DOI: http://doi.org/10.32792/utq.jceps.09.02.29

Proposed Biometric-Based Cryptographic Key Generation

Kadhim H. Kuban[1], *Rasha Basim Al-Khafaji*[2]

[1,2] Computer Science Dept., College Of Education For Pure Science, Thi-Qar University, Thi-Qar, Iraq.

Received 07/4/2019, Accepted 29/4/2019, Published 02/06/2019

Abstract:

The need for information security and privacy is increasing in recent times. Since several valuable data and files are stored in an organization server system and moreover personal information are being shared in WWW, the need for providing security and permitting only the authorized user is becoming indispensable. The effectiveness and the flexibility of the cryptographic key generation schemes make it suitable for integrating it with the biometric features (Biometric cryptosystems) . This work propose an efficient approach based on multimodal biometrics Face and Fingerprint for generation of secure cryptographic key.

Keywords: Biometric , Biometric cryptosystems , Multimodal , Face , Fingerprint, Cryptographic Key , SVD, Gabor filters.

1-Introduction

A biometric is a science and it defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being [1]. Information security and privacy has become an important factor in the present world. Biometric recognition is one of the most important techniques for the security privacy due to its distinctive nature of biometric traits [2]. The biometric techniques are relates to the parts of human body which are unique, cannot be stolen and is not easily transferable compared to traditional methods such as Identification badges, Personal Identification Number (PIN), password, smartcards etc.. The commonly used biometric features include speech, fingerprint, face, Iris, voice, hand geometry, retinal identification, and body odor identification [3]. There are two types of biometric systems: unimodal and multimodal. Unimodal systems employ single biometric sample, such as face or fingerprint. Multimodal systems employ two or more modalities, such as face and fingerprint. Using two or more modalities increases recognition accuracy, strengthens the proof as data is acquired from different sources [4] .

In this research work , we generation the cryptographic key from biometric features by combining multiple biometric modalities . The key is generated by extract the feature from face and fingerprint by using SVD and Gabor filter.

2- Related work

Many researches are available for generating cryptographic keys from biometric modalities and multimodal biometrics based user authentication. A great deal of attention have been received on developing approaches for cryptographic key generation from biometric features and authenticating users by combining multiple biometric modalities. A review of some recent researches is presented here.

B. Chen and V. Chandran [5] have presented a technique that produces deterministic bit-sequences from the output of a repetitive one-way transform via entropy based feature extraction process coupled with Reed-Solomon error correcting codes. The technique was evaluated by means of a 3D face data and was thus confirmed to be reliable in key generations of suitable length for 128-bit Advanced Encryption Standard (AES). Muhammad Khurram Khana et. al.[6] suggested a novel multi- models biometrics authentication system on space limited tokens using face and fingerprint modalities . Combining biometrics and cryptography is found to be a promising solution, at the same time biometric encryption system must be acceptable only when it can consider a minute change in the selection of similar biometric modalities during the time of generating decisive keys . M. Nageshkumar et al. [7] have presented an authentication method utilizing two features i.e. face and palmprint for multimodal biometric system identification. The robustness of the person authentication has been enhanced by the combination of both palmprint and face features. The final evaluation was made by fusion at matching score level architecture where features vectors were created autonomously for query measures and afterwards these are assessed to the enrolment template, which were stored during database preparation. Multimodal biometric system was stretched out via fusion of face and palmprint recognition . Feature level fusion of fingerprint and iris is suggested by A.Jagadeesan et al. [8] for cryptographic key generation. Fingerprint and iris are preprocessed and values are generated and stored for fingerprint x and y coordinate values as two vectors and iris vice versa. With the help of permutation, shuffling values are interchanged finally cryptographic key is generated for encrypting the message . According to Selvarani et. al.[9] the data from the cloud is accessed by the secret key which is wrapped by the two different biometric modalities viz. Fingerprint and the Iris for decryption. Only after decryption the user gets the original message. Thus the user secures their data from unauthorized access.

