transaction is performed, it never could be denied by party while less than one tenth (8.1%) disagree. From the privacy view, nearly four out of five (79.3%) either agree or strongly agree that their information is well protected. Furthermore, more than three quarters (77.4%) either agree or strongly agree rather than less than one tenth (9.9%) disagree that they trust in the ability of a smart card system to protect their privacy.

TABLE 51: Frequency and percentage of respondents' response to the security section's items

Variables	Questions		Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Security	I trust in the technology that smart card system is using.	N	6	39	59	212	327
		%	1	6.2	9.1	33.6	51.0
	I am not worried about the security of smart card system.	N	6	68	89	252	245
		%	1.0	10.8	10.4	39.4	38.4
	Smart card systems are trustworthy.	N	6	14	124	299	196
		%	1.0	2.3	19.4	46.6	30.6
	Security will be important when using smart card.	N	6	6	38	218	365
		%	1.0	1.0	6.1	34.6	57.4
	Overall, the smart card system is secure.	N	12	10	99	271	245
		%	1.9	1.7	15.5	42.4	38.4
Data integrity	I feel that message will be transmitted correctly from the original to the recipient.	N	17	36	73	226	288
		%	2.7	5.6	11.4	35.3	45.0
	I believe that smart card prevents accidental loss of data and data decay.	N	22	30	116	296	174
		%	3.5	4.7	18.2	46.3	27.3
Non-Repudiation	I believe that in smart card if a certain transaction is performed, it never could be denied by party.	N	12	38	90	246	251
		%	2.1	6.0	14.1	38.6	39.2
Privacy	I believe that my information is well protected.	N	6	43	82	328	180
		%	1	6.8	12.9	51.2	28.1
	I trust in the ability of a smart card system to protect my privacy.	N	12	50	80	240	255
		%	2.0	7.9	12.6	37.5	39.9
Verification	I believe that smart card is able to confirm the identity of cardholder before using a card.	N	30	32	64	261	254
		%	4.7	5.0	10.0	40.8	39.5
Confidentiality and Authentication	Access to confidential information is strictly limited by the use of special codes and passwords.	N	43	42	110	213	228
		%	6.9	6.6	17.2	33.5	35.8
	Only authorized individuals are able to access to confidential information.	N	35	28	101	247	225
		%	5.5	4.4	15.9	38.8	35.3

Regarding the verification of smart card technology, once respondents were asked that smart card is able to confirm the identity of cardholder before using a card, approximately four out of five (80.3%) either agree or strongly agree rather than below one out of seven (9.7%) disagree.

At last, nearly 14% of those responding either disagree or strongly disagree that access to confidential information stored in smart card chip is strictly limited by the use of special codes and passwords while almost 70% agree. In addition, another related item to smart card authentication was created that only authorized individuals are able to access to confidential information and more agree (74.1%) than disagree (9.9%).

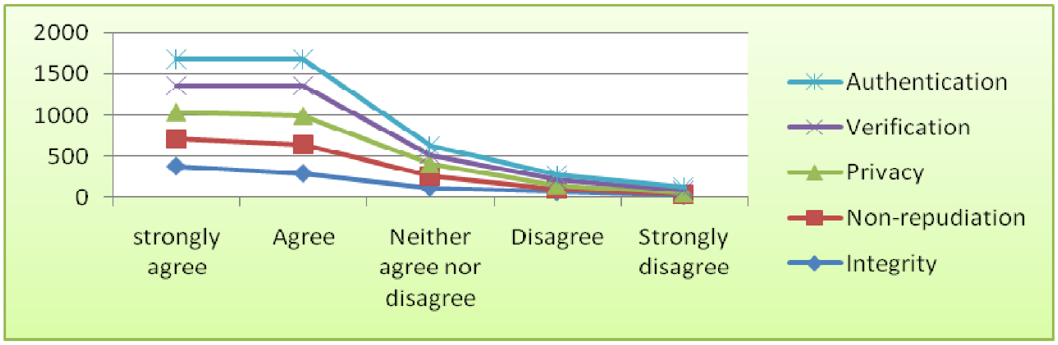


FIGURE 2: Users' opinions about smart card security principals

Figure 2 reveals the users' opinions about smart card security principals. As it is clarified from this Figure, the results in these five principals is to support of the previous question which was about the security of smart card and more than 80% of respondents recognized smart card as a secure device.

Therefore, as it is shown in Table 5, it can be concluded that the correlation between privacy, integrity, non-repudiation, authentication, verification and security is statistically significant. Furthermore, the correlation of all factors on security is positive.

Moreover, Table 6 indicates that there is a positive correlation between the total score of security and satisfaction (correlation coefficient = 0.732). Additionally, as the simple correlation of 0.621 between satisfaction and adoption indicates there is a fairly strong relationship between them. Therefore, it can be concluded that the correlation between security, satisfaction and adoption is statistically significant and positive.

