Finger Knuckle Print Authentication Using AES and K-Means Algorithm

Muthukumar Arunachalam[1] and Kannan Subramanian[2]
[1]Department of Electronics and Communication Engineering, Kalasalingam University, India
[2]Department of Electrical and Electronics Engineering, Kalasalingam University, India

Abstract: *In general, the identification and verification are done by passwords, PIN number, etc., which can be easily cracked by hackers. Biometrics is a powerful and unique tool based on the anatomical and behavioural characteristics of the human beings in order to prove their authentication. Security is the most important thing in the world. Password is used for security, but it does not provide the effective security. So biometrics can be used to provide the higher security than the password. Finger Knuckle Print (FKP) is a unique biometric anatomical feature for an individual person. Biometric systems are suffered to a variety of attacks. In order to avoid these attacks, the biometric combined cryptography is the major tool. Bio-crypto system is to provide the authentication as well as the confidentiality of the data. This paper presents biometric key, which is generated from key points of FKP using k-means algorithm and secret hash value also generated using Secure Hash Algorithm (SHA) function, which is encrypted with the FKP extracted key points by Symmetric Advanced Encryption Standard (AES) algorithm. The key points extraction of FKP was derived using Scale Invariant Feature Transform (SIFT). Hence encrypted secret hash value secures biometric data and the secret value. The hash function protects the biometric data from malicious tampering, and it provides error checking functionality.*

Keywords: *Biometric cryptosystems, key point's extraction, K-Means algorithm, SIFT algorithm, AES, SHA function.*

Received August 30, 2012; accepted April 23, 2013; published online August 9, 2015

1. Introduction

Biometrics is defined as the measure of human body characteristics such as fingerprint, eye, retina, voice pattern, iris and hand measurement. It is a powerful and unique tool based on the anatomic and behavioural characteristics of the human beings. Most anatomical characteristics used for security application are fingerprint, iris, face and palm print [6, 7, 11, 19]. Apart from anatomical characteristics, behavioural characters like voice, signature and gait moments are also used to recognize the user. The most of the biometric systems that are presently used in real time applications typically use a single biometric characteristic to authenticate a user. So, authentication leads to major and important part in the secured way of communication. Currently, passwords and smartcards are used as the authentication tool for verifying the authorized user. However, passwords can be easily cracked by dictionary attacks and smart cards may be stolen or missed. Thus, the authorised user cannot be identified and the hackers will be allowed. So, the biometrics is an only remedy for the problems. This paper discusses about the new biometric identifier named as Finger Knuckle Print (FKP) shown in Figure 1. Many researches are going on this new emerging biometric because, which is an also unique characteristic like fingerprint, Iris, etc., in order to prove the genuine user. The FKP recognition system contains data acquisition, ROI extraction, feature extraction, coding, and matching process [28, 31]. The features of FKP are extracted using the Gabor filtering with the cropped region of interest. The Gabor filter features are matched for recognition the user which was explained by Zhang *et al*. [28, 31].

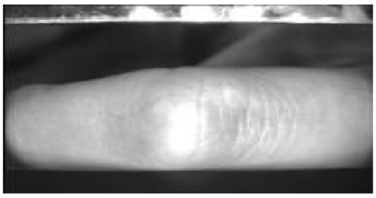


Figure 1. An image of FKP.

The average values of global and local orientation features of finger back surface or FKP were analyzed and matched with Fourier transform and Gabor filter respectively [30]. Zhang *et al*. [29] proposed the score level fusion with FKP was performed with the phase congruency, local feature and local phase features. David [16] proposed a novel approach to extract the invariant features as key points used for object recognition using Hough transform. The local information of FKP was accessed using Scale Invariant Feature Transform (SIFT) and Speed Up Robust Features (SURF) [1, 16, 21]. The SIFT algorithm is used to get the key points using the scaling and invariant features which were matched to prove the user authentication [1, 16]. Kumar *et al*. [13, 14] proposed a new method of triangulation, which was used to authenticate the hand vein images of finger knuckle surface of all fingers. The fingerprint recognition was done with image segmentation, K-

Means clustering and by Gongping George *et al*. [4, 18, 27]. Orthogonal linear Discriminant analysis was also used to recognize the FKP along with Gabor filter with its key points [25].

Along with biometrics, cryptography occupies a major role in the security applications. In normal cryptography method, cipher text is encrypted with a key of numerical values. This key value is easily cracked by other persons. While we were using the longer key value, it is hard to store in our human memory. Biometric values are the only way to keep the key as a confidential one from cracking and stealing. To avoid the cracking and stealing, only the possible method is to encrypt the data or message with the key using symmetric encryption [23, 26]. Analyzing and comparing of all possible biometrics are discussed by Uludag *et al*. [24] based on various factors, which say that each biometric has its own importance and unimportance. The key generation from the biometric data consists of three modes: Key release mode, key binding mode, and key generation mode [7, 8]. In that key release mode is very convenient to generate a key for biometric data [7, 10]. The Biometric Crypto-system is to provide more security and authentication than the normal passwords and smart card systems. In early days, there was a numerous research were done in this field.