3-Theortical Background

This section discusses background of the study , particularly Singular Value Decomposition (SVD) , Gabor filters and then using Elliptic curve to generated a key.

3.1 Singular Value Decomposition (SVD)

The Singular Value Decomposition (SVD) is a factorization of a real or complex matrix . SVD is effective compared to other linear approximation techniques. It has many practical and theoretical applications like scientific computing, signal processing, automatic control along with image compression [10] . The main idea of the SVD is that it can be performed on any real m × n matrix. It factorizes matrix A into three matrices U, S and V , as follow:

$$A = USV^T \qquad (1)$$

$$A=[u_1\ldots\ldots u_r\ldots\ldots u_m]\begin{bmatrix} \sigma_1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & \sigma_r & & \\ & & & & \cdot & \\ & & & & & \cdot \\ & & & & & & 0 \end{bmatrix}\begin{bmatrix} V_1{}^T \\ \cdot \\ \cdot \\ V_r{}^T \\ \cdot \\ \cdot \\ V_n{}^T \end{bmatrix} \qquad (2)$$

Where :-

U is m × m orthogonal matrix .

S is m × n matrix with singular values on the diagonal.

V is n × n orthogonal matrix

Where U is a left singular matrix and V is the right singular matrix and S is a diagonal matrix [11].

3.2 Gabor filters

The Gabor filters were originally introduced by Dennis Gabor (Gabor, 1946). They have been used widely in image analysis due to their nature of frequency characteristic, spatial locality and orientation selectivity [12] . The 2-D Gabor function in the spatial domain can be defined as follow :

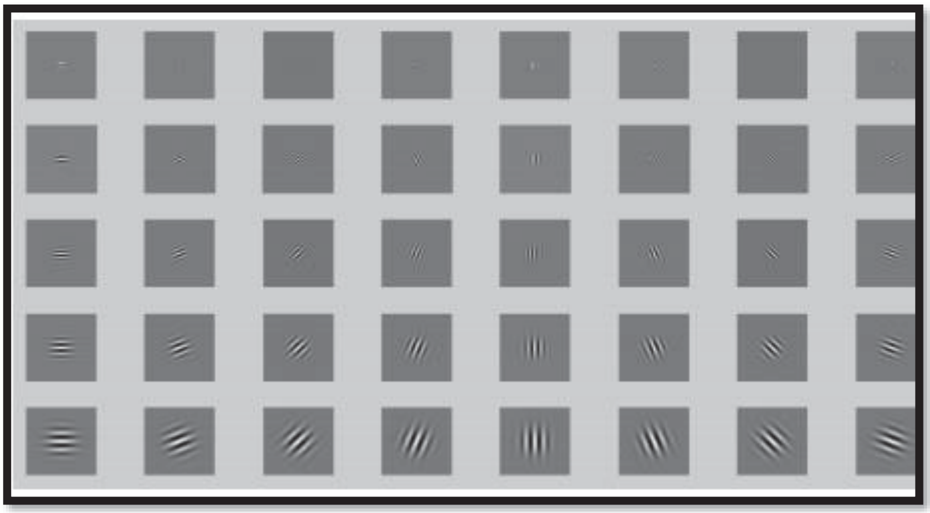
$$\varphi_{u,v}(x,y)=\frac{f_u^2}{\pi\gamma n}\,e^{-\left(\frac{f^2}{y^2}x'^{\,2}+\frac{f^2}{y^2}y'^{2}\right)}e^{-j2\pi f u x'} \qquad (3)$$

The parameters of the $\varphi_{u,v}(x,y)$ are defined as follow :

