International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3337-3342
© Research India Publications. http://www.ripublication.com

Hiding Fingerprint Minutiae in Multiple Facial Images Using BPCS

Kadhim H. Kuban Alibraheemi

Department of Computer Science, College of Education for Pure Sciences,
Thi-Qar University, Thi-Qar, Iraq.

Orcid: 0000-0002-4749-8673

Abstract

Recently, biometric systems have been subjected to various attacks, making their security and integrity imperative. In this research, a robust and immune method was proposed against potential attacks on biometric data. The suggested method is to hide the minutiae of a person's fingerprint in the bit plane of a several randomly selected individual facial images by a particular key using BPCS steganography. The key used to select the host images is encrypted using the RSA algorithm. To compute the performance of the proposed scheme, different experiments were achieved with different biometric databases. The average PSNR of stego images shows low degradation. The PCA as a face recognition approach was adopted. The well known metrics; FAR, FRR, and Accuracy of the system are computed to facial images before and after fingerprint hiding. The results of the implementation of the proposed method proved its efficiency by hiding the fingerprint minutiae in host images in a safe manner. Also, the proposed method proved its ability in increasing the security of both the fingerprint minutiae and facial images.

Keywords: Biometric, BPCS Steganography, Fingerprint Minutiae, PCA, RSA.

INTRODUCTION

Steganography is the process of transmitting messages in a confidential manner so that the recipient is able to know the existence of the message to be transferred and ensures its confidentiality. Steganography is a form of data hiding. During the past two decades, there have been several steganography techniques that hide secret messages in multimedia objects. The main goal of steganography technique is to hide secret information (or message) inside other message (host object) in a way that makes the eavesdropper not expect or detect the second secret message [1], [2]. In general, when using the technique of hiding information, this information is not preserved in its original form, but is converted to an equivalent file of multimedia such as; audio, video, and image which is hidden within other object. This information is transmitted over the network and upon arrival to the recipient the secret information is extracted from the carrier medium. There are basic requirements for the process of hiding information depending on the user's application and needs; some of these requirements are [1]:

1. Immunity: hidden data should not be affected by the different stages of the embedding process.
2. Capability: maximum size of embedded data.
3. Key security: the key of steganography must be kept secret.

Steganography is different from cryptography. In encryption, the eavesdropper can analyze, modify, and re-sends the message without being able to breach the encryption algorithm. In Steganography, the eavesdropper does not expect a confidential message to exist in another message [3].

The most important weakness of data hiding systems is the effect it leaves on the carrier media, which makes the eavesdropper of the message which containing hidden information by observing the modification or change in this image, which leading him to expect there is a confidential information in those contacts [4], [5].

The main components of steganography as showed in Figure 1 are; cover-object (carrier), secret message, and password [1] A hidden message can represent text, image, video, or any important information.

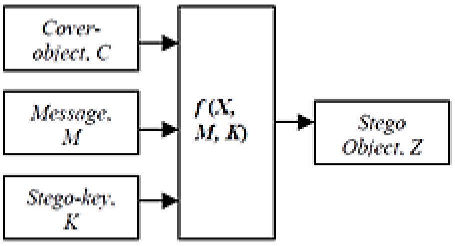


Figure 1. Basic Steganographic Model

The password is called stego- key which used by the sender and receiver to hide or retrieve the confidential message from the carrier medium. The carrier is called cover-object which takes different forms that may be text, image, audio or video. The stego -key with the secret embedded message is called stego-object. There are multiple carriers that are suitable for being a cover object. Yashpal Lather, et al 2015 [6] have reviewed in detail many of these carriers. Recently biometrics has been widely used both in cryptography and steganography after these biometric systems have been subjected to serious attacks. It became increasingly popular compared to traditional techniques such as identification cards (ID), passwords, etc [7]. One of the reasons for this popularity and widespread use is that they cannot be reproduced or shared. By using biometrics, the user has no need to memorize long and random passwords [8]. Furthermore, unlike the case of smart cards, identification cards as well as passwords those are subject to change or replaced if lost while not possible with biometrics [9]. Despite the advantages of biometrics, it has recently been subjected to serious attacks, which has reduced its security. Ratha et al. [8] analyzed the various attacks on the biometric templates and classified them into eight categories. Several modes have been proposed to protect biometric templates from potential attacks. Cryptography and steganography are among the techniques that employed for that purpose. In cryptographic systems, biometrics was used to achieve authenticity as well as to generate a cryptographic key or to bind a cryptographic key to a biometric template. In steganography, biometrics has been used to hide secret messages or other biometrics. In this paper new approach was suggested to hide fingerprint minutiae in multiple face images in order to decrease the degradation in the host images.

