A Robust Multimodel Biometric Crypto System

Komal, Chander Kant

Abstract—Biometric based authentication has several advantages over traditional password or PIN based authentication process because biometric is consists of physical or behavioural characteristics i.e fingerprint, face, Finger Knuckle Print (FKP), iris, voice etc. Unimodal biometric system h as some drawbacks i.e non universality, inter-class variation, intra-class variation; system can be circumvented by the skilled imposter etc. These drawbacks can overcome by multimodal biometric system as it combines more than one modality for authentication. When multimodal system combined with cryptography it makes system more robust and secure. In this paper, a robust multimodal biometric crypto system has been proposed, in which two modalities (FKP and face) are used for authentication of a person and one modality (fingerprint) is used for key generation. AES algorithm with fingerprint based key is used for securing the biometric templates. At authentication time, decision level fusion with AND rule is used for making the final decision. The proposed multimodal biometric crypto system is more robust and secure as compare with other multimodal biometric systems. Experimental results are shown with the help of MATLAB3. 2017b.

Keywords—Biometric crypto system; Face recognition; Finger recognition; FKP recognition; Multimodal biometric System.

I. INTRODUCTION

Traditional authentication schemes such as password, card, key etc. are not sufficient and can be easily forgotten, lost, stolen or shared. These problem can overcome by biometric authentication system because there is no key to be lost or password to be forgotten and only single biometric trait (Finger, face, FKP, etc.) can be used to access several accounts without the need of remembering anything like password, pin etc. Biometric based system can be used for personal data privacy or financial transactions in the federals, state or central governments, and in the military, in the banking, in health services, in commercial applications etc [1]. But there are also some limitations in the unimodal biometric system i.e. non universality, inter-class variation, intra-class variation, system can be circumvented by the skilled imposter, etc. Multimodal biometric system overcomes these problems and increases the security of the system using more than one biometric trait [2]. If an imposter is able to steal one biometric trait even then he/she will not crack the system.

The combination of multimodal biometric with cryptography makes the biometric systems more secure. There are two type of cryptography technique: symmetric key and asymmetric key cryptography technique. In symmetric key cryptography, same key is used for encryption and decryption process. In our proposed system, we have been using symmetric key based AES algorithm. In AES algorithm, 128 bit, 192 bit or 256 bit key is used for encryption or decryption process [3]. This paper proposes a multimodal biometric crypto system, in which two modalities (FKP and face) are used for authentication of a person and one modality (fingerprint) is used for key generation. AES algorithm with fingerprint based key is used for securing the biometric templates. The key generation process uses the K-mean clustering algorithm to generate the key from fingerprint features set. The proposed system is called a 'novel multi-modal biometric crypto system'.

Many researches were conducted in the field of multi-biometric crypto system. The system has two phases: 1) Encryption phase 2) Decryption phase [4]. In encryption phase, encrypt the modalities using secret key. In decryption phase, decrypt the encrypted modalities using secret key and find out the original template. Bo et al [5] described the multi-biometric cryptosystem and different levels of fusion. Decision level fusion is best for biometric cryptosystem because it is easy to apply and less time consuming. Other level of fusion may increase the complexity of the biometric cryptosystem [6]. The proposed system fuses the biometric modalities at decision level and after then takes final decision.

The following section 2 discussed about the related work has been done in this area. Next section 3 discussed feature extraction process of fingerprint, face & FKP and a biometric based key generation process using k-mean clustering algorithm. Section 4 includes the architecture of proposed multimodal biometric crypto system. Section 5 shows the experimental results and discussion. Last section includes the summary and conclusion of this paper

II. RELATED WORK

Multimodal biometric Fusion has achieved significant attention in few years because it increases the performance of system. Cryptography with multimodal biometric improves the security of the system. Some cryptography techniques with multimodal biometric has been studied in the literature.Jagadiswary and Saraswady [7] designed a multimodal sstem by fusing finger-print, retina and finger-vein with cryptographic techniques. Proposed system has GAR of 94%, FAR of 1.46% and FRR of 1.07%.Bala and Joanna [8] proposed a multimodal system with iris and palm vein. Features of both the modalities were extracted with the help of feature extraction process and then a Blow fish

Revised Manuscript Received on August 19, 2019.

Komal, Ph.D Scholar, Department of Computer Science and Application, KUK, Haryana (136119), India.

Dr.Chander Kant, Assistant Professor, Department of Computer Science and Application, KUK, Haryana (136119), India.

cryptography algorithm is applied to secure the feature set. FAR and FRR of the proposed system is very low.

S. More et al. [9] proposed a multimodal system with finger-print, face, iris and palm-print input modalities. Features of the input modalities are extracted with feature extraction process and then apply Data Encryption Standard (DES) cryptographic algorithm for securing the features. Experimental results are shown with the help of MATLAB.

Gawande et al. [10] proposed a multimodal system by combining finger-print and iris at feature extraction level and then apply cryptographic technique to secure templates of input modalities. Publically available CASIA database is used for showing the results. Results of this proposed system is improved with cryptographic encryption. Raghu and Deepthi [11] proposed a multimodal authentication system based on cryptographic encryption technique. User defined secret key is used to combine features of finger-print and iris. Experimental shows that proposed system is better than unimodal system with cryptographic techniques.

Ashok et al. [12] poposed a system which will help the users to update their biometric password and resolves many issues present in existing biometric systems. Hashing function is used to create biometric password. Cryptography with biometric improves the security of the sytems and performs better than many existing systems.

S1 and Mathew [13] proposed a encrypted biometric system in which secret key is generated with the help of biometric modality. 32 bit fingerprint id is used to encrypt the Iris. Blow fish encryption technique is used to encrypt the template at enrolment time. During authentication decryption process has been done and then verify that the user is genuine or imposter.

Arunachalam and Subramanian [14] proposed a system to improve the security with the help of biometric key. In this system,FKP and finger-print are used to generate the biometric key with the help of K-mean algorithm. AES encryption technique is used to encrypt the template. CRC (Cyclic Redundancy Check) is also used to check errors and remove malicious tempering.

E.S.SHAMEEM S. [15] proposed a multi biometric system which combines FKP and face. This system is called as Multi-modal Biometric Authentication System (MMBAS) which uses Scale Invariant Feature Extraction (SIFT) process to reduce complexity of the system and remove errors caused by distorted samples. Experimental results show that proposed system is far better than other existing system.

