AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print

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

Abstract: *In general, the identification and verification are done by passwords, pin number, etc., which are easily cracked by others. In order to, overcome this issue biometrics is a unique tool to authenticate an individual person. Biometric is a quantity which consists of an individual physical characteristics of fingerprint, Finger Knuckle Print (FKP), iris, face and so on. These characteristics are not easily cracked by others. Nevertheless, unimodal biometric suffers due to noise, intra class variations, spoof attacks, non-universality and some other attacks. In order to, avoid these attacks, the multimodal biometrics i.e., a combination of more modalities is adapted. They are combined with cryptography, which will give more security for physical characters of biometrics. Bio-crypto system provides the authentication as well as the confidentiality of the data. This paper proposes to improve the security of multimodal systems by generating the biometric key from fingerprint and FKP biometrics with its feature extraction using K-means algorithm. The secret value is encrypted with biometric key using symmetric Advanced Encryption Standard (AES) Algorithm. This paper also, discusses about the integration of fingerprint and FKP using package model cryptographic level fusion in order to improve the overall performance of the system. The encryption process will give more authentication and security for the system. The Cyclic Redundancy Check (CRC) function protects the biometric data from malicious tampering and also it provides error checking functionality.*

Keywords: *AES algorithm, biometric crypto-systems, CRC, cryptographic level fusion methodology, k-means algorithm, multimodal biometrics.*

Received May 17, 2013; accepted September 19, 2013; published online September 4, 2014

1. Introduction

Biometrics is a powerful and unique tool based on the anatomical and behavioral characteristics of the human beings. Biometrics is defined as the measure of human body characteristics such as fingerprint, Finger Knuckle Print (FKP), eye, retina, voice pattern, iris and hand measurement. Most anatomical characteristics used for security application are fingerprint, iris, face and palm print [7, 20, 23]. Apart from anatomical characteristics, behavioral characters like voice, signature and gait moments are also used to recognize the user. Therefore, authentication leads an important part in the secured way of communication. Currently, passwords and smartcards are used as the authentication tools for verifying the authorized user. However, passwords can be easily cracked by dictionary attacks and smart cards may be stolen or missed. Therefore, the authorized user will not be identified and the hackers are allowed. The biometrics is the only remedy for the problems. This paper discusses about the two biometric identifiers named as fingerprint and FKP. Analyzing and comparing of all possible biometrics are discussed by Uludag *et al*. [33] on various factors, states 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, 8]. The biometric crypto-system is to provide more security and authentication than the normal passwords and smart card systems. In early days, numerous researches are done in this field. Cryptosystem proposed by Juels and Wattenberg [22] is commenced as fuzzy commitment scheme method. In that paper, they have explained the concept of area of combining error correcting codes with cryptography. Then, Juels and Sudan [21] proposed one more crypto system named as the fuzzy vault system with the feature of order invariance.

Many researches are going on FKP [3, 25] biometric as it has unique characteristic like fingerprint, iris, etc., in order to identify the genuine user. The features of FKP are extracted using the gabor filtering with the cropped region of interest Lin *et al*. [24, 26]. Lin *et al*. [27] has proposed the score level fusion with FKP and its recognition has performed with the phase congruency, local feature and local phase features. David [13] has proposed a novel approach to extract the invariant features as key points, which are used for

object recognition through hough transform. The local information of FKP is accessed using Scale Invariant Feature Transform (SIFT) and Speed Up Robust Features (SURF) [9, 13, 36]. The SIFT algorithm is used to get the key points using the scaling and invariant features, which are matched to prove the user authentication [9, 13]. The fingerprint recognition was done with image segmentation and K-means clustering [5, 14, 19, 28].

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 [34]. This key value is easily cracked by other persons. While using the longer key value, it is hard to store in human memory. Biometric values keep the key as a confidential one from cracking and stealing. The only possible method to avoid the cracking and stealing is to encrypt the data or message with the key using symmetric encryption [34, 35].

Cryptography means an algorithm to convert a normal text into an unreadable format named as cipher text, which is known to sender and receiver alone. Cryptographic method consists of two main classifications; one is symmetric cipher and another one is an asymmetric cipher [12, 34]. 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 only utilize the symmetric cipher so that, biometric key is shared between the encryption and decryption process [7, 11]. Here, the key generated from biometrics is the important. Features are extracted from the biometrics [4, 29] and the extracted feature is converted into the key which is adaptable for the cryptographic process. The feature extraction process extracts the person's input information from the biometric data. 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. The algorithm adapted for feature extraction is K-means algorithm. Symmetric encryption [12, 34] is done using various algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), block ciphers etc., a lot of research has been carried out in the field of authentication and biometric key generation.