Cryptosystem proposed by Juels and Wattenbeg [10] as fuzzy commitment scheme method, they explained the concept of area of combining error correcting codes with cryptography. Then, Juels and Sudan [9] proposed one more crypto system named as the fuzzy vault system with the feature of order invariance. The key is generated by taking pixel value from finger print and it is hashed. A message is encrypted using the biometric key (Iris) with the error detecting and hash codes and then in reverse order. Message will be decrypted by giving biometric data as a key input [26]. Cryptography means an algorithm to convert a normal text into an unreadable format named as cipher text, which is known for sender and receiver alone. Cryptographic method consists of two main classifications; one is symmetric cipher, and another one is an asymmetric cipher [22, 23]. In symmetric cipher, a common key is used for both encryption and decryption process. In asymmetric method, public key is used for encryption, and its private key is used for decryption process. Biometric crypto system can utilize the symmetric cipher only so that, biometric key is shared between encryption and decryption process [7, 9]. Here, the key generated from biometrics, which is the important process. In general, features [3, 12, 16] are extracted from the biometrics and then the extracted feature is converted as the key which is adaptable for the cryptographic process. The feature extraction, extracts the person's information from the biometric data given as an input. Feature values extracted from biometrics are analyzed by various clustering methods. The various clustering methods are hierarchical clustering, K-Means clustering and different statistical distribution's methods. Here, the algorithm adapted for feature extraction is K-Means algorithm. Symmetric encryption [17, 22, 23] is done by various algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) [2], Block ciphers, etc.

A lot of research has been carried out in the field of authentication and biometric key generation. Hao *et al*. [5] proposed the two-layer error correction technique for correcting errors in the key, which is generated from biometrics. Biometric key is a string of random bits, and it produces 140bit key, which is used for AES encryption. AES algorithm is very complicated to crack the code and to get the information from that, for a cryptanalyst. Biometric crypto systems consist of two phases: encryption phase and decryption phase. In the encryption phase, the extracted features of biometric data are stored in the database. During the decryption phase, the acquired biometric data are matched with the stored templates which are shown in Figure 2. In these systems, data are stored with biometric key values but confidentiality of the data is somewhat low in performance.

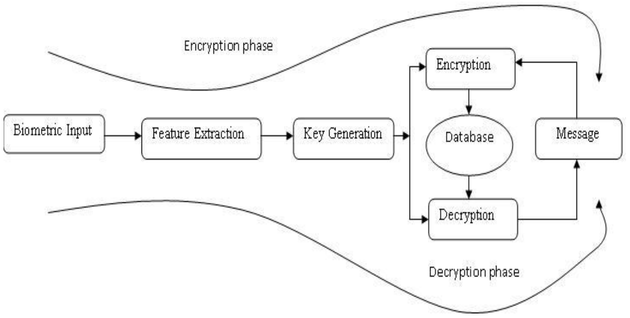


Figure 2. General biometric crypto-system.

In order to improve the template security of the system as well as confidentiality of the system, this paper proposes a new method of generating the key with FKP as the biometric data, which is used to encrypt the secret value with the AES algorithm, along with the Secure Hash Algorithm (SHA). The rest of this paper is arranged as follows, Section 2 describes about structure of the proposed work. Section 3 gives the details of the key point extraction of FKP. Section 4 discuss about the clustering process using K-Means Algorithm. Section 5 explains about the Bio-encryption and decryption phase. The experimental results and the analysis are given in section 6. Finally section 7 provides the conclusion.

2. Structure of The Proposed Work

Biometrics is a technique used to provide unique individual characteristics of a human being. The cryptography is a method, which gives the security as well as authentication for a system. So, this paper proposes a new technique named as biometric crypto-system to merge the above two process, to provide template security and authentication for individuals. The biometric crypto system is a new tool to give the solution for avoiding the key memorized, so here, the biometric character itself acts as a key for a system. In symmetric cryptography, a single key is used for both the encryption and decryption purpose. According to this methodology, a key must be similar to both encrypting and decrypting process. In this paper, FKP is acting as a biometric key for the crypto systems. For encryption and its reverse process, this paper uses the AES algorithm.

In this paper, biometric key is generated from the FKP biometrics. Here first, the key points extraction process is done . After obtaining the FKP key points values, it can be clustered using the K-Means algorithm with the Euclidean distance. In this algorithm, centroid also got, which is given as the key for encryption process as well as the decryption process. The database used for this paper was from the Polytechnic university Hongkong [20]. The key generated from the FKP, which is used for the AES encryption and Decryption is of 128 bits. Using K-Means algorithm, 128 bits were gotten from FKP with eight clusters. In order to provide the error free decryption and to provide confidentiality, Secured Hash algorithm-256 (SHA-256) is included in this paper.