TABLE 5: Correlation between security and security principals

		Security	Integrity	Non-Repudiation	Privacy	Verification	Authentication
Security	Pearson Correlation	1.000					
Integrity	Pearson Correlation	.340**	1.000				
Non- Repudiation	Pearson Correlation	.314**	.408**	1.000			
Privacy	Pearson Correlation	.428**	.363**	.242**	1.000		
Verification	Pearson Correlation	.317**	.222**	.203**	.307**	1.000	
Authentication	Pearson Correlation	.296**	.254**	.290**	.290**	.268**	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

TABLE 7: Correlation between attitude toward use, satisfaction and adoption

		Adoption	Satisfaction	Security
Adoption	Pearson Correlation	1.000		
Satisfaction	Pearson Correlation	.621**	1.000	
Security	Pearson Correlation	.636**	.732**	1.000

**Correlation is significant at the 0.01 level (2-taile).

6. CONCLUSION

In order to use any new system and technology, it is needed that users can trust on it. Therefore, being secure can motivate consumers to accept any fresh technologies and smart card technology as well. Findings of this study demonstrate that most of the students (81.8%) found smart card secure so they trust on the smart card systems. Besides, more than nine out of ten stated that security will be important when using smart card. On the other point of view, anxiety which have a negative effect on the user satisfaction does not have large impact on the users acceptance because most of the users (76.3%) suppose that the messages will be transmitted correctly from the original to the recipient (card and card reader) and also they have faith that smart card prevents accidental loss of data and data decay. Additionally, the majority of the participants believe that smart card with the ability of limiting the access to the confidential information by using the special codes and passwords is able to confirm the identity of cardholder before using a card (verification and authentication).

The results of this study illustrate that security has an important and positive effect on user satisfaction and consequently on user acceptance. It means that with increasing the level of security, the level of user acceptance will be increased. Finally, further investigation needs to be carried out in the future to identify factors that will provide users better understanding of the system and also establish new techniques to increase the security level of the smart card.

7. REFERENCES

[1] Adams, A. and Sasse, M. A. (1999), Users Are Not the Enemy. Why Users Compromise Computer Security Mechanisms And How To Take Remedial Measures. *Communications of the ACM*. 42(12), 42-46.

[2] I. Al-Alawi, & M.A. Al-Amer, “Young Generation Attitudes and Awareness Towards the Implementation of Smart Card in Bahrain: An Exploratory Study”. *Journal of Computer Science,* Vol. 2 No. 5, 2006, pp. 441-446.

[3] American National Standard Institute. (1985). *ANSI X9.17*. Financial institution key management (wholesale).

[4] Argy, P. and Bollen, R. 1999. Australia: raising the e-commerce comfort level. *IT Professional*, 1 (6), 56–57.

[5] Bailey, J. E., and Pearson, S. W. (1983). Development of a Tool For Measuring and Analyzing Computer User Satisfaction, *Management Science.* 29, 530–544.

[6] *Consultation on Australian Government Smartcard Framework*; *Smartcard Implementation Guide. (*2007). Australian government office of the privacy commissioner.

[7] Everett, D. (1993). Smart Card Tutorial, Part 11 The Development Environment. First Published in July 1993.

[8] Ferrari, J., Mackinnon. R., Poh. S., and Yatawara. L. (1998). *Smart Cards: A Case Study.* International Technical Support Organization IBM Corp.

[9] Igbaria, M. and Parasuraman, S. (1989). A path analytic study of individual characteristics, computer anxiety, and attitudes towards microcomputers. *Journal of Management.* 15(3)*,* 373-388.

[10] Leonard, L. N. K., Cronan, T. P., and Kreie, J. (2004). What influences IT ethical behavior intentions, planned behavior, reasoned action, perceived importance, or individual characteristics? *Information and Management*. 42(1), 143-158.

[11] Masrom. M, Ismail.Z, Ahmad. R and Taherdoost. H. (2009). Evaluating Measurement Models For the Acceptance of Smart Card Technology: Security Aspects. *Proceeding of the 3rd*

[12] *International Conference on Informatics and Technology, Kuala Lumpur, Malaysia*.170-175.

[13] Liaw, S.S., and Huang, H. M. (2003). An investigation of user attitudes toward search engines as an information retrieval tool. *Computers in Human Behavior.* 19(6), 751–765.

[14] National Institute of Standards and Technology. (1999). *FIPS 46-3*. The Data Encryption Standard.

[15] National Institute of Standards and Technology. (2000). *FIPS 196*. The Advanced Encryption Standard.

[16] Rankers, P., Connell, L., Collins, T. and Russell, D. 2001. Secure contactless smartcard ASIC with DPA protection, *IEEE Journal of Solid-State Circuits*, 36 (3), 559–565.

[17] Rankl, W. and Effing, W. 2003. Smart Card Handbook, John Wiley.

[18] Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 21(2), 120-126.