Feng *et al.* [16] has proposed the two-layer error correction technique for correcting errors in the key and the key is generated from biometrics. For a cryptanalyst, AES algorithm is very complicated to crack the code and to get the information from that. Most biometric systems that are presently used in real time applications typically use a single biometric characteristic to authenticate the user. The challenges encountered by the unimodal biometric systems are noise in the sensed data, non-universality, spoofing, and intra-class variations. The key is generated by taking pixel value from fingerprint. A message is encrypted using the biometric key (iris) with the error detecting codes and the message will be decrypted by giving biometric data as a key input [35]. In these systems, data are stored using single biometric key values but this munimodal biometric has its own durability and weakness. These limitations of the munimodal biometric system can be solved by integrating the multiple sources of biometric information. Such systems are known as multimodal biometric systems, which are more reliable due to the presence of multiple, independent pieces of data. The limitations of munimodal biometric systems can be overcome by using multimodal biometrics where two or more sources have been used to validate identity. In [1, 32] high security has been achieved by the means of verifying the user's presence continuously. Their system of fingerprint and face biometric data requires the presence of the user at all time, for continuous monitoring, hence, it is not suitable for access control applications. In their approach, the system administrator provides the decision rules in accordance with the security level. In the above reference, the authors use multimode biometrics and the single mode crypto systems. Along with them, this paper proposes multimodal biometrics combined with cryptography using AES in order to improve the security of template and system performance. The fusion methodology is needed for integrating the various biometrics and it is explained in [1, 6, 11, 32]. Bo *et al*. [11] explains about the multibiometric cryptosystems and various levels of cryptographic fusion methods. The two main types of cryptographic fusion methods [11] are fusion at biometric level [31] and decision level. This paper proposes a scenario of integrating the biometrics of fingerprint and FKP combined with AES to form a multimodal biometric crypto system and also examines the system using the decision level fusion i.e., package model cryptographic fusion.

Multibiometric crypto systems consist of two phases: Encryption phase and decryption phase. In the encryption phase, encrypted secret value is stored using the biometric keys. During the decryption phase, using the biometric keys only, the secret value is decrypted which is shown in Figure 1. In these systems, data are stored with biometric key values but confidentiality of the data is low. 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 and fingerprint as the biometric data, which is used to encrypt the secret value with the AES algorithm, along with the Cyclic Redundancy Check (CRC) [10]. 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 minutiae point and key point extraction of fingerprint and FKP. Section 4 discusses about the clustering process using K-means algorithm. Section 5 explains about the multibiometric encryption

and decryption phase. The experimental results and the analysis are given in section 6. Finally, section 7 provides the conclusion.

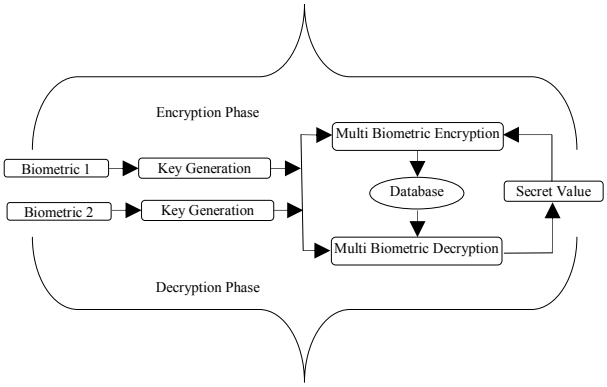


Figure 1. General multibiometric crypto-system.

2. Structure of Proposed Work

Biometrics is a technique used to provide unique individual characteristics of a human being. The unimodal biometric has a number of disadvantages, which is discussed in the introduction section. This paper proposes the multimodal biometrics by integrating fingerprint and FKP. The cryptography is a method, which gives the security as well as authentication for a system. This paper proposes a new technique named as multibiometric crypto-system to merge the above two process, to provide template security and authentication for individuals. The multimodal biometric crypto-system is a new tool to offer a solution to prevent the key memorized. The biometric character itself acts as a key for the 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. This paper identifies the role of fingerprint and FKP as biometric keys for the multimodal biometric crypto systems. For encryption and its reverse process, this paper uses the AES algorithm.

In this paper, biometric keys are generated from the fingerprint and FKP biometrics. The minutiae points and key points extraction processes are done. After obtaining the fingerprint minutiae points and FKP key points values, they can be clustered using the K-means algorithm with the Euclidean distance. In this algorithm, centroid is attained, which is given as the key for encryption process as well as the decryption process. The databases used for this paper were from the Polytechnic university Hongkong [30] and FVC2004 DB1, DB2, DB3, DB4 [18]. The keys generated from the fingerprint and FKP are used for the AES encryption and decryption and they are of 128 bits each. Using K-means algorithm, 128 bits were obtained from fingerprint and FKP with eight clusters. In order to, provide the error free decryption and to provide confidentiality, CRC [10] is included in this paper.

The overview of the proposed work is as shown in Figures 2 and 3. This work consists of two phases: The first one is a multibiometric encryption phase and the second is a multibiometric decryption phase. In the multibiometric encryption phase shown in Figure 2, the secret codeword is generated by concatenating the CRC value with secret value. The secret codeword is:

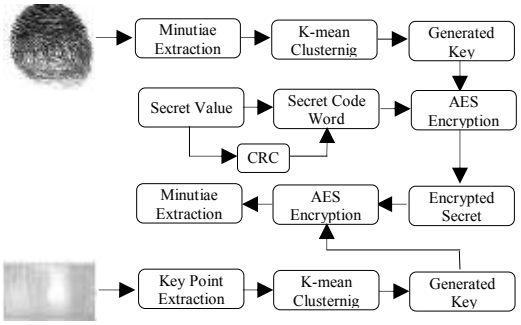


Figure 2. Multibiometric encryption phase.

