Received: May 20, 2018

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

RSA Cryptography based Multi-Modal Biometric Identification System for High-Security Application

Kolli Vasavi[1]* **Yaratha Madhavee Latha[2]**

[1]*Department of Electronics and communication engineering, Rayalaseema University, Kurnool, India*
[2]*Department of Electronics and communication engineering, Malla Reddy Engineering College for Women, JNTUH, Hyderabad, India*
* Corresponding author's Email: karnati.vasavi@gmail.com

Abstract: In recent days the requirements of Biometric Identification System (BIS) increased enormously. BIS Uni-modal Biometric systems (UM-BS) have different kinds of problems like non-universality, noisy data, unacceptable error rate and spoof attacks. These limitations are solved by using multi-modal Biometric systems (MM-BS).MM-BS uses two or more individual modalities, like face, Palm, iris, retina, fingerprint, etc. This paper has introduced feature-level fusion and Rivest Shamir Adleman (RSA) encryption based FEP-RSA-MM biometrics system. This FEP-RSA-MM system has taken combination of Face, iris and Palm biological characters for individual Identification. FEP-RSA-MM was implemented by using MATLAB and the performance were calculated and assessed in terms of Recall, Sensitivity, Specificity, Accuracy, F-Score, Precision, Mean Square Error, Root Mean Square (RMS) Error, etc. The performance of this FEP-RSA-MM system mainly depends on the accuracy. The accuracy of FEP-RSA-MM system is 93.33 % and it improved compared to two existing methods GF-FLF-MM, SIFT-KNN-MM, FLF-GSO-MM and SLF-PSO-MM.

Keywords: Multi-modal biometric systems, Face-Iris-Palm, Feature level fusion, Bi dimensional empirical mode decomposition, False acceptance ratio, False rejection ratio.

1. Introduction

Normally Biometric systems working in the principle of measuring the biological characters and testing the biological characters (such as hands, fingers, feet, irises, faces, retinas, teeth, ears, veins, signatures, voices, typing styles, odors, gaits, DNA, etc.) of individuals. The biological characters (features) of each individual extracted and stored in the database which is named as a biometric database or biometric templates. For testing the biological features, this database is used to identify the individual feature to improve the security [1]. Biometric systems are of two different types: UM-BS and MM-BS. UM-BS contains only one biometric characteristic of the individual recognition. BIS that use a combination of two or more biometric modalities to determine an individual is called MM-BS. The main objective of MM-BS is to improve the recognition rate [2]. UM-BS has some limitations like high spoofing rate, uniqueness, high error rate, non-universality, and noise. For example, face recognition is disturbed by position, sadness, happiness and the density of lighting [3]. To overcome the UM-BS limitations, now a day MM-BS is used, that improves the accuracy and population coverage [4]. This method combines multiple features from each modality to deliver the enhanced recognition results [5].

The key to successful MM-BS is in an effective fusion method, which is essential to fuse the information given by multiple domain experts. In a given problem domain, the enhanced set of experts is determined by the fusion and then an appropriate function is fused optimally which is shown by individual experts [6-7]. Pieces of evidence in a MM-BS is integrated in several different levels such as Prior Matching Fusion (PMF) and After Matching

Fusion (AMF) [8]. There are two types of PMF, those are Sensor level Fusion (SLF) and Feature level Fusion (FLF). In the SLF, multiple sensors deliver the raw data and then these data are processed and integrated for generating new data from which features are extracted. For example, in the case of face BIS, both 2-D texture information and 3-D depth (range) information (obtained using two different sensors) is combined to generate a 3-D texture image of the face and this image is subject to feature extraction and matching [9]. The individual person is represented by a new feature set which is created by fusing the extracted feature sets of FLF from multiple data sources [10]. The minimal feature set is exposed from the high-dimensional feature vector while performing the selection/ transformation procedure [11].

The palm print and finger print features were extracted by Gabor filtering and the feature level was used for fusing the features of palm and finger print [12]. The image description and feature extraction of face and fingerprint images were performed by Scale Invariant Feature Transform (SIFT) and then the classification of biometric traits were made by K Nearest Neighbour (KNN) classifier [13]. The FLF Fusion improves the pieces of evidence after matching it can be classified into three different types: Match score level Fusion (MSLF), Rank level Fusion (RLF) and Decision level fusion (DLF). In MSLF, the match scores are set by multiple classifiers and the match scores are combined to create a single scalar score [14].

For example, the generated match scores of face and hand modalities are fused by the simple sum rule for achieving a new match score that is used for making the decision [15]. RLF is an identification system and each classifier rank of ELF is associated with every enrolled identity. Thus, fusion strengthens the multiple ranks associated with an identity and achieve a new rank which establish the final decision. In DLF, the majority voting use by choosing the speaker label which is voted most by all classifiers. The speaker label chooses randomly in the highest amount of votes, when the speaker does not receive majority [16].

The existing studies related to the biometric systems have some advantages and disadvantages. To enhance the security and classification accuracy, a new multimodal FEP-RSA-MM biometrics system is introduced. In that face, iris and palm biological characters are taken to identify the individuals. Fusion-based matching techniques are used in the classification process. The RSA encryption technique is used for security purpose. The confidentiality of this FEP-RSA-MM system improved by using key generation of RSA algorithm. Then the combination of face & iris, iris & palm and face & palm used to improve the accuracy. Finally, the performance parameters like accuracy, execution time, error rate, Precision (P), Recall (R), False Positive (FP), False negative (FN), True Positive (TP), True Negative (TN) are calculated.

