# Secure Cryptographic System using Face Biometrics

**Shital V Bhalke[1] Dr S.A Angadi[2]**
[1,2]Department of Computer Science & Engineering
[1,2]Belagavi, Karnataka 590018, India

*Abstract*— Face biometric approach can be applied for a wide variety of problems for individual identification and verification. This leads to identification of persons based on their physiological and behavioral traits. Users cannot easily remember complex and long cryptographic keys, in this approach users need not remember the keys, and the keys cannot be easily stolen or cracked by attackers as they are lacking sufficient knowledge of biometric features. In this paper we propose powerful method based on face biometrics. The main objective is to increase the security in communication of information on internet, as with increase in use of internet information security is becoming more and more important. This proposed system uses graph representation based on face feature extraction and its further use in secret key generation for implementing the DES algorithm. This proposed system uses face image as an input from the publically available database and locates total 13 landmark points on image and construct fully connected graph considering landmark points as nodes, 64-bit sub key is generated using Eigen vector of adjacency matrix as seed from graph. Encryption of the information is performed using 64-bit key same method is employed for decryption using DES algorithm.

***Key words:*** Biometric, Cryptographic Key, Landmark Points, Information Security

## I. INTRODUCTION

A broad research area in "computer vision" is focused on facial feature recognition. This area of study has many applications in security, as we can use facial recognition as a form of biometric identification which is then combined with cryptography for secure communication of information.

Biometric is a widely used methods of recognizing persons in relation to their "physiological or behavioral" characteristic. Among those measurable characteristics are face, fingerprints, hand geometry, handwriting, signatures, iris, retinal, vein, and voice. Now a day's biometric technologies are becoming base for a large array of strongly and highly secure authentication and personal verification solutions methods. This technology is becoming important day by day as the level of attackers like security breaches, intruders and transaction fraud increases.

Sensors are the devices that are commonly used for collecting biometrics using which we can acquire the data and it converts data into digital form for recognition. Sensors can be digital cameras which are used for face recognition, telephones which are used for voice recognition. Those devices used for recognition must have high quality as it has greater impact on recognition results.

Key generation based on biometrics requires extracting a cryptographic key from biometric template which represents individual distinct and unique features signifying data achieved from a biometric sample. Not all biometric devices are template based. For example, voice recognition is based on "models." Biometric templates are compared in a biometric recognition system; templates can be changed between vendors as well as biometric modalities.

Biometric-based solutions provide privacy of personal data and confidentiality in financial transactions. The need for biometrics based authentication can be found in many applications like "military, workstation, commercial applications, remote access to resources, enterprise-wide network security infrastructures, government IDs, applications logon, secure electronic banking, domain access, investing and other financial transactions and retail sales are already benefiting from these technologies." The healthy growth of global economy depends on faith in this electronic transaction.

It can be utilized alone or it can also be integrated with technologies such as encryption/decryption keys, digital signatures and smart cards to provide all aspects which are required in our daily lives. The current methods like utilization of "complex passwords and PINs" are not considerably exact methods than as personal authentication using biometrics which is more accurate.

The reason behind this is that the passwords can be easily hacked or cracked by an attackers, no need to remember passwords(convenient),provides audit trail and is becoming cost effective and socially acceptable.

Cryptography is the study of generating in secret code; in data and telecommunications, cryptography is essential when communicating over any untrusted medium". There are various methods for communication of information on internet. Securing the information plays an important role on internet, the generally used method to provide security is done by encryption and decryption of the information by using cryptographic keys.

The plaintext or original message that is to be sent through an untrusted medium is encrypted using a secret code before sending it over the medium. The encrypted message which is in unreadable form is known as cipher text; at the other end of the medium where receiver receives encrypted message is decrypted to get back the original message or plaintext.

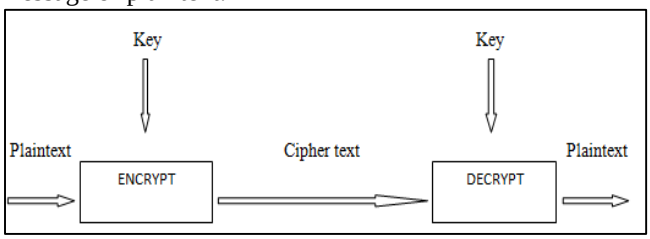


Fig. 1: Simple Cryptographic System

Generally there are two Cryptographic schemes that are used are:

Symmetric or secret key cryptography (for encryption and decryption it uses same key) - Symmetric key cryptography is useful when we want to encrypt files on own computer and intend to decrypt them ourselves. As "key distribution" is problem in this case it is less useful if we need to send keys to second party to be decrypted. Communicating encryption key securely to corresponding

 

user is not much easy than communication of the original text in secure manner. DES (Data Encryption Standard) is most commonly used symmetric cryptosystem. Symmetric key system is simpler and faster but main problem is that both sender and receiver must know how to exchange the keys in secure way; this study focuses on symmetric cryptography (DES).