S. Chaudhary and R. Nath [16] proposed a system by integrating face, Iris and voice using sum rule fusion technique at match score level. The proposed system is far better than unimodal systems. Publicly available databases are used to check the performance of the system. Experimental results are shown with the help of MUBI tool.

Anne Wincy, Jacob Vetha Raj [17] proposed a multimodal system using FKP, face and palm-print. SIFT and Speeded Up Robust Features (SURF) processes are used to extract the feature set and Support Vector Machine (SVM) are used as classifier. FAR and FRR of the proposed system is lower than unimodal system. experimental results show that proposed system is very effective and reliable.

III. FEATURE EXTRACTION AND KEY GENERATION PROCESS

3.1 Fingerprint feature extraction

Fingerprint is the oldest and most essential biometric modality. Fingerprint is the combination of ridges and valleys [18]. For minutiae point extraction, algorithm is described in Fig. 4. Sensor is used to capture the fingerprint, but it can have some noises. An enhancement method is used to reduce the noises, increases the contrast of fingerprint image and remove false feature points. Noise can be removed with the help of median filter. In first step, adds 2×2 matrix of 0's to the image. In second step, splits whole image into 3×3 matrices. In third step, calculates central pixel [19].

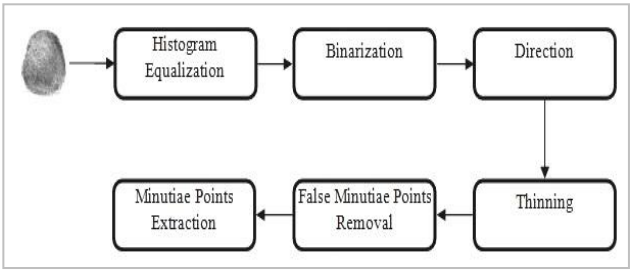


Fig 1: Fingerprint feature set extraction process

After using median filter, histogram equalization is used to increase the pixel size to enhance the visualization as shown in Fig 5b. After then binarization is used to reduce the false connection between ridges by Fourier transformation and transform the original image in to binary image. Each pixel in the image contains xand y coordinates and several number of blocks in fingerprint image are specified as P and Q in horizontal and vertical direction, which are given in Equation (1) given below to get the frequency transform image

$$F(u,v) = \sum_{x=0}^{P-1} \sum_{y=0}^{Q-1} f(x,y) \exp\left(-j2\pi \left(\frac{ix}{P} + \frac{jy}{Q}\right)\right) \quad (1)$$

Where: *i= 0, 1, 2, ..., 31 and j=0, 1, 2, ..., 31*

Adaptive thresholding method is applied after frequency transformation of image [20]. Binarization transforms gray scale to binary image. In the image, ridges have 0 value and valleys have value 1. Hence colours of ridges are black and valleys are viewed as white in colour. The direction information of fingerprint is acquired by altering valleys and ridges to curves. Direction information is important to detect the minutiae points. Gradient vector is used to estimate the direction. The next thining step is the skeletonization of fingerprint. This step is used to increase the visibility of bifurcation and terminations. Thinned ouput is obtained by two morphologic operations 'open' and 'close'. Image enlargement and noise removal is done by open operation. Image contraction and small cavities removal is done by close operation [21]. Crossing Number (CN) table as shown in Table 1 can help to find out the feature points in thinned fingerprint. The CN table is a 3×3 matrix of pixels value in which examined the neighbourhood of each value to find

out the ridge termination and bifurcation

Property of CN value is used to classify the value of all the pixels [22].

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

Above equation (2) is used to calculate the value of CN. Pixel value of one is corresponds to ridge termination and pixel value of 3 is corresponds to bifurcation. Table 1 shows the 3×3 Crossing Number table.

Table1: Crossing Number Table

M4	M3	M2
M5	M	M1
M6	M7	M8

After this step, apply Euclidean Distance method to remove false points. This method is used to find out the distance between the ridge terminations and bifurcations [23]. Below equation (3) is used to calculate the Euclidean Distance.

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

Condition to check whether the minutiae point are true or false is if distance is medium only then minutiae points are true otherwise points are false [24].

Next part of this section includes FKP feature extraction process. FKP has unique texture and characteristics like fingerprint. Most of researches have been going on FKP recognition.

3.2 FKP feature extraction process

Finger of every person has three joint, first joint is proximal phalanx where finger joins hand, second joint is middle or proximal inter phalanx and third joint is distal phalanx [25]. A finger knuckle of every person is characterized by no of creases on back side of finger [26]. Structures of these creases are unique. First step is to capture the FKP image from sensor. After this, extract the Region of Interest (ROI) and apply pre-processing techniques on FKP image to enhance the quality of image. After then extract the key points of input FKP image as shown in Fig 2 [27]. FKP feature extraction process has some steps which are as follows:

- Capture the input image through sensor.
- Extract Region of Interest (ROI) through edge detection technique
- Apply image enhancement techniques to increase the quality of image.
- Apply SIFT algorithm to extract the feature set.

.

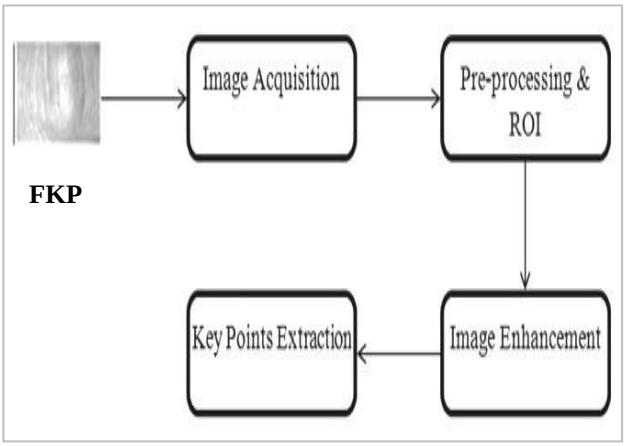


Fig 2: FKP feature set extraction process

SIFT algorithm is used for detection of key points and then extracting local key points from input image [28].

Next part of this section includes face feature set extraction process. Every human being has different facial characteristics and these are used to authenticate a person.