This research work is composed as follows, Section 2 presents an extensive survey recent papers based on MM-BS. The section 3 briefly described the MM-BS using feature level fusion with correlation based matching. The section 4 describes about an experimental result of a FEP-RSA-MM and conventional methods. The conclusion of this research work is given in the section 5.

2. Literature review

There are several methods present for MM-BS. In this section, a brief review of some important contributions to the existing literatures is presented.

O. Al-Hamdani, A. Chekima, J. Dargham, S.H. Salleh, F. Noman, H. Hussain, A. Ariff, and A.M. Noor [17] introduced a reliable system in the multimodal biometrics verification scenario for speech, Electrocardiogram (ECG) and Phonocardiogram (PCG) signals. Features of the heart and speech signals were represented by Mel Frequency Cestrum Coefficients (MFCC) based feature extraction. Results showed that the MM provided better performance, with the use of simple-sum score fusion and pricewise-linear normalization technique. The EEG based biometrics have some limitation that is the human heartbeats are not constant in all events, it will change depends upon the situation like joy, sorrow, shock and nervous, etc.

M.S.M. Asaari, S.A. Suandi, and B.A. Rosdi [18] considered the fusion of finger vein and finger geometry recognition to introduce a multimodal finger biometrics. The Band Limited Phase Only Correlation (BLPOC) determined the similarity between the finger vein images and the recognition of finger geometry using the width-centroid contour distance (WCCD) which is combined with centroid contour distance (CCD). Compared with the single type of feature, the fusion of WCCD and CCD improved the accuracy of finger geometry recognition. If the non-linear distortion is present in finger-vein images, it disturbs the performance of BLPOC-based finger vein matching.

M.S. Aslan, Z. Hailat, T.K. Alafif, and X.W. Chen [19] presented the Auto Encoder (AE) in multi-channel multi-modal feature learning for face recognition to integrate the Alternating Direction Method of Multipliers (ADMM). The AE was used

to paralyze/ distribute the optimization tasks by dividing the energy consumption into several sub bands. A number of samples are required in the Convolutional Neural Network (CNN) to avoid over-fitting, which is more complex.

N. Radha, and A. Kavitha [20] developed the multimodal biometrics system that employed the biometrics like iris and fingerprint. Rank level fusion was used for performing the biometrics fusion then using the Fisher Linear Discriminant (FLD) the features from the biometrics was extracted. The accuracy of the system is better. The rank level fusion system has rank aggregation problem (also referred to the data fusion problem).

A. Jagadeesan, T. Thillaikkarsai, and K. Duraiswamy [21] has presented a multimodal biometrics (Iris and fingerprint) for generating a secure cryptographic key. First, the minutiae points and texture properties identified from the iris and finger point respectively. Then a 256-bit secure cryptographic key was produced by fusing the extracted features and this key used in BIS. Security of the BIS is good as well as it gives better accuracy. Low-level cryptographic techniques have been used in this biometric system.

V. Sireesha, and S.R.K. Reddy [22] has introduced the two levels of fusion in an iris and fingerprint images for the biometric authentication. The features of iris and fingerprint are extracted by feature extraction module which has modified LDP and gabor based features. There are two levels of fusions are used such as SLF and FLF and these techniques are used for fusing the features of iris and fingerprint. Here FLF used glowworm swarm optimization (GSO) and SLF used the particle swarm optimization (PSO) for shortlisting the optimal features. The recognition accuracy of FLF-GSO-MM and SLF-PSO-MM was only 90% and 85% respectively.

The above mentioned methods have some problems like less accuracy, more complexity. In order to overcome these constraints, the FEP-RSA-MM system is developed and detail explanation about this method is given in Section 3.

3. FEP-RSA-MM system

Multi-modal biometric systems are high-performance security systems. To improve the security and classification accuracy in this paper a new FEP-RSA-MM system is introduced. The FEP-RSA-MM System consists of three major parts: training, testing and matching. The Fig. 1 shows the FEP-RSA-MM system.