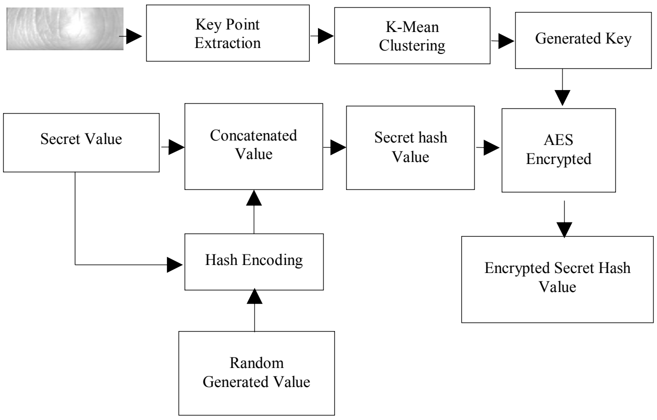


Figure 3. Bio-Encryption phase.

The overview of the proposed work is shown in Figures 3 and 4. This work consists of two phases; the first one is a Bio-encryption phase, and the second one is a decryption phase. The Bio-encryption phase shown in Figure 3, the secret value is concatenated with the random generated value. The secret hash value is generated by concatenating the secret value with the secret value coded with HMAC function. The secret hash value is encrypted using adva AES need encryption standard with the FKP biometric key to generate the encrypted hash key.

In the Bio-Decryption phase, the reverse process of encryption phase is done. The encrypted secret hash value is decrypted by the FKP biometric key to give the secret hash value. Secret value is removed from the secret hash value and then secret hash value is compared with the hash code value for error free decryption in order to prove that original secret value is extracted from the decryption phase. From these processes the authentication as well as confidentiality is proven.

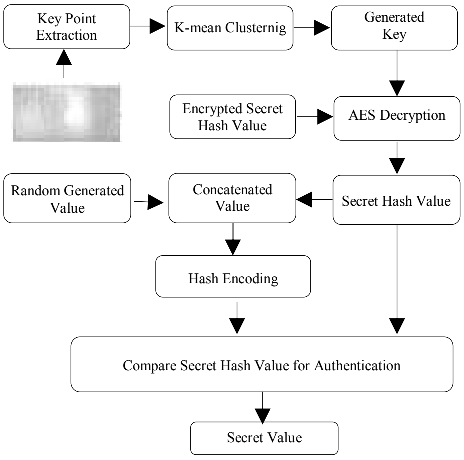


Figure 4. Bio-Decryption phase

3. Key Point Extraction of FKP

FKP is an emerging tool of biometrics. The FKP consists of a number of curvatures. The paper proposes a feature extraction of FKP using SIFT algorithm [16]. The process of feature extraction is shown in Figure 5, which consists of two steps i.e., histogram equalization and SIFT key point extraction. Each valid key point is been characterized by two parameters: x-coordinate and y-coordinate.

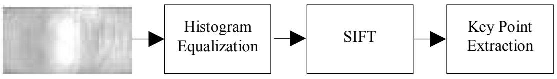
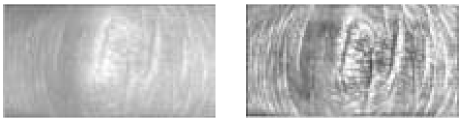


Figure 5. Feature Extraction of FKP.

The first process of feature extraction is histogram equalization, which is used to enhance the input image of FKP in order to acquire the spatial characters correctly. Histogram equalization is used to enhance the visualization effect by increasing the pixel size which is shown in Figure 6-b. The next step of feature extraction is to extract the key points from FKP using the SIFT [16]. The SIFT algorithm is mainly used for image matching purpose. SIFT is used for detection and extracting local features of an image. The first step of SIFT process is to find the difference of Gaussian function convoluted with the FKP image to detect the key point locations which is invariant to scale change. The difference of Gaussian is calculated by Equations 1 and 2.

$$L(x,y,\sigma)= G(x,y,\sigma) * I(x,y) \tag{1}$$



a) Input image of FKP. b) Histogram equalization.