3.3 Face Feature extraction process

Every individual face has some organs like eyes, nose, ears etc. and each organ has some shape or size [29]. Characteristics of these organs are different person to person. In face recognition, geometrical distribution of these organs and relative distance between them is used to find out the eigen values (features set) of face [30].

Generally, Face recognition includes four phases: Face detection, pre-processing, feature set extraction and identification phase as shown in Fig.3. In face detection phase, detect the Region of Interest (ROI) from the input face image. Pre-processing phase mainly includes: removing extra noise, gray scale normalization. Gray scale normalization eliminates the illumination effect on image and improves the recognition rate by image enhancement. After then PCA algorithm is used to extract the face feature set [31].

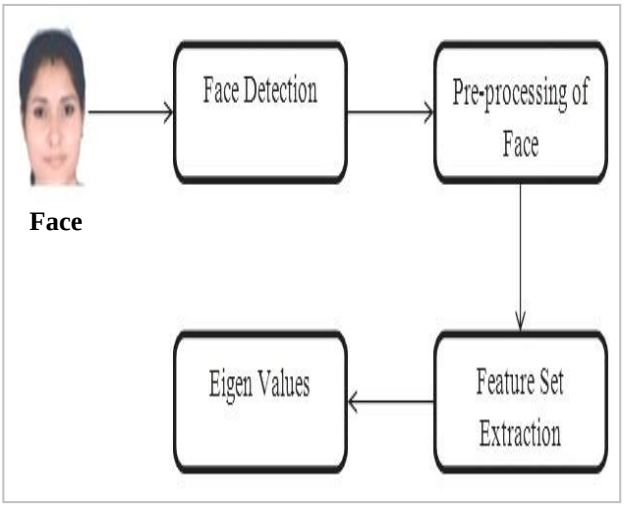


Fig 3: Face feature set extraction process

PCA algorithm is used to transforms the multi-dimensional data into low-dimensional data [32]. Steps involved in PCA algorithm: i) Noise reduction, gray scale normalization and angle orientation processing are performed. ii) Collected 'n' images are denoted as I_1, I_2, I_3, ..., I_n.

. Inside the records circulating framework, the data maker will post their surenesses constantly. for instance, prosperity office X(table 1) disperses their substances after predictably and singular U visits the therapeutic center X in March for the disease D. Later in June buyer U visits the prosperity office X for the comparable issue D. prosperity center X appropriates their dataset in April and later in August. By and by, the supporter U exists in the all posted datasets with the unclear QI regards. An adversary may in like manner use these conveyed datasets to predict the purchaser U and the fragile characteristics in 100 percent certainty. There may be various works have achieved to deal with the surenesses dispersing privateness issues. additionally, those posted works decay the bits of knowledge programming to guarantee the non-open privateness[7].

- Extract minutiae points from fingerprint.
- Initialize centroid and cluster with extracted minutiae points.
- Find Euclidean distance between two minutiae points and centroids.
- Assign cluster with minimum distance.
- If (no of cluster is optimum)

Calculate centroid value and number of clusters

Else

Go to step 2.

Calculate the distance between initial centroid value and minutidae points using Euclidean distance method. Minutiae points are grouped in new cluster until an optimum number of clusters are reached. When condition met then minutiae points cannot move to the next cluster. Calculate centroid value at optimum level.

Next section includes the architecture of proposed multimodal biometric crypto system. Proposed system is more secure than the existing multimodal biometric systems because it uses the AES algorithm with biometric key to encrypt the FKP and face templates.

IV. PROPOSED WORK

The architecture of proposed multi-model biometric crypto system integrating face and FKP is shown in Fig 4. In the enrolment phase, first step is to capture three modalities i.e fingerprint, face and FKP through sensor and then remove extra noise from images using median filtering and detect the Region of Interest (ROI). Second step is to extract the valuable feature set by applying appropriate algorithms. Third step is to generate a key from fingerprint feature set using K-mean clustering algorithm and apply this key to encrypt the feature sets of face and FKP using AES encryption. Encrypted feature set of face and FKP is stored in Encrypted Face Template (EFT) and Encrypted FKP Template (EFKPT) respectively. Next step is to transform the key using substitution transformation method and make the Encrypted Key (EK). Last step in the enrolment phase is to store the EFT, EFKPT and EK in the Database.

In authentication phase, only face and FKP modalities are used for identification of a person. Fingerprint modality is used only in the enrolment phase for the key generation process. First step is to obtain the Encrypted Key (EK) from the database and decrypt it using the same transformation method and get the original Key (K). Next step is to obtain the EFKPT and EFT from database and decrypts the templates with AES decryption algorithm using same K generated in the enrolment phase. After this step, we get the original FKP template (FKPT) and Face Template (FT). Next step is to match the obtained templates of FKP and face from database with the templates generated at the authentication time. If the matching score of both matcher are greater than the set thresholds t1 and t2 respectively only then it gives positive result otherwise not. In our proposed system we used the decision level fusion with AND Rule because it is very easy to use and gives precise results. If output of both matchers is positive only then accept the user otherwise reject him/her.