[19] Shelfer, K., M., and Procaccino, J., D. (2002). Smart card evolution. *Communications of the ACM*. 45(7): 83-88.

[20] T. Kilicli, "*Smart Card HOWTO*," 2001.

[21] Taherdoost. H, Masrom. M, and Ismail. Z. (2009). Evaluation of Smart Card Acceptance: Security, Technology and Usage. *Conference Proceedings of International Conference on e-Commerce, e-Administration, e-Society, and e-Education (e-case).* Singapore. pp.765-779.

[22] Vandenwauver, M. (1994). introduction to cryptography, Katholieke Universiteit Leuven.

[23] Vijayasarathy, L., R. (2004). Predicting consumer intentions to use online shopping: the case for an augmented technology acceptance model. *Information and Management*. 41(6), 747-762.

[24] Whitman, M., E., and Mattord, H., J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.

The Three Dimensions of Security

Malik F. Saleh *msaleh@pmu.edu.sa*
Management Information Systems, Chair
Prince Mohammad Bin Fahd University
Al Khobar, 31952, Saudi Arabia

Abstract

Security is an issue of generally recognized importance. Security starts with you, the user. It is well known that a formal security policy is a prerequisite of security. Having a policy and being able to enforce it is a totally different thing. This paper explains the three aspects of security that should be combined to create a well-rounded solution for securing organizations. This solution examines people, policy and enforcement as three dimensions in the world of security. This paper serves as 1) a conceptual framework for securing organization 2) the basis for formal policy-to-enforcement; 3) It raises awareness that the users should be informed of their roles and responsibilities in protecting the organization; and 4) evidence for writing policies that can be implemented and enforcement involves understanding the policies by the users.

Keywords: Dimensions of Security, Security, Policy, People, Enforcement of Security.

1. INTRODUCTION

Security is an issue of generally recognized importance. Protecting an organization means securing the organization. Security is achieved from the prevention of attacks and from achieving the organization's mission despite attacks and accidents. The traditional information security objectives are confidentiality, integrity, and availability. Achieving these three objectives does not mean achieving security [1].

It is well known that a formal security policy is a prerequisite of security. Having a policy and being able to enforce it is a totally different thing. The security policy is the first line of defense. Without a well-designed policy, the security of the system becomes unpredictable and governed by the system administrator [2]. Employees are the greatest threat to an organization's security. Their non-compliance with security policies not only threatens the integrity of the system, but also costs the organization a significant amount of money due to the loss of information or due to fixing problems that the user causes [3]. Therefore, Security starts with you, the user.

Does added security make things more difficult to use? Will people always resent the extra steps? Norman [4] argues that the answer to both questions is the same: not necessarily. Both are design issues that require understanding of the need for security and the workings of the mechanisms that enforce them. We tolerate the added security because it seems necessary and the amount of effort it demands usually seems reasonable.

Effective policy enforcement involves many steps such as ensuring that the policies are understood by all the users, regularly checking to see if the polices are being violated, and having well-defined procedures and guidelines to deal with incidents of policy violation [3] . Looking at protecting the information at an organization we found that all organizations share a common risk, the users. To achieve security, different elements in this risk should be dealt with individually as well as in unity.

This paper explains the three aspects of security (see Fig.1) that should be combined to create a well-rounded solution for securing organizations. This solution examines people, policy and enforcement as three dimensions in the world of security. It serves as 1) a conceptual framework for securing organization 2) the basis for formal policy-to-enforcement; 3) It raises awareness that the users should be informed of their roles and responsibilities in protecting the organization; and 4) evidence for writing policies that can be implemented; and enforcement involves understanding the policies by the users. In order to make effective protection, organizations need to have an overall policy. That policy needs to be implemented in multiple ways and it should be a simple policy.

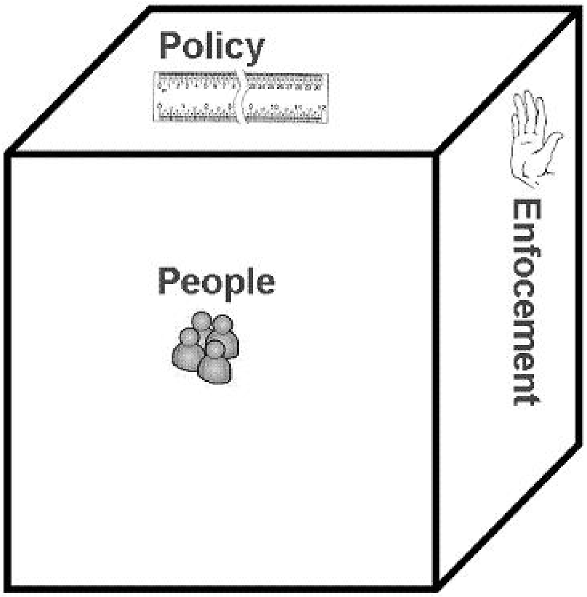


FIGURE 1: The Three Dimensions of Security

2. BACKGROUND AND RELATED WORK

Users, policies, and enforcement are important topics for the security and audit community and each part has received a fair amount of research attention. To frame the discussion on the combination of the three parts, we categorize the prior research into work that addresses each part individually but in relation to the other parts. We also discuss research from the computer policy community and the availability of enforcement products from different vendors.