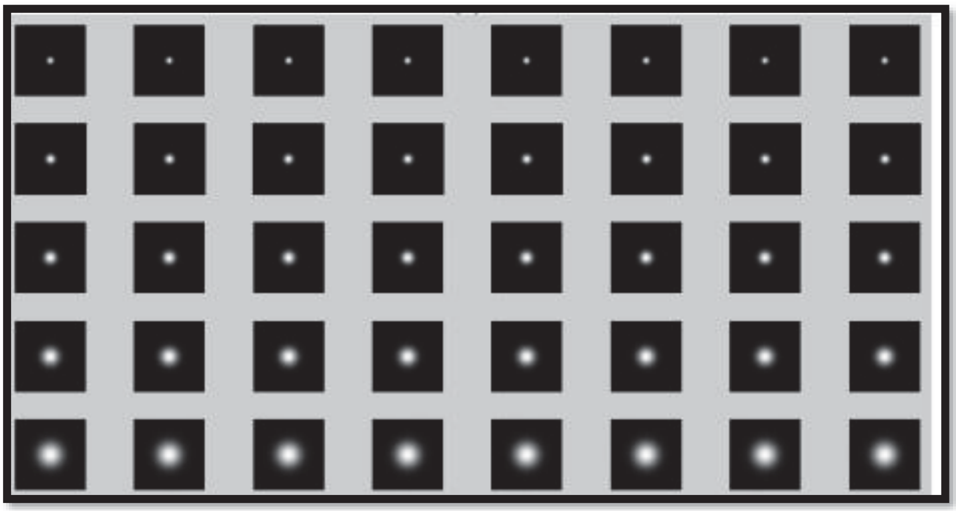
$$x' = x\cos\theta_v + y\, sin\theta_v \qquad (4)$$

$$y' = -x\sin\theta_v + y\cos\theta_v \qquad (5)$$

Where u defines as the scale of the Gabor filters . Gabor filters with 5 scales (u=0,….,4) and 8 orientations (v=0,….,7) . The real parts and the magnitude responses of Gabor filters with 5 scales and 8 orientations are shown in Figure (1) (a) and (b).



(a)



(b)

Figure (1) : (a) Real Parts (b) Magnitude Responses of Gabor wavelets with 5 scales and 8 orientations [13]

Gabor facial feature is extracted from an image through convolution between facial image and Gabor wavelets as defined as follow :

$$Gu,v\ (x,y)=I(x,y)*\varphi u,v(x,y) \qquad (6)$$

Where $I(x,y)$ represent grey-scale face image ,$\varphi u,v(x,y)$ represent the Gabor wavelets and convolution is denoted by $*$ operator [13] .

3.3 Elliptic Curves Diffie-Hellman

Elliptic curve suggested by Victor S.Miller in 1997 gives solutions to many issues in providing high security by finding the curves whose group orders are divisible by a small prime in order to provide a fast algorithm . Elliptic Curve Cryptography is a public-key cryptography system , in which a key pair is a public key and a private key . In ECC we call these predefined constants as Domain Parameters . the equation of the elliptic curves is [14] :

$$y^2 = x^3 + ax + b \qquad (7)$$

4- The proposed system :

The steps involved in the proposed system are :-

a- Feature extraction from face .
b- Feature extraction from fingerprint .
c- Merge the face features and fingerprint features .
d- Generation of cryptographic key from merge features .

As shown in Figure (2) the block diagram of proposed system in (training and testing).