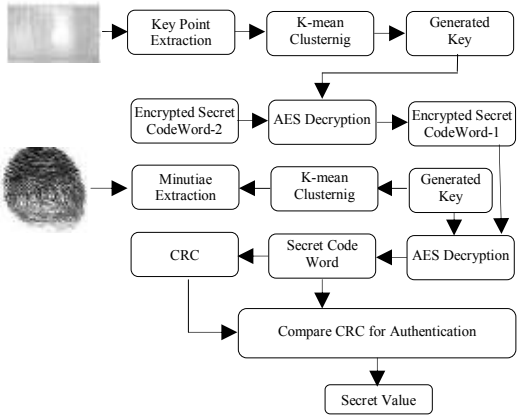


Figure 3. Multibiometric decryption phase.

Encrypted using AES along with the fingerprint biometric key to generate the encrypted secret codeword-1. The same encryption process is repeated with FKP and the biometric key is used for the second time to generate encrypted secret code word-2. This type of encryption is named as package model cryptographic fusion. In the multibiometric decryption phase, the reverse process of encryption phase is done. The encrypted secret codeword-2 is decrypted by the FKP biometric key to give the encrypted secret code word-1, which is again decrypted by fingerprint biometric key to get the secret codeword. Secret codeword is compared with the CRC codeword value for error free decryption in order to prove that the original secret value is extracted from the decryption phase as shown in Figure 3. From these processes the authentications as well as confidentiality are proven.

3. Feature Extraction of Fingerprint and FKP

3.1. Minutiae Extraction of Fingerprint

Fingerprint is one of the most important biometric anatomical characteristics. The fingerprint is framed of valleys and ridges. For minutiae extraction, the proposed system follows the algorithm described in [2,

8, 33], which are depicted in the Figure 4. Each valid minutia point has been characterized by three parameters: x-coordinate, y-coordinate, orientation and ridge associated with it. The fingerprint is captured using sensors, but it has some noises while capturing. In order to, reduce the noise, to increase the contrast between ridges and furrows, the acquiring minutiae points and remove false minutiae points from those minutiae points in the fingerprint, enhancement method is used. In fingerprint, median filter is used to remove the noise. In this, first step appends two rows and columns of zeros to the whole image. Second step separates the image into 3×3 matrices. Third step calculates central pixel based upon the median of all the pixel values.

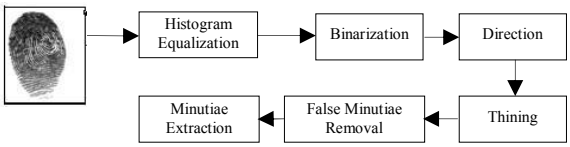


Figure 4. Minutiae extraction process flow.

By using this median filter, noise is removed from fingerprint and the next step is histogram equalization. Histogram equalization is used to enhance the visualization effect by increasing the pixel size which as shown in Figure 5-b. In this binarization, adaptive thresholding method is used [17]. Fast fourier transform is used to divide the whole image to reduce the spurious connection between the ridges. Each pixel contains x and y coordinates and the number of blocks in the whole image are specified as M and N in horizontal and vertical, which are used for Equation 1 to obtain the image in frequency transform.

$$F(u,\ v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp(-j2\pi(\frac{ux}{M}+\frac{vy}{N})) \quad (1)$$

Where: u= 0, 1, 2, …, 31 and v= 0, 1, 2, …, 31.

The next consecutive operation in binarization is adaptive thresholding method. In the original fingerprint image, binarization is used to transform the 8 bit gray image to 1 bit binary image. In this value, 0 is considered as ridges and value 1 is considered as furrows. After the binarization operation is over ridges is viewed as black colour and furrows in white colour. Adaptive thresholding method is used to binarize the image. The direction information of fingerprint is to be considered for authentication. Thus, the orientation information is obtained by converting ridges and furrows to flow curves pointing the direction. For detecting minutiae, direction is important. Direction estimation is based on gradient vector. The next step is thinning and it is defined as skeletonization of fingerprint. It is used to make the terminations and bifurcations to be visible clearly. In this, binary morphologic operations are used to obtain the thinned output. 'open' and 'close' are the two morphologic operations used. Open operation is used to expand the image and eliminate the background noise. Close operation is used to shrink the image and reduce the small cavities. The thinned fingerprint is shown in Figure 5-c. The thinned fingerprint is used to obtain minutiae extraction, which is done by Crossing Number (CN) algorithm.

The *CN* method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighbourhood of each ridge pixel using a 3×3 window. After the *CN* for a ridge pixel has been computed and the pixel can then be classified according to the property of its *CN* value.