RELATED WORK

Several methods were used to hide biometric data into other biometric. This section presents a review to the methods closely related to the proposed method as follows:

Anil K. Jain and Umut Uludag 2003 [10] proposed an approach to increase the security of face images. A user can be authenticated by his image in addition to the fingerprints hidden in that image.

Saeid Fazli and Maryam Z. Nejad (2012) [11] proposed a novel watermarking approach to protect fingerprint minutiae. They used the DWT to hiding the minutiae data in face image of the same individual.

Sabah A. Gitaffa (2015) [12] proposed generating encryption key from two keys to encrypt fingerprint image, then embedding the encrypted image in a face image. The stego-face image can be used for biometric purposes.

Rohit Thanki and Komal Borisagar (2015) [13], the face image is used as a host medium and SVD as an application is applied to wavelet coefficients of the fourth level of the facial image and a single matrix is obtained to hide the watermark. Fingerprints are taken as a watermark. The degradation caused by this approach affected on accuracy of face recognition systems.

This paper, suggest a new approach to secure fingerprint template for a person by embedding fingerprint minutiae in multiple face images for that person before storing it in the multimodal biometric database that can be used to increase the security of authentication systems. Embedding minutiae in several images are done to reduce the degradation in face images that might be affecting on accuracy for face recognition system [13].

METHODOLOGY

In this section, we discuss several concepts needed for the proposed method.

Fingerprint Minutiae Extraction

Fingerprints have been used to identify persons extensively for many of the characteristics that are unique to these biometric from other biometrics such as iris and facial images. Fingerprints were characterized by many features such as; ease of use, low cost and high reliability. Various approaches are used to identify fingerprints, but the minutiae-based method is the most widely used. Detection of minutiae in fingerprint image as shown in Fig. 2 is described by a list of features that involves; location, direction, and types of minutiae [14].

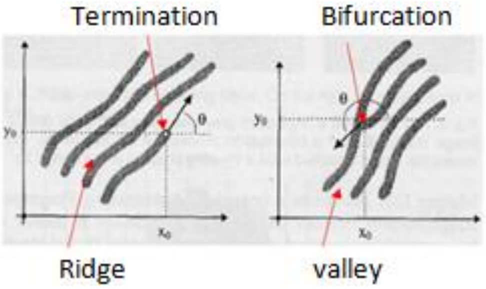


Figure 2. Types of minutiae

As shown in Figure 3, the minutiae extraction process was passed through the following stages.

A. Fingerprint Image Preprocessing

i. **Fingerprint Image Enhancement**: based on Short Time Fourier Transforms (STFT) analysis [15].

ii. **Fingerprint Image Binarization**: A global binarization based on the Otsu threshold method [16] is used.

iii. **Fingerprint Image Segmentation**: Segmentation is based on Only a Region of Interest (ROI) for each fingerprint image, and then the interested regions are recognized by two steps; firstly is the estimation of direction and variation to each block. Secondly; a well known operation "OPEN" and "CLOSE" as morphological operations are performed.

B. Minutiae Extraction

Minutiae are extracted by the following steps.

i. **Fingerprint Ridge Thinning**: Thinning is the procedure of decreasing the density (thickness) of each line of patterns to one pixel width. This is done using a morphological operation presented in [17].

ii. **Minutiae Marking**: In this step, fingerprint minutiae are detected and marked. The more accurate minutiae detection process yields to a better identification results.

C. False Minutia Removing*:* Sometimes the previous steps may lead to pseudo fingerprint minutiae and this type of minutiae should be removed according to the distances between them [18]. After implementing this procedure, each extracted minutiae will have position and direction, (x,y) and (θ) respectively.