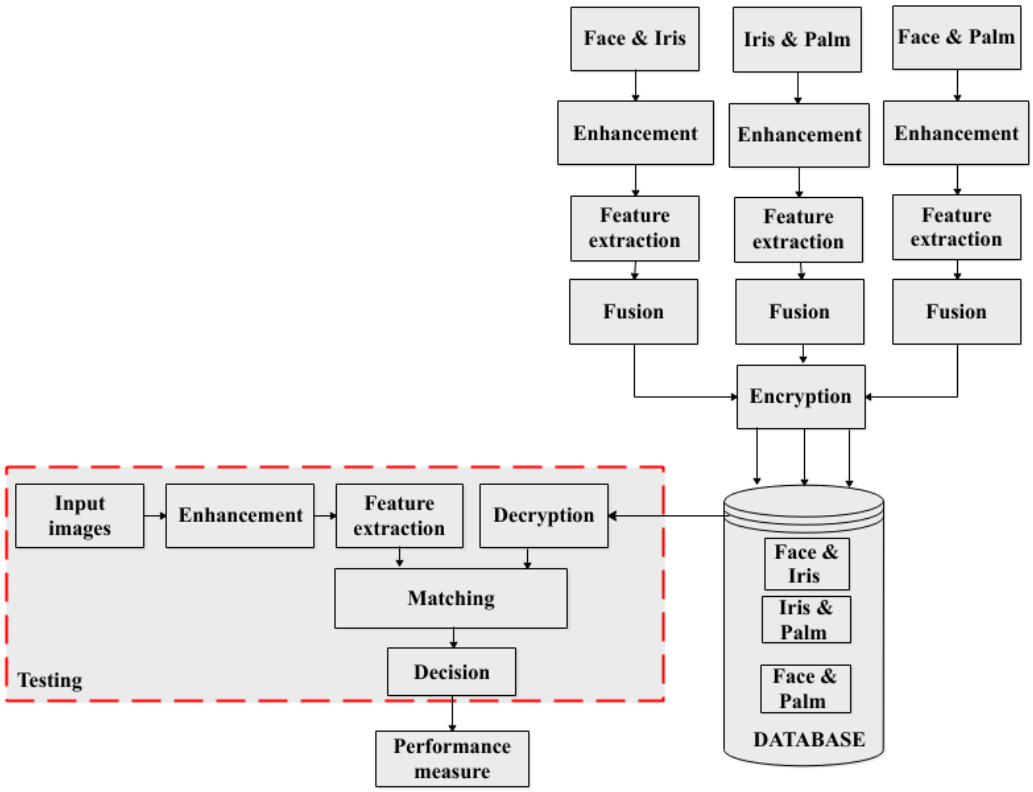


Figure.1 FEP-RSA-MM system

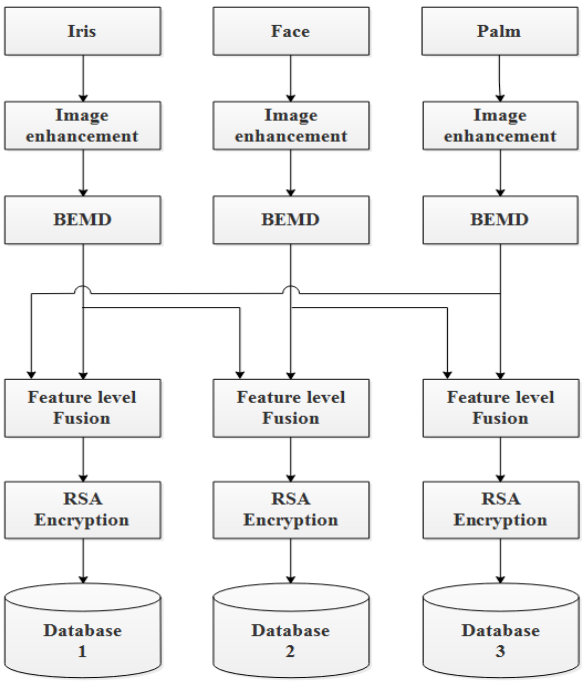


Figure.2 Database storing structure of FEP-RSA-MM system

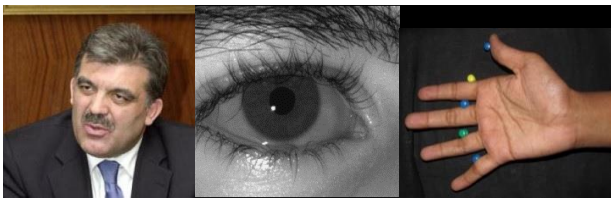


Figure.3 Image acquisition

3.1 FEP-RSA-MM Training

The FEP-RSA-MM Training section consists of six major steps like image acquisition, image enhancement, Feature extraction, fusion, database training and RSA encryption. Three different combinations of inputs are taken for training such as Face & Iris, Face &Palm and iris &Palm. The input images are enhanced with the help of Sharpening filter. The enhanced feature values are extracted by the feature extraction techniques (Empirical mode decomposition (EMD) and Minutiae), the feature values are added by the fusion technique. The feature values are encrypted by the RSA technique and it is saved in the database. The database storing structure of FEP-RSA-MM system presented in the Fig. 2.

3.1.1. Image Acquisition

In this FEP-RSA-MM system, three types of biological characters are taken to identify the individual's biological characters such as Face, iris, and Palm, that is shown in Fig. 3. Face, iris images captured using the digital mobile camera and the palm image captured from the Palm sensors.

3.1.2. Image enhancement

An ideal high-pass filter is used for image enhancement to make an image sharpening. These filters emphasize fine details in the image and the quality of an image highly degrades when the high frequencies are attenuated or completely removed. In contrast, enhancing the high-frequency components of an image leads to an improvement in the image quality. For example, if the face image is given as an input, then the filter function for an ideal high pass filter is expressed as Eq. (1),

$$J_F(u,v) = \begin{cases} 0 & if \quad D(u,v) \le D0 \\ 1 & if \quad D(u,v) > D0 \end{cases} \tag{1}$$

Where $D(u,v)$ is the distance between centre of the frequency rectangle and $J_F(u,v)$ is the enhanced image. Similarly, the iris and palm images are enhanced by this filter and it is expressed as $J_I(u,v)$ and $J_P(u,v)$ respectively.

3.1.3. Feature extraction

Enhanced image features are extracted in this section. Bi-dimensional Empirical mode decomposition (BEMD) feature extraction technique is used for Face, iris and palm feature extraction.

