Fingerprint bio-Crypto key generation using Scale Invariant Feature Transform (SIFT)

S. Partheeba
Research Scholar,
Department of Computer Science
PSGR Krishnammal college for women
Coimbatore, India.

N. Radha, PhD
Assistant professor,
Department of Computer Science
PSGR Krishnammal college for women
Coimbatore, India.

ABSTRACT
Network security has become a great threat to the network accessible resources that consists of policies to prevent, monitor unauthorized access, modification, and misuse of computer network. Several algorithms and techniques were proposed for the secure transmission of data and to protect user's privacy. Secret-key cryptography and public-key cryptography are the techniques used for the protection of security issues. However, such a key needs to be stored in a protected place or it should be transported by a shared communication line. So generation of cryptographic key using biometric traits of both sender and receiver during communication avoids key storing and improves security strength. The proposed approach for detecting the quality of fingerprint by using the method called orientation certainty level (OCL). If the image has good quality then feature extraction will be done using Scale Invariant Feature Transform, otherwise poor quality image will get ignored. By using cover image the obtained cancellable template will get hidden. Then the hidden image will be transmitted from sender to receiver and receiver to receiver to sender by using Variable Least Significant Bit techniques. Finally the performance metrics like FAR (False Acceptance Rate), FRR (False Rejection Rate), and Accuracy of the proposed work is compared with the existing system.

Keywords
Cryptography key, Orientation Certainty Level, Scale Invariant Feature Transform, Variable Least Significant Bit

1. INTRODUCTION
Biometric authentication or simply biometrics refers to establishing automatic personal recognition based on the physical and behavioral characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.). Biometrics offers greater security and convenience than traditional identity authentication systems (based on passwords and cryptographic keys). Since biometrics characteristics are inherently associated with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. Biometric system prevents the user for transmitting confidential information across insecure networks from intruders. Cryptography is classified in to symmetric and Asymmetric cryptography respectively. In symmetric-key cryptography, the same key is used by both sender end and receiver end. In asymmetric or public-key cryptography, a private key and a public key are used for security. The private key is held secret by the receiver and only the public key is announced to the public. Some of the widely used asymmetric cryptography techniques are RSA (rivestshamir and adleman), Diffie-Hellman, DSA (digital signature algorithm), and ECC (elliptic curve cryptography). Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The main objective of the proposed work is to detect the quality of fingerprint which is used to encrypt the transmission data. If the image has good quality then the minutiae points are extracted by using the proposed method which includes minutiae extraction by using Scale Invariant Feature Transform (SIFT) algorithm. This technique is used to hide variable amount of data in cover file in more secure way. It hides variable amount of data in every individual pixel of each sector of cover file. Modular Distance Technique (MDT) is used to implement VLSB stegnography with small data hiding capacity and large key size. The key size of modular distance technique is almost 27 times of the size of the square of cover image.

2. LITERATURE REVIEW
A. Jagadeesan et al. [1] proposed secured cryptographic key generation from multimodal biometrics feature level fusion of fingerprint and Iris. They proposed the technique comprised of three modules namely feature extraction, multimodal biometric template generation and cryptographic key generation. Multi- biometric template obtained is used to generate the secure 256-bit cryptographic key which is capable of providing better user authentication and high end security. The technique was evaluated using 3D face data and it was proved to generate keys of suitable length for 128-bit AES (Advanced Encryption Standard). The features, minutiae points and texture properties have been extracted from the iris images and fingerprint. Then, the extracted features have been combined together at the feature level to obtain the multi-biometric template.

Sunil V. K. Gaddam et al. [2] proposed an efficient cancellable biometric key generation scheme for cryptography. The system introduced a technique to produce cancellable key from fingerprint so as to surmount the problems. Extracting minutiae points from fingerprint, the key used in the AES encryption is the generated key from the whole process. The cancellable biometric system introduces a novel method to generate a cryptographic key. Once the key is generated, AES encryption progressed to generate a secured feature matrix, but initially encryption process does not occur in the key generation from the whole process.

M.S.Durairajan el al. [3] proposed biometrics based key generation using Diffie-Hellman key exchange for enhanced security mechanism. The cryptographic methods to solve the problem of security by implementing various methods for key exchange. Shared key is the major constraint established by Diffie-Hellman algorithm. This algorithm generates the shared key with the help of receiver's public key and sender's private key. The fingerprint instead of random number as a

private key in the algorithm provides better security for data transfer over the network with high confidentiality.