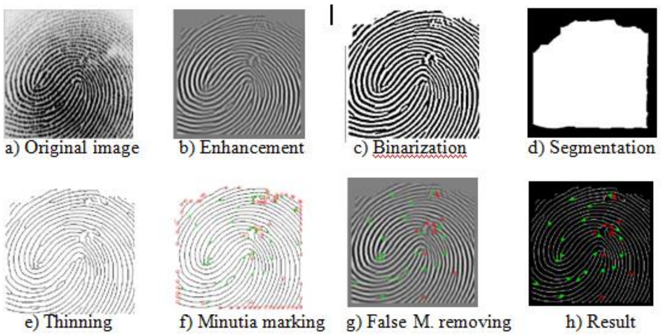


Figure 3. Minutiae extraction stages

BPCS Steganography

The Bit Plane Complexity Segmentation (BPCS) was proposed by Eiji Kawaguchi in 1997 [19]. In this method, the multi-valued image P, consisting of n bits pixel per plane, is decomposed into a set of n binary images, e.g. If P in gray mode, then n = 8 can be decomposed into P = [P_7 P_6 P_5 P_4 P_3 P_2 P_1 P_0] where P_7 is the Most Significant Bit (MSB) plane and P0 is the Least Significant Bit (LSB) plane. Each bit plane can be segmented into two regions; informative region consists of simple pattern, and a noisy region consists of complex pattern. In BPCS, each noisy region is replaced with another informative region without changing the quality of the image [20]. Regions that are not random are not modified [19]. Figure 4 shows an example of a bit plane slicing

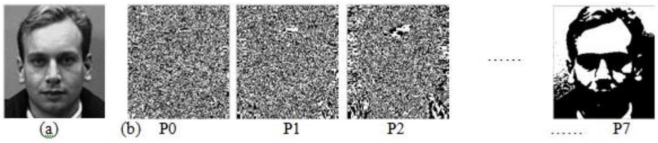


Figure 4. a) Original image, b) 8 bit planes

Each bit plane of an image can be represented by a set of bits corresponding to the locations of bits of binary number of each pixel in the image. The slicing of MxN image into n bit planes is given by [20]:

$$P_i = \{b_i \mid b_i \ \text{is the value of}\ i^{th}\ \text{bit position in}\ (b_{n-1} . b_{n-2} . \dots . b_0)\}^{M\times N}$$

$$\forall\ i = 0.1. \dots . n-1 \qquad (1)$$

A particular complexity parameter α is used to control whether a region is noisy or informative [19].

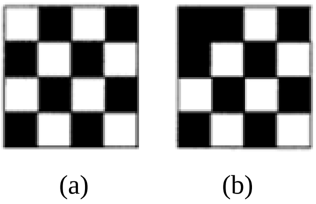


Figure 5. BPCS Image complexity measure

Image complexity is measured by the number of differences between adjacent bits. For example, look at Fig.5. In the first step, the bits in the first row are compared to the bits in the second row and the number of differ pairs is observed. In the same way, the bits in the second row are compared to the bits in the third row, and the bits in the third row are compared to the bits in the fourth row, and each time the differences are recorded. In the same way as compared to rows, the comparison is made vertically from the first column with the second column. So, the complexity of the image is defined as, the actual number of different adjacent pairs of bits divided by the total number of adjacent pairs of bits that may be different, so α will be in the interval [0, 1]. For Figure (5 b) α is:

$$\alpha = \frac{(3+4+4)+(3+4+4)}{24}$$

BPCS considers a block random if its complexity measure α has passed a certain threshold [19].

PROPOSED SCHEME

To realize the goals mentioned previously, this research propose a new approach to secure biometric data. This work suggests hiding fingerprint minutiae of a person in 8 face images of that person. First, select a secret key (key_1) consists of 8-bit. Then, the fingerprint data is hidden in face images that its index corresponds to key bits with value "1". The images that correspond to the bits with value "0" doesn't used.

For example: if the key_1=01011000, then the secret data must embed in the images that have indexes (1, 3, 4) only. Figure 6 explain the proposed algorithm in details.

A. Embedding Algorithm

Step1. Select 8 different face images of a person.

Step2. Select two secret keys, key_1 of 8 bits (sum (1's)≥2) and key_2 of 15 bits.

Step3. Select the face images that its indexes correspond to index of bits with value "1" in key_1.