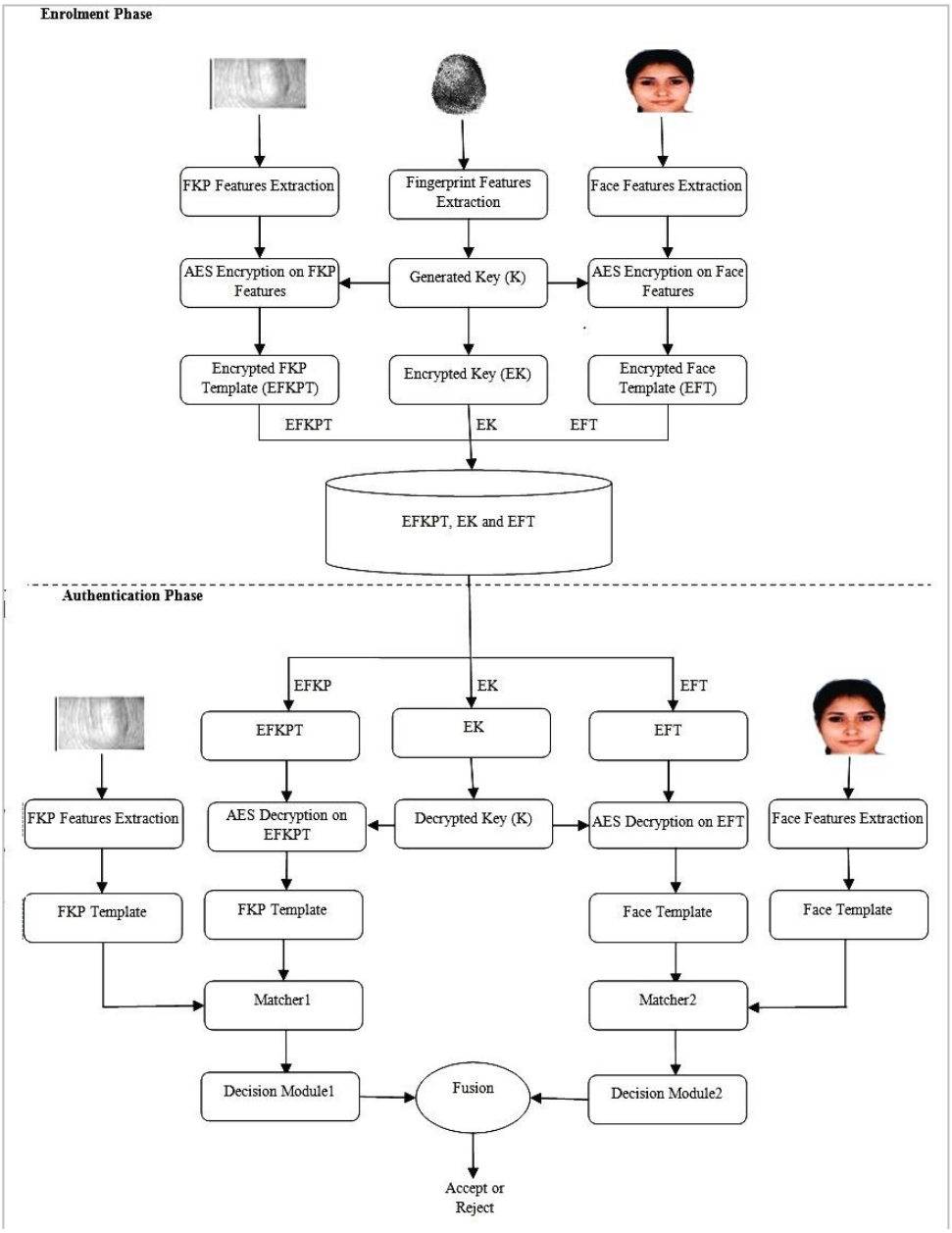


Fig 4: Architecture of proposed multimodal biometric crypto system

V. EXPERIMENT RESULTS AND DISCUSSION

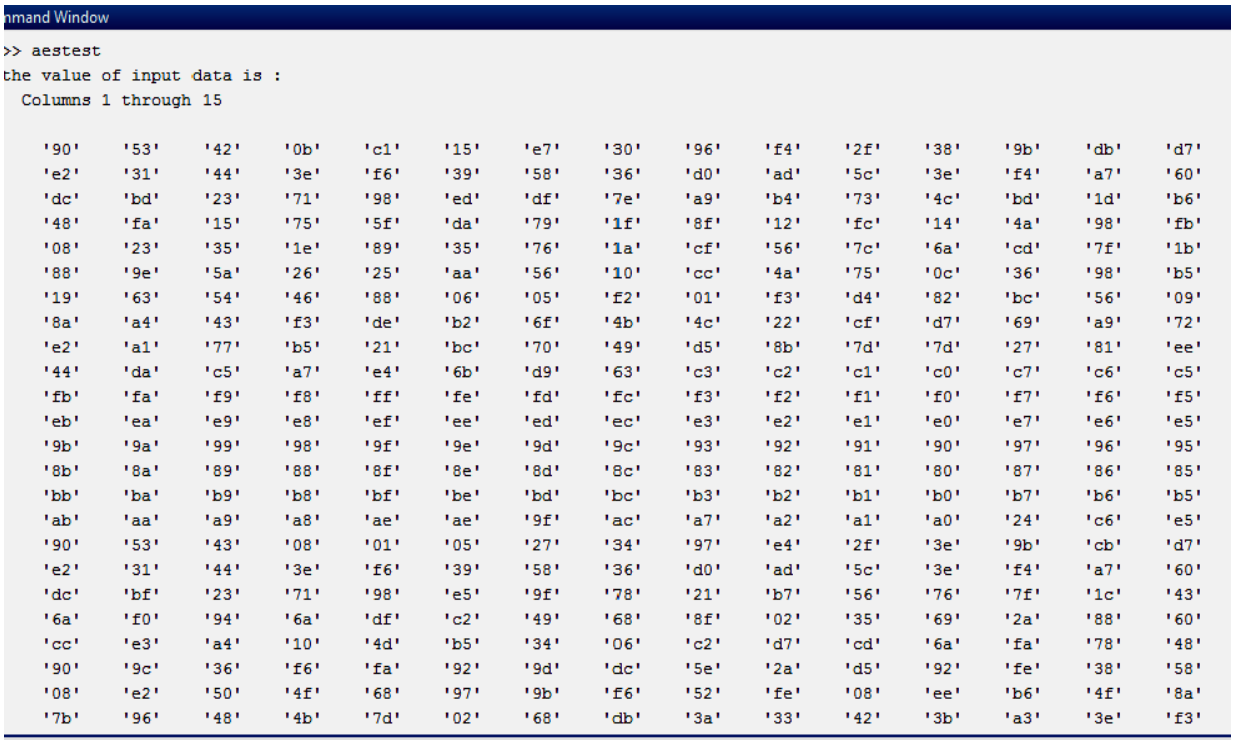
Our proposed system is implemented in Matlab 2017b. Sample biometric data for finger, FKP and face taken from CASIA, PolyU and NIST database respectively [36, 37, 38]. In our proposed work, AES encryption with 128 bit biometric key is used to secure the biometric template. In the last, decision level fusion with AND rule is used for making the final decision.

Fingerprint feature extraction process is shown in Fig 1.The feature set of fingerprint are grouped into.

