Efficient Approach for Image Encryption Using Key Matrix Generation from Combined Fingerprint Images for Two Level Security

Dr. Sheshang D. Degadwala
Head of Computer Department,
Sigma Institute of Engineering,
Vadodara, Gujarat, India.

Arpana D. Mahajan
Asst. Prof. Computer Department,
Sigma Institute of Engineering,
Vadodara, Gujarat, India.

Megha D. Randeri
M.E. Student, Computer Engineering Department, SIE,
Vadodara, Gujarat, India.

***Abstract*— In recent Era, Security has been most important issue to be considered with different forward looking and preventing measures. Several cryptographic algorithms are developed for encryption and decryption using a secret key. The issue with this strategy is that user ought to recall the key or store the key in a database, which make the framework under danger. Once the put away key is bargained, at that point an attacker can get to the private information effectively. To maintain uniqueness of key, a biometric feature such as fingerprint can be used, whereas randomness can be induced using different combinations of fingerprints. In this paper, we propose a technique to generate the key matrix by extracting minutiae points from the combined minutiae template of fingerprints of the sender and receiver. This system contains four phases. One is Enrolment Phase, second is Authentication Phase, third is Key Generation phase and last is Cryptographic phase. For encryption of the original image using generated key matrix, we use Hill cipher.**

Keywords*— *Fingerprints, Minutiae Points, Cryptography, Hill Cipher.

I. INTRODUCTION

As of late, the advance in the correspondence innovations is bringing about exchange of data in the openly shared media. To secure these, there is a huge intrigue appeared by the researchers in the cryptographic area prompting numerous creative and productive encryption strategies. Each encryption technique needs to utilize secure keys. The cryptographic keys might be an arbitrary number or password. There are different techniques to produce such keys; a few strategies are proposed to create cryptographic keys from the biometric for example, iris, fingerprints, signature and so forth as in [1, 3, 4, 5]. There is a critical development in the field of biometric innovations in recent years, and many of them are deployed according to the specific application and their acceptability to the users. Fingerprints have been utilized for over a century and are the most generally utilized type of biometric recognizable proof. This unique mark of an individual is interesting and stays unaltered over a person's lifetime. On a finger, the unique patterns formed by the ridges make up fingerprints. A valley is the area between two consecutive ridges. Among various minutiae types, the ridge endings and bifurcations are utilized commonly. Ridge endings are point where the ridge terminates and bifurcation are points where a single ridge divides into two ridges. In this paper, we propose a new technique of encrypting an image using key matrix, which is generated from mixed fingerprints of sender and receiver. The proposed technique has four phases namely: Enrolment phase, Authentication phase, Key Generation phase and Cryptographic phase. In enrolment phase, the fingerprints of both sender and receiver are acquired and stored on the server along with identification key generated from their minutiae points. In authentication phase, the sender's given fingerprint and the fingerprint stored on the server is compared. If the matching score is within threshold value, the authentication is successful. If authentication is successfully completed, the sender generates mixed fingerprint image from his/her own fingerprint and receiver's finger print from server. Then in Key generation phase, cryptographic key matrix is generated from the combined minutiae templates of sender's and receiver's fingerprint images. Here we will generate 8x8 self-invertible key matrix. Finally in cryptographic phase, the original image is converted into 256x256 matrix form and divided into 8x8 sub matrices. Each sub matrix is encrypted using Hill cipher with previously generated key matrix. Encrypted image is created by combining each encrypted sub matrix in same order.

Fig 1: Identification Key Generation

II. METHODOLOGY

A. Fingerprint Image Enhancement

First, the fingerprint image is selected from the NIST Biometric Fingerprint dataset. Image Enhancement is needed to reduce the noise in the fingerprint image and make it clearer. This is achieved using filters like Median filter, Weiner or Gabor filter. Then Median filtering is a nonlinear filtering, which can protect the edge of the image.

B. Histogram Equalization

The first histogram of the original fingerprint image is of the bimodal type, the histogram after equalization involves the range from 0 to 255 and perception impact is upgraded.