The motivation for this paper was due to the challenges of enforcing policies on the users that the users don't understand. We acknowledge that security is still heavily reliant on technological solutions, but the vulnerability and the risk is attributed to the users. We argue that these challenges are due to writing policies without getting users involved in policy writing and due to lack of training to the users. Further, policies should inform the users of their roles and responsibilities in protecting the organizational assets.

This paper is organized in different sections. Section 2 discusses briefly the related work and the fact that each of the users, the policy and enforcement are covered in detail in the literature. Section 3 examines the users; section 4 examines the policies in relation to the users. Section 5 examines enforcing policies on the users. We conclude that the three dimensions of security are of a non-technical nature. All these dimensions must be taken into account in designing and creating a comprehensive information security plan for organizations.

3. THE PEOPLE DIMENSION

Who are the users? According to [5], the users are the enemy. The interaction between the users and the system is responsible for the functioning of the system and in most cases, this very interaction, according to [6], is the greatest risk. The threat posed by legitimate users in an organization has been labeled as "The Enemy Within" [7]. Most users put their firms at risk through either their sense of security or their ignorance. A small minority of users are believed to be actively seeking to damage the company from within [7]. Figure 2 explains this risk.

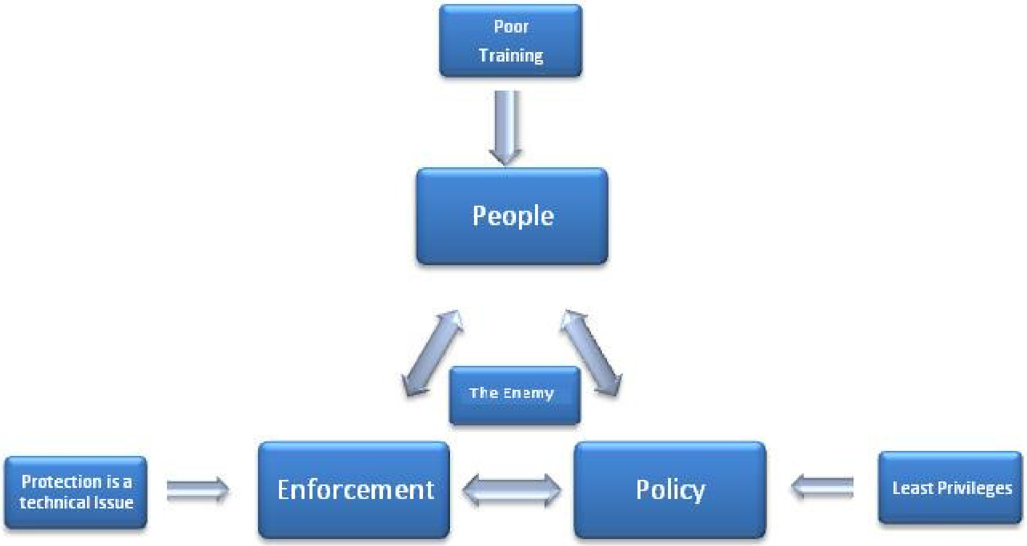


FIGURE 2: Issues affecting security

According to [8] the users are not the enemy. Users are often told as little as possible because they are seen as “inherently insecure.” The inadequate knowledge lies at the root of users’ “insecure” behaviors. Users perceived threats to the organization to be low because of their own judgments and because their roles in the system was not important

Many users do not understand the technical issues associated with privacy and security management [6, 9]. User behavior plays a part in many security failures, and it has become common to refer to users as the “weakest link” in the security chain [10]. Blaming the users will not lead to effective security systems. To address the weakest link in the security chain, organizations have to address this issue by transforming the end-users from users of the system to the enforcers of security by training end-users on security related issues. In general, users tolerate the added security because it seems necessary and the amount of effort it demands usually seems reasonable.

Phishing attacks that exploits user vulnerabilities rather than taking advantage of system vulnerabilities, take advantage of users’ inability to distinguish legitimate company websites from fake ones. A great deal of effort has been devoted to solving the phishing problem by prevention and detection of phishing emails and phishing Web sites [11]. With all these efforts, phishing is still an issue for users and organizations. Automated detection systems should be used as the first line of defense against phishing attacks, but since these systems are unlikely to perform flawlessly, they should be complemented by warning users about the threat, through toolbars and browser extensions, and training users not to fall for attacks.