8 clusters.centroid value of each cluster is used to construct the Biometric key. 128 bits fingerprint key is generated using these centroid values of each set. Fingerprint key is shown in Fig 5.

Fig 5: Fingerprint key generation

Input data size is 1024 bits and sample of input data of FKP is shown in Fig 6

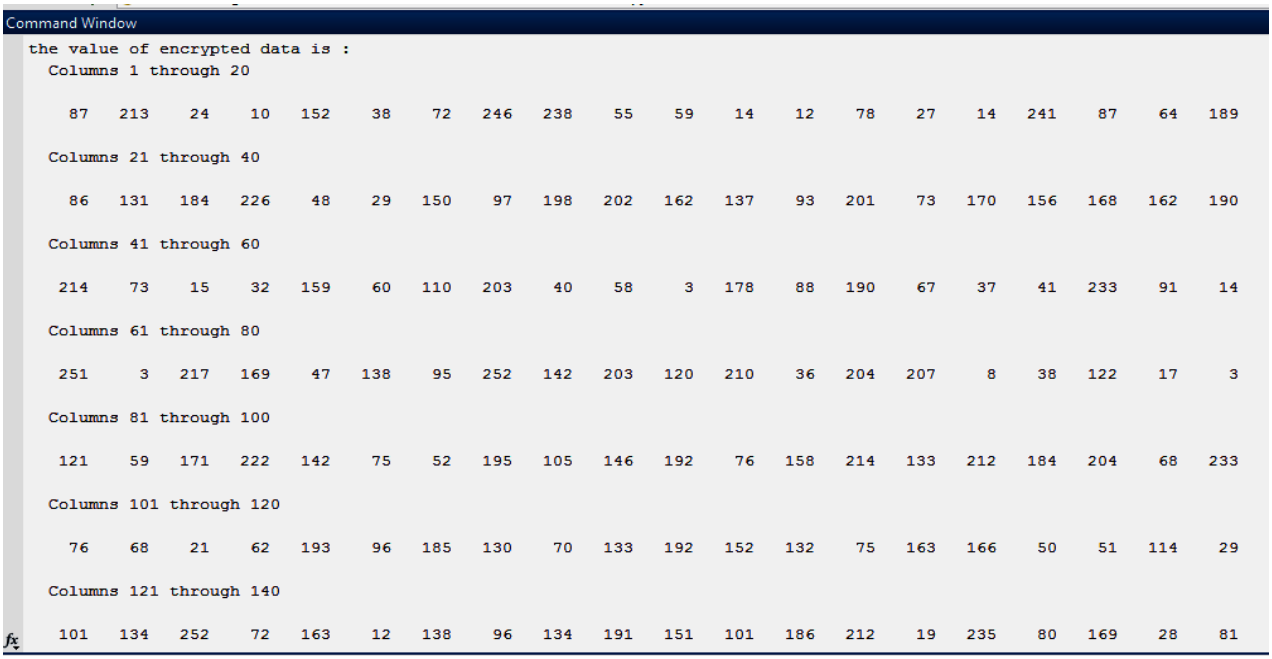


```
>> aestest
the value of input data is :
  Columns 1 through 15

   '90'   '53'   '42'   '0b'   'c1'   '15'   'e7'   '30'   '96'   'f4'   '2f'   '38'   '9b'   'db'   'd7'
   'e2'   '31'   '44'   '3e'   'f6'   '39'   '58'   '36'   'd0'   'ad'   '5c'   '3e'   'f4'   'a7'   '60'
   'dc'   'bd'   '23'   '71'   '98'   'ed'   'df'   '7e'   'a9'   'b4'   '73'   '4c'   'bd'   '1d'   'b6'
   '48'   'fa'   '15'   '75'   '5f'   'da'   '79'   '1f'   '8f'   '12'   'fc'   '14'   '4a'   '98'   'fb'
   '08'   '23'   '35'   '1e'   '89'   '35'   '76'   '1a'   'cf'   '56'   '7c'   '6a'   'cd'   '7f'   '1b'
   '88'   '9e'   '5a'   '26'   '25'   'aa'   '56'   '10'   'cc'   '4a'   '75'   '0c'   '36'   '98'   'b5'
   '19'   '63'   '54'   '46'   '88'   '06'   '05'   'f2'   '01'   'f3'   'd4'   '82'   'bc'   '56'   '09'
   '8a'   'a4'   '43'   'f3'   'de'   'b2'   '6f'   '4b'   '4c'   '22'   'cf'   'd7'   '69'   'a9'   '72'
   'e2'   'a1'   '77'   'b5'   '21'   'bc'   '70'   '49'   'd5'   '8b'   '7d'   '7d'   '27'   '81'   'ee'
   '44'   'da'   'c5'   'a7'   'e4'   '6b'   'd9'   '63'   'c3'   'c2'   'c1'   'c0'   'c7'   'c6'   'c5'
   'fb'   'fa'   'f9'   'f8'   'ff'   'fe'   'fd'   'fc'   'f3'   'f2'   'f1'   'f0'   'f7'   'f6'   'f5'
   'eb'   'ea'   'e9'   'e8'   'ef'   'ee'   'ed'   'ec'   'e3'   'e2'   'e1'   'e0'   'e7'   'e6'   'e5'
   '9b'   '9a'   '99'   '98'   '9f'   '9e'   '9d'   '9c'   '93'   '92'   '91'   '90'   '97'   '96'   '95'
   '8b'   '8a'   '89'   '88'   '8f'   '8e'   '8d'   '8c'   '83'   '82'   '81'   '80'   '87'   '86'   '85'
   'bb'   'ba'   'b9'   'b8'   'bf'   'be'   'bd'   'bc'   'b3'   'b2'   'b1'   'b0'   'b7'   'b6'   'b5'
   'ab'   'aa'   'a9'   'a8'   'ae'   'ae'   '9f'   'ac'   'a7'   'a2'   'a1'   'a0'   '24'   'c6'   'e5'
   '90'   '53'   '43'   '08'   '01'   '05'   '27'   '34'   '97'   'e4'   '2f'   '3e'   '9b'   'cb'   'd7'
   'e2'   '31'   '44'   '3e'   'f6'   '39'   '58'   '36'   'd0'   'ad'   '5c'   '3e'   'f4'   'a7'   '60'
   'dc'   'bf'   '23'   '71'   '98'   'e5'   '9f'   '78'   '21'   'b7'   '56'   '76'   '7f'   '1c'   '43'
   '6a'   'f0'   '94'   '6a'   'df'   'c2'   '49'   '68'   '8f'   '02'   '35'   '69'   '2a'   '88'   '60'
   'cc'   'e3'   'a4'   '10'   '4d'   'b5'   '34'   '06'   'c2'   'd7'   'cd'   '6a'   'fa'   '78'   '48'
   '90'   '9c'   '36'   'f6'   'fa'   '92'   '9d'   'dc'   '5e'   '2a'   'd5'   '92'   'fe'   '38'   '58'
   '08'   'e2'   '50'   '4f'   '68'   '97'   '9b'   'f6'   '52'   'fe'   '08'   'ee'   'b6'   '4f'   '8a'
   '7b'   '96'   '48'   '4b'   '7d'   '02'   '68'   'db'   '3a'   '33'   '42'   '3b'   'a3'   '3e'   'f3'
```