3.1.3.1. Bi dimensional empirical mode decomposition

Empirical modal decomposition is an adaptive decomposition that is capable of analysing the non-linear and non-stationary processes. The features are extracted straight from the data called Intrinsic Mode Function (IMF) and this decomposition technique extracts the finite number of oscillatory components. The extension of the EMD named as BEMD which is used to analyse the two dimensional data (e.g. image). BEMD is a highly adaptive decomposition and the characterization of image depends on the decomposition in the IMF. The image is decomposed into a redundant group of signals named IMF and a residue. Adding all the IMF's and residue is comprised in the reconstruction process of BEMD. Reconstruction of original image occurs without loss of information and distortion. The IMF is represented by two following properties.

- The amount of zero crossing and the amount of extrema points is equivalent or differs only by one.
- It has a zero local mean.

The given image is J_F (i.e., Enhanced face image) and the BEMD sifting process is defined as follows,

Step 1. Fixed.$\varepsilon, j \leftarrow 1$

Step 2.$R_{j-1} \leftarrow J_F\ (residue)$

Step 3. Obtain the j^{th} IMF.

a. $h_{j,k} \leftarrow r_{j-1}, k \leftarrow 1$ (k,iteration of the sifting loop).

b. Obtain the local maxima and minima of $h_{j,k-1}$.

c. Calculate the upper envelope and lower envelope functions $U_{j,k-1}$ and $L_{j,k-1}$ by interpolating respectively, local minima and local maxima of $h_{j,k-1}$.

d. Calculate the local mean surface.

e. Update: $h_{j,k} \leftarrow h_{j,k-1} - m_j, k \leftarrow k+1$

The IMF updation is given in the following Eq. (2).

$$m_{j,k-1} \leftarrow \frac{(U_{j,k-1}+L_{j,k-1})}{2} \tag{2}$$

f. The stopping criterion such as standard deviation is calculated.

g. Repeat the steps b-f until $SD_{(j)} < \varepsilon$, let $IMF_j \leftarrow h_{j,k}(j^{eme}IMF)$.

Step 4. Update the residue by using the following Eq. (3)

$$R_j \leftarrow R_{j-1} - IMF_j \tag{3}$$

Step 5. Repeat the step 3 with $j \leftarrow j+1$ until the amount of extrema in R_j is less than 2 that is the residue does not comprise any extrema points. The sifting process is stopped by the standard deviation ($SD(k)$) which is calculated from the two consecutive sifting of the Eq. (4).

$$SD(k) = \sum_{j=1}^{T} \frac{|h_{j,k}-h_{j,k-1}|}{h_{j,k-1}^2} \tag{4}$$

Where, the amount of iterations is denoted as$T$.

After completing the decomposition, the original image is reconstructed by adding all the IMFs and the last residue from the Eq. (5). The face reconstructed image is described as (J_{Fr}).

$$J_{Fr} = \sum_{j=1}^{L+1} C_j \tag{5}$$

Where, the j^{th} residue or IMF is represented as C_j and the amount of IMFs is denoted as l. The following Fig. 4 shows that the flowchart for bi dimensional empirical mode decomposition. Similarly, the features of iris and palm images extracted by BEMD and it express as J_{Ir} and J_{Pr} respectively.

3.1.4. Feature level fusion

The feature extracted value such as J_{Fr} , J_{Ir} and J_{Pr} combined through the FLF process, which combines two or more distinct entities into new whole entities. This FLF performs before RSA cryptography and it combines the biometric information such as face & iris, iris & palm, face & palm. FLF concatenates the extracted features. The dimensionality of the fused feature vector maximizes by the feature set of concatenation. The steps which are performed in the FLF are,

a) Normalization of feature vector
b) Fusing the feature vector

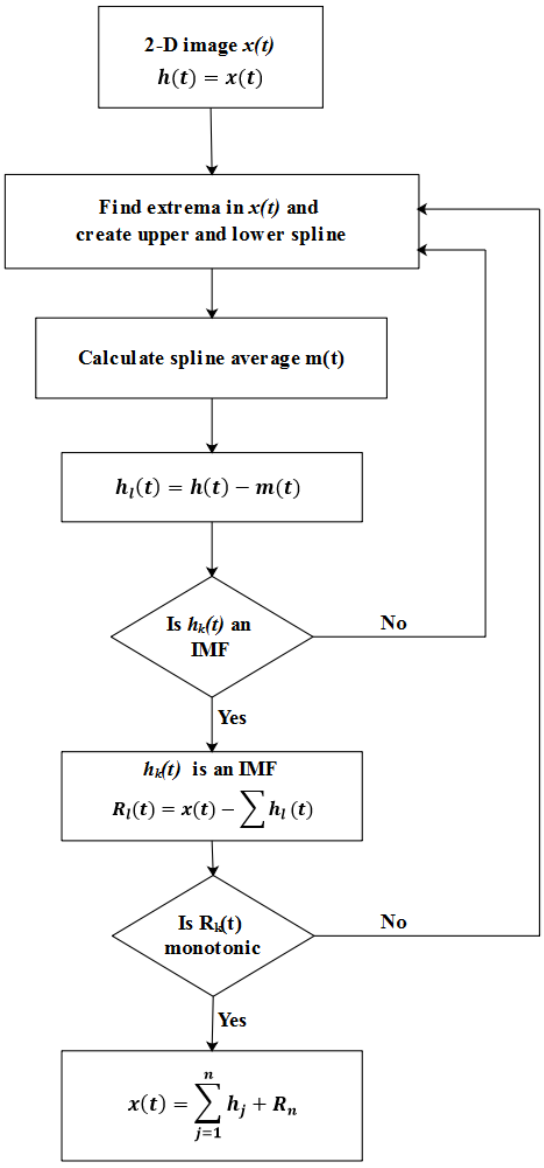


Figure.4 Flowchart for BEMD

3.1.4.1. Normalization of feature vector

The feature vectors which are extracted from face & iris, iris & palm, face & palm are incompatible in nature. Because of the variation in its own range and distribution. This problem overcome by normalizing the feature vector.