Step4. Extract minutiae from fingerprint image of same person.

Step5. Convert minutiae data to binary matrix with dimensions M×32, where M is the number of the minutiae.

Step6. Divide the binary matrix into blocks, each with size 8×8 bits and randomize the blocks by an extended key using XOR.

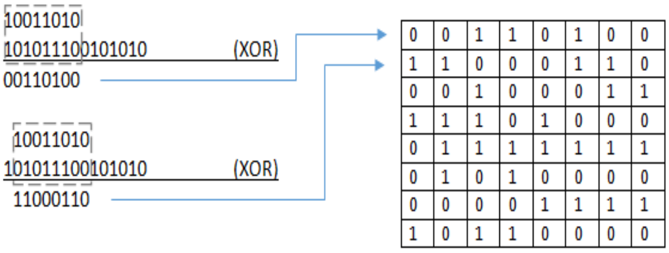
Step7. Compute N by dividing the number of blocks by the number of ones in key_1.

Step8. Distribute the blocks on the face images by embedding N blocks in second bit planes P_1 of selected image in step3 using BPCS steganography and leave other images without any change.

Step9. Encrypt key$_1$, key$_2$ and M using RSA algorithm and embed it in the first image using LSB technique.

The extended key can be derived using XOR between key$_1$ and key$_2$ in overlapping manner to produce 8×8 matrix.

For example, let Key$_1$=10011010 and Key2=101011100101010



0	0	1	1	0	1	0	0
1	1	0	0	0	1	1	0
0	0	1	0	0	0	1	1
1	1	1	0	1	0	0	0
0	1	1	1	1	1	1	1
0	1	0	1	0	0	0	0
0	0	0	0	1	1	1	1
1	0	1	1	0	0	0	0

In addition, the extended key should be used to select a starting point in each cover image and hide the secret data starting from that point. For example, if the index of cover image is (2), then we will start looking for random regions from the point I(i,j), where *i* and *j* are the decimal values of the row (2) and column (2) from the extended key respectively. In the example above, i=198 and j=92. The columns of binary minutiae matrix were 32 bits after converting the (x,y,θ) to binary form by allocating (8,8,16) bits to them respectively.The result of this procedure is 8 stego images that can be stored in a database to be used in identity recognition using PCA or other analytical face recognition method without affecting on accuracy. If we recognize an identity through the face, then we need to ensure that the recognized face is actually for this identity by matching his/her fingerprint with fingerprint minutiae hidden in the recognized class.

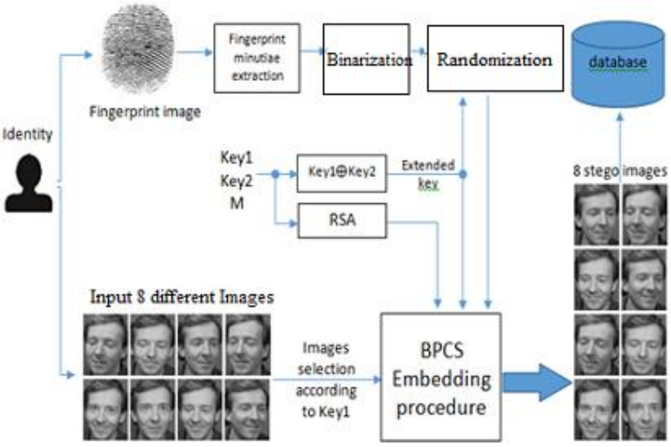


Figure 6. Block diagram of embedding fingerprint minutiae

B. Extraction Algorithm

The steps of extraction algorithm as shown in Figure 7 are:

Step1: Extract the encrypted keys from first image and decrypt it using RSA.

Step2: Select face images according to Key$_1$.

Step3: Extract fingerprint minutiae matrix (M×32) from the selected images using BPCS technique.

Step4: De-randomize minutiae matrix using extended key.

Step5: Convert the binary minutiae matrix to decimal form.