B.RajaRao et al. [4] proposed fingerprint parameter based cryptographic key generation. The proposed work mainly concentrates on the approach to reduce the cost associated with lost keys, addresses non-repudiation issues and also provides increased security of digital content. They have used ECC (elliptic curve cryptography) algorithm for providing higher security with good performance in terms of computational and bandwidth requirements.

P.Balakumar et al. [5] proposed the biometrics system in fingerprint and iris. These two features combined with the help of the fusion algorithm. The pre-processed image is normalized and filtered to remove the noise. Thinning is used to remove thickness of the image. After minutiae points are extracted by using Crossing Number model. Then mapping function is performed and cryptography key is generated by shuffling the vectors. This method provides better security but biometric quality is not detected.

Muthukumar Arunachalam et al. [6] proposed AES based multimodal biometric authentication using cryptography level fusion with fingerprint and finger knuckle print. The main objective of the work is to generate the biometric key from fingerprint and finger knuckle biometrics with its feature extraction using k-Means algorithm for improvement of the security. To improve the overall performance of the system they discussed additionally about the integration of fingerprint and finger knuckle print using package model cryptographic level fusion.

N. Lalithamani et al. [7] proposed an effective scheme for generating irrevocable cryptography key form cancellable fingerprint templates. An approach of cancellable fingerprint using the minutiae points extracted from the fingerprints. The cancellable templates are generated and irrevocable keys are extracted from the cancellable templates. The fingerprint image is enhanced using average filtering and gabor filtering. The proposed work has evaluated the effectiveness of scheme using fingerprint from publicly available the security analysis.

Unsang Park et al. [8] proposed fingerprint verification using sift features. An approach sift points are only limited by the condition of local minimum and maximum in a given scale space, resulting in a large number of feature points. The fingerprint matching in two steps in point wise match and trimming false matches with geometric constraints. The minutiae based technique involves connecting broken ridges and extracting skeleton of the ridge pattern. It removes all the texture information used in the sift operator.

S.Malathi et al. [9] proposed partial fingerprint matching based on sift features. An novel approach of fingerprint matching based on scale invariant feature transform that features and matching is achieved using modified the point matching process. The neuro technology database using the matching process. The original fingerprint involves normalization process using histogram equalization technique to obtain better accuracy. The sift operator using point wise matching method of the sift key points of the fingerprint.

Subhas Barman et al. [10] proposed fingerprint based crypto-biometric system for network security. An approach for the generation of the cryptographic key from cancelable fingerprint template of both the sender and the receiver. The cancelable fingerprint templates of them were securely transmitted to each other using a key-based steganography technique. The templates were combined with concatenation based feature level fusion technique to get a combined template. The elements of combined template were then shuffled using shuffle key and then the hash of shuffled template generated a unique session key for communication. A revocable key for symmetric cryptography was generated from irrevocable fingerprint and privacy of the fingerprints is protected by the cancelable transformation of fingerprint template in the proposed approach. However it lacks session based cryptographic key.

3. METHODOLOGY

The first process in the proposed methodology is quality checking of the acquired fingerprint. The Orientation Certainty Level (OCL) algorithm is used to detect the quality of fingerprint received from both sender and receiver. After checking the quality, if it is bad, it will be rejected else it will be passed on to the extraction Process. The fingerprint undergoes minutiae extraction process based on Scale Invariant Feature Transform (SIFT) approach. Therefore the cancellable templates of both sender and receiver are exchanged by hiding them inside a cover image. This process is done by using improved steganography method. After generating stego-image, the receiver receives the sender's template and merged with its own cancellable template by using feature-level fusion technique. By using this fused template, a cryptographic key is generated.

The steps involved in the proposed system are as follows:

- Fingerprint acquisition and Quality check
- Minutiae point extraction
- Hiding cancellable template using VLSB stegnography

3.1 Fingerprint Acquisition and Quality Check

In this proposed work minutiae points are considered only in (x, y) coordinate values whereas biometric features are stored as (x, y, Θ) form. Initially, the fingerprints are obtained from both sender and receiver. The obtained fingerprints are checked for its quality by using this proposed technique such as Orientation Certainty Level (OCL) approach.