Research shows that training continues to have a significant organizational impact. Surveys have also found that the computer literacy requirements have skyrocketed in almost every end-user category. End-user training has three phases: initiation, formal training and learning, and post-training [12,13]. For security related issues, a discovery and disclosure approach should be followed. The disclosure should provide users with a sense of security that raises their awareness of the threats that their information systems face. While the discoverer may never disclose the finding, it educates the users. According to [13], the post-training phase has focused on the evaluation of training and learning immediately after training. However, organizations are more interested in long-term effects of training and the areas of end-user learning, rather than training. Organizations want to know if the training has been transferred to the workplace, and whether learning continues after formal training has ended.

Training according to [14] should:

1. Change the way the users think and act when it comes to security

2. Measure the success of the training program and
3. Continually address the importance of security.

The training program should consist of static topics that will be evaluated on a yearly basis, while a dynamic monthly component would consist of topics that were relevant at the time. Both components of the training are solicited opinions from different stakeholders. The idea of getting users involved in security related issue has a long-term impact on the culture of the organization and it will enforce all security policies of the organization.

4. THE POLICY DIMENSION

It is well known that formal security policy is a prerequisite of security. According to [15] the security policy is a direction-giving document for security within an organization. The policy defines the role information security has to play in reaching and supporting the organization's vision and mission. It should complement the organization's business objectives and reflect management's willingness to operate the organization in a controlled and secure manner. If a special-purpose security policies is defined, it is according to [16], perhaps best explained in terms of the principle of least privilege which holds that each user be granted the minimum access needed to accomplish their task. End-users therefore, will have the least privileges in the organization, but does a one size hits all work for all end-users!

It is argued [3] that policies should be written so that they are clear, concise and easy to understand. A security policy should be measurable, achievable, realistic, traceable and enforceable. Vague policies will increase the occurrence of non-compliance. Therefore, the security policy should inform the end-users of their roles and responsibilities in protecting the organizational assets. It is also argued by [15] that the roles and responsibilities in the security policy is one of the most important components of the policy, as this part tells exactly what is expected of users in terms of information security in the organization. The roles and responsibilities should cover all aspects of information security, as well as the individual responsibilities of all parties using the organization's information resources.

For example, the Security rule codified in the Code of Federal Regulations (CFR) has special information security implications that cannot be ignored. A comprehensive security awareness and training program is delineated as a standard to meet, with periodic updates as part of the program. Further, the CFR addresses controls that involve personnel, including clearance procedures for hiring and termination, and other human resources related matters [17].

Two challenges are faced when writing policies in natural language and implementing the technical details. First, the design of policy languages that allow flexibility and maximum expressivity is a popular research direction. In order to have all representation from different stakeholders when writing security policies, it is important to use flexible policy languages to demonstrate that a wide range of enforceable policies that can be specified [18]. Second, end-users are not technical to know the details of the policy therefore users have to approve the implemented policy by testing the implementation and experiencing the impact on their work.

There are a growing number of strict security and privacy audit and compliance requirements. This creates a need for policy-based systems [18]. Although an information security policy is a vital part of an organization's strategy for achieving information security, it is not always easy to put this document together. There are often differing opinions within the organization as to what constitutes a policy [15]. Organizations create policies to eliminate risk. Assessing risk can be seen as a three-phase process: identification, estimation, and evaluation. In the security world, the entire risk assessment process is called certification. Certification includes identification of risks, estimation of the consequences of accepting the identified risks, and evaluation of proposals for mitigating those identified risks [19]. Therefore the more strict the policy, the less risk organizations are willing to take for their resources.

5. THE ENFORCEMENT DIMENSION

One of the deadly sins of information security according to [20] is not realizing that the protection of information is a business issue and not a technical issue. Information security enforcement is an essential and integral part of corporate governance. The driving force for making security part of corporate governance has seen several documents on corporate governance such as the ISACA's Control Objectives for Information and Related Technologies (COBIT). These documents have been supported by a growing set of laws and legal requirements. Organizations implementing COBIT, and other standards for corporate governance, will realize the benefits of a proven solution for corporate governance. Therefore, policy enforcement starts at the top of the pyramid.

The practicality of any security policy depends on whether that policy is enforceable and at what cost [16]. Users cannot always see what effect a policy might directly have on them. The ability of the end-user of an organization to understand its policy is important to ensuring that the policy is followed. It is argued [3] that effective policy enforcement involves assuring that the policies are understood by all users, and having well-defined procedures to deal with incidents of policy violation.

Effective policy enforcement involves several elements and the policies need to be implemented in multiple ways: Monitoring, documenting, training, implementing enforcement technologies, and others. Organizations must have a unified way of enforcing policies in different products that the organization acquires.

5.1 Monitoring of the Working Environment

Constant monitoring of the working environment, the configuration, and the network to ensure that violations have not occurred is the first step in enforcing policies. Constantly monitoring the configuration of computers is a valuable practice to identify breaches of security. A computer may be infected or suddenly out of compliance at any time it is connected to the network. For instance, consider using a policy enforcement system to isolate computers from the network if its antivirus application isn't running [21].