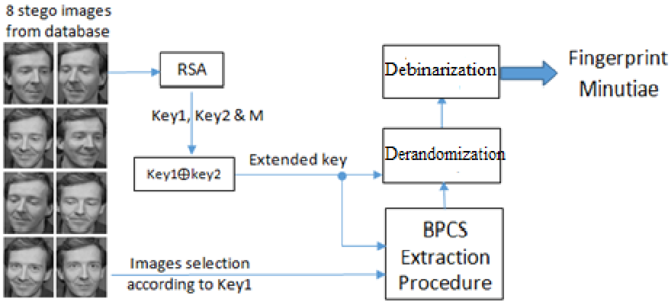

8 stego images from database
RSA
Key1, Key2 & M
Key1⊕key2
Extended key
Images selection according to Key1
Debinarization
Derandomization
BPCS Extraction Procedure
Fingerprint Minutiae

Figure 7. Block diagram of extraction fingerprint minutiae

EXPERIMENTAL RESULTS

The proposed method was implemented using MATLAB R2013a. It was tested using images from AT&T database, Faces94 database, Faces96 database and Yale database for face images. The fingerprint images were acquired from several databases and attached to faces images arbitrarily. This is done because no actual data were available and no foundation agreed to grant us actual data of its members for privacy and secrecy reasons. The size of fingerprint images was 256×256. Face images size shown in Table (4). The experimental results carried out with 40 persons each person with 10 facial images and just single fingerprint, two images are used as testing images for all enrolled and not enrolled individuals. In RSA cryptosystem we used (32881, 3) as public key and (32881, 33) as a private key. The average time of extracting and hiding fingerprint minutiae was 5.9 seconds. The extracting time of hidden data was 0.1 second in average. Principal Component Analysis (PCA) was the face recognition method used in this test and implemented two times; one before embedding fingerprint minutiae and the other after. In both experiments, some of the performance metrics like accuracy, False Acceptance Ratio (FAR), False Rejection Ratio (FRR) are calculated using the following formulas [21].

$$Recognition\ Rate \ = \frac{Number\ of\ Persons\ Correctly\ Recognized}{Total\ Number\ of\ Trials} \tag{2}$$

$$FAR = \frac{Number\ of\ Unauthorized\ persons\ recognized\ as\ authorized\ person}{Total\ number\ of\ Unauthorized\ Trials} \tag{3}$$

$$FRR = \frac{Number\ of\ Authorized\ persons\ recognized\ as\ Unauthorized\ persons}{Total\ number\ of\ Authorized\ Trials} \quad (4)$$

These metrics was computed in cases of key persistence and key alteration as shown in the tables below.

Table 1. Face recognition statistics before embedding fingerprint

DB	No. of training images	No. of testing images		Accuracy %	FAR %	FRR %
		Enrolled	Not enrolled			
Faces94	320	80	40	100	0	0
Faces96	104	26	14	90.4	0	19.2
AT&T	240	60	20	85	10	20
Yale	88	22	8	82.4	12.5	22.7

Table 2. Face recognition statistics after embedding fingerprint with key persistence (01010011)

DB	No. of training images	No. of testing images		Accuracy %	FAR %	FRR %
		Enrolled	Not enrolled			
Faces94	320	80	40	100	0	0
Faces96	104	26	14	90.4	0	19.2
AT&T	240	60	20	85	10	20
Yale	88	22	8	82.4	12.5	22.7

Table 3: Face recognition statistics after embedding with key alteration

DB	No. of training images	No. of testing images		Accuracy %	FAR %	FRR %
		Enrolled	Not enrolled			
Faces94	320	80	40	100	0	0
Faces96	104	26	14	90.4	0	19.2
AT&T	240	60	20	85	10	20
Yale	88	22	8	82.4	12.5	22.7

Also, PSNR of cover images was computed to determine the amount of degradation after hiding fingerprint minutiae. PSNR was computed by the following formula [12].