- Sobel operator is applied to the pixels of each fingerprint block, thus constructing a gradient vector of the image.
- By performing principal component analysis on the image block gradients, an orthogonal basis for an image block can be formed by finding eigen values and eigen vectors. Principal components analysis is a multivariate procedure which rotates the data such that maximum variability is projected onto orthogonal axes.
- The resultant first principal component contains the largest variance contributed by the maximum total gradient change in the direction orthogonal to ridge orientation.
- The direction is given by the first eigenvector and the value of the variance corresponds to the first eigen value, λ_{max} .

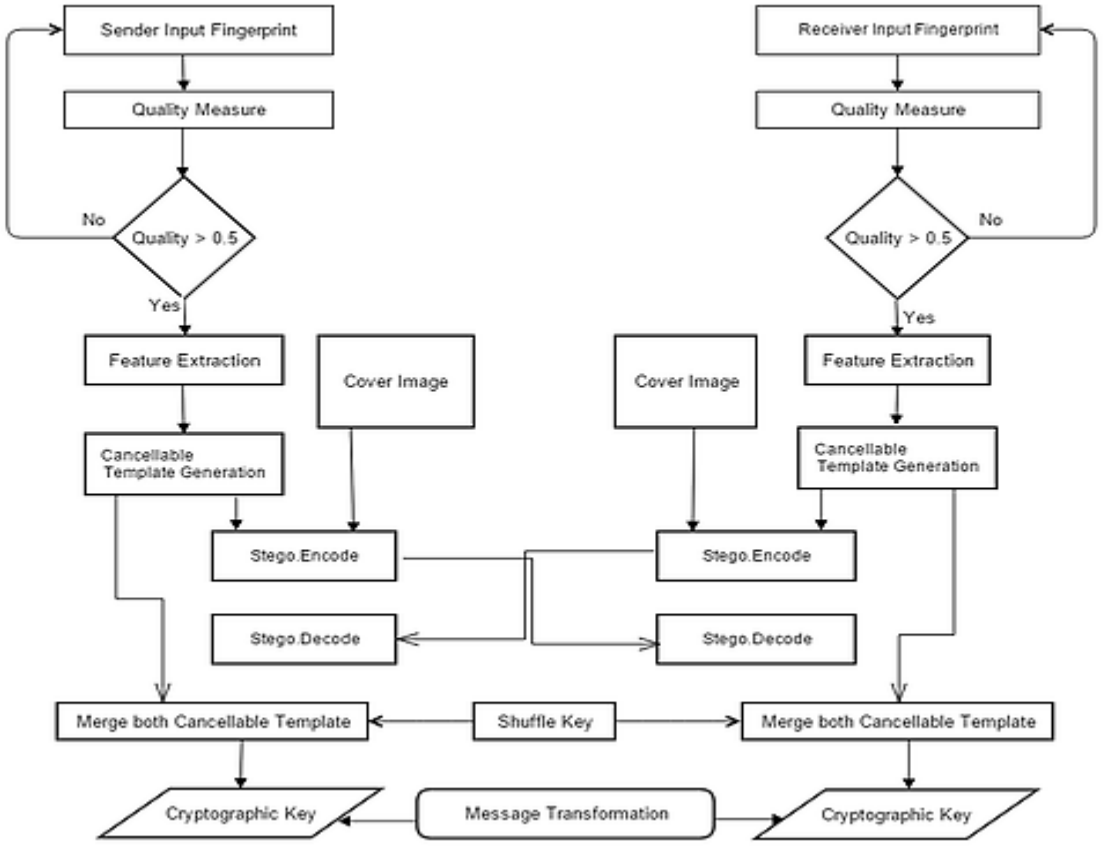

Fig.1 Overview of crypto-biometric system

On the other hand, the resultant second principal component has the minimum change of gradient in the direction of ridge flow which corresponds to the second eigen value, λ_{min} .

OCL Algorithm:

Input: Fingerprint image I

Output: OCL quality score $Q_{ocl.}$

1. The input image I is a fingerprint image, the common approach to compute local level information is to subdivide the image into blocks and pixel indexing within an image I with dimensions $I_{w,}$ $I_{h.}$ The image into pixel I (1,1), the block V(1,1), with dimension $V_{w,}$ $V_{h.}$
2. Constructing gradient vector by applying Sobeloperator to each pixel by using equation

$$C = \frac{1}{N}\sum_N \left(\begin{bmatrix} dx \\ dy \end{bmatrix} [dx\ dy]\right) = \begin{bmatrix} a & c \\ c & b \end{bmatrix} \quad (1)$$

The ratio orientation certainty level (OCL) between the two Eigen values thus gives an indication of how strong the energy is concentrated along the dominant direction with two vectors pointing to the normal and tangential direction of the average ridge flow respectively.