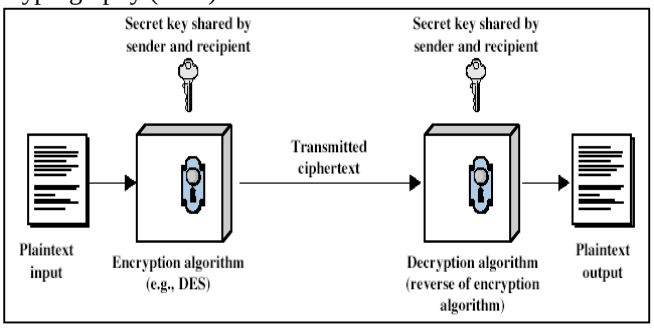


Fig. 2: Symmetric Cryptographic System

Asymmetric or public key cryptography (for encryption and decryption it uses different keys) in. This case it has two related key-pair (public and private key). A public key is known to everyone as it is public so that whoever wants to send a message can send using public key. A second key is kept secret so that only receiver knows it which is private key. Any type of message including text, binary files, or documents can be encrypted using the public key of receiver and it can be decrypted by using the same algorithm but with the help of private key that is matching to public key or it can also be done in vice-versa. And these two cryptographic systems must provide Security requirements like Authentication, Integrity, Non-repudiation, Privacy (Confidentiality).

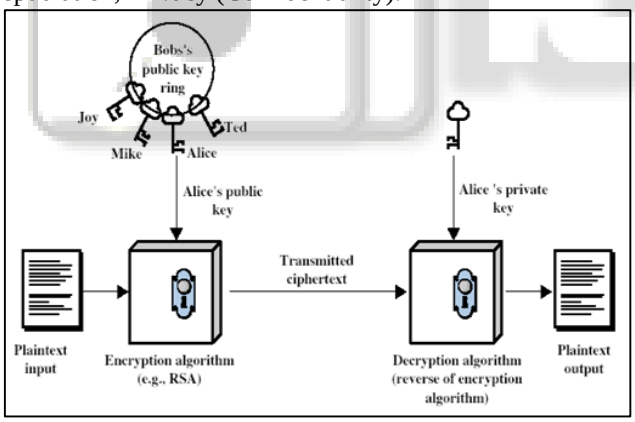


Fig. 3: Asymmetric Cryptographic System

Biometric cryptosystems integrates strengths of biometric and cryptography, cryptography provides greater and manageable security levels, biometrics provides high authenticity and removes need to remember passwords and can be used for both authentication and for encryption. It is considerably enough strong to create, copy and in sharing.

## II. RELATED WORK

Proposed work is inspired from many of research work on biocryptosystem techniques. It explains verity of references that discuses many concepts which are related to cryptographic based on biometrics.

Mr.P.Balakumar and Dr.R.Venkatesan [1] - have proposed the system where first the features are extracted from Fingerprint and Iris, in case of fingerprints it points minute locations in Cartesian co-ordinate system and iris feature are extracted by applying morphological operations on obtained iris texture. Fusion algorithm fuses those extracted features by taking input as feature vectors; it involves shuffling of individual feature vectors, concatenation of shuffled vectors and merging of concatenated shuffled vectors. Finally k-bit biometric key is generated from biometric template vector. Final key generated is very difficult to theft as it uses combined features. Using False Rejection Rate (FRR) and False Acceptance Rate (FAR) proposed system is tested and it can be observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique.

Raikoti Sharanabasappa1 and Sanjaypande M. B [2] - Have presented the system that uses face biometrics and propose biocrptography. From the face image 128 bit Principal component analysis (PCA) feature vector at encryption and decryption stage is extracted, by thresholding then binary vector is obtained. It makes use of Freed Solomon algorithm to generate error correction code (ECC) and DES algorithm to encrypt/decrypt message using biokeys. Distinct bits are to be selected from biokeys and are saved in a lookup table. Using biokeys and ECC a final key is obtained which is used by DES algorithm. Proposed scheme is tested by using ORL face database.