5.2 Documenting All Security Incidents

While documenting all security incidents, organizations also need to document the methods used to detect and deal with security violation. Part of the monitoring of the work environment should be on generating reports and possible trends in security violations and analyzing trends of security related issues.

5.3 Implementing Enforcement Technologies

Policy enforcement technologies extend the familiar notion of granular access control beyond user and machine identity, into the endpoint computer's configuration and network environment. This capability for enhanced examination of a target machine is generally implemented through a proprietary software agent [21]. For instance, implementing a data loss prevention product when sending an e-mail, the product will check the policy and it would require approval before allowing data to be sent in an email. Another application may be implemented to allow you not to copy data into removable media.

Enforcement technologies exist from many vendors. The Trusted Computing Group has created an open architecture for endpoint integrity. The architecture enables network operators to enforce policies regarding endpoint integrity at or after network connection. This standard architecture ensures multi-vendor interoperability across a wide variety of endpoints, network technologies, and policies [22]. Other products are available from different vendors such as: Cisco Network Admission Control [23], Microsoft Network Access Protection [24], Endpoint Security Mailing List, and others.

Cisco Network Admission Control (NAC) enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. It allows noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network. The decision is made based on a policy that exists on Cisco Secure Access Control Server [23].

Microsoft Network Access Protection (NAP) solution enforces the policy by constant monitoring and assessing the health of client computers when they attempt to connect or communicate on a network. Computers that are not in compliance with the policy can be provided with restricted network access until their configuration is updated and brought into compliance with the policy. Noncompliant computers can be quarantined or automatically updated so that users can quickly regain full network access without manually updating or reconfiguring their computers [24].

5.4 User Training

Training continues to have a significant organizational impact. End-user training takes the largest portion (38.4%) and it deals with the teaching of skills to effectively use computer applications [12]. Training and user education should focus on procedural issues rather than effective use of computer applications. A procedural attack takes the form of a social engineering attack. It is argued by [25] that a social engineering attack manipulates people into performing actions or giving confidential information. While [26] argues that an appearance of authority may be interpreted as having actual authority in social engineering attacks. The study in [26] also supports the concept that understanding of the value of information as well as proper usage of information is as important as an awareness of social engineering efforts.

It is typical for organizations to mandate that users declare and acknowledge receiving the information security policy. In signing a user declaration upon employment before access to electronic information is granted, the user acknowledges his/her responsibility with regard to information security. A user should know his individual responsibilities in protecting information assets within his organization [15]. One way to ensure that users know their responsibilities in protecting the organization is by training them on how to protect the organization.

Enforcement technologies make enforcement possible for physical and computer security. But for protecting the organization from the vulnerabilities of its users, it requires more than an automated system. Social engineering attacks bypass the enforcement technology by attacking the weakest link, the users. Such attacks according to [27] can occur on both a physical and psychological level. The physical setting for these attacks occurs where a victim feels secure: often the workplace, the phone, even around the water cooler. Psychology is often used to create a rushed situation that helps the social engineer to get information about accessing the system from an employee. In both cases the attack is possible due to inadequate education of the users.

6. CONCLUSION AND CONTRIBUTION

It is clear that the three dimensions of security are of a non-technical nature. All these dimensions must be taken into account in designing and creating a comprehensive information security plan for organizations, because no single dimension, or product or tool on its own will provide a proper all inclusive solution. While it is the responsibility of organizations to provide physical and computer security, organizations should take responsibility in providing training and education in security related issues and against social engineering attacks. This type of attack is preventable by training and educating users of the threats.

Users are often the weakest link in an otherwise secure organization and, consequently, are targeted by social engineering attacks. The only protection against social engineering attacks is to educate the users. A discovery and disclosure approach should be followed. The disclosure should provide users with a sense of security that raises their awareness of the threats that their information systems face. Organizations are more interested in long-term effects of training and the areas of end-user learning, rather than training. Organizations want the training to be transferred to the workplace. Signing and acknowledging the receipt of an information security policy should be after educating and training the users. The user declaration and acknowledgement should also be read and signed again on an annual basis.

We provided evidence for writing policies that can be implemented. Implementation requires understanding of those policies by the users. A formal security policy is a prerequisite of security. Vague policies will increase the occurrence of non-compliance. Therefore, the security policy should inform the end-users of their roles and responsibilities in protecting the organizational assets. Organizations should enforce policies in a unified way. The ability of the end-user of an organization to understand its policy is important to ensuring that the policy is followed. Effective policy enforcement involves assuring that the policies are understood by all users, and having well-defined procedure to deal with incidents of policy violation.