3. Find Eigen values by performing principal component analysis by using equation

$$\lambda_{max} = \frac{(a+b)+\sqrt{(a-b^2+4c^2)}}{2} \quad (2)$$

And

$$\lambda_{min} = \frac{(a+b)-\sqrt{(a-b^2+4c^2)}}{2} \quad (3)$$

Where a, b, c, d are the elements of the covariance matrix C of the gradient vector for an N points image block.

4. Compute orientation certainty level between two eigen values by using equation.

$$ocl = 1 - \frac{\lambda_{min}}{\lambda_{max}} = 1 - \frac{(a+b)-\sqrt{(a-b^2+4c^2)}}{(a+b)+\sqrt{(a-b^2+4c^2)}} \quad (4)$$

Orientation certainty level (OCL) value changes in the range [0, 1]. Where 0 indicates lowest concentration of the energy along ridge-valley direction and can be interpreted as the low quality block. Thus the fingerprint quality is detected and low quality fingerprint is rejected.

5. The fingerprint quality was checked using OCL. The next phase as follows:

3.2 Minutiae point extraction using scale invariant feature transform

If the image has good quality then the minutiae points are extracted by using this proposed method which includes minutiae extraction by using Scale Invariant Feature Transform (SIFT) algorithm. SIFT based minutiae extraction consists of two steps of processing which includes pre-processing, descriptor extraction. In pre-processing, high pass filter is used to perform the brightness calibration. A SIFT descriptor is proposed by computing the gradient magnitude and orientation at each point in the region around the sampling point. These samples are accumulated into orientation histograms which summarizes the contents over the sub-regions. The suggested descriptor consists of the SIFT

descriptor of the minutia and SIFT descriptors at several sampling points around the minutiae.

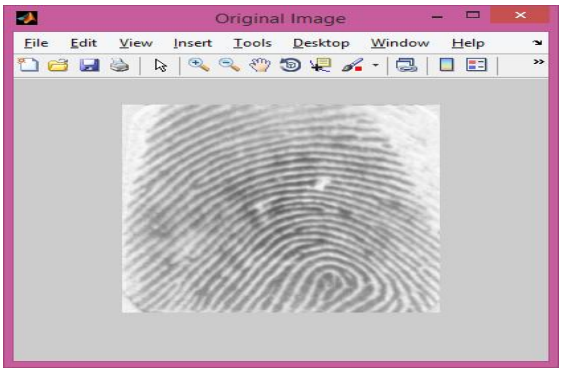

Fig.2 Fingerprint original image

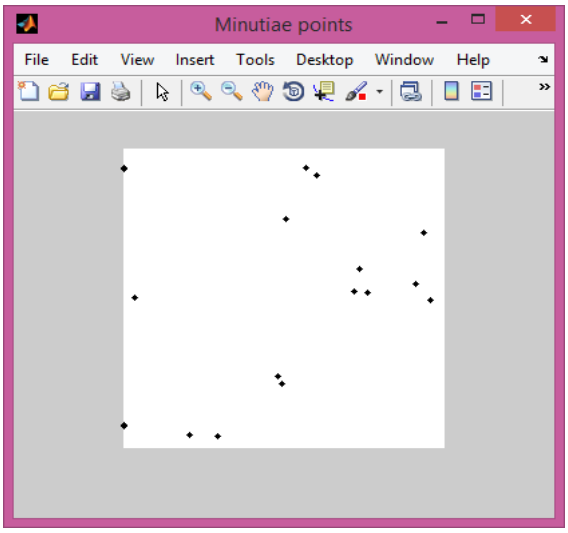

Fig.3 Extracted minutiae points

SIFT Algorithm

Step 1: Perform high pass and low pass filter by using equations (5) & (6).

Step 2: Detect minutiae points by equation (7).

Step 3: Samples the detected minutiae points.

Step 4: Extract the minutiae points by using equation (8).