3.1.4.2. Fusing the feature vector

The final fused vector achieved by concatenating the feature vector from face & iris, iris & palm, face & palm. The fused vector (F_v) is shown in the following Eq. (6).

$$F_v = \begin{bmatrix} (J_{Fr}J_{Ir})_1, (J_{Fr}J_{Ir})_2, \dots (J_{Fr}J_{Ir})_n \; (J_{Ir}J_{Pr})_1, (J_{Ir}J_{Pr})_2, \dots (J_{Ir}J_{Pr})_n \\ (J_{Fr}J_{Pr})_1, (J_{Fr}J_{Pr})_2, \dots (J_{Fr}J_{Pr})_n \end{bmatrix} \quad (6)$$

Where, $J_{Fr}J_{Ir}$, $J_{Fr}J_{Ir}$ and $J_{Fr}J_{Pr}$ defines the normalized vectors of face & iris, iris & palm, face & palm respectively. These fused vectors are sent to the RSA cryptography technique for encrypting the feature values to improve the security of authentication process.

3.1.5. RSA cryptography

The fused vector (F_v) is given to the RSA cryptography technique and this encryption standard is used to improve the database security. RSA cryptography is the popular cryptography system. It is used for the security purpose in the wide range of networks. In the RSA, the boundary of security should be raised. The public and the private key-generation algorithm is the most difficult part of RSA cryptography. RSA cryptography is employed for generating the two large prime numbers p and q. A modulus n is calculated by multiplying p and q. The link between the users is established by the numbers that are employed for both the public and private keys. This public key is given to the receiver side with plain text. FEP-RSA-MM system contains of two main steps and it is given as follows,

a) Key generation

b) Encryption

3.1.5.1. Key generation algorithm

Input: Generate or choose large random prime numbers.

Output: Public Key (n, e) and private key (d).

1. Two different prime numbers such as $p$and q is generated.

2. Compute the modulus $n = p \times q$.

3. Compute the $\varphi(n) = (p-1) \times (q-1)$.

4. Choose for public exponent an integer e such that $1 < e < \varphi(n)$ and $gcd(\varphi(n), e) = 1$.

5. Compute the private exponent $d = e^{-1} mod \varphi(n)$ (employing the extended euclidean algorithm).

6. Public key=(e, n).

7. Private key(d).

3.1.5.2. RSA encryption algorithm

Input: Plain text for encryption and receiving user's public key (n,e)

Here, the plain text which is given to the RSA encryption is the fusion vectors of face & iris, iris & palm, face & palm.

Output: The encrypted cipher-text.

1. Obtain A's authentic public key(n, e).

2. Characterize the message as an integer m in the interval$[0, n-1]$.

3. Calculate$c = {F_v}^e mod n$.

4. Deliver the cipher text c to$A$.

This RSA encryption gives three different cipher texts such as face & iris, iris & palm, face & palm and these cipher texts stored in three different databases.

3.2 FEP-RSA-MM testing

Image Acquisition is a process to capture the biological input image. The captured input image is enhanced by the high-pass filter. Enhanced image feature values are extracted by the BEMD same like in the section 3.1.3. After that, the feature values are fused by the fusion technique. Finally, the fused feature values are given for matching. Then the cipher texts of face & iris, iris & palm, face & palm decrypted in the FEP-RSA-MM testing by RSA decryption. The private key of RSA decryption received from the key generation algorithm.

3.2.1. RSA decryption algorithm

Input: The receiver's private key (d) and the received encrypted cipher text

Output: The original plain text.

1. Use the private key d to recover $F_v = c^d mod n$.

After finishing the RSA decryption, the trained feature values from the data base and the input image from the testing is given as the input to the correlation based matching.

3.3 Correlation based matching

In the FEP-RSA-MM, correlation based matching section is the most important process, which is processed by two input feature values: database feature values and input image feature values. A matching technique predicts the decision of individuals based on the correlation among the features. Then the image based biometric verification (e.g., face, palm and iris) obtained by this correlation based encoding. The trained image fused feature vector and input matching image fused feature vector represents as $F_v(x, y)$ and $g(x, y)$ at position (x, y) respectively. The size of the trained image is $W_f \times H_f$ and the input matching image is $W_g \times H_g$, where, $W_f < W_g$ and $H_f < H_g$. These $F_v(x, y)$ and $g(x, y)$ extracted from the integers. The correlation among the $F_v(x, y)$ and $g(x, y)$ denoted as $w_{f,g}(p, q)$ which is shown in Eq. (7) and it is calculated in relative displacement of (p, q).

$$w_{f,g}(p, q) = \sum_{(x,y) \in S(p,q)} F_v(x - p, y - q)\, g(x, y) \quad (7)$$

Where the overlapping region of trained image $F_v(x, y)$ over the input matching image $g(x, y)$ denoted as $S(p, q)$. The identification of individual person depends on the correlation value among the biometric traits.

Multi-model biometric systems play a major role in recognition systems. In this paper, there are three kinds of biometric features such as face, iris and palm considered while performing the authentication process. Now a day, hackers stole individual's biometric traits for accessing the user's data. Because of this issue, the biometric features fused by the FLF in order to enhance the security of user's data. Furthermore, the RSA cryptography used for encrypting the fused vector to improve the robustness of this system.