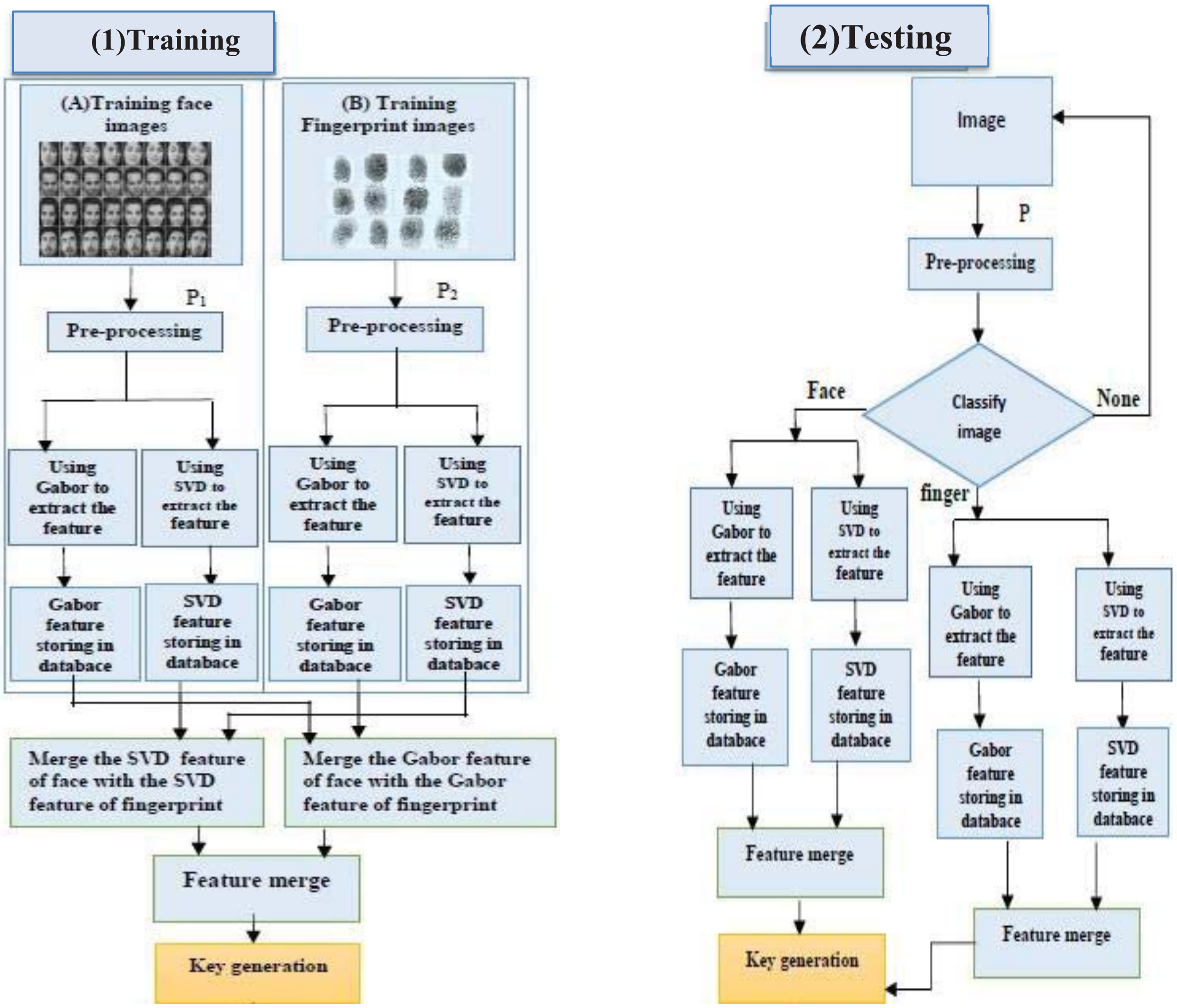

(1)Training
(A)Training face images
(B) Training Fingerprint images
P1
P2
Pre-processing
Pre-processing
Using Gabor to extract the feature
Using SVD to extract the feature
Using Gabor to extract the feature
Using SVD to extract the feature
Gabor feature storing in database
SVD feature storing in database
Gabor feature storing in database
SVD feature storing in database
Merge the SVD feature of face with the SVD feature of fingerprint
Merge the Gabor feature of face with the Gabor feature of fingerprint
Feature merge
Key generation
(2)Testing
Image
P
Pre-processing
Classify image
Face
None
finger
Using Gabor to extract the feature
Using SVD to extract the feature
Gabor feature storing in database
SVD feature storing in database
Feature merge
Key generation
Using Gabor to extract the feature
Using SVD to extract the feature
Gabor feature storing in database
SVD feature storing in database
Feature merge

Figure (2) the block diagram of proposed system

In order to implement our proposed system, there are several steps that need to be taken to implement the previous scheme in practice It includes the following :

Step1: image read

The images are read from the file, whether the images of the face or images of the fingerprints here the system uses different types of images .