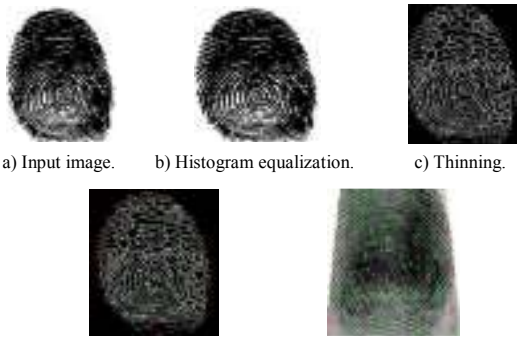
$$CN = 0.5\sum_{i=1}^{8}|p(i)-p(i+1)| \quad (2)$$

CN is calculated by using the Equation 2. A ridge pixel with a *CN* of one corresponds to a ridge ending and a *CN* of three corresponds to a bifurcation which is shown in Table 1.

Table1. Crossing number table.

P4	P3	P2
P5	P	P1
P6	P7	P8

Next step is false minutiae removal. It is implemented using Euclidean distance Equation 3, which is used to find the distance between termination and bifurcation.



a) Input image. b) Histogram equalization. c) Thinning.

d) False removal. e) Minutiae points.

Figure 5. Minutiae points extraction.

$$Distance=\sqrt{(u_i-u_j)^2+(v_i-v_j)^2} \quad (3)$$

The minutia extracted output image is shown Figure 5-e and removed false minutiae output image is shown in Figure 5-d.

1. If *Distance* is too small, then minutiae are false.
2. If *Distance* is medium, then minutiae are true.
3. If *Distance* is large, then minutiae are true.

Based on the above condition false minutiae are removed.

3.2. 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 [13]. The process of feature extraction as shown in Figure 6,

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. 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 7-b. The next step of feature extraction is to extract the key points from FKP using the SIFT [13].

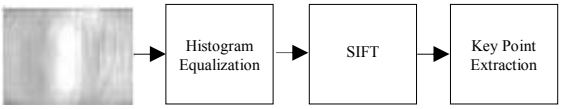
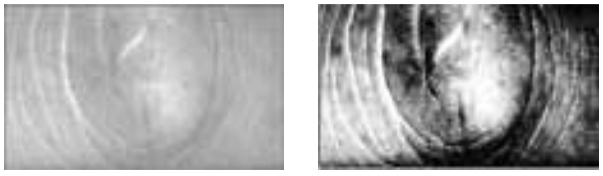


Figure 6. Feature extraction of finger knuckle print.

The SIFT algorithm is mainly used for image matching purpose. SIFT is also, 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 on order to detect the key point locations which are invariant to scale change. The difference of gaussian is calculated by Equations 4 and 5.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{4}$$

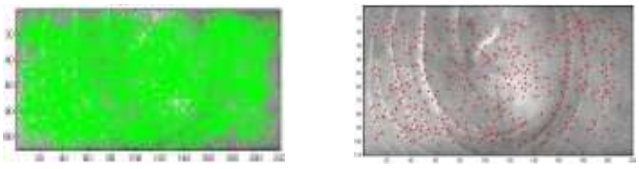


a) Input image of FKP. b) Histogram equalization.

Figure 7. Histogram process.

$$D(x, y, \sigma) = G(x, y, k\sigma) * I(x, y) - G(x, y, \sigma) * I(x, y)$$
$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \tag{5}$$

The above equation $I(x, y)$, $G(x, y, \sigma)$, $L(x, y, \sigma)$ 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 6.



a) Key Point localization of FKP. b) Key points of FKP.

Figure 8. Key points extraction using SIFT.

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{6}$$

The next step is to detect the local maxima and minima of $D(x, y, \sigma)$ by comparing 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 8-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 8-b. The key points selected are scale invariant points.

4. Key Generation using K-means Algorithm

Clustering is the process of grouping a non-linear set of objects. This approach assigns 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 minutiae and key points, which are used as the keys for the AES encryption process.

The minutiae and key points taken from the feature extraction process are clustered using this algorithm. Consider the points given as the input data vectors $M = (m_1, \ldots, m_n)$. The process of fingerprint and FKP K-means clustering is shown below [5, 14, 28]. K-means algorithm starts by initializing the first co-ordinate values as the centroid and defines the numbers of clusters to be split.

Algorithm 1*: K-means Algorithm*

1. *Minutiae and Key points are taken from fingerprint and FKP.*
2. *Initialize cluster and centroid with minutiae and key points.*
3. *Find the distance between two points with centroid value.*
4. *Assign number of clusters with minimum distance.*
5. *If (optimum number of clusters is reached)*
   Calculate centroid and clusters
   Else
   Go to step 2.

According to the problem, this paper proposes the eight numbers of clusters to be defined for the each biometrics and these objects are assigned to each cluster initially. Then, according to the initial centroid value, calculate distance between centroid and key points is calculated using Euclidean distance Equation 7. The minimum distance is retained in the updated distance matrix:

$$\|c_i - m_k\|^2 = \sum_{j=1}^{r} [c_i(j) - m_k(j)]^2 + \sum_{j=r+1}^{p} [c_i(j) - m_k(j)]^2 \tag{7}$$

The key points are grouped into new clusters until an optimum cluster is reached. When optimum cluster value is reached, there is no possibility of movements

for the minutiae and key points to move on the next cluster. At optimum level, centroid value is also calculated.