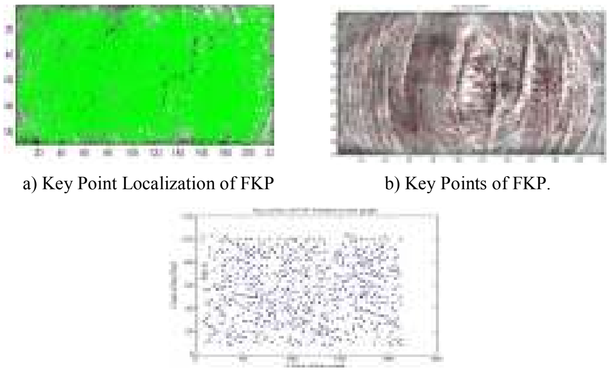
Figure 6. Histogram process.

$$D(x,y,\sigma)= G(x,y,k\sigma)*I(x,y)-G(x,y,\sigma)*I(x,y)$$
$$D(x,y,\sigma)= L(x,y,k\sigma)- L(x,y,\sigma) \tag{2}$$

In the Equation 2 $I(x, y)$, $G(x, y, \sigma)$, $L(x, y, \sigma)$, and $D(x, y, \sigma)$ represents the image, Gaussian function, scale-space of image and difference of Gaussian function respectively. The Gaussian function is calculated using Equation 3.

$$G(x,y,\sigma)= \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{3}$$

The next step is to detect the local maxima and minima of $D(x, y, \sigma)$ by comparing the each pixel value of FKP image with the neighbour pixel values. They are selected, if the pixel value is higher or lower than the reference neighbour pixels. These localized key points are shown in Figure 7-a. These selected values are named as key points. To eliminate the low contrast points along the edge of the image, Taylor's expansion method is used. After applying the Taylor expansion, stable key points are selected and located by eliminating the low intensity pixel key points. The orientations of key points are assigned for the selected key points. The key points taken from the FKP is shown in Figure 7-b.The key points selected are scale invariant points. The selected key points co-ordinates are plotted in a graph which is shown in Figure 7-c.



a) Key Point Localization of FKP

b) Key Points of FKP.

c) Key Point of FKP are plotted on the graph

Figure 7. Key points extraction using SIFT.

4. K-Means Clustering

Clustering is the process of grouping a non-linear set of objects. This approach can assign the database of *n*-objects into *k*-number of clusters ($k<n$). The main concept of this K-Means approach is every object in the database must contain in any of the clusters or group, then every cluster must contain a minimum of one object. Then each cluster can be used to find a mean vector; according to this approach, it comes under the category of the centroid model.

In this paper, K-Means clustering is used to find the set of key points, which is used as the key for the AES encryption process. The process of FKP K-Means clustering is shown in Figure 8 [4, 15].

The key points are taken from the feature extraction process are clustered using this algorithm. Consider the key points are given as the input data vectors' $M=(m1, \ldots, mn)$. K-Means algorithm starts by initializing the first co-ordinates values as the centroid and defined the numbers of clusters to be split. According to our problem, this paper proposes the eight number of clusters to be defined, and to these objects are assigned to an each cluster initially. Then, according to the initial centroid value, calculate distance between centroid and key points using Euclidean distance Equation 4. The minimum distance is retained in the updated distance matrix.

$$\|c_i - m_k\|^2 = \sum_{j=1}^{r} [c_i(j) - m_k(j)]^2 + \sum_{j=r+1}^{p} [c_i(j) - m_k(j)]^2 \tag{4}$$

The key points were grouped into new clusters until an optimum cluster is reached. The optimum cluster value is reached, there after there are no possible movements For the key points to move on the next cluster. At optimum level, centroid value is also calculated. The Centroid and key point value are calculated from the key points using this algorithm.

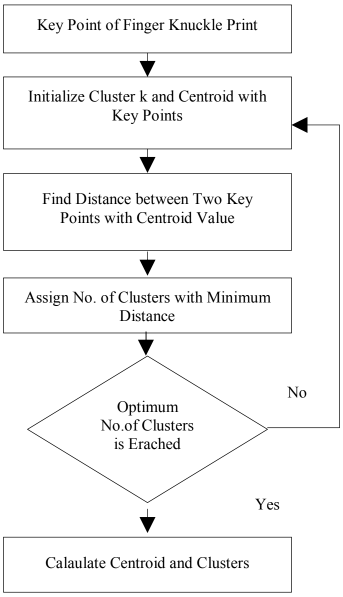

Key Point of Finger Knuckle Print
Initialize Cluster k and Centroid with Key Points
Find Distance between Two Key Points with Centroid Value
Assign No. of Clusters with Minimum Distance
Optimum No.of Clusters is Erached
No
Yes
Calaulate Centroid and Clusters

Figure 8. FKP K-means clustering process flow.