Margarita Osadchy, Benny Pinks [3] - This study introduces SCiFI system; this system acquires face images of individuals in public places by camera which is called client machine. It runs face recognition algorithm in secure way so that it does not reveals privacy and confidentiality and compares faces with database of registered faces weather the acquired images matches one of the suspect which are stored in server, if not then it does not reveals information to any party. In specific applications of SCiFI decreases privacy of camera based surveillance.

Priyanka.M [6] et al - have proposed system that uses sessions, totally 24 colour images are used on hourly basis. In key generation phase it considers pixel values of images into three channels red, green and blue and those values are stored in array size of "pxq" where p and q are resolution of images, finally the key is generated from pixel values. In encryption phase the sender of the message uses RC5 algorithm which takes input key ,as it works on hourly basis encryption done on nth hour considers nth image in the database and send it to the receiver along with the session log which contains time at which message has been encrypted and for decryption it refers to the session log to generate the decryption key from the particular image. The generated key need not be stored; it can be generated anywhere using image and session. This system is easy to implement and complex for cracking.

Raikoti Sharanabasappa1 and Sanjaypande M. B [8] – This proposes "a unique security architecture" where face features and its corresponding templates are used as the key for document security. A framework requires users to register their face instances to the system. Those instances stored in system are used for training purpose. In encryption phase for encryption of message when user selects folder all files within this are encrypted with previously stored templates of the user face instances. In decryption phase it requires verification of user through face instance and

 

template generated here is used for decryption of encrypted files. It uses "Rinjdal method" for the cryptographic structure. Using camera images are acquired in real time and face part is "segmented based on skin segmentation". For further face recognition Eigen face based template are generated and matching is carried out. That leads to noteworthy low FAR in comparison to FRR and performance is improved in encryption process and recognition rate.

## III. PROBLEM DEFINITION

Face recognition based cryptographic systems have huge applications including information security, secret message transfer. In this proposed system we planned to address the issue of extracting face features for generation of secret key, which will be employed for encryption of information using the DES algorithm. It is also planned to employ graph representation of the face image for representing the unique and repeatable features of the face which will be used for generation of the key for encryption and decryption.

## IV. SYSTEM DESIGN

System design of "Secure cryptographic system using face biometrics" describes about appearance of proposed system to the end users and gives explanation about features of its segments.

Proposed system uses one image as input for encryption of plaintext message that generates encryption key of 64-bit length and image with different expressions of same person can be used to decrypt the plaintext as it also generate same key of 64-bit length as shown in above figure. Proposed system uses DES (Data Encryption Standard) algorithm for encryption and decryption as shown in following figure.

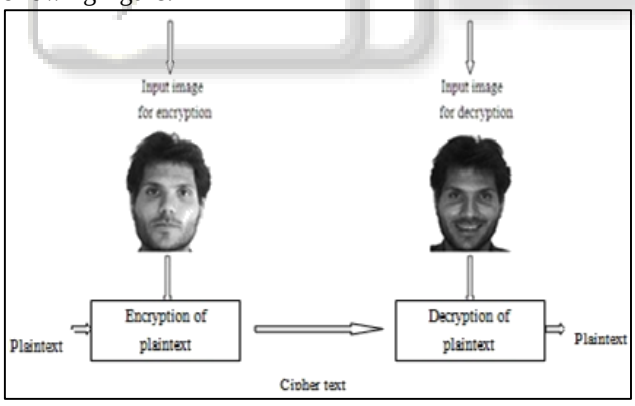


Fig. 4: System Architecture of "Secure Cryptographic System Using Face Biometrics"

Proposed system has following 5 stages.

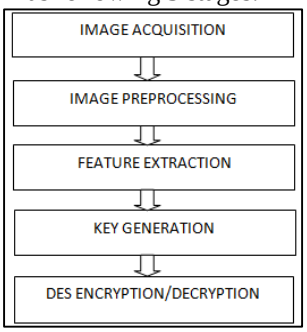


Fig. 5: Block Diagram of Proposed System

### A. *Image Acquisition*

Images are generally acquired from digital camera are stored in facial databases. But in this system we are using publically available database named "Aleix face database", which contains total of 4000 face images of 126 peoples with different facial expressions. Images are stored in JPG format and are gray scale images.