C. Fingerprint Image Binarization

The procedure to get a binary image from a given greyscale image is called Binarization. It makes clear the differentiation between the ridges and valleys, so that minutiae extraction is encouraged. Binarization results in a binary image having ridges as foreground and valleys as background.

D. Thinning

Thinning is the way toward lessening the thickness of each line of ridges to a single pixel. The prerequisites of a thinning algorithm are A) The thinned fingerprint image ought to be of single pixel width without any disruptions. B) Each ridge ought to be as thin as its middle pixel. C) Wipe out noise and singular pixels. D) No further evacuation of pixels ought to be conceivable after thinning procedure.

E. Minutiae Extraction

The vast majority of the finger-scan technologies depend on Minutiae. Minutiae-based systems speak to the fingerprint by its features like terminations and bifurcations. The Crossing Number (CN) strategy is utilized for minutiae extraction. By analysing the neighbourhood of each ridge pixel utilizing 3x3 window, the ridge endings and bifurcations are removed. For a ridge pixel P the crossing number CN is calculated as

$$CN = 0.5 \sum_{i=0}^{9} |P_i - (P_{i+1})| \, , P_9 = P_1 \quad (1)$$

Where P_i is the pixel value in the neighbourhood of P [5].
Minutiae are described in three co-ordinate system as (x,y,θ). In the first place, all x co-ordinates, y co-ordinates and θ co-ordinates are added independently. The resultant average values of X and Y co-ordinates are in decimal and the co-ordinate θ is in radian.
Step 1: The binary values XBi, YBi and θBi of Xi, Yi and θi for given i^{th} minutiae are taken.
Step 2: In order as follows, all the binary values are merged.
MBi= X Location (9bits) + X Location (9bits) + angle (3 bits)
Step 3: the merged binary string MBi is converted to decimal for obtaining the single coordinate value M1i.

F. Cryptographic Key Matrix Genenration from Combined Fingerprints

The fingerprints of sender and receiver are taken. The minutiae points from sender's finger print image (FP1) and minutiae points from the receiver's finger print image (FP2) are combined to form a combine minutiae template using vector concatenation operation. This generated combined minutiae template is used to generate 8x8 self-invertible cryptographic key matrix using key generation algorithm.

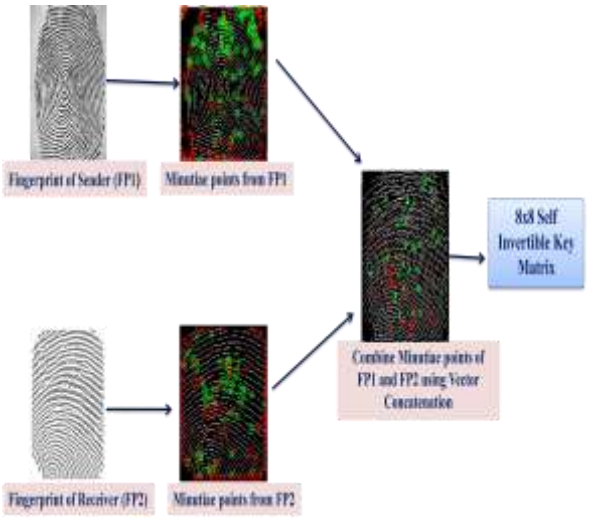

Fig 2: Combined Minutiae Template

G. Performance Parameters

- *ENTROPY:*
  It measures the degree of randomness and depends on the probability of pixel values.
  $$E = \sum_{x=0}^{255} [P(x) X \log_2(\frac{1}{P(x)})] \quad (2)$$

- *Unified Average Changing Intensity (UACI):*
  The difference between the original image and the ciphered image is measured by UACI. It is used to access the strength of the encryption algorithm.
  $$UACI = \frac{1}{256 \times 256} \sum_{i=1}^{256} \sum_{j=1}^{256} \frac{|Aij - Bij|}{255} \times 100\% \quad (3)$$

- *Mean Square Error (MSE):*
  MSE is used to measure the distortion (Difference) between the original cover image and the decrypted image.
  $$MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (X_{j,k} - X'_{j,k})^2 \quad (4)$$

- *Peak Signal to Noise Ration (PSNR):*
  The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a decrypted image. Higher PSNR means the better quality of the decrypted image.
  $$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (5)$$

III. PROPOSED SYSTEM

Proposed work deals about image encryption using self-invertible key matrix generated from mixed minutiae points from biometric fingerprints for Hill cipher.