5. Multibiometric 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 [12, 34]. Here, symmetric encryption is used because an individual person can be authenticated to prove his/her individuality in both phases of encryption and decryption. The authenticated person alone 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 CRC [10] algorithm.

The overview process of AES algorithm is shown in Figure 9 [15, 34]. The AES can perform the block cipher with the key length of 128 bits, 192 bits and 256 bits. In this paper, 128 bits key is used, which is obtained from the fingerprint and FKP. The AES algorithm is processed in matrix form in terms of bytes. The input and output matrix consist of four rows and four columns of one byte each. So, the secret codeword values of 128 bits (16 bytes) are arranged in 4×4 matrixes with each of one byte. Biometric keys of 128 bits 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 codeword consists of 16 bytes and fingerprint biometric key consists of 16 bytes (128 bits) enter the first round of AES algorithm [34]. 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 16 bytes. The 16 bytes 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. The resulted word is XORed with the second word and similarly for third and fourth word also. From this, another four words of key are obtained, which are used for second round of encryption process and they are represented as w [4, 7] in Figure 9. Similarly, key is expanded up to ten rounds. Finally, the key is expanded to 44 words. The four bytes are taken as input and generated as output. These four processess are done up to ten rounds repeatedly and continuously. Finally, after the completion of ten rounds, encrypted secret codeword-1 and 2 value is generated.

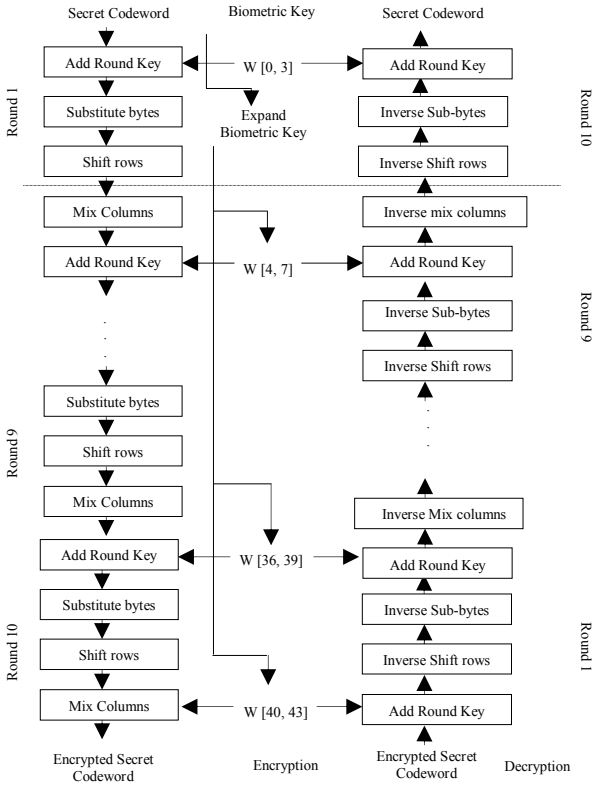


Figure 9. Overview of AES encryption and decryption [34].

The fingerprint and FKP K-means clustering feature values are used as the biometric key for multibiometric encryption as well as decryption purposes. The overview of multibiometric encryption phase is shown in Figure 2. The multibiometric encryption phase consists of following steps:

- *Step* 1: Is to generate the secret codeword of 128 bits which is the concatenated values of secret value and the CRC bits. CRC bits are generated by dividing the secret value with common divisor in both encryption and decryption phase, in order to find the remainder values which is concatenated with secret value.
- *Step* 2: Is to extract the minutiae points from the fingerprint and the extracted points are clustered using K-means algorithm. The centroid values calculated from k-means clustering are converted into fingerprint biometric key of 128 binary bits.
- *Step* 3: Is to encrypt the secret codeword of 128 bits with the fingerprint biometric key value of 128 bits using AES algorithm to generate encrypted secret codeword-1. The overview process of AES algorithm is shown in Figure 9 [34].
- *Step* 4: Is to extract the key points from the FKP and the extracted key points are clustered using K-means algorithm. The centroid values calculated from K-means clustering are converted into FKP biometric key of 128 binary bits.
- *Step* 5: Is to encrypt the encrypted secret codeword-1 with the FKP biometric key value of 128 bits using AES algorithm to generate encrypted secret codeword-2. This method of encrypting the secret codeword in overlapping form is known as package model cryptographic fusion process.