- Perform high pass and low pass filter by using equations.

$$I_H(x,y) = I(x,y) - \frac{1}{k^2}\sum_{i=1}^{k}\sum_{j=1}^{k} I(i,j) + b \quad (5)$$

Where $I(x,y)$ denotes the gray value of the image at position (x,y) and k is the size of high pass window which is selected as 16 and the bias value b is equal to 128. It calculates average intensity within $k \times k$ window and subtracts average from the center pixel biased at b. The low pass filter is used to decrease the noise and is denoted as:

$$I_L(x,y) = \frac{1}{2}\left(\frac{1}{m^2}\sum_{i=1}^{m}\sum_{j=1}^{m} I_H(i,j) + \frac{1}{n^2}\sum_{i=1}^{k}\sum_{j=1}^{k} I_H(i,j)\right) \quad (6)$$

Where the size of two low pass windows m and n are selected as 4 and 2 respectively and the reason that low pass filter uses two windows and uses the average of two averages is that the pixel in the smaller window is more similar to the target pixel. Detect minutiae points by equation. The detected minutiae m is defined as:

$$D_M(m) = (x_m, y_m, \theta_m) \quad (7)$$

Minutiae are detected from the thinning image. The type of minutiae can also be classified into ridge bifurcation and ridge ending. A ridge ending minutiae is a point where a ridge terminates, while a ridge bifurcation Minutiae is a point where a ridge splits from a single path to two paths.

- Samples the detected minutiae points.
- Extract the minutiae points by using equation.

The descriptor of detected minutiae is defined as:

$$D(m) = \left\{S(m), \{S(p_i)\}_{i=1}^{d}\right\} \quad (8)$$

Where $S(m)$ denotes the SIFT descriptor of minutiae, d denotes the number of sampling points and $S(p_i)$ denotes the SIFT descriptor of sampling point around minutiae m.

3.3 Hiding cancellable template using VLSB steganography

This technique is used to hide variable amount of data in cover file in more secure way. It hides variable amount of data in every individual pixel of each sector of cover file. Modular distance technique (MDT) is used to implement variable least significant Bit (VLSB) stegnography with small data hiding capacity and large key size. Initially, all reference pixel or points in cover image usually centre point is selected and the distance between the reference pixel and the pixel under process is calculated by using either Euclidean, chess board or city block distances.

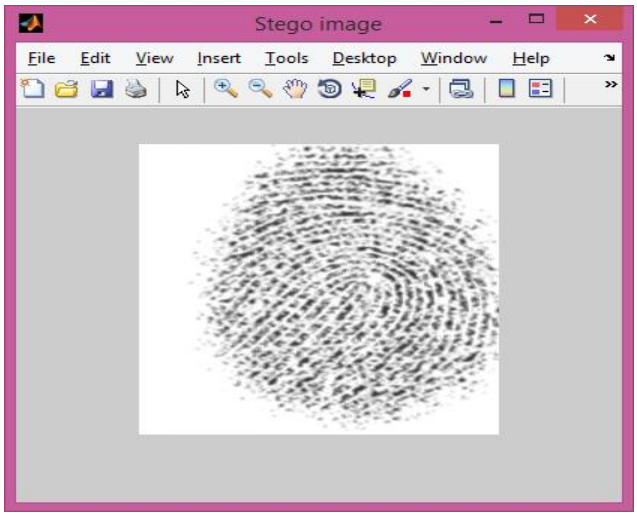

Fig.4 Stego image in data hiding technique

Algorithm

1. Calculate distance Dist (i, j) between each pixel in cover image by using distance formula either equations (9).
2. Compute modular value of the distance Mod (Dist (i, j)).
3. Find number of bits "Bi" to hide in the cover image.
4. Calculate the total bits "Be" embedded in cover image by using equation (12).

- Calculate distance Dist (i, j) between each pixel in cover image by using distance formula either equations

$$Euclidean\ Distance = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (9)$$

Compute modular value of the distance Mod (Dist (i, j)), Where i =1 to n and j = 1 to n. The gray scale image is a 2-D array of pixels having ''R'' number of row and ''C'' number of columns, so the total number of pixels ''N'' is:

$$N = R \times C \quad (10)$$

And each pixel's intensity is represented by 8 bits. So the total size the image in bits is:

$$Size_{total} = N \times 8 \quad (11)$$

Find number of bits "Bi" to hide in the cover image. Calculate the total bits "Be" embedded in cover image by using equation

$$B_e = \sum_{i=1}^{N} Bi \quad (12)$$

The modular distance technique of stegnography is to hide data in a cover file in non-perceivable manner but if snoopers comes to know about the presence of secret, the snoopers has to try "K" different combinations to extract the hidden data exactly. The key size of MDT depends on the size of cover image and number of types of distances. An image with rows "R" and colums "C" will have a total of "N" pixels in the image. Using MDT user can hide a number of bits "Bi" ranging from 0 to 8 bits eacg pixel in the image. So there are 9 possible values for a single pixel and three choices of distance type in MDT.The total key size "K" of modular distance technique is:

$$K = 3 * (R * C) * C_1^9 \quad (13)$$

$$K = 3 * (R * C) * 9 \quad (14)$$

$$K = 27 * (R * C) \quad (15)$$

And

$$K = 27 * N \quad (16)$$

N: Size of the cover image

R: Number of rows of the cover image

C: Number of columns of cover image

K: Number of possible keys

The reference point also contribute a lot to the key size as there are "N" number of points/ pixels is cover image and any of the pixel can be used as a reference. The reference point used on the sender side during data hiding process should be kept secret without the knowledge of an exact reference the retrieval of data is impossible. Now if the reference point is considered then the key size will be:

$$K = 27 * N * N \quad (17)$$

$$K = 27 * N^2 \quad (18)$$

$$K = 27 * (R * C)^2 \quad (19)$$

So there are a total "K" number of possible ways to hide data in a cover image.Larger the value of ''K'' more difficult it would be for an unauthorized person to extract data from the stego-Image even if the snoopers came to know that some data is hidden in the image he must have to try ''K'' various combinations to retrieve data exactly.

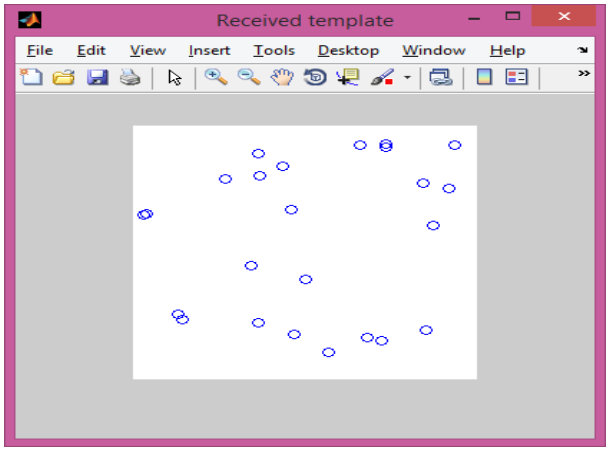

Fig.5 Received cancelable template

3.4 Generating Cryptography Key

The stego-image is sent to the receiver from sender and vice-versa. After receiving cancellable template from counter partner it is merged with its own cancellable template that means sender has its own cancellable template T_{CS} and received cancellable template T_{CR} from receiver. Then merged cancellable fingerprint template is divided into two equal parts of same size. The divided values are denoted as:

$$V_1 = \left[v_1 \ldots . v_{n/2}\right] \quad (20)$$

$$V_2 = \left[v_{n/2+1} \ldots v_n\right] \quad (21)$$

The elements in two parts are shuffled by using modulo operation and stored in another vector. The shuffled vector is combined and denoted as:

$$SV = [SV_1 \cup SV_2) \quad (22)$$

The shuffled vector is converted into a matrix and denoted as:

$$MV = (a_{ij}) sqrt(|SV|) * sqrt(|SV|) \quad (23)$$

Finally, the irrevocable key vector is generated from matrix MV as follows:

$$IK_v = \{k_i : P(k)\}, i = 1, \ldots, |SV| \ where\ P(k) = |SM_{ij}| mod\ 2. \quad (24)$$

And $SM_{ij} = MVi, j: i + size, j + size, -1 < i, j < sqrt(|SV|)$ (25)

Thus the cryptography key is generated which is more secured and irrevocable.

3.5 Encryption and Decryption process

The key obtained after the above process is used to encrypt a message that has to be reached to the Receiver. And the receiver receives the message encrypted text and decrypts it using the generated key. Thus the key generation process relies mainly on the fingerprint of the sender and receiver alone, and that too has an increased privacy of usage since only the cancellable templates are into the process of key production.

Fig.6 Framework of encryption and decryption process

4. EXPERIMENTAL RESULTS

The proposed work is evaluated in tool MATLAB 2014a version is used throughout the implementation. This research work has used FVC2002 data base for taking fingerprints and 120 images has been used for obtaining various results. In this research work SIFT algorithm is used for extracting minutiae point and VLSB stegnography technique for hiding variable amount of data in every individual pixel of each sector's cover file, for this process MDT (modular distance technique) algorithm were used. The metrics like FAR (0.5%), FRR (0.13%) and Accuracy of 91% are evaluated for comparison of the existing and the proposed system.