Fig 6: Sample of input data of FKP

Encryption of FKP data is done with this 128 bits fingerprint. Sample of encrypted Input data of FKP is shown in Fig 7.



```
the value of encrypted data is :
  Columns 1 through 20

    87   213    24    10   152    38    72   246   238    55    59    14    12    78    27    14   241    87    64   189

  Columns 21 through 40

    86   131   184   226    48    29   150    97   198   202   162   137    93   201    73   170   156   168   162   190

  Columns 41 through 60

   214    73    15    32   159    60   110   203    40    58     3   178    88   190    67    37    41   233    91    14

  Columns 61 through 80

   251     3   217   169    47   138    95   252   142   203   120   210    36   204   207     8    38   122    17     3

  Columns 81 through 100

   121    59   171   222   142    75    52   195   105   146   192    76   158   214   133   212   184   204    68   233

  Columns 101 through 120

    76    68    21    62   193    96   185   130    70   133   192   152   132    75   163   166    50    51   114    29

  Columns 121 through 140

   101   134   252    72   163    12   138    96   134   191   151   101   186   212    19   235    80   169    28    81
```

Fig 7: Encrypted input data of FK

Same process of encryption will be done for face biometric data. Then store the encrypted biometric data in the database. After then encrypt the fingerprint key using substitution method and store that key in the database so that no one can easily find out the original key. Encrypted fingerprint key is shown in Fig 8.

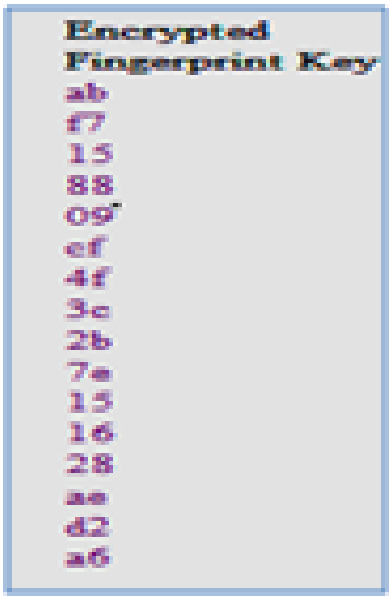


Fig 8: Encrypted fingerprint key

At the time of authentication, same key is used to decrypt the data. Decrypted data is shown in Fig 9

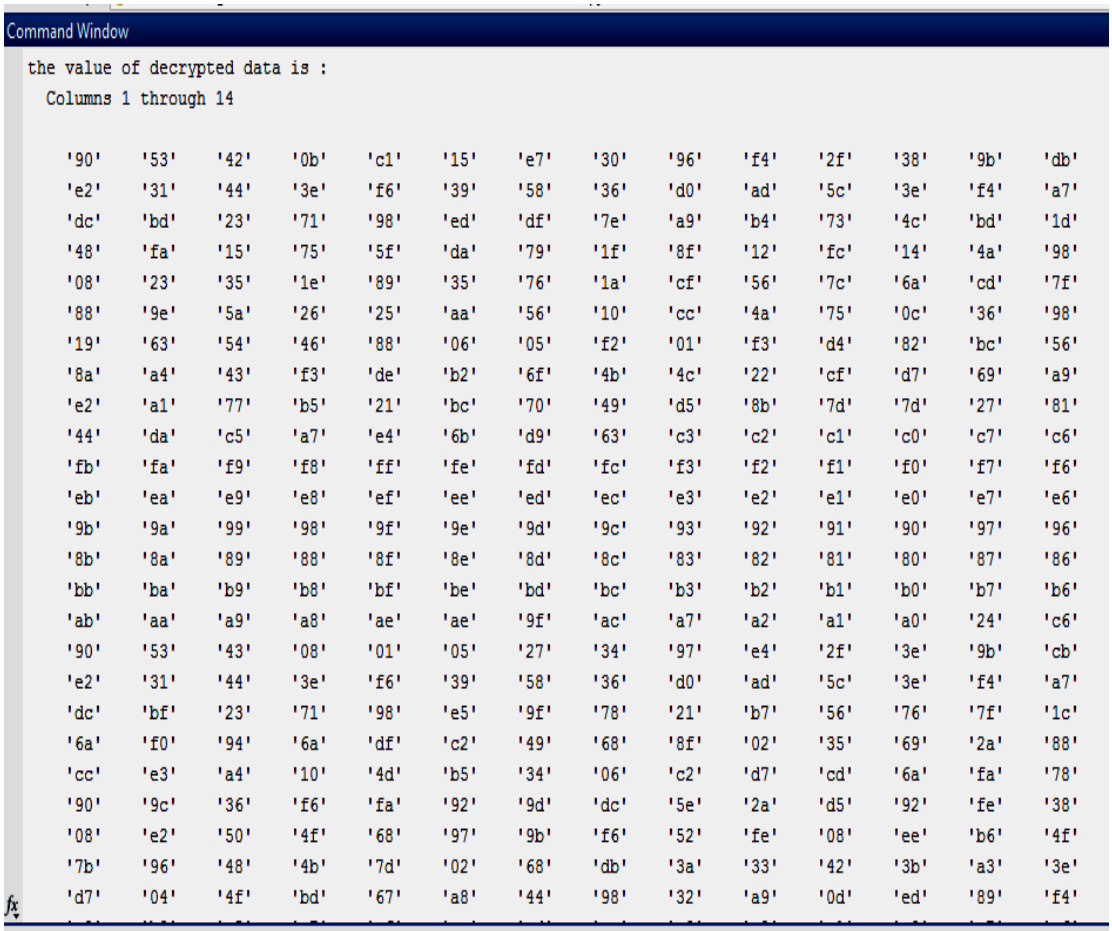


Fig 9: Decrypted data of FKP

Same decryption process will be done for face data. Then match the enrolled decrypted data with the data given at authentication time. If the output of both the matcher is 'Yes' only then system accepts the user otherwise reject him/her.