5. Bio-Encryption and Decryption Phase

Cryptography is a process of converting the input plaintext into output cipher text. In order to overcome the drawback of password authentication, this paper proposes a symmetric encryption named as AES [2, 22, 23] is adapted. Here, symmetric encryption is used because an individual person can be authenticated to prove his/her individuality in both phases of encryption and decryption. So, the authenticated person alone only can login into the system, nobody else can utilize their characteristics. In order to avoid the crack or steal the characteristics, this paper proposes a template security by encrypting the data with biometric key, which will be stored in the database. Then, to provide individuality, this paper provides SHA-256 algorithm. The FKP K-Means clustering feature values are used as the biometric key for encryption as well as decryption purposes. The Bio-encryption phase consists of two steps:

- *Step* 1: Is to generate the secret hash value.
- *Step* 2: Is to encrypt the secret hash value with the FKP vector values as the key using AES algorithm to generate encrypted secret hash value.

In the Bio-encryption phase, the first step is to concatenate the original secret value (message) with the hash code secret value to generate the secret hash value. In this hash coding is done by the Hash based Message Authentication Code (HMAC) function with the SHA. The hash coding is done for the secret value. The random value generated, which is concatenating the secret value. This hash coding is done in order to prove that no modifications or any other is not included in that original encrypted value which shown in Figure 3.

The next step of Bio-encryption phase is an encryption phase. Here, the secret hash value is encrypted by biometric key of 128bits, which is generated from the FKP points values with K-Means algorithm, which also shown in Figure 3. Secret hash value has generated with 256 bits of SHA data with input of 64bits, which is encrypted by 128bits of biometric key using AES algorithm. The 256bits of SHA are generated with the random value undergoing various processes of appending zeros, initializes the hash buffer and summing with the split values of random input. The output of the SHA value consists of 256bits, so this value is converted into 64bits by XOR the four 64bits of 256 values. This SHA 64 bits is concatenated with input of 64 bits to generate 128bits of a message for encryption. The overview process of AES algorithm is shown in Figure 9 [23]. The AES can perform the block cipher with the key length of 128bits, 192bits and 256bits. In this paper, 128bits key is used, which is obtained from the FKP. The AES algorithm is processed in matrix form in terms of bytes. The input and an output matrix consist of four rows and four columns of one byte each. So, the secret hash values of 128bits (16 bytes) are arranged in 4×4 matrixes with each of one byte. Then, biometric key of 128bits are also arranged in the same format like the input matrix. AES algorithm consists of ten rounds; each round contains four different types of transformation. The transformations are substitute bytes, shift rows, mix columns and add round key. Secret hash value consists of 16bytes and finger print biometric key of 16bytes (128bits) enter the first round of AES algorithm [23]. To involve the biometric key for all the ten rounds, biometric key must be expanded. The biometric key expansion is another process, in which the key is arranged in matrix form of 16bytes. The 16bytes can be grouped into four words w [0, 3]. These four words are used as the key for the first round. In this first word is XORed with the byte substitution using S box with the last word. This resulted word is XORed with the second word and similarly for third and fourth word also. From this, one more four words of key are obtained, which is used for second round of encryption process, and it is represented as w [4, 7] in Figure 9. Similarly, key is expanded up to ten rounds. Finally, the key is expanded to 44 words.

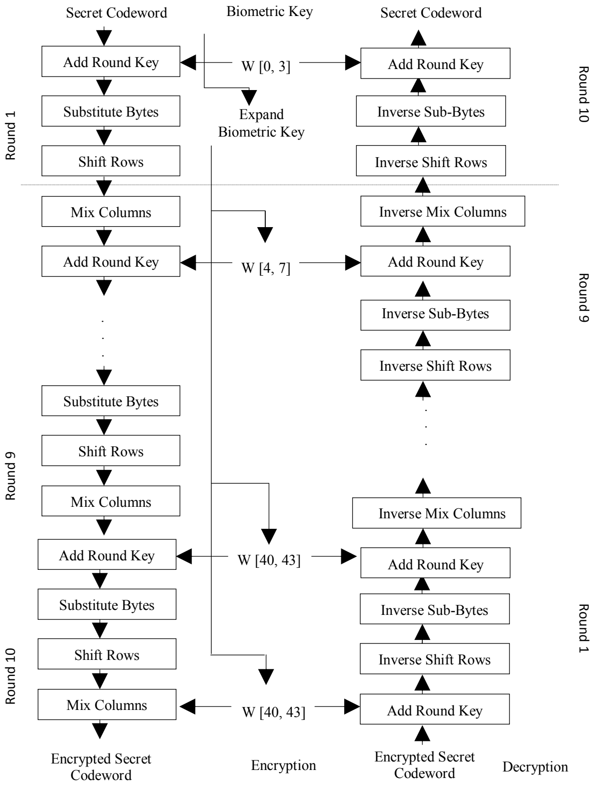


Figure 9. Overview of AES Encryption and Decryption [23].