4.1 False Acceptance Rate:

$$FAR = \frac{wrongly\ \ accepted\ \ individuals}{total\ \ number\ \ of\ wrong\ \ matc\ hing}$$

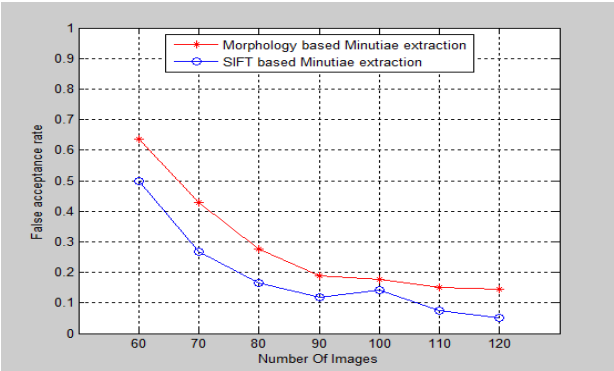

Fig.7 Comparison of false acceptance rate between existing and proposed system

In the above Fig.7, shows the resulted False Acceptance Rate (FAR) obtained in the proposed and existing technique is analysed. From the result, it is observed that the proposed technique results in lesser False Acceptance Rate for all the persons, whereas the existing techniques results with higher percentage of False Acceptance Rate.

4.2 False Rejection Rate:

$$FRR = \frac{wrongly\ rejected\ individuals}{total\ number\ of\ correct\ matching}$$

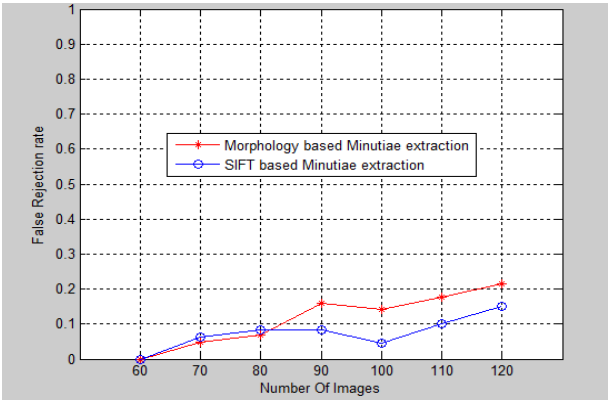

Fig.8 Comparison of false rejection rate between existing and proposed system

In the above Fig.8, the comparison of False Rejection Rate (FRR) obtained in the proposed and existing technique is analysed. From the result, it is observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique.

4.3 Accuracy

In the below Fig.9, the comparison of Accuracy (91%) obtained in the proposed and accuracy (85%) of existing technique is analysed. From the result, it is observed that the SIFT based minutiae technique results in better accuracy when compared to the Morphological based minutiae technique.

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative}$$

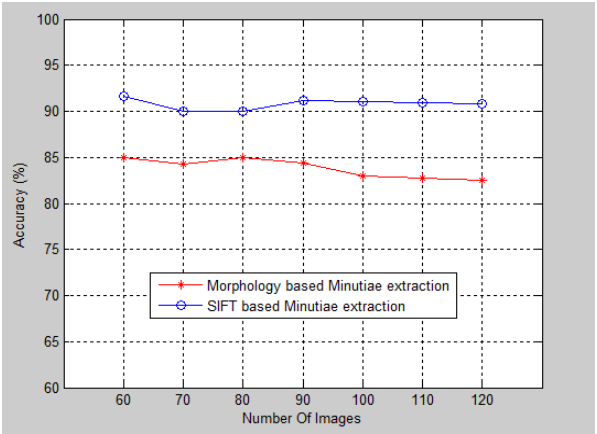

Fig.9 Comparison of accuracy between existing and proposed system

5. CONCLUSION

The proposed work addresses the secured transmission of data using cryptographic technique. The OCL, SIFT and VLSB algorithms are used to improve the quality and security of cancellable template from one end to other end. Finally 256-bit bio-crypto key is generated for secured transmission over networks and has been shared between sender and receiver.

By applying the SIFT algorithm the accuracy is improved and to decrease the FAR and FRR which will improve the level of security in user authentication. Thus, the experimental result of the proposed system is achieved and cryptographic key is generated for secured transmission. For future enhancement, multi-modal biometric traits can be used for the key generation and different cryptographic algorithms can be used to improve the security and overall performance. Different combination of multimodal biometric can be used to improve the level of security.