4. Results and discussions

The FEP-RSA-MM system was analysed with the help of MATLAB 2017b and the work was done by I_3 system with 2GB RAM. This FEP-RSA-MM system developed with the biometric features of palm, face and iris to enhance the security of the desired system. The performance of the FEP-RSA-MM system was evaluated in terms of Recall, Precision, False Measure, Sensitivity, specificity, Accuracy, False Rejection Ratio, False acceptance ratio and geometric mean.

There are three different biometric combinations are used in this FEP-RSA-MM system such as Face & Iris, Face & Palm and Iris & Palm. From these combinations, the features are extracted by BEMD. In FEP-RSA-MM system, the specific person is identified by anyone biometric combination of same person. Initially, two images were taken from one person to extract the biometrics of 6 images. Totally 60 images of 10 people (20 images for face, 20 images for palm and 20 images for iris) were extracted and trained by FEP-RSA-MM and it was stored in the database. Testing was performed by using 30 images of 10 people (10 images for face, 10 images for palm and 10 images for iris). The generation of database and testing is defined as follows.

In FEP-RSA-MM training, three different data bases for three different combinations like Face & Iris, Face & Palm and Iris & Palm were generated. Here, the database generation of Face&Palm are explained in details. Hence, there are 20 face images and palm images were taken separately. The pre-processed image of face presented in Fig. 5.a, and this pre-processed image is converted into grayscale. Then the image is reshaped at the size of 128×128, it is shown in Fig. 5 (b). After that the BEMD algorithm extracts the features from the respective face image is shown in Fig. 5 ©. Likewise, the palm segmentation is used in the palm images that is shown in Fig. 6 (a). The pre-processing of palm images is achieved by converting the RGB to grayscale images and the features are extracted by BEMD algorithm that is shown in Fig. 6 (b) and Fig. 6 (c) respectively. These two features (face and palm features) are fused by the feature level fusion (data fusion). RSA encryption takes place on the fusion images, then it is encrypted and stored in the data base. Beside the FEP-RSA-MM testing is performed, in that one image is taken and it is converted from RGB to grayscale. BEMD is used for extracting features from the images. Before performing the matching progress, the images from the database are decrypted by using RSA. By using the decrypted features and individual features, the identification of a specific person is performed with the help of matching.

(a) (b) (c)

Figure.5 (a) Input image, (b) Pre-processed image, and (c) BEMD feature extraction

(a) (b) (c)

Figure.6 (a) Input image, (b) Pre-processed image, and (c) BEMD feature extraction

Table.1 Example of fusion structure

1st face image BEMD feature values	1st palm image BEMD feature values

Table.2 Example for FEP-RSA-MM database

1st face & 1st palm RSA encrypted feature database value
2nd face & 2nd palm RSA encrypted feature database value
⋮
⋮
20th face & 20th palm RSA encrypted feature database value

The extracted BEMD features of the face and palm images (Fig. 5.c and 6.c) are fused by feature level fusion, that is shown in the following Table 1.

These fusion values of face and palm are encrypted by RSA encryption and it is stored in the database. The database security is adopted by using the RSA encryption algorithm. The structure of the database is shown in the Table 2.

The input images which are used in the training is taken as input to the testing section. Testing also takes three different combinations such as Face & Iris, Face & Palm and Iris & Palm. BEMD feature extraction and Data fusion of testing is same like the FEP-RSA-MM training. Based on the correlation function, the similarity between the specific person to the database images are discovered.

The Table 3 shows the allocating class for different images from the database. The first and second row represents the pictures and the respective classes for the images.

The Table 4 shows the three different biometric feature combination (Face&Palm, Face&Iris and Palm&Iris) of input images, pre-processed images and BEMD feature extracted images.

From the classes of Table 3, the correlated values are discovered to find the true positive, true negative, false positive and false negative to determine the following performance measures like recall, precision, sensitivity, false measure, specificity, accuracy, gmean, Flase Acceptance Ratio (FAR) and False Rejection Ratio (FRR) by using Eq. (8-16).

4.1 Recall (R)

Recall is the ratio between the amount of TP to the combination of TP and FN and the equation for the Eq. (8).

$$R = \frac{TP}{TP+FN} \tag{8}$$

4.2 Precision (P)

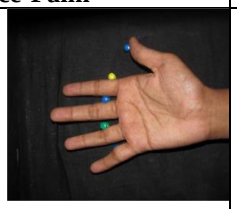
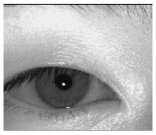
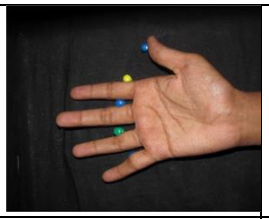
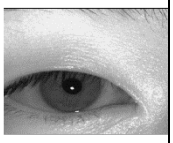
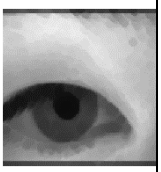
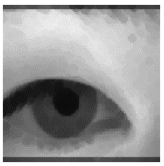
Precision is the ratio between the sum of TP and TN to the sum of TP, TN, FP and FN. This precision is also named as Positive Predictive (PP) value. The mathematical equation for Precision is given in the following Eq. (9).

$$P = \frac{TP+TN}{TP+TN+FP+FN} \tag{9}$$

Table.3 Class allocating of FEP-RSA-MM system

Picture	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}
Class	1		2		3		4		5		6		7		8		9		10	