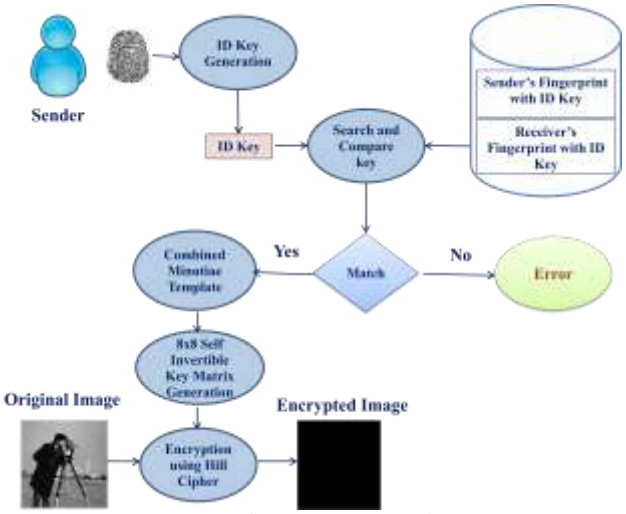

Fig. 3 shows the overall view of encryption process for Grayscale as well as RGB images.

A. *Encryption Algorithm*

Step 1: Input the original image.
Step 2: Convert the original image into 256x256 matrix format.
Step 3: Divide the 256x256 image into 8x8 sub matrices segments.
Step 4: Generate 8x8 self-invertible key matrix using key matrix generation algorithm.
Step 5: Encrypt each 8x8 sub matrix of image using generated key matrix using Hill Cipher.
Step 6: Combine each encrypted sub matrices to generate final encrypted image.
Step 7: Stop.

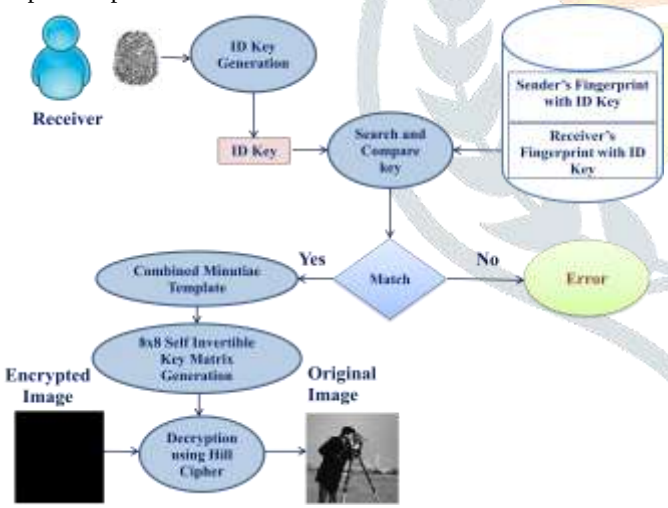

Fig 4: Decryption Process

B. *Decryption Algorithm*

Step 1: Input Encrypted Image.
Step 2: Receiver is authenticated by his/her own fingerprint image.
Step 3: Convert encrypted image into 256 x 256 matrix form.
Step 4: Divide encrypted image into segments of 8 x 8 sub matrix.
Step 5: Generate 8 x 8 self-invertible key matrix by using above key matrix generation algorithm.
Step 6: Decrypt each sub matrix using Hill Cipher algorithm using 8x8 self-invertible key matrix.
Step 7: Recover the original image by combining each decrypted sub matrix in same order.
Step 8: Stop.

IV. EXPERIMENTAL RESULTS

The proposed system is implemented in Matlab and various Grayscale and RGB images inbuilt in Matalb have been taken for experiments. For fingerprint images, NIST Biometric Fingerprint dataset has been used.

EXPERIMENT 1:
To compare time elapsed for encrypting RGB image using Hill Cipher for different size of key matrix.