Step2: Pre-processing

Pre-processing processes on the face images and fingerprints images include the following :

(A) Pre-processing steps on face images :

a- change the size of the face images to the size of 256×256 to the purpose of facilitating calculations.

b- Convert the color face images to grayscale.

c- Convert the face images into double type.

(B) Pre-processing steps on fingerprints images :

a- Change the size of the fingerprints images to the size of 256×256 to the purpose of facilitating calculations .
b- Convert the color fingerprints images to grayscale.
c- Convert the fingerprints images to double type .
d- Inverse black white and vice versa .
e- Delete background .
f-Find the edges .
g- Find the important part of the fingerprint .

Step3 : Classify images

The processed image is classified as a face image or a fingerprint image through compute the discrete wavelet transform (dwt) .

Step4:- Features extraction

(A) Using SVD to extract the feature from image
a- Pre-Processing for SVD to extract the feature
b- Calculate the mean of images
c- Reshape the mean image array into (256×256)
d- Compute SVD .
e- Select first U_{colu} and select first V_{colu}
f- Calculate feature extraction
g- Elect the active features

(B) Features extraction by Gabor filter
a- Pre-Processing for Gabor Features Extraction
b- Calculate Average of Gabor filter
c- compute magnitudes of Gabor-filtered image
d- Calculate the dawn sampling
e- Calculate feature vector and elect the active feature .

Key generation using Elliptic-Curve Diff-Hellman

Step One :- Select two numbers (a ,b) // where $((4a^3 + 27b^2) \bmod p \neq 0)$
Step Two :- Find the set of points (G) on the elliptic curve //according to equation (7)
Step Four :- Calculate distance of each point into G from the origin point (0,0) in domain .
Step Five :- Generate key (P_m) by find the nearest distance to each value of feature and replace it by the point

5- Experiments results and analysis

The proposed system was implemented in MATLAB (R2014b) . The performance of proposed system has been implemented and evaluated by selecting Face94 database for face and FVC2000 database for fingerprint .

5.1 Experiment One: using Face94 database

A set of images was used in the training process and testing process of the face94 database ,where 260 images were used for training and testing purposes. These images were divided into Set , where Set 1 , Set2 , Set3 …… Set26 for face Each group contains 5 training images and 3 images for testing . The table (1)

are display the experiments performed on the Face94 database and the results obtained. Through the experiments conducted on all set of training and testing images obtained the recognition rate from the proposed method is a higher than the recognition rate when using single SVD and single Gabor approach. The mean recognition rates of SVD , Gabor, and Proposed methods are 95.40%, 90.44 % and 98.7**%** respectively with Euclidean distance classification method
for every training set and the corresponding testing set, the accuracy of proposed method is higher than single Gabor and single SVD .

Table (1): Recognition results on Face94 database

Classification Method	Experiment performed on	Method		
		Gabor	SVD	Proposed method
Euclidean Distance	Set1	84.48	94.14	98.85
	Set2	90.15	95.22	99.22
	Set3	82.23	95.35	98.88
	Set4	86	96.45	98.91
	Set5	89.12	95.3	99.42
	Set6	88.29	95.41	99.51
	Set7	92.08	96.8	98.75
	Set8	95.50	98.21	98.5
	Set9	92	98.3	98.3
	Set10	94.2	95	99.7
	Set11	92.51	94.5	98.62
	Set12	88.5	95.23	98.25
	Set13	90.14	93.12	97.5
	Set14	93.5	97.20	99.3
	Set15	92.51	96.35	98.75
	Set16	92.60	95	98.51
	Set17	91.65	94.13	98.8
	Set18	92.15	95	97.65
	Set19	89.14	97.4	98.85
	Set20	91.50	97.19	99.47
	Set21	90	95.3	99.32
	Set22	88.75	95	98.66
	Set23	92.51	95.5	98.21
	Set24	93.5	95.3	97.5
	Set25	89.77	95.33	98.53
	Set26	91.89	97.2	99.92
	Mean Accuracy(%)	**90.44**	**95.40**	**98.7**