Table 4. Comparison for different biometrics pre-processing and BEMD feature extraction

	Face-Palm		**Face-Iris**		**Palm-Iris**	
Input images						
Pre-processed images						
BEMD Feature extracted images						

4.3 False measure

False measure or balanced F-score is the ratio between the harmonic mean of precision (P) and recall (R) to the sum of precision and recall, it is given in the following Eq. (10).

$$FM = \frac{2.R.P}{R+P} \tag{10}$$

4.4 Sensitivity (S_e)

Sensitivity (S_e) is also called as TP rate and it is a basic property of image processing, it is calculated by using Eq. (11).

$$S_e = \frac{TP}{TP+TN} \tag{11}$$

4.5 Specificity(S_p)

The negative characteristics of this FEP-RSA-MM is calculated by specificity (S_p), it is also named as TN rate. The mathematical equation for S_p is shown in Eq. (12).

$$S_p = \frac{TN}{TN+TP} \tag{12}$$

4.6 Accuracy (A)

The accuracy of the respective image is determined based on the specificity $(S|p)$ and sensitivity (S_e). Quantity of the image is accurately represented by using the following Eq. (13).

$$A = \frac{TP+TN}{TP+FP+TN+FN} \tag{13}$$

4.7 Gmean

The harmonic mean of TP, TN, FP and FN is defined as the Gmean, it is also named as geometric mean. The following Eq. (14) represents the G-measure.

$$TP_{rate} = \frac{TP}{P}$$

$$TN_{rate} = \frac{TN}{P}$$

$$G_{mean} = \sqrt{TP_{rate} TN_{rate}} \tag{14}$$

4.8 False acceptance ratio (FAR)

FAR, is the measure of the Biometric Security System (BSS) incorrectly accepts an unauthorized

operator. The following Eq. (15) describes the FAR mean.

$$FAR = \frac{FP}{FP+TN} \quad (15)$$

4.9 False Rejection Ratio (FRR)

FRR is the measure of the likelihood that the BSS will incorrectly reject an access attempt by an authorized user. The equation for FRR is given in the following Eq. (16).

$$FRR = \frac{FP}{TP+FN} \quad (16)$$

In Table 5, it shows the FEP-RSA-MM method Face-Palm, Face-Iris and Palm- Iris. The true positive (TP) value of the three combinations is lesser than the true negative (TN) of three combinations. False positive (FP) rate of the Face- Palm is 1, Face-Iris is 0 and Palm - Iris is 2, the false negative rate of the FEP-RSA-MM system is zero except Face-Iris. FAR rating and FRR of FEP-RSA-MM method is also much better. The performance plot of the tp, tn, fp, fn, FRR and FAR is shown in Fig. 7.

The Table.6. shows the performance comparison of FEP-RSA-MM with FLF-GSO-MM [22] and SLF-PSO-MM [22]. Here the FAR is reduced when compared to the existing methods and then the FRR is increased, because this system has the cryptography technique that is RSA for encrypting the fusion vectors. By utilizing the cryptography technique, the confidentiality of this FEP-RSA-MM is improved. But, the existing methods are not having the cryptography technique.

The Table 7 shows the performance of FEP-RSA-MM method Sensitivity, Recall, Specificity, Accuracy, Precision, False Measure and Gmean. In that Accuracy of the Proposed Face-Palm is 95%, Face-iris is 95% and the Palm - Iris is 90%. Compared to the existing systems FEP-RSA-MM methods provided better performance in all terms. The performance analysis of FEP-RSA-MM is shown in the Fig. 8.

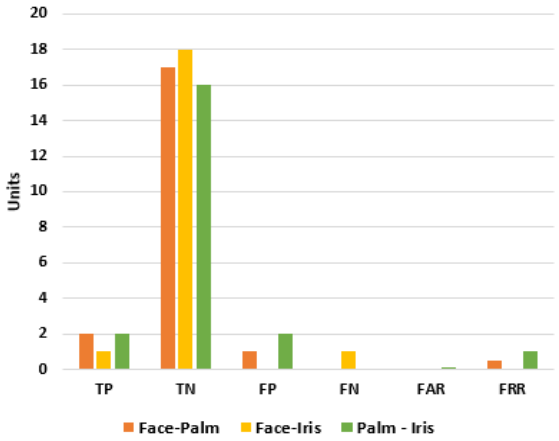


Figure.7 FEP-RSA-MM method performance

Table 5. FEP-RSA-MM method performance

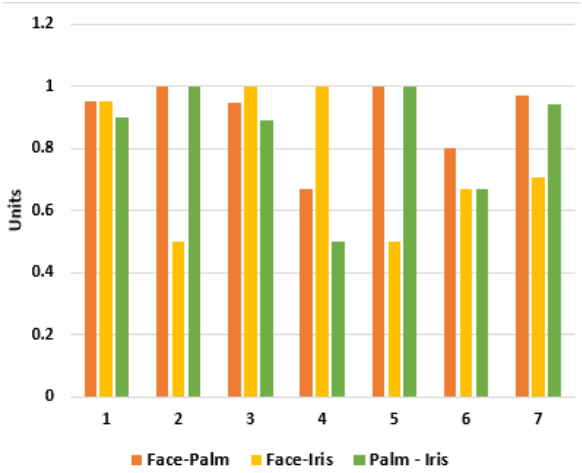
Performance	True positive (TP)	True negative (TN)	False positive (FP)	False negative (FN)	False acceptance ratio (FAR)	False Rejection Ratio (FRR)
Face-Palm	2	17	1	0	0.0556	0.5
Face-Iris	1	18	0	1	0	0
Palm - Iris	2	16	2	0	0.1111	1