Next step is to evaluate the performance of the system. Performance of the proposed system is calculated with the help of False Accept Rate (FAR) and False Reject Rate (FRR). FAR is the number of imposter accepted as a genuine user and FRR is the number of genuine user rejected as an imposter. The point where FAR=FRR on ROC curve is called Equal Error Rate (EER) point. This point indicates that false acceptance is equal to false rejections. Accuracy of the system depends on EER and threshold value of the system. Lower the value of EER, higher will be the accuracy of the system. Accuracy of the system increases with increase in value of threshold but after certain value accuracy decreases due to increase of FRR of the system

Accuracy of proposed system with different threshold values is shown in Fig 10.

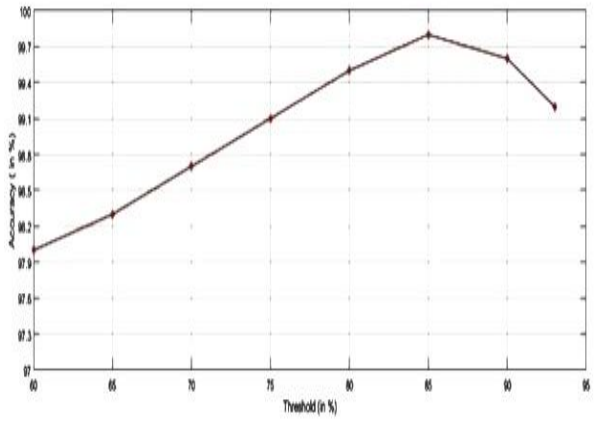


Fig 10: Accuracy of proposed system with different threshold values

FAR and FRR also depends on the threshold value. FRR increases with the increase in threshold but FAR decreases with threshold. FRR and FAR of the proposed system with different threshold values is shown in Fig 11.

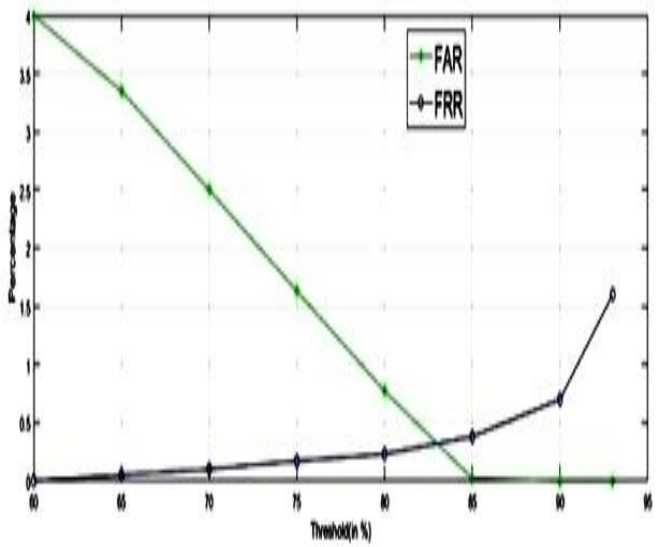


Fig 11: FAR and FRR with different threshold values

EER of the proposed system is around 0.3 and accuracy of the system is around 99.8. Table 2 shows that our proposed system has higher accuracy and lower EER as compare with existing multimodal system combining face and FKP. Fig 12 shows the bar chart which represents the accuracy of both the systems.

Table 2: Accuracy of the systems

S. no	Modalities	Accuracy (%)
1	Face and FKP with AES	99.8
2	Face and FKP [15]	99.45
3	FKP [16]	96.26
4	Face [17]	93

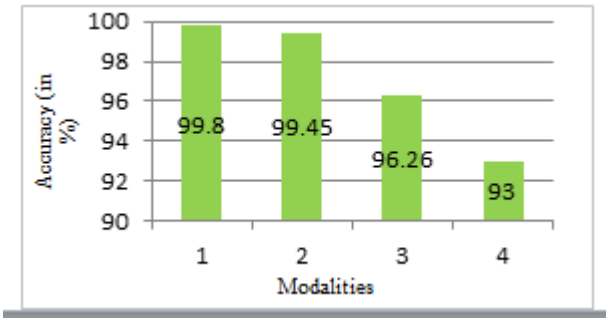


Figure 12: Bar chart showing accuracy of the systems

VI. CONCLUSION

In this paper, a robust multimodal biometric crypto system has been proposed, in which FKP and face templates are encrypted with AES algorithm using fingerprint based key. The proposed system is more robust and secure as compare with existing systems. One of the limitations is that complexity of the system may increase due to cryptographic technique with multimodal system. Cryptography technique is little bit difficult to implement with multimodal system but it makes the system more secure and robust. Future work will be focused on making the system more robust and reliable by integrating liveness detection technique

REFERENCES

1. AK. Jain, *Pankanti*, & A Ross. (2006) "Biometric: A Tool for Information Security", *IEEE Transactions On Information Forensics And Security*, 1(2): 125-144.
2. A. Gambhir, S. Narke, S. Borhade & G. Bokade. (2014) "Person Recognition using Multimodal Biometrics", *International Journal Of Emerging Technology And Advanced Engineering*, 4(4): 725-728.
3. AK. Muthu& S, Kannan. (2015) "AES Based Multimodal Biometric Authentication Using Cryptographic Level Fusion With Fingerprint And Finger Knuckle Print", *The International Arab Journal of Information Technology*, 12(5).
4. A. Upadhyaya, VShokeen& G Srivastava. (2015) "Image Encryption: Using AES, Feature extraction and Random No. Generation",*IEEE conference*.
5. Bo F., X. Simon, L. Jianping& H. Dekun. (2009) "Multibiometric Cryptosystem: Model Structure and Performance Analysis," *IEEE Transactionson*