### B. *Image Preprocessing*

In this module images from the databases are resized according to the requirement and unwanted part of it is removed. The General purpose of the preprocessing module is to reduce variations in face due to illumination. So that the performance of the system improves in order to recognize them. The preprocessing is important as the strength of face recognition highly depends on it. In some cases colored images are to be converted to gray scale images to extract features easily.

### C. *Feature Extraction*

In feature extraction module using "vision.CascadeObjectDetector" method landmark points on face regions like eyes, nose and lips are to be located and 4 other boundary points also located. Totally it locates 13 landmark points on face image shown as follows.

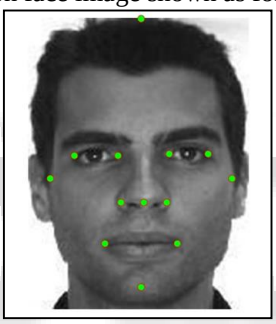

Fig. 6: Located Landmark Points

From the located points it constructs fully connected graph which contains edge from each point to each point and calculate distance between each two points using Euclidian distance formula. As shown in following figure

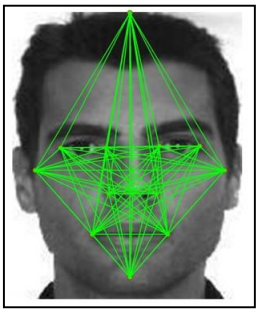

Fig. 7: Fully Connected Graph

Euclidean distance between two points A(x1, y1) and B(x2, y2) is calculated by using following formula. Where (x1, y1) and (x2, y2) are co-ordinates of points A and B respectively.

$$d = \text{Sqrt}((x1-x2)\ ^2+ (y1-y2)\ ^2).$$

Calculated values using Euclidean distance formula are stored in form of adjacency matrix of size 13*13.And finally 13 Eigen values from adjacency matrix is obtained; those obtained values are used as feature vector in feature extraction module.

 

### *D. Key Generation*

Feature vector from feature extraction module is used to generate 64-bit key. Here we have extracted those 13 Eigen values as a seed for generation of cryptographic key and converted to binary 64-bit number; this generated 64-bit binary number is used as key.

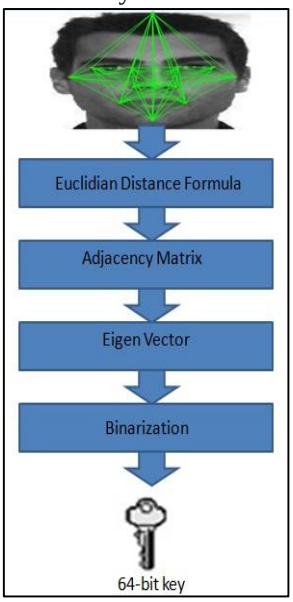


Fig. 8: Flow of key generation method

### *E. DES Encryption/Decryption*

Encryption and decryption of a given plaintext document is carried out by using 64-bit key generated from key generation module giving both plaintext and key as input to DES algorithm.

### *F. DES (Data Encryption Standard)*

Data encryption standard has been developed as a cryptographic standard for general use by public. It is symmetric or secretes key cryptography designed with following objectives in mind.

- High level of security
- Cryptographic security do not depend on algorithm secrecy
- Economical hardware implantation
- Exportable
- Efficient (high data rate)
- Completely specified and easy to implement
- Adaptable to diverse application
- Can be validated

To encrypt plaintext many of encryption/decryption algorithm makes use of substitution and permutation techniques. Where substitution maps one value to another and permutation does reordering of input bits positions. These techniques are used in 16 rounds of DES algorithm, as many as rounds are there it will be more secure. Encryption of the plaintext is infeasible to attackers as A non-linearity is introduced, it is feasible to the user with its secrete key. Infeasibility is achieved by using S-boxes where output from these are smaller than the input or input can be smaller than output. Main problems with symmetric key cryptography are key distribution.