6. REFERENCES

[1] A. Jagadeesan, 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, 7(2), No.2, 2010.

[2] Sunil V. K. Gaddam, Manohar Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security, 11(9), PP.61-69, No.2, 2010.

[3] M.S. Durairajan, Dr.R.Saravanan, **"**Biometrics based key generation using Diffie Hellman Key Exchange for enhanced security Mechanism", International Journal of Chem Tech Research, 6(9), PP.4359-4365, No.9, 2014.

[4] B.Raja Rao, Dr.E.V.V.Krishna Rao, S.V.Rama Rao, M.Rama mohan rao, "Fingerprint Parameter Based Cryptographic Key Generation", International Journal of Engineering Research and Applications(IJERA), 2(12), PP.1598-1604, Issue 6, 2012. ISSN:2248-9622.

[5] Mr.P.Balakumar, Dr.R.Venkatesan, "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris", International Journal of computer science Issues(IJCSI), 8(9), Issue 5, No.2,2011. ISSN:1694-0814.

[6] Muthkumar Arunachalam, Kannan Subramanian, "AES Based Multimodal Biometric Authentication using Cryptography Biometric Features of Fingerprint and Iris",The International Arab Journal of Information Technology ",12(9), No.5, 2015.

[7] Barman, S., Samanta, D., & Chattopadhyay, S. (2015)." Fingerprint-based crypto-biometric system for network security". *EURASIP Journal on Information Security*, *no.*1, pp.1-17, 2015.

[8] N.Lalithamani, Dr.K.P.Soman, "An Effective Scheme for Generating Irrevocable cryptographic key from Cancelable Fingerprint Templates", International journal of Computer Science and Network security(IJCSNS), 9(3), No.3, 2009.

[9] Deepika Sahu, Rashmi Shrivas, "Minutaie Based Fingerprint Matching for Identification and Verification", International journal of science and Research(IJSR), 5(3), Issue.3, 2016. ISSN:2319-7064

[10] A.Jagadeesan, T.Thillaikkarasi, Dr.K.Duraiswamy, " Cryptographic Key Generation from Multiple Biometric Modalities:Fusing Minutiae with Iris Feature", International Journal of Computer Applications, 2(6), No.6, 2010

[11] K.Hemanth, Srinivasulu Asadi, Dabbu Murali, N.Karimulla, M.Aswin, " High Secure Crypto Biomertic Authentication Protocol", International Journal of Computer Scince and Information Technologies, Vol.2, No.6, PP.2496-2502, 2011. ISSN: 0975-9646

[12] R.Divya, V.Vijayalakshmi, "Analysis of Multimodal Fusion Based Authentication Techniques for Network", International Journal of Security and its Applications, Vol.9, No.4, PP.236-246, 2015.

[13] Nalini.P, "SIFI Based Minutia Descriptors for Fingerprint Combination Protection", International Journal of Science, Engineering and Technology Research(IJSETR), 4(11), Issue 11, 2015.

[14] N.Lalithamani, Dr.K.P.Soman, "Towards Generating Irrevocable Key for Cryptography from Cancelable Fingerprints", IEEE.2009.

[15] Ravi K Sheth, Sarika P.Patel, "Analysis of Cryptography Techniques", International Journal of Research in Advance Engineering, 1(2), Issue.2, 2015.

[16] Arunprakash.K, Narayanan R.C, Dr. Krishnamoorthy .K," Reduction of false Acceptance Rate using Cross Validation for Fingerprint Recognition biometric System" International journal for trends in Engineering and technology,3(1), Issue.1, 2015

[17] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, Parvinder S. Sandhu, " Fingerprint Verification System using Minutiae Extraction Technique", International Journal of Computer, Electrical, Automation, Control and information Engineering, vol.2, No.10, 2008.

[18] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P. Chenna Reddy, " Implementation of LSB Steganography and its evaluation for various file formats", International journal of Advanced Networking and Applications, vol.2, Issue.5, Pages:868-872(2011).

[19] Janani. B, Dr.N. Radha, "Cancelable Template Generation Based on Improved Quality Fingerprint for Person Authentication", International journal of engineering and computer science, vol. 4(1), Issue.1,PP:9892-9898,2015. ISSN:2319-7242.

[20] Ms.S.Malathi, Dr.C.Meena, "Partial Fingerprint matching based on SIFI Features", International Journal on Computer Science and Engineering(IJCSE), Vol.02, No.04, PP.1411-1414, 2010.