The basis for a formal policy-to-enforcement was shown to consist of:

- Constant monitoring of the working environment, the configuration, and the network to ensure that violations have not occurred is the first step in enforcing policies.
- Analyzing possible trends in security violations and analyzing trends of security related issues.
- Implementing enforcement technologies
- Training in security related issues will have a significant organizational impact

This conceptual framework combined the users, the policies and the enforcement into a solution that transformed the users from being the weakest link, the enemy within, in an organization into responsible users who play a role in organization security. This role begins with training the users in security related issues and participants in writing security policies. This role ends in users enforcing policies and transforming organization into secure ones (see Fig. 3)

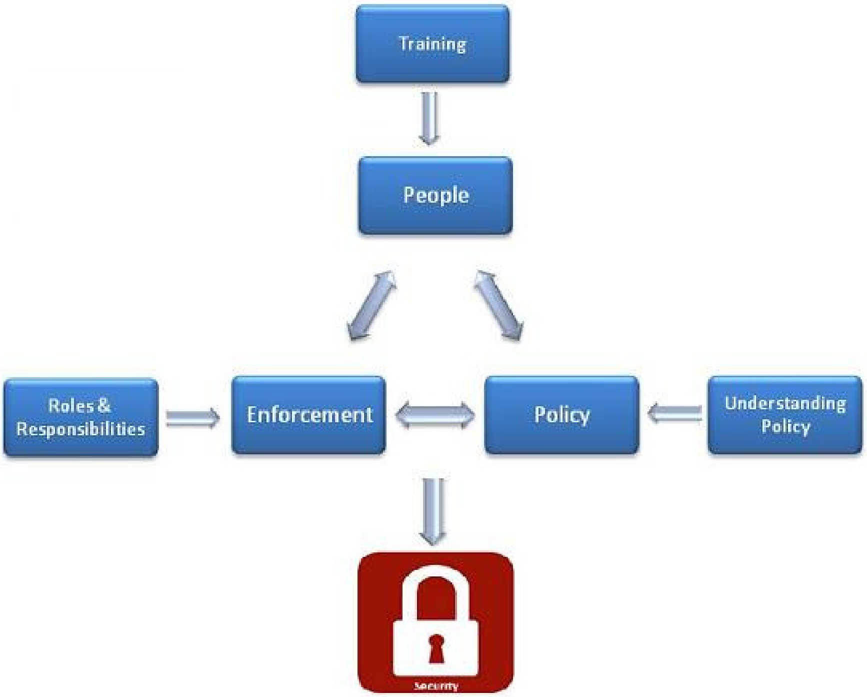


FIGURE 3: Model for the three dimensions of security

7. FUTURE WORK

For the future work, we propose tracking the usage of social networking websites like Facebook and Twitter in aiding social engineering attacks. A social engineering attack gathers information about users before performing actions against an organization.

In addition to social engineering attacks, we propose protecting the configuration systems. It is also desirable to encrypting the exchange of messages between systems to avoid eavesdropping. Many systems implement automatic updates that require downloading and installing new software. Many implementations are implemented without the users being involved. An investigation that compares automatic updates versus manual updates by the users will be carried out.

8. REFERENCES

[1] Saleh, M.F., *Information Security Maturity Model* International Journal of Computer Science and Security (IJCSS), 2011. **5**(3): p. 21.

[2] David, J., *Policy enforcement in the workplace.* Computers & Security, 2002. **21**(6): p. 506-513.

[3] Madigan, E.M., C. Petrulich, and K. Motuk, *The cost of non-compliance: when policies fail*, in *Proceedings of the 32nd annual ACM SIGUCCS fall conference*. 2004, ACM: Baltimore, MD, USA. p. 47-51.

[4] Norman, D.A., *The Way I See it: When security gets in the way.* interactions, 2009. **16**(6): p. 60-63.

[5] Vidyaraman, S., M. Chandrasekaran, and S. Upadhyaya, *Position: the user is the enemy*, in *Proceedings of the 2007 Workshop on New Security Paradigms*. 2008, ACM: New Hampshire. p. 75-80.

[6] Schneier, B., *Secrets and Lies: Digital Security in a Networked World*. 2000, New York: John Wiley & Sons, Inc.

[7] Corporation, M. *The Enemy Within*. 2005 [cited June 20; Available from: http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/.

[8] Adams, A. and M.A. Sasse, *Users are not the enemy.* Communications of the ACM, 1999. 42(12).

[9] Gross, J. and M.B. Rosson. *Looking for Trouble: Understanding End-User Security Management*. in *Computer Human Interaction for the Management of Information Technology (CHIMIT)* 2007.

[10] Sasse, M.A., S. Brostoff, and D. Weirich, *Transforming the 'Weakest Link' - a Human/Computer Interaction Approach to Usable and Effective Security.* BT Technology Journal, 2001. **19**(3): p. 122-131.

[11] Kumaraguru, P., et al., *Teaching Johnny not to fall for phish.* ACM Trans. Internet Technol., 2010. **10**(2): p. 1-31.