5.2 Experiment Two :using FVC 2000 database:

A set of images was used in the training process and testing process of the FVC2000 database ,where 80 images were used for training and testing purposes. These images were divided into Set , where Setf1 , Setf2 , Setf3 …… Setf26 for fingerprint each group contains 5 training images and 3 images for testing. The table (2) are display the experiments performed on the FVC2000 database and the results obtained. Through the experiments conducted on all set of training and testing images obtained the recognition rate from the proposed method is a higher than the recognition rate when using single SVD and single Gabor approach.The mean recognition rates of SVD , Gabor and Proposed methods are 83.57%, 86.95% and **98.5%** respectively with Euclidean distance classification method for every training set and the corresponding testing set, the accuracy of proposed method is superior than single Gabor and single SVD .

Table (2): Recognition results FVC2000 database

Classification Method	Experiment performed on	Method		
		Gabor	SVD	Proposed method
Euclidean Distance	Setf1	84	77.6	98.23
	Setf2	87.56	79.71	99.82
	Setf3	85.26	81.32	97.88
	Setf4	86.75	84.3	99
	Setf5	83.12	81.32	98
	Setf6	85.27	84.41	97.65
	Setf7	87.08	85.8	97.86
	Setf8	89.54	86.24	98.56
	Setf9	87.23	85.13	98.3
	Setf10	87.12	82.21	98.87
	Setf11	84.76	81.15	98.22
	Setf12	89.55	85.23	99.19
	Setf13	86.26	83.73	97.85
	Setf14	89.27	81.25	98.4
	Setf15	85.51	84.75	97.75
	Setf16	85.17	83.22	98.51
	Setf17	88.65	82.17	98.26
	Setf18	85.34	81.67	99.25
	Setf19	88.28	86.56	98.11
	Setf20	87.29	82.73	99.23
	Setf21	85.33	81.8	99.46
	Setf22	87.75	85.38	99.45
	Setf23	88.32	85.5	99.42
	Setf24	89.25	87.35	98.18
	Setf25	87.45	85.83	98.63
	Setf26	89.78	86.52	98.42
	MeanAccuracy(%)	**86.95**	**83.57**	**98.51**

5.3 Face and Fingerprint Based Key Generation:

After we extracted the features from faces and fingerprints. The second part of Proposed system consist of generation key (512-bit) from these features . The key is generated from the images stored in the database after the extraction of the features them and during enrollment , the key is generated from the second input images and compare the key in the second input with the key in enrollment . If the key matches in the second input with the key in the enrolment then it say that the person is authorized . The example about key generation shown in table (3) .

Table (3) : The Key generation from face and fingerprint verified.

Sample	Key Generation

Person1	729 729 -729 132 132 359 -729 713 710 -729 729 -729 729
	746 746 -746 147 147 601 -746 710 553 -746 746 -746 746
	-729 194 729 -729 729 729 -132 -194 278 0 0 194 132
	-746 227 746 -746 746 746 -147 -227 416 0 0 227 147
	132 132 132 8 132 132 132 132 250
	147 147 147 98 147 147 147 147 312

Person2	729 729 -729 -729 710 250 -729 359 -132 -729 508 -554 729
	746 746 -746 -746 553 312 -746 601 -147 -746 618 -228 746
	-508 278 729 -729 0 -729 0 -194 278 713 132 554 0
	-618 416 746 -746 0 -746 0 -227 416 710 147 228 0
	132 278 132 194 194 132 710 729 250
	147 416 147 227 227 147 553 746 312