From the chart in Figure 5, it is concluded that time required for encrypting RGB image using Hill cipher is lesser for 8x8 matrix than 4x4 matrix. So in proposed system, from 4x4 matrix generated from minutiae points are converted in 8x8 self-invertible matrix.

TABLE 1: Experiment 1

RGB Images	Time Elapsed in Seconds	
	4x4 Key Matrix	8x8 Key Matrix
Airplane .bmp	0.923	0.503
Baboon.bmp	0.822	0.488
Lighthouse.bmp	0.804	0.499
Lena.bmp	0.812	0.479
Peppers.bmp	0.815	0.495
Boat.bmp	0.907	0.496
St Stephen.bmp	0.827	0.507

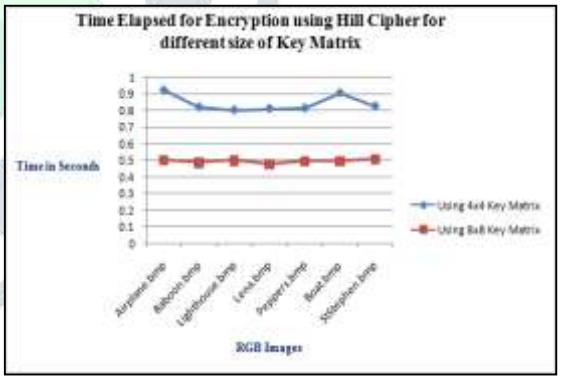

Fig 5: Time Elapsed for Different Size of Key Matrix

EXPERIMENT 2:
To compare ENTROPY for encrypted images in proposed system for both Grayscale and RGB images.

TABLE 2: Experiment 2

Images	ENTROPY for Grayscale Images	ENTROPY for RGB Images
Airplane .bmp	7.99	7.631
Baboon.bmp	7.996	7.621
Lighthouse.bmp	7.996	7.631
Lena.bmp	7.994	7.62
Peppers.bmp	7.995	7.643
Boat.bmp	7.994	7.657
St Stephen.bmp	7.753	7.861

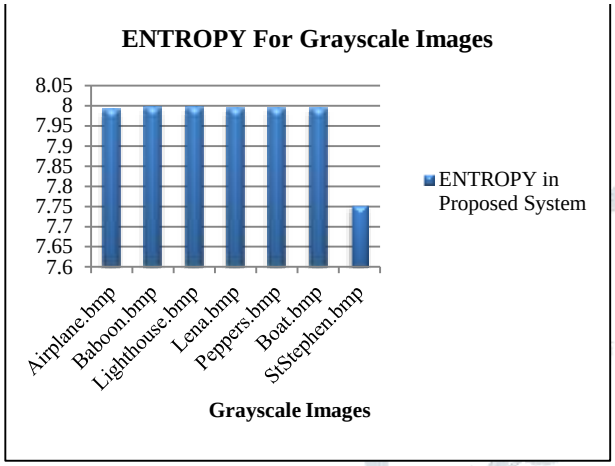

Fig 6: ENTROPY for Grayscale Images

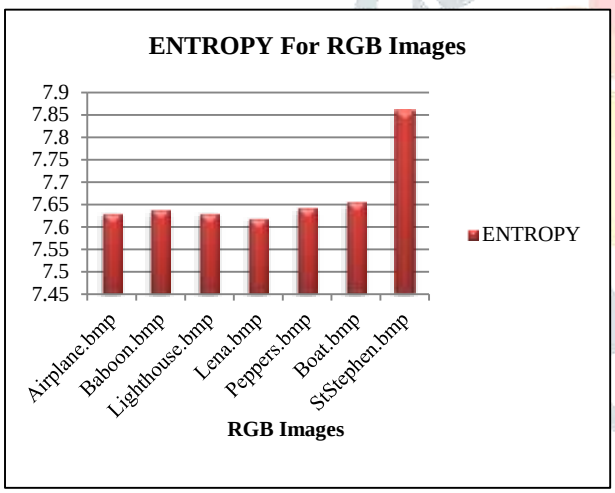

Fig 7: ENTROPY for RGB Images

From the charts in Figure 6 and Figure 7, it is concluded that in proposed system ENTROPY for Grayscale images are closer to standard value 8 than RGB images.