In the first round, the input and key undergo the process of add round key; in this process, each byte of input is XORed with the each byte of key to form 4×4 byte matrix. In this matrix, each byte need to under go through substitution process concerning to S box, a new 4×4 matrix was obtained by replacing the value with S box. Each row of this four row matrix is shifted, and new matrix is framed by each row of the state is shifted cyclically by a particular offset, while leaving the first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This operation is followed for each block. The mix columns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output. Then, these four processess are done up to ten rounds repeatedly and continuously. Finally, after the completion of ten rounds, encrypted secret hash value is generated.

The next phase of this paper is Bio-Decryption phase, which is shown in Figure 4. The Bio-Decryption phase also consists of two steps; the first step is to decrypt the encrypted secret hash value with the FKP vector values as the key using AES algorithm to generate secret hash value and the second step is to compare the secret hash value generated in order to prove for the authentication and confidentiality. The biometric FKP key is generated using the same procedure as discussed in section 4. Using this key encrypted secret hash value is decrypted by the AES decryption algorithm. AES decryption is done by the reverse process of AES encryption is shown in Figure 9. Here, also four processes namely add round key, Inverse mix columns, inverse shift rows and inverse substitution bytes are also done, which are similar to encryption but in reverse order. Key expansion process is common for both encryption and decryption. In decryption phase, the last four words of encryption key become first four words of key in this phase. Likewise, all the key words are processed in reverse order of the decryption process to produce the secret hash value. The secret hash value consists of concatenated value of secret value with hash encoded value. So, the secret value alone undergoes a process of hash encoding along with random generated value, which is compared with the secret hash value which is obtained from the decryption process to prove authentication and finally secret value is received.

6. Experimental Results and Analysis

Experiments in this paper are conducted using the FKP database from FKPROI of Hong Kong Polytechnic University [20]. This database contains FKP images with its region of interest alone by cropping the outer surface image. This database consists of four sub databases; they are left index FKP, left middle FKP, right index FKP, and right middle FKP. Each sub database consists of 165 fingers of 12 images each. Totally, database consists of 660 folders of 7920 FKP images. The FKP image is enhanced with histogram equalization, which is shown in Figures 6-b and 10.

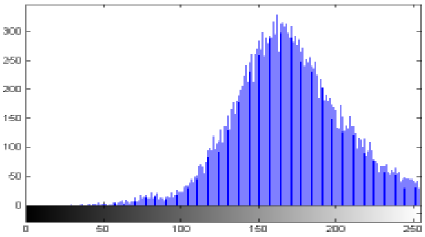


Figure 10. Histogram equalization of FKP.

The output of FKP key point localization and key point's extractions are shown in Figures 6-a and b. The key point values of FKP are grouped into eight clusters, and its centroid value is found, which is converted into 128 binary bits, which are used as biometric key for Bio-encryption and decryption phase. The centroid value of K-Mean clustering biometric FKP key is shown in the Figure 11.

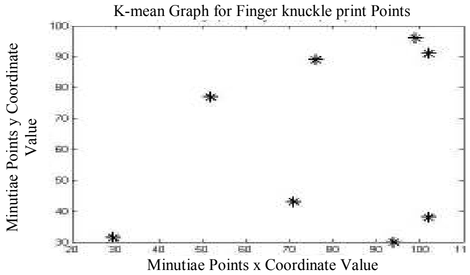
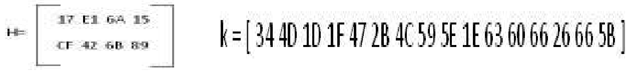


Figure 11. K-Mean Clustering graph for FKP points.

The hash value to be concatenated with the message is generated by SHA algorithm. For example, a hash code of 64bits generated is shown in Figure 12-a. The centroid value is converted into binary value of 128bits, which is shown in Figure 12-b. For this paper, simulation is performed by 10 images of each database subset.



```
H= [ 17 E1 6A 15
     CF 42 6B 89 ]
```

```
k = [ 34 4D 1D 1F 47 2B 4C 59 5E 1E 63 60 66 26 66 5B ]
```

a) SHA code output.

b) Key value of FKP.

Figure 12. SHA Process and key generation.

Table 1 consists of all parameters which are used in this paper to perform all the steps. For enhanced security, this paper involved 10 rounds of encryption and decryption on AES algorithm. For example, an encryption and the decryption phase outputs were taken from an image of FKP are shown in Figure 13.

Table 1. Parameters used for bio-encryption and decryption phase.