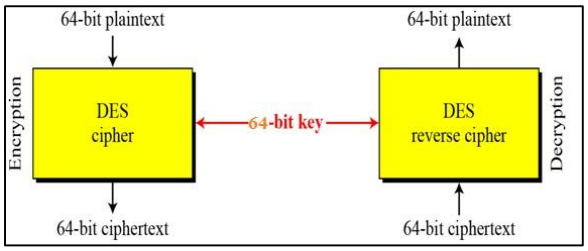


Fig. 9: Encryption and decryption with DES

## V. TESTING AND ANALYSIS

Proposed system "Secure cryptographic system using face biometrics" has been tested for face images of different persons under different facial expressions that are in frontal view. It can be applied only to the frontal view images as we are taking boundary points. Totally 100 images are used for testing purpose of 10 different users as per requirement. Each folder contains 10 images of same persons that are selected as per requirement. Among all those it is working correctly for 86 images which generates same repeatable 64-bit key that can be used for encryption/decryption of messages using DES algorithm securely with repeatability percentage is about 86%.

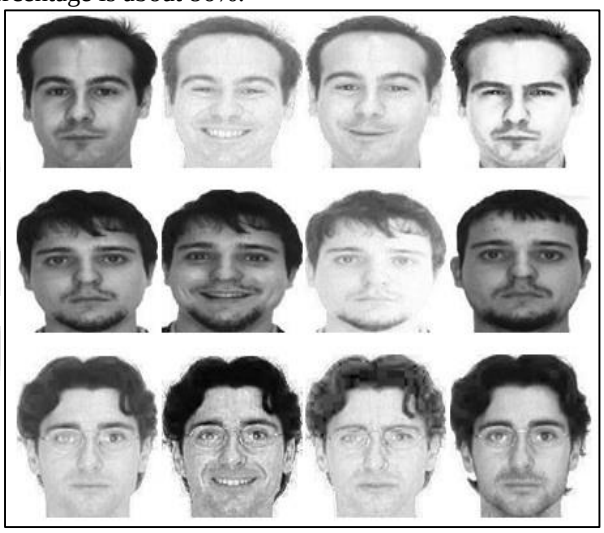

Fig. 10: Sample images with variations in their facial expressions

Following bar graph shows its repeatability to 86 face images out of 100 which are used for testing.

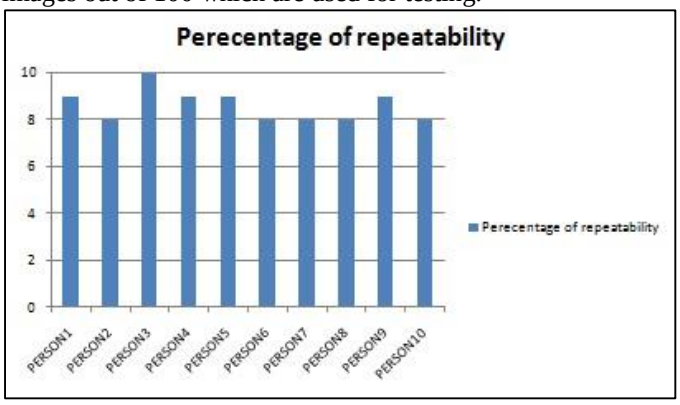


Fig. 11: Repeatability of key generation

Following pie chart shows accuracy of "Secure cryptographic system using face biometrics" which is 86% accurate.

 

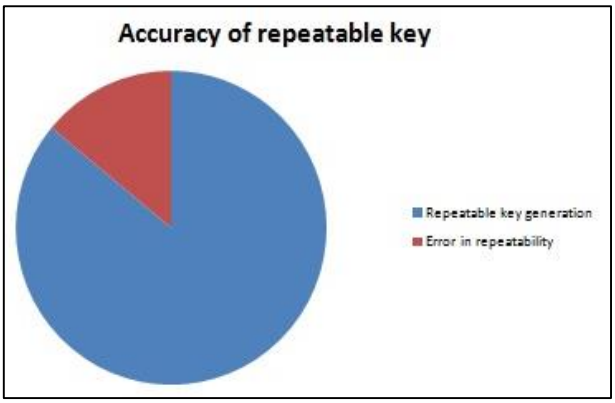


Fig. 12: Accuracy of repeatable key generation

Details of repeatable 64bit key generation are written in following table. It contains number of persons; number of tested images, number of images generates same key and lastly its accuracy in percentage as follows.