EXPERIMENT 3:

To compare UACI values between the original image and encrypted image for both Grayscale and RGB images.

TABLE 3: Experiment 3

Images	UACI for Grayscale Images	UACI for RGB Images
Airplane .bmp	32.48	27.853
Baboon.bmp	26.96	20.022
Lighthouse.bmp	28.408	21.476
Lena.bmp	28.593	21.758
Peppers.bmp	29.547	23.05
Boat.bmp	26.659	22.698
St Stephen.bmp	31.629	26.861

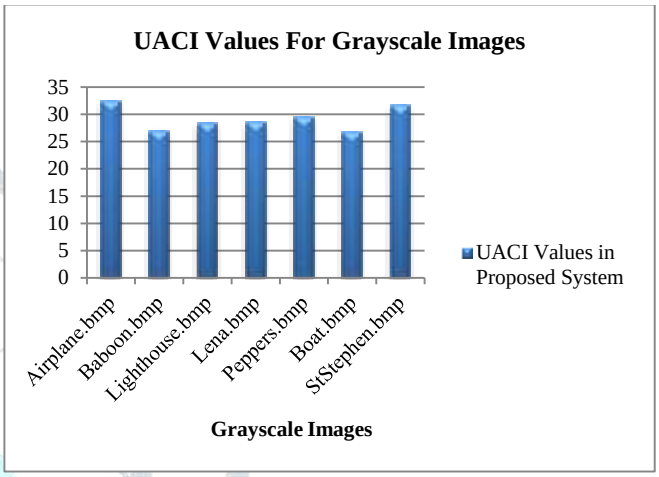

Fig 8: UACI for Grayscale Images

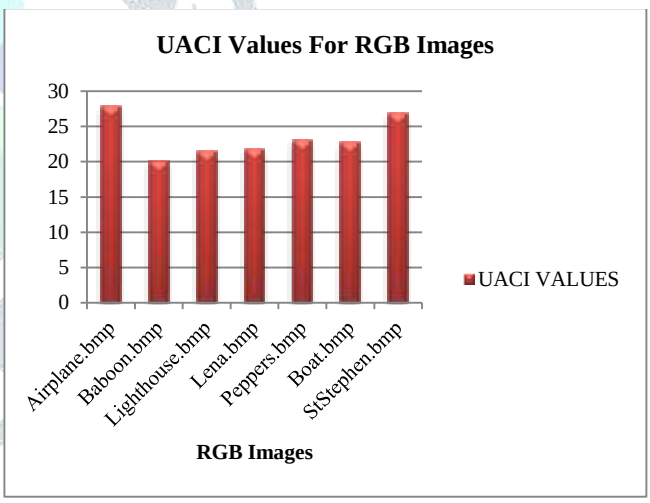

Fig 9: UACI for RGB Images

From the charts in Figure 8 and Figure 9, it is concluded that UACI values in proposed system are near to its standard value 33 for Grayscale images. For RGB images also the results is good enough.

V. CONCLUSION

Hereby it is concluded that we can use a novel approach for providing two level security using biometric fingerprint to the images being transferred in an open world. First the sender is verified by its fingerprint and identification key stored on the secure server and then 8x8 self-invertible key matrix is generated by extracting minutiae points from the fingerprint images of both sender and receiver. Using the generated secured key matrix, the original image is encrypted using Hill Cipher and sent to the receiver. The receiver decrypts the image in a same manner after authentication. The proposed

system ensures the strength of the encryption by Unified Average Changing Intensity (UACI) and also speeds up the encryption process by taking 8x8 self-invertible key matrix.

REFERENCES

[1] Dawahdeh Z.E., Yaakob, S.N., Razif bin Othman, R., *"A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher"*, Journal of King Saud University Computer and Information Sciences (2017).

[2] Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, *"Fingerprint-based crypto-biometric system for Network security"*, EURASIP Journal on Information Security, Springer (2015).

[3] Panduranga H T, Naveen Kumar S K, *"Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique",* International Journal of Computer Applications (0975 – 8887) Volume 60– No.16, December 2012.