Parameter	Size
No. of Key Points	430-545 Points
K-Means Clustering	8 Clusters
Processing Format	Hex Decimal, Binary
FKP **key Point Value**	128 Bits
Secret Value	64 Bits
Hash Encoded Value	256 Bits
No. of Rounds for AES	10 Rounds

```
*****************************************
*                                       *
*              C I P H E R              *
*                                       *
*****************************************

Initial state :                 [illegible]

Initial round key :             [illegible]

Final state :                   [illegible]
```

```
*****************************************
*                                       *
*     I N V E R S E   C I P H E R       *
*                                       *
*****************************************

Initial state :                 [illegible]

Initial round key :             [illegible]

Final state :                   [illegible]
```

Figure 13. Bio-encryption and decryption phase output.

$$GAR = \frac{No.\ of\ genuine\ attempts\ accepted}{Total\ no.\ of\ genuine\ attempts} \quad (5)$$

$$FRR = \frac{No.\ of\ genuine\ attempts\ rejected}{Total\ no.\ of\ genuine\ attempts} \quad (6)$$

In order to define the accuracy of the biometric systems, many parameters are available, and in this paper; Genuine Acceptance Rate (GAR) and False Rejection Rate (FRR) are considered. The GAR and FRR are calculated by Equation 5 and 6. The number of key points is high; the GAR is high but FRR is low. If this is not happened, FRR is high, and then system will not be a valid one. According to this proposed approach, the GAR is increased with more key points and with the maximum cluster size. The comparison of proposed approach with the existing approach is shown in Table 2 and also shown in the ROC graph on Figure 14. The overall performance of this proposed approach was 99.4%.

Table 2. Comparison for proposed approach.

Algorithm	GAR (%)	FRR
SIFT[7]	98	2
Comp Code[19]	96.5	3.5
ImComp Code and Mag Code[21]	97	3
LGIC[20]	99.14	0.96
SIFT with K-Means and AES Algorithm (Proposed)	99.4	0.6

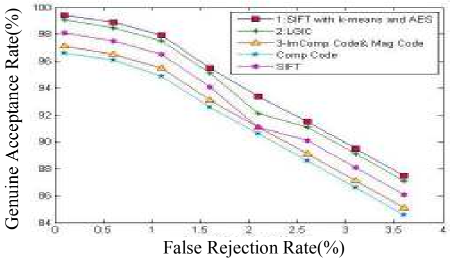


Figure 14. ROC curves of proposed system compared with existing system.

7. Conclusions

This paper presented a method of cryptosystems based on the FKP key generation using K-Means algorithm. According to this work, the authentication and confidentially are done by generating secret hash value by hash function, which is encrypted by AES algorithm to generate the encrypted secret hash value. The reverse process is done in Bio-decryption phase. This type of system secures the data very effectively. In future, this work will be extended to multibiometrics key generation with the fusion values.

Acknowledgment

The authors gratefully acknowledge the management of Kalasalingam University, Krishnankoil, Tamilnadu, India, for the facilities provided to carry out this research work.

References

[1] Badrinath G, Nigam A., and Gupta P., "An Efficient Finger-Knuckle-Print based Recognition System Fusing SIFT and SURF Matching Scores," *in Proceedings of the 13th international conference on Information and communications security*, Beijing, China, pp. 374-387, 2011

[2] Federal Information Processing Standards Publication 197., "Advanced Encryption Standard (AES) ," 2001.

[3] Ferrer M., Travieso C., and Alonso J., "Using Hand Knuckle Texture for Biometric Identifications," *IEEE A&E Systems Magazine*, pp.23-27, 2006.

[4] George A., "Efficient High Dimension Data Clustering using Constraint-Partitioning K-Means Algorithm," *the International Arab Journal of Information Technology*, vol. 10, no. 6, pp. 467-476, 2013.

[5] Hao F., Anderson R., and Daugman J., "Combining Crypto with Biometrics Effectively," *IEEE Transaction on Computers*, vol. 55, no. 9, pp. 1081-1088, 2006.

[6] Hong L., Jain A., and Bolle R., "On-Line Fingerprint Verification," *IEEE Transactions Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314, 1997.

[7] Jain A. and Pankanti S., "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744-747, 2007.

[8] Jain A., Ross A., and Pankanti S., "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 2, pp. 125-143, 2006.

[9] Juels A. and Sudan M., "A Fuzzy Vault Scheme," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 237-257, 2006.

[10] Juels A. and Wattenbeg M., "A Fuzzy Commitment Scheme," *in Proceedings of the 6th ACM conference on Computer and Communications Security*, Singapore, pp 28-36, 1999.

[11] Kumar A. and Passi A., "Comparison and Combination of Iris Matchers for Reliable Personal Authentication," *Pattern Recognition*, vol. 23, no. 3, pp. 1016-1026, 2010.

[12] Kumar A. and Zhang D., "Improving Biometric Authentication Performance from the User Quality," *IEEE Transactions on Instrumentation And Measurement*, vol. 59, no. 3, pp. 730-735, 2010.

[13] Kumar A. and Zhou Y., "Personal Identification using Finger Knuckle Orientation Features," *Electronics Letters*, vol. 45, no. 20, pp. 1023-1031, 2009.