Information Forensics and Security, 4(4): 867-882.
6. U. Uludag, S. Pankanti, & S. Prabhakar. (2004) "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE*, 92(6): 948-960.
7. D. Jagadiswary, d. Saraswady. (2016) "multimodal biometric fusion using image encryption algorithm", *proceedings of the international conference on informatics and analytics*, pondichery, india.
8. b. Kiranbala ,j.lourdujoanna. (2014) "multi modal biometrics using cryptographic algorithm", *european journal of academic essays*, 1(1): 6-10.
9. SharmilaS.More, BhawnaNarain, B.T. Jadhav. (2018) "Data Encryption Standard Algorithm in Multimodal Biometric Image", International Journal of Computer Sciences and Engineering, 6(8): 869-874.
10. UjwallaGawande , Kamal O. Hajari , Yogesh G. Golhar. (2014) "Novel cryptographic algorithm based fusion of multimodal biometrics authentication system", International Conference on Computing and Communication Technologies, *IEEE*, Hyderabad, India.
11. I. Raghu , p. P. Deepthi. (2012) "multimodal biometric encryption using ridge and iris feature map", ieee students' conference on electrical, electronics and computer science,bhopal, india.
12. [ashok a., poornachandran p., dr. Krishnashreeachuthan, (2012) "secure authentication in multimodal biometric systems using cryptographic hash functions", *communications in computer and information science*, 335: 168-177.
13. Sheena S1 and Sheena Mathew. (2016) "MULTIMODAL BIOMETRIC AUTHENTICATION: SECURED ENCRYPTION OF IRIS USING FINGERPRINT ID", *International Journal on Cryptography and Information Security (IJCIS)*, 6(3/4): 39-46.
14. MuthukumarArunachalam and Kannan Subramanian. (2015) "AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print", The International Arab Journal of Information Technology, 12(5): 431-440.
15. E.S.SHAMEEM S. (2015) "Development of An Efficient Multimodal Biometric Authentication System Using Scale Invariant Feature Transform – Chapter-5," *Ph.D Thesis*, Department Of Information Technology Pondicherry Engineering College, Puducherry: 113-139.
16. Chaudhary S., Nath R. (2015) "A New Multimodal Biometric Recognition System Integrating Iris, Face and Voice", *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4): 145-150.
17. Anne Wincy, Jacob Vetha Raj. (2018) "Palmprint, Finger Knuckle Print and Face Features For The Human Recognition System", *International Journal of Advanced Research in Computer Science*, 9(2): 70-79.
18. AM. Mouad, VH. Mahale , P. Yannawar, & AT. Gaikwad. (2016) "Overview of Fingerprint Recognition System," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*.
19. W. Yang, S. Wang, H. Jiankun and C. Valli. (2019) "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia*.
20. H. Francis,F. Lam & Z. Hui. (1998) "Adaptive Thresholding by Variational Method," *IEEE Transaction on Image Processing*, 7(3): 468-478.
21. A. Kumar & Z. David. (2010) "Improving Biometric Authentication Performance from the User Quality," *IEEE Transactions on Instrumentation and Measurement*, 59(3), 730-735.
22. A. Kumar, A. Ross, & P. Sharath. (2006) "Biometrics: A Tool for Information Security," *IEEETransactions on Information Forensics andSecurity*, 1(2): 125-143.
23. M. Redhu, Dr.Balkishan. (2013) "Fingerprint Recognition Using Minutiae Extractar," *International Journal of Engineering Research and Applications (IJERA)*, 3(4): 2488-2497.
24. Wencheng Y., Song W., Jiankun H., Guanglou Z. and Craig V. (2019) "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Multidisciplinary Digital Publishing Institute (MDPI)*: 1-19.
25. A. Meraoumia, S. Chitroub1 & A. Bouridane, (2011) "Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-biometric System of Person Recognition," *IEEE ICC2011 Proceedings*.
26. S. Singh, C. Kant, (2018) " An Efficient Multi-Modal Biometric Verification System Using FKP and Iris", *IOSR Journal of Engineering (IOSRJEN)*, 8(4): 28-35.
27. S. Suganthi Devi & A. Suhasini. (2016) "ImplimentationOf Fkp Based Biometric Identification System Using Pca With Neuro Fuzzy Neural Network," *Journal of Recent Research in Engineering and Technology*, 3(9): 19-32.
28. G. David. (2004) "Distinctive Image Features from Scale-Invariant Keypoints," *the International Journal of Computer Vision*, 60(2): 91-110.
29. S. Goe;. A. Kaushik& K. Goel. (2012) "A Review Paper on Biometrics: Facial Recognition," *International Journal of Scientific Research Engineering & Technology (IJSRET)*.
30. H. Joshi & AN. Bagade. (2016) Comparative Analysis of Face Recognition techniques, *International Conference on Recent Innovations in Engineering and management.*
31. S. Kumar, S. Singh & J. Kumar. (2017) " A Study on Face Recognition Techniques with Age and Gender Classification," *IEEE Conference Proceedings*.
32. FK. Shakir. Kak1 & F. Mustafa, & Valente. (2018) " A Review of Person Recognition Based on Face Model," *Eurasian Journal of Science & Engineering, September:* 157-168.
33. Anne W., Jacob VRY. (2018) "Palmprint, Finger Knuckle Print And Face Features For The Human Recognition System," *International Journal of Advanced Research in Computer Science*, 9(2), 70-79.
34. Fatima M. &Safia N. (2012) "Privacy Preserving KMeans Clustering: A Survey Research," *theInternational Arab Journal of InformationTechnology*, 9(2): 194-200.
35. Manhua L., Xudong J., and Alex C. (2007) "Efficient Fingerprint Search based on Database Clustering," *Pattern Recognition*, 40(6): 1793-1800.
36. Chinese Academy Of Science - Institute Of Automation, Database Of The Eye Grayscale Images. Http://Www.Sinobiometrics.Com Last Visited 2019.
37. Polyu Finger Knuckle Print Database., Available At:Http://Www.Comp.Polyu.Edu.Hk/~Biometrics/FKP. Htm Last Visited 2019.
38. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.