The overview of multibiometric decryption phase is shown in Figure 3. The key generation of fingerprint and FKP is same for both encryption and decryption phases. The multibiometric decryption phase consists of following steps:

- *Step* 1: Is to decrypt the encrypted secret codeword-2 with the FKP biometric key value of 128 bits using AES algorithm to generate encrypted secret codeword-1. The overview process of AES algorithm is shown in Figure 9 [34].
- *Step* 2: Is to decrypt the encrypted secret codeword-1 with the fingerprint biometric key value of 128 bits using AES algorithm to generate secret codeword.
- *Step* 3: Is to compare the secret codeword with CRC bits. If the remainder of the received secret code word is zero, then secret value is released to prove user is authenticated as well as a genuine one. If it fails, the secret value is not released and the user is proved as imposter one.

6. Experimental Results and Analysis

Experiments in this paper are conducted using the fingerprint database FVC [18]. This database consists of four sub databases, first three sub databases are collected from various sensors and fourth sub database is generated synthetically. Each sub database consists of 80 fingerprint images. The details of each database are shown in Table 2. The followed experiments in this paper are conducted using the FKP database from FKPROI of Hong Kong Polytechnic University [30]. 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.

Table 2. FVC 2004 database details.

Name of Database	Sensor Type	Image Size	Resolution
DB1	Optical Sensor	640×480	500 dpi
DB2	Optical Sensor	328×364	500 dpi
DB3	Thermal Sweeping Sensor	300×480	512 dpi
DB4	SFinGe v3.0	288×384	about 500 dpi

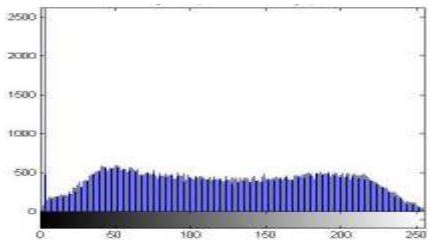


Figure 10. Histogram equalization of fingerprint.

The output of fingerprint minutiae extraction is shown in Figure 5. The fingerprint image is enhanced with histogram equalization, which is shown in Figure 5-b and 10. The minutiae values of fingerprints are grouped into eight clusters and its centroid value is found. The FKP image is enhanced with histogram equalization, which is shown in Figures 7-b and 11. The output of FKP key point localization and key point's extractions are shown in Figures 8-a and b. The key point values of FKP are grouped into eight clusters and its centroid value is found. The centroid values of both biometrics are converted into 128 binary bits of each which is shown Figure 14. These 128 binary bits are used as biometric key for multibiometric encryption and decryption phase.

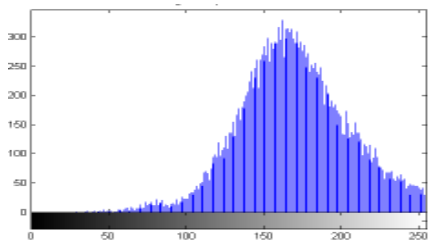


Figure 11. Histogram equalization of FKP.

The centroid value of K-mean clustering for both fingerprint and FKP is shown in the Figures 12 and 13. Here, CRC divisor of 10101 is used in both encryption and decryption phase. The remainder value concatenated to the secret value is 0111 by using CRC algorithm.

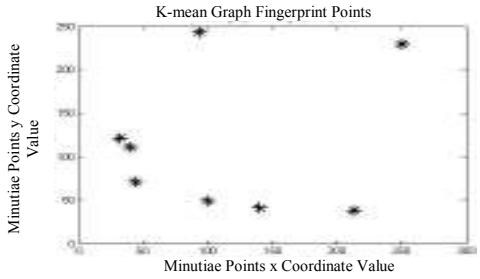


Figure 12. K-mean clustering graph for fingerprint points.

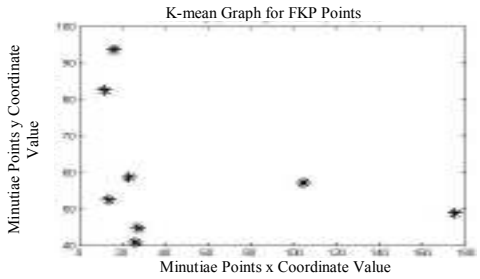
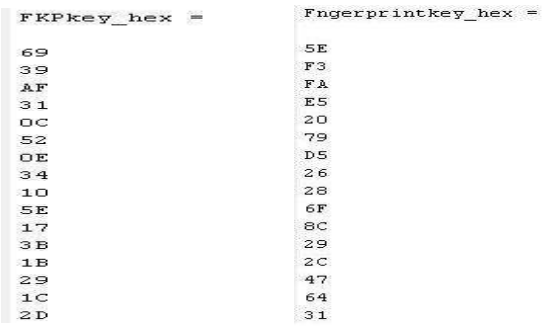


Figure 13. K-mean Clustering graph for FKP points.



a) FKP key value. b) Fingerprint key value.

Figure 14. Key generation.

For this paper, simulation is performed by 10 images of each database subset for both biometrics. For example, an encryption and the decryption phase output are taken from both biometric images of fingerprint and FKP is shown in Figure 15. Table 3 consists of all parameters which are used in this paper to perform all the steps. In Figure 15, initial state represents the secret codeword, which is the concatenated value of secret value and CRC value.

Table 3. Parameters used for multibiometric encryption and decryption phase using fingerprint.