[14] Kumar A. and Prathyusha V., "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape," *IEEE Transactions on Image Processing*, vol. 18, no. 9, pp. 2127-2136, 2009.

[15] Liu M., Jiang X., and Kot A., "Efficient Fingerprint Search based on Database Clustering," *Pattern Recognition*, vol. 40, pp. 1793-1803, 2007.

[16] Lowe D., "Distinctive Image Features from Scale-Invariant Keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[17] Mahmud M., Khan M., Alghathbar K., Abdullah A., and Idris M., "Intrinsic Authentication of Multimedia Objects Using Biometric Data

Manipulation," *the International Arab Journal of Information Technology*, vol. 9, no. 4, pp. 336-342, 2012,.

[18] Meskine F. and Bahloul S., "Privacy Preserving K-Means Clustering: A Survey Research," *the International Arab Journal of Information Technology*, vol. 9, no. 2, pp. 194-200, 2012.

[19] Ne'ma B. and Ali H., "Multi Purpose Code Generation Using Fingerprint Images," *the International Arab Journal of Information Technology*, vol. 6, no. 4, pp. 418-423, 2009.

[20] Poly U FKP., Database: http://www4.comp.polyu.edu.hk/~biometrics/, last visited 2013.

[21] Qing L., "Finger Knuckle Print Recognition based on SURF Algorithm," *in Proceedings of the 8th International Conference on Fuzzy Systems and Knowledge Discovery*, Shanghai, pp. 1879-1883, 2011.

[22] Schneier B., *Applied Cryptography Protocols, Algorithms*, Wiley Publication, 1996.

[23] Stallings W., *Cryptography and Network Security Principles and Practice*, Prentice Hall, 2013.

[24] Uludag U., Pankanti S., Prabhakar S., and Jain A., "Biometric Cryptosystems: Issues and Challenges," available at: http://www.cse.msu.edu/~jain/BiometricCryptosystemsIssuesAndChallenges.pdf, last visited 2004.

[25] Wankou Y., Changyin S., and Zhongxi S., "Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA," *in Proceedings of the 30th Chinese Control Conference*, Yantai, China, pp. 2975-2978, 2011.

[26] Wu X., Qi N., Wang K., and Zhang D., "A Novel Cryptosystem based on Iris Key Generation," *in Proceedings of the 4th International Conference on Natural Computation*, Jinan, pp. 53-56 2008.

[27] Yang G., Zhou G., Yin Y., and Yang X., "K-Means Based Fingerprint Segmentation with Sensor Interoperability," avalible at: http://asp.eurasipjournals.com/content/pdf/1687-6180-2010-729378.pdf, last visited 2010.

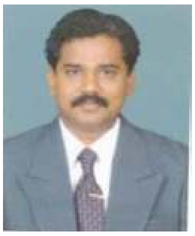
[28] Zhang L., Zhang L., and Zhang D., "Finger-Knuckle-Print: A New Biometric Identifier," *in Proceedings International Conference on Image Processing.* Cairo, pp. 1981-1984, 2009.

[29] Zhang L., Zhang L., Zhang D., and Guo Z., "Phase Congruency Induced Local Features for Finger-Knuckle-Print Recognition," *Pattern Recognition*, vol. 45, no. 7, pp. 2522-2531, 2012.

[30] Zhang L., Zhang L., Zhang D., and Zhu H., "Ensemble of Local and Global Information for Finger-Knuckle-Print Recognition," *Pattern Recognition*, vol. 44, no. 9, pp. 1990-1998, 2011.

[31] Zhang L., Zhang L., Zhang D., and Zhu H., "Online Finger-Knuckle-Print Verification for Personal Authentication," *Pattern Recognition*, vol. 43, no. 7, pp. 2560-2571, 2010.

Muthukumar Arunachalam received his BE (ECE) and ME (Applied Electronics) degrees from Madurai Kamaraj University and Anna University in 2004 and 2006 respectively. Currently, he is pursuing a PhD in ECE at Kalasalingam University, India. He is Assistant Professor of Electronics and Communication Engineering, Kalasalingam University, Krishnankoil-626126, India, where he has been since July 2007. His area of interest is image processing, signal processing, biometrics and wireless communication. He is a life member of ISTE.



Kannan Subramanian received his BE., ME., and PhD degrees from Madurai Kamaraj University, India in 1991, 1998 and 2005 respectively. He is Professor and Head of Electrical and Electronics Engineering, Kalasalingam University, Krishnankoil-626126, India, where he has been since July 2000. He was a visiting scholar in Iowa State University, USA (October 2006–September 2007) supported by the Department of Science and Technology, Government of India with BOYSCAST Fellowship. He is a Sr. Member of IEEE, Fellow of IE (I), Sr. Member in CSI, Fellow in IETE, Life member SSI and Life member of ISTE.