[12] Gupta, S., R.P. Bostrom, and M. Huber, *End-user training methods: what we know, need to know.* SIGMIS Database, 2010. **41**(4): p. 9-39.

[13] Compeau, D., et al., *End-user training and learning.* Commun. ACM, 1995. **38**(7): p. 24-26.

[14] McCoy, C. and R.T. Fowler, *"You are the key to security": establishing a successful security awareness program*, in *Proceedings of the 32nd annual ACM SIGUCCS fall conference*. 2004, ACM: Baltimore, MD, USA. p. 346-349.

[15] Höne, K. and J.H.P. Eloff, *Information security policy what do international information security standards say?* Computers & Security, 2002. **21**(5): p. 402-409

[16] Schneider, F.B., *Enforceable security policies.* ACM Transactions on Information and System Security, 2000. **3**(1): p. 30-50.

[17] Craig, J.S., *The human element: training, awareness, and human resources implications of health information security policy under the Health Insurance Portability and Accountability Act (HIPAA)*, in *2009 Information Security Curriculum Development Conference*. 2009, ACM: Kennesaw, Georgia. p. 95-99.

[18] Johnson, M., et al., *Optimizing a policy authoring framework for security and privacy policies*, in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 2010, ACM: Redmond, Washington. p. 1-9.

[19] Hall, D.E., *Requirements and policy challenges in highly secure environments*, in *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*. 2004, ACM: Paris, France. p. 897-898.

[20] Solmsa, B.v. and R.v. Solms, *The 10 deadly sins of information security management.* Computers & Security, 2004. **23**: p. 371-376.

[21] Bird, T. *What is policy enforcement, and why should we care?* 2004; Available from: http://www.computerworld.com/s/article/98080/What_is_policy_enforcement_and_why_should_we_care_?taxonomyId=17&pageNumber=3.

[22] Group, T.C. *Trusted Network Connect*. 2010 [cited 2011 June 28]; Available from: http://www.trustedcomputinggroup.org/developers/trusted_network_connect/.

[23] Cisco. *Network Admission Control.* 2011 [cited 2011 June 28]; Available from: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html.

[24] Microsoft. *Network Access Protection*. 2011 [cited 2011 June 28]; Available from: http://www.microsoft.com/windowsserver2008/en/us/nap-main.aspx.

[25] Robling, G. and M. Muller, *Social engineering: a serious underestimated problem.* SIGCSE Bull., 2009. **41**(3): p. 384-384.

[26] Kvedar, D., M. Nettis, and S.P. Fulton, *The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition.* J. Comput. Small Coll., 2010. **26**(2): p. 80-87.

[27] Orgill, G.L., et al., *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*, in *Proceedings of the 5th conference on Information technology education*. 2004, ACM: Salt Lake City, UT, USA. p. 177-181.

INSTRUCTIONS TO CONTRIBUTORS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

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 IJS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJS appears in more focused issues. Besides normal publications, IJS 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.

IJS LIST OF TOPICS
The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Attacks, security mechanisms, and security service
- Authorisation
- Cellular/wireless/mobile/satellite networks securi
- Public key cryptography and key management
- Cryptography and cryptanalysis
- Data integrity issues
- Database security
- Denial of service attacks and countermeasures
- Design or analysis of security protocols
- Distributed and parallel systems security
- Formal security analyses
- Information flow
- Intellectual property protection
- Anonymity and pseudonymity
- Code security, including mobile code security
- Biometrics
- Authentication
- Confidentiality, privacy, integrity, authenticatio
- Data confidentiality issues
- Data recovery
- Denial of service
- Dependability and reliability
- Distributed access control
- Electronic commerce
- Fraudulent usage
- Information hiding and watermarking
- Intrusion detection

- Key management
- Network and Internet security
- Network security performance evaluation
- Peer-to-peer security
- Privacy protection
- Revocation of malicious parties
- Secure location determination
- Secure routing protocols
- Security in ad hoc networks
- Security in communications
- Security in distributed systems
- Security in e-mail
- Security in integrated networks
- Security in internet and WWW
- Security in mobile IP
- Security in peer-to-peer networks
- Security in sensor networks
- Security in wired and wireless integrated networks
- Security in wireless communications
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless PANs (Bluetooth and IEEE 802.
- Security specification techniques
- Tradeoff analysis between performance and security
- Viruses worms and other malicious code
- Multicast security
- Network forensics
- Non-repudiation
- Prevention of traffic analysis
- Computer forensics
- Risk assessment and management
- Secure PHY/MAC/routing protocols
- Security group communications
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in content-delivery networks
- Security in domain name service
- Security in high-speed networks
- Security in integrated wireless networks
- Security in IP networks
- Security in optical systems and networks
- Security in satellite networks
- Security in VoIP
- Security in Wired Networks
- Security in wireless internet
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security policies
- Security standards
- Trust establishment
- WLAN and Bluetooth security

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