| NO. OF PERSONS | NO. OF TESTED IMAGES | NO. OF IMAGES GENERATES REPEATABLE KEY | PERECENTAGE OF ACCURACY |
|---|---|---|---|
| PERSON 1 | 10 | 9 | 90% |
| PERSON 2 | 10 | 8 | 80% |
| PERSON 3 | 10 | 10 | 100% |
| PERSON 4 | 10 | 9 | 90% |
| PERSON 5 | 10 | 9 | 90% |
| PERSON 6 | 10 | 8 | 80% |
| PERSON 7 | 10 | 8 | 80% |
| PERSON 8 | 10 | 8 | 80% |
| PERSON 9 | 10 | 9 | 90% |
| PERSON 10 | 10 | 8 | 80% |

Table 1: Details of repeatable key generation

Sample for encryption and decryption of given plaintext message and key using encryption key from person image and decryption from same person image but with different view is shown in following table.

Input message for encryption/decryption is

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

| INPUT IMAGE FOR ENCRYON | INPUT IMAGE FOR DECRYPON | 64-BIT KEY GENERATED | ENCRYPTED MESSAGE |
|---|---|---|---|
| P11 | P13 | 1101010010010100 0111110111111010 0100101000111110 1111010100011 | 1000100000011111010 1010010100100000001 1101110000000010010 0001011110 |
| P21 | P22 | 1110000100010100 1 0111101111110000 1000101001011110 1111010100101 | 101001011 000110010 01 0000000100001111 1101001111010000011 0110101000 |
| P41 | P43 | 1110110110010100 1 1111101111111011 0 1100101001111110 1 1111010100111 | 0101110001011101000 1 0111001101101000 1 1011100110100110011 1101101011 |

Table 2: Encryption/decryption sample

## VI. CONCLUSION

With increase in use of internet, information security becoming more important now a days in communication technologies. In this work, we propose a novel algorithm for key generation using face image features. This method uses the graphical representation of an image to extract the properties of the image. A 64-bit key is generated from those extracted properties that can be used as key for encryption and decryption of plaintext. This proposed method is easy in its implement. The power of key is much better than others. It is a responsible and adaptive method of key generation for securing the information. Here user does not need to remember the keys during encryption and decryption as the key is generated using the physiological characteristic of the person.

Proposed system works well with face images of different expressions. Future work is to work on images where persons has goggle and scarf on their face and with pose angle of image equal to or greater than 45 degree.

## REFERENCES

[1] Mr.P.Balakumar and Dr.R.Venkatesan "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[2] Raikoti Sharanabasappa1 and Sanjaypande M. B, "A Unique Document Security Technique using Face Biometric Template" International Journal of Advanced Science and Technology Vol. 50, January, 2013.

[3] Margarita Osadchy, Benny Pinkas University of Haifa "SCiFI – A System for Secure Face Identification"

[4] Gokulakumar.A.S, Venkataraghavan.C, Kavya priya.S, Suganya.T "Encryption of Cryptographic key technique by crossover of Iris and Face Biometric key" International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

[5] Dr.R.Seshadri, T.Raghu Trivedi, "Efficient Cryptographic Key Generation Using Biometrics". Proceedings on the International Journal on Computer Technology and Application, ISSN: 2229-6093, Vol-2, Pp: 183-187.

[6] Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K-"A New Randomized Cryptographic Key Generation Using Image" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013.

[7] Damir Omerasevic, Narcis Behlilovic, Sasa Mrdovic, "CryptoStego- A Novel Approach for Creating Cryptographic Keys and Messages", 2013-IEEE, Pp: 83-86.

[8] Raikoti Sharanabasappa1 and Sanjaypande M. B. " A Unique Document Security Technique using Face Biometric Template" International Journal of Advanced Science and Technology Vol. 50, January, 2013

[9] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani "A Novel Cryptographic Key Generation Method Using Image Features" Research Journal of

 

Information Technology 4(2): 88-92, 2012 ISSN: 2041-3114.

[10] Munmun Bhagat "Face Image Retrieval using Sparse Code words with Encryption" ISBN: 978-81-927230-0-6, NCITM: 2014.

[11] Jo ,J. G. Jo, J. W. Seo, and H. W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop 2007, LNCS 4613, pp. 38-49, Springer Verlag, 2007.

[12] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for securing Digital Image". Proceedings on the International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Pp: 285-291.

[13] K Hemanth, Srinivasulu Asadi, Dabbu Murali, N Karimulla and M Aswin "High Secure Crypto Biometric Authentication Protocol" K Hemanth et al (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011, 2496-2502.



 