Parameter	Size
No. of Genuine Points(Finger print)	18-26 points
No. of Key Points (FKP)	430-545 points
K-means Clustering	8 clusters
Processing Format	Hex Decimal, Binary
Finger Print Key Value	128 bits
FKP Key Value	128 bits
Secret Codeword	128 bits
No. of Rounds for AES	10 rounds

That concatenated value is given as input for AES algorithm using 128 bits of fingerprint biometric key values to give encrypted secret codeword-1. One more encryption is done for encrypted secret codeword using 128 bits key value of FKP to give encrypted secret codeword-2 by package model cryptographic fusion and is shown as the final state in Figure 16.

In decryption phase vice versa process of encryption was done, which is shown in Figure 15. 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.

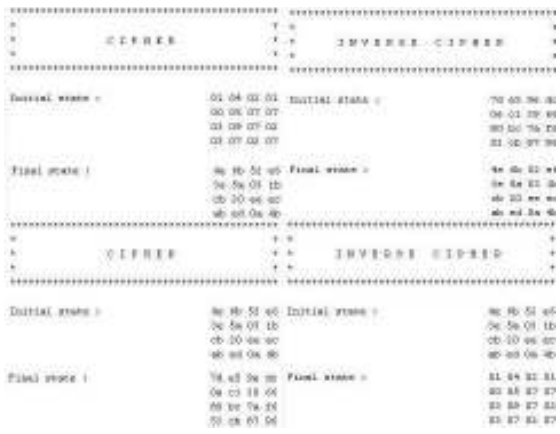


Figure 15. Multibiometric encryption and decryption phase output.

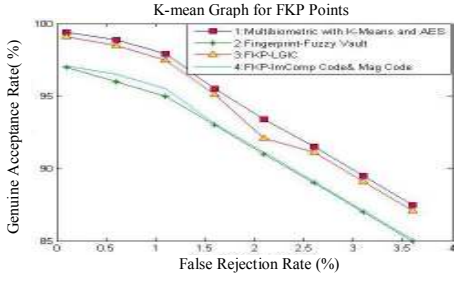


Figure 16. ROC curves of proposed system compared with existing system.

$$GAR = \frac{No.\ of\ genuine\ attempts\ accepted}{Total\ no.\ of\ genuine\ attempts} \quad (8)$$

$$FRR = \frac{No.\ of\ genuine\ attempts\ rejected}{Total\ no.\ of\ genuine\ attempts} \quad (9)$$

The *GAR* and *FRR* are calculated by Equations 8 and 9. If the number of imposter points is very low in fingerprint then the *GAR* is high but *FRR* is low. If this does not happen, *FRR* is high and system will not be valid one.

When the number of key points is high with *FKP*; the *GAR* is high but *FRR* is low. If this does not happen, *FRR* is high and then system will not be a valid one. According to this proposed approach, the *GAR* is increased with more genuine points, key points and with the maximum cluster size. The comparison of proposed approach with the existing approach is shown in Table 4 and also shown in the ROC graph in Figure 16. The overall performance of this proposed approach is 99.4%.

Table 4. Comparison for proposed approach.

Algorithm	GAR (%)	FRR (%)
FKP-ImComp Code and Mag Code [7]	97	3
FKP-LGIC [6]	99.14	0.96
Fingerprint-Fuzzy Vault [8]	97	3
Multibiometric with K-means and AES Algorithm (Proposed)	99.4	0.6

7. Conclusions

This paper presents a method of multibiometric cryptosystems based on the fingerprint and FKP key generation using K-means algorithm. According to this research work, the authentication and confidentially are done by generating secret codeword using CRC function. Here, the secret codeword is encrypted double times by AES algorithm with two different keys generated from fingerprint and FKP to produce the encrypted secret codeword 1 and 2 by package model cryptographic fusion. The reverse process is done in multibiometric decryption phase. This type of system secures the data very effectively.

Acknowledgements

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

References

[1] Abhishek N., Karthik N., and Anil K., "Multibiometric Cryptosystems based on Feature Level Fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no.1, pp. 255-268, 2012.

[2] Ajay K. and David Z., "Improving Biometric Authentication Performance from the User Quality," *IEEE Transactions on Instrumentation*

and Measurement, vol. 59, no. 3, pp. 730-735, 2010.

[3] Ajay K. and Venkata P., "Personal Authentication using Hand Vein Triangulation and Knuckle Shape," *IEEE Transactions on Image Processing*, vol. 18, no. 9, pp. 2127-2136, 2009.

[4] Ajay K. and Yingbo Z., "Personal Identification using Finger Knuckle Orientation Features," *Electronics Letters*, vol. 45, no. 20, pp. 1023-1031, 2009.

[5] Aloysius G., "Efficient High Dimension Data Clustering using Constraint-Partitioning K-Means Algorithm," *the International Arab Journal of Information Technology*, vol. 10, no. 5, pp. 467-476, 2013.

[6] Anil J., Karthik N., and Arun R., "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270- 2285, 2005.

[7] Anil K. and Sharath P., "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transaction on Information Forensics and Security*, vol. 2, no. 4, pp. 744-747, 2007.