Person3	729 729 -729 -729 729 -729 -729 729 -729 -729 729 -729 729
	746 746 -746 -746 746 -746 -746 746 -746 -746 746 -746 746
	-729 729 729 -729 729 729 -278 508 278 8 0 -8 8
	-746 746 746 -746 746 746 -416 618 416 98 0 -98 98
	8 8 132 194 194 132 0 0 132
	98 98 147 227 227 147 0 0 147

6- Performance evaluation

The performance of such system is evaluated using the data in confusion matrix . A confusion matrix associated with a classifier shows the predicted and actual classification . it composed of four cases : True positive (TP) , True negative (TN) , False positive (FP) , False negative (FN) . The prediction accuracy and classification error can be obtained from this matrix as follows [15] :

$$Ac = \frac{TP+TN}{TP+TN+FP+FN} \qquad (8)$$

7- Conclusion

In this paper, we have attempted to generate a secure cryptographic key by using multiple biometrics modalities of human being, so as to provide better security. An efficient approach for generation of secure cryptographic key based on multimodal biometrics (face and fingerprint) has been presented in this paper

. Firstly, the features have been extracted from the face and fingerprint images respectively. Then, the extracted features have been combined together at the feature level to obtain the multi-biometric template. Lastly, a 512-bit secure cryptographic key has been generated from the multi-biometric template . The experimental results have demonstrated the efficiency of the proposed approach to produce user-specific strong cryptographic keys.

References:

[1] M.Marimuthu , A.Kannammal ,” Dual Fingerprints Fusion for Cryptographic Key Generation“, International Journal of Computer Applications, Volume 122 , No.23, July 2015 .

[2] Mr.P.Balakumar , Dr.R.Venkatesan , “ A Survey on Biometrics based Cryptographic Key Generation Schemes “ , International Journal of Computer Science and Information Technology & Security , Vol. 2, No. 1, 2012 .

[3] Gokulakumar.A.S , et al., “Encryption of Cryptographic key technique by crossover of Iris and Face Biometric key “ , International Journal of Innovative Research in Computer and Communication

[4] Saad Abuguba , et al.,” An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level “ International Journal of Computer Science and Network Security ,Vol.15 , No. 6 , June 2015.

[5] A. Jagadeesan , et al,. “ Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature “ , International Journal of Computer Applications ,Volume 2 , No.6, June 2010.

[6] Muhammad Khurram Khana and Jiashu Zhanga, "Multimodal face and fingerprint biometrics authentication on space-limited tokens ", Neurocomputing, volume:71, no. 13-15, pp.3026-3031, August 2008.

[7] Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy, “An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image”, International Journal of Computer Science Issues, Vol. 2, 2009.

[8] A.Jagadeesan Dr. K.Duraiswamy, “Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris” , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[9] Selvarani et.al., “Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Higher Security”, Research Journal of Applied Sciences, Engineering and Technology 11(1): 95-101, 2015 .

[10] Rehna. V. J and Jeyakumar. M. K, “ Singular Value Decomposition Based Image Coding for Achieving Additional Compression to JPEG Images” , 2012 .

[11] Lijie Cao , “ Singular Value Decomposition Applied To Digital Image Processing “ .

[12] Urszula Marmol , “USE OF GABOR FILTERS FOR TEXTURE CLASSIFICATION OF AIRBORNE IMAGES AND LIDAR DATA “ , Vol.:22 , 2011 .

[13] Lim Song Li and Norashikin Yahya , “Face Recognition Technique using Gabor Wavelets and Singular Value Decomposition (SVD) “ ,November , 2014 .

[14] G. Mary Amirtha Sagayee, S Arumugam and S. Anandha Mala ,” Biometric Encryption using Elliptic Curve “ , Vol. 2, No. 5, October 2011 .

[15] CONFUSION MATRIX, FROM HTTPS://CLASSEVAL.WORDPRESS.COM/INTRODUCTION/BASIC-EVALUATION-MEASURES 2016 [ONLINE].