Table 6. Comparison of FAR and FRR

Methods	Image	FAR	FRR
FLF-GSO-MM [22]	Fused image (Iris and Fingerprint)	0.11	0.11
SLF-PSO-MM [22]	Fused image (Iris and Fingerprint)	0.22	0.11
FEP-RSA-MM	Fused image (Face, Iris and Palm)	0.055	0.5

Table 7. FEP-RSA-MM method performance

Performance	Accuracy	Sensitivity	Specificity	Precision	Recall	False Measure	G-mean
Face- Palm	0.9500	1.0000	0.9444	0.6667	1.0000	0.8000	0.9718
Face-Iris	0.9500	0.5000	1.0000	1.0000	0.5000	0.6667	0.7071
Palm - Iris	0.9000	1.0000	0.8889	0.5000	1.0000	0.6667	0.9428



1-Accuracy, 2- Sensitivity, 3- Specificity, 4-Precision, 5- Recall, 6- False Measure, 7- G-mean.

Figure.8 FEP-RSA-MM method performance

Table 8. Performance analysis of FEP-RSA-MM

Methods	Features	Accuracy
GF-FLF-MM [12]	Palm and finger print	87
SIFT-KNN-MM [13]	Face and fingerprint	92.5
FLF-GSO-MM [22]	Iris and fingerprint	90
SLF-PSO-MM [22]	Iris and fingerprint	85
FEP-RSA-MM	Face, iris and palm	93.33

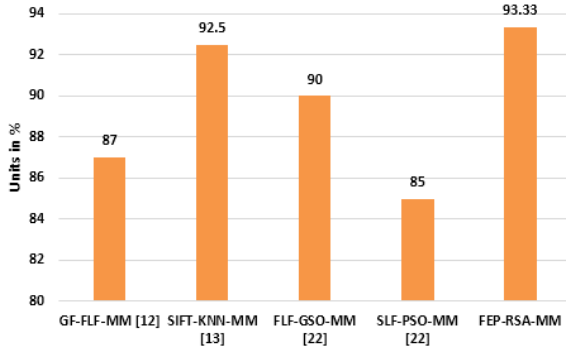


Figure.9 Performance analysis of FEP-RSA-MM

From the Table 8 and Fig. 9 conclude that the performance of the FEP-RSA-MM improved compared to the existing methods of GF-FLF-MM [12], SIFT-KNN-MM [13], FLF-GSO-MM [22] and SLF-PSO-MM [22]. The existing methods of GF-FLF-MM [12], SIFT-KNN-MM [13], FLF-GSO-MM [22] and SLF-PSO-MM [22] gave 87%, 92.5 %, 90% and 85% accuracy respectively and these methods process two kinds of features. But, FEP-RSA-MM method gives 93.33 % accuracy while processing three types of features like face, iris and palm. The data which is present in the FEP-RSA-MM system is protected from the hackers using RSA. By improving the confidentiality in the biometric systems, the third person will not hack this FEP-RSA-MM system. The processing time for face & iris, iris & palm, face & palm are 545.856, 533.821, 567.410 seconds in system with Intel I3 processor, 2GB RAM. The overall processing time of this FEP-RSA-MM is 549.029 seconds. The average calculation volume (i.e., encryption time) of RSA is 521.161 seconds.

5. Conclusion

FEP-RSA-MM system developed by using MATLAB for multi-modal biometric identification. In FEP-RSA-MM system, Face, iris, and palm biological characteristics are used for the individual recognition. The FEP-RSA-MM system is combination of BEMD and RSA techniques. BEMD extracts the features (palm, iris and face) from the individuals and the RSA cryptography used for improving the security by encrypt and decrypt the biological features. This FEP-RSA-MM system provided high security in the biometric identification and it also provided better classification accuracy. The existing methods of GF-FLF-MM [12], SIFT-KNN-MM [13], FLF-GSO-MM [22] and SLF-PSO-MM [22] gave 87%, 92.5 %, 90% and 85% accuracy respectively. But, the FEP-RSA-MM method gives 93.33% even with the processing of three different biometric features. Furthermore, the accuracy of this system can be improved by utilizing the classifier and the confidentiality of this system can be improved by using the cryptography technique, e.g. quantum cryptography in future.

References

[1] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics", *EURSAIP Journal on Information Security*, Vol.2011, No.1, pp.3, 2011.

[2] M.O. Oloyede, and G.P. Hancke, "Unimodal and multimodal biometric sensing systems: a review", *IEEE Access*, Vol.4, pp.7532-7555, 2016.

[3] S. Bashir, S. Sofi, S. Aggarwal, and S. Singhal, "Unimodal & Multimodal Biometric Recognition Techniques A Survey", *JCSN International Journal of Computer Science and Network*, Vol.4, No.1, pp.148-155, 2015.

[4] A.K. Jain, R.M. Bolle, and S. Pankanti, "BIOMETRIC: Personal identification in networked society", *Springer Science & Business Media*, Vol.479, 1999.

[5] Y.G. Kim, K.Y. Shin, E.C. Lee, and K.R. Park, "Multimodal biometric system based on the recognition of face and both irises", *International Journal of Advanced Robotic Systems*, Vol