[8] Anil K., Arun R., and Sharath P., "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143, 2006.

[9] Badrinath G., Aditya N., and Phalguni G., "An Efficient Finger-knuckle-print based Recognition System Fusing SIFT and SURF Matching Scores," *in Proceedings of ICICS*, Beijing, China, pp. 374-387, 2011.

[10] Behrouz A., *Data Communication and Networking*, McGraw Hill, 2007.

[11] Bo F., Simon X., Jianping L., and Dekun H., "Multibiometric Cryptosystem: Model Structure and Performance Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 867-882, 2009.

[12] Bruce S., *Applied Cryptography Protocols, Algorithms*, Wiley Publication, 1994.

[13] David G., "Distinctive Image Features from Scale-Invariant Keypoints," *the International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[14] Fatima M. and Safia N., "Privacy Preserving K-Means Clustering: A Survey Research," *the International Arab Journal of Information Technology*, vol. 9, no. 2, pp. 194-200, 2012.

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

[16] Feng H., Ross A., and John D., "Combining Crypto with Biometrics Effectively," *IEEE Transaction on Computers*, vol. 55, no. 9, pp. 1081-1088, 2006.

[17] Francis H., Lam F., and Hui Z., "Adaptive Thresholding by Variational Method," *IEEE Transaction on Image Processing*, vol. 7, no. 3, pp. 468-47, 1998.

[18] FVC2004., available at: http://bias.csr.unibo.it/fvc2004/, last visited 2004.

[19] Gongping Y., Guang-Tong Z., Yilong Y., and Xiukun Y., "K-Means based Fingerprint Segmentation with Sensor Interoperability," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, no. 54, pp. 1-12, 2010.

[20] Hong L., Anil K., and R. Bolle., "On-line Fingerprint Verification," *Pattern Analysis and Machine Intelligence*, *IEEE Transactions*, vol. 19, no. 4, pp. 302-314, 1997.

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

[22] 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.

[23] Kumar A. and Passi A., "Comparison and Combination of Iris Matchers for Reliable Personal Authentication," *Pattern Recognition*, vol. 43, no. 3, pp. 1016-1026, 2010.

[24] Lin Z., Lei Z., and David Z., "Finger-Knuckle-Print: A New Biometric Identifier," *in Proceedings of the 16th IEEE International Conference on Image Processing*, Cairo, Egypt, pp. 1981-1984, 2009.

[25] Lin Z., Lei Z., David Z., and Hailong Z., "Ensemble of Local and Global Information for Finger-Knuckle-Print Recognition," *Pattern Recognition*, vol. 44, no. 9, pp. 1990-1998, 2011.

[26] Lin Z., Lei Z., David Z., and Hailong Z., "Online Finger-Knuckle-Print Verification for Personal Authentication," *Pattern Recognition*, vol. 43, no. 7, pp. 2560-2571, 2010.

[27] Lin Z., Lei Z., David Z., and Zhenhua G., "Phase Congruency Induced Local Features for Finger-Knuckle-Print Recognition," *Pattern Recognition*, vol. 45, no. 7, pp. 2522-2531, 2012.

[28] Manhua L., Xudong J., and Alex C., "Efficient Fingerprint Search based on Database Clustering," *Pattern Recognition*, vol. 40, no. 6, pp. 1793-1803, 2007.

[29] Miguel A., Carlos M., and Jesus B., "Using Hand Knuckle Texture for Biometric Identifications," *Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, pp. 23-27, 2006.

[30] PolyU FKP Database., available at: http://www.comp.polyu.edu.hk/~biometrics/FKP.htm, last visited 2013.

[31] Ramya M., Muthukumar A., and Kannan S., "Multibiometric based Authentication using Feature Level Fusion," *in Proceedings of*

International Conference on Advances in Engineering, Science and Management, Tamil Nadu, India, pp. 191-195, 2012.

[32] Sim T., Zhang S., Janakiraman R., and Kumar S., "Continuous Verification using Multimodal Biometrics," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 687-700, 2007.

[33] Uludag U., Pankanti S., Prabhakar S., and Anil K., "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004.

[34] William S., *Cryptography and Network Security Principles and practice*, Prentice Hall, 2011.

[35] Xiangqian W., Ning Q., Kuanquan W., and Zhang D., "A Novel Cryptosystem based on Iris Key Generation," *in Proceedings of the 4th International Conference on Natural Computation*, Jinan, China, pp. 53-56, 2008.

[36] Zhu L., "Finger Knuckle Print Recognition based on SURF Algorithm," *in Proceedings of the 4th International Conference on Fuzzy Systems and Knowledge Discovery*, Shanghai, China, pp. 1879-1883, 2011.

Muthukumar Arunachalam received 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 Communicatio Engineering, Kalasalingam University, India, where he has been since 2007. His area of interest is: Image processing, signal processing, biometrics and wireless communication. He is a life member of ISTE.

Kannan Subramanian received 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, India, where he has been since 2000. He was a visiting scholar in Iowa State University, USA, 2006-2007 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.