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad dB \quad where \quad MSE = \frac{1}{[N \times N]^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[C(i.j) - S(i.j)]^2 \quad (5)$$

Table 4. PSNR for different numbers of stego-images after embedding 36×32 bits minutiae matrix

DB	Image Size	No. of images/ PSNR averages						
		2	3	4	5	6	7	8
AT&T	112×92	57.6	59.1	60.3	61.3	62.2	62.5	62.7
Faces94	200×180	63	64.6	65.8	66.5	67.5	67.8	68.3
Faces96	196×196	63.3	65.2	65.9	66.9	68	68	68.2
Yale	320×243	66.4	68.2	68.9	69.9	70.5	71.3	71.4

CONCLUSIONS

Biometric security is a vital and promising technology, but the challenges faced by these biometrics have slowed their development. In this research, a method was proposed to hide the fingerprint minutiae of a particular person in the bit plane domain of multiple facial images for that person. The performance of the suggested method has been proved through the difficulties in detection the random secret data among big amount of random cover data without using the extended key. The values of PSNR, FAR, FRR and accuracy after hiding data in the stego-images show that the degradation was very little and not affect on the system work. The proposed work can be developed to hide other biometric data, such as iris data in addition to fingerprint minutiae to introduce robust multimodal biometric system.

REFERENCES

[1] Arup Kumar Bhaumik, et al, "Data Hiding in Video", International Journal of Database Theory and Application, June 2009.

[2] K. A. Navas and M. Sasikumar, "Image Fidelity Metrics: Future Directions", IETE Technical review, Vol 28, Issue 1, Jan-Feb , 2011.

[3] Abdullah M. A. A. Ja'far ,"Audio Hiding In Audio Files by Using Low-Bit Encoding ", Informatics Institute for Postgraduate Studies M.Sc thesis, Baghdad, Iraq,, (2003).

[4] Provos N., "Probabilistic Methods for Improving Information Hiding", Center for Information Technology Integration, University of Michigan, USA, January 31, 2001.

[5] Polpitiya D. and W. J. Khan, "Information Hiding in Audio Files with Encryption", Washington University, USA, Version 1.0, 2001.

[6] Yashpal Lather, *et al,"* Review Paper on Steganography Techniques", International Journal of Computer Science

and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 571-576

[7] Arun Ross and Anil K. Jain, "Human Recognition Using Biometrics: An Overview", Annals of Telecommunications vol. 62, No 1/2, PP. 11-35, Jan/Feb 2007.

[8] N.K. Ratha, J.H. Connell and R.M. Bolle, “An analysis of minutiae matching strength”, Proc. 3rd AVBPA, Halmstad, Sweden, June 2001, pp. 223-228.

[9] Manvjeet Kaur, et al, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 22 2008.

[10] Anil K. Jain and Umut Uludag, "Hiding Fingerprint Minutiae in Images", 3115 Engineering Building, East Lansing, MI, 48824, USA, 2003.

[11] Saeid Fazli and Maryam Z. Nejad, "An Improved Watermarking Algorithm for Hiding Biometric Data", International Journal of Science and Engineering Investigations, Iran, vol. 1, issue 2, March 2012.

[12] Sabah A. Gitaffa, "Implementation of Hiding Secured Fingerprint in Face Image for Biometric Application", Journal of Engineering and Development, Baghdad, Iraq Vol. 20, No.1, January 2016.

[13] Rohit Thanki and Komal Borisagar, " Multibiometric Template Security Using CS Theory – SVD Based Fragile Watermarking Technique", WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, India, Volume 12, 2015.

[14] Vikram Singh and Kalpna Kashyap, "A SURVEY PAPER ON HYBRID SYSTEM FOR FINGER PRINT INDENTIFICATION", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 1, Issue 4, November – December 2012.

[15] Sharat Chikkerur, Alexander N. Cartwright and Venu Govindaraju, "Fingerprint enhancement using STFT analysis", The Journal of Pattern Recognition Society, USA, 40 (2007) 198 – 211.

[16] Otsu, N., "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 9, No. 1, 1979, pp. 62-66.

[17] Lam, L., Seong-Whan Lee, and Ching Y. Suen, "Thinning Methodologies-A Comprehensive Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 14, No. 9, September 1992, page 879, bottom of first column through top of second column.

[18] Manvjeet Kaur, et al, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 22 2008.

[19] David Salomon, "Data Privacy and Security", Library of Congress Cataloging-in-Publication Data, Springer-Verlag New York, 2003.

[20] Souvik Bhattacharyya, et al, "A Robust Image Steganography Method Using PMM in Bit Plane Domain", World Academy of Science, Engineering and Technology, Vol. 8, No. 9, 2014.

[21] Jyouti Malik, et al, "Reference Threshold Calculation for Biometric Authentication", Modern Education and Computer Science, India, 2014, 2, 46-53.