[4] M.Marimuthu, A.Kannammal, *"Dual Fingerprints Fusion for Cryptographic Key Generation"*, International Journal of Computer Applications, volume 122, July 2015.

[5] Sharda Singh, Dr. J. A. Laxminarayana, *"RSA Key Generation Using Combination of Fingerprints"*, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, (AETM'15).

[6] Mrs. Afreen Fatima Mohammed, *"Biometric Based Authentication Using Two-Stage Fingerprint Privacy Protection for File Storage on Server"*, IJCSMC, Vol. 5, Issue. 3, March 2016, pg.377 – 387

[7] Mofeed Turky Rashid, Huda Ameer Zaki, *"RSA Cryptographic Key Generation Using Fingerprint Minutiae"*, Iraqi Journal for Computers and Informatics(IJCI), volume 1, issue 1, 2014.

[8] Goutham L, Mahendra M S, Manasa A P, Mr. Prajwalasimha S N, *"Modified Hill Cipher Based Image Encryption Technique"*, (IJRASET), Volume 5 Issue IV, April 2017.

[9] Gang Zheng, Wanqing Li, Ce Zhan, "*Cryptographic Key Generation from Biometric Data using Lattice Mapping",* International Conference on Pattern Recognition, IEEE, 2006.

[10] N. Lalithamani, Dr. K.P. Soman, "*An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancellable Fingerprints Biometrics".* International Conference on Advances in Recent technologies in Communication and Computing, IEEE, 2009.

[11] G. Patel, G. Panchal, "*A Chaff-point Based Approach for Cancellable Template Generation of Fingerprint Data",* Springer International Publishing, ICTIS, 2017.

[12] R. K. Jangid, Noor Mohmmad, A, Didel, S. Taterh, "*Hybrid Approach of Image Encryption using DNA cryptography and TF Hill Cipher Algorithm",* International Conference on Communication and Signal Processing, IEEE, 2014.

[13] P. L. Sharma, M. Rehan, "*On Securtiy of Hill Cipher using Finite Fields*", International Journal of Computer Application, volume 71, May 2013.

[14] F. Abundiz-Perez, C. Cruz-Hernandez, M. A. Murillo-Escobar, R. M. Lopez-Gutierrez, A. Arellano-Delagado, *"A Fingerprint Image Encryption Scheme based on Hyperchaotic Rossler Map"*, Hindawi, volume 2016.

[15] N. H. Barnouti, *"Fingerprint Recognition Improvement Using Histogram Equalization and Compression Methods"*, International Journal of Engineering Research and General Science, volume 4, issue 2, April 2016.

[16] Cryptography www.cryptographyworld.com/concept.htm

[17] R. K. Nichols, "*ICSA Guide to Cryptography",* McGraw-Hill, chapter 22.

[18] B. K. Sy, A. P. Kumara Krishnan, "*New Trends and Developments in Biometrics",* INTECH publisher, pp 191-218.

[19] R. K. Sharma, *"Generation of Biometric Key for Use in DES"*, IJCSI International Journal of Computer Science Issues, 9(6), 2012, 312-315.

[20] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil K.Jain, *"Biometric Cryptosystems Issues and Challenges"*, Proceedings of the IEEE, 92(6), 2004, 948-960.

[21] Abhishek Nagar, *"Designing Biometrics-based Cryptosystem"*, Post-Graduate diss, Department of Mathematics, IIT Delhi- May 2006.

[22] Pankaj Bhowmik, Kishor Bhowmik, Mohammad Nurul Azam, Mohammad Wahiduzzaman Rony, "*Fingerprint Image Enhancement and It's Feature Extraction for Recognition",* International Journal of Scientific & Technology Research (IJSTR), volume 1, issue 5, June 2012.

[23] Preeti Poonia, Praveen Kantha, *"Comparative Study of Various Substitution and Transposition Encryption Techniques",* International Journal of Computer Applications, volume 145 – No 10, July 2016.

[24] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigraphy, *"Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm",* International Journal of Security, volume 1 – issue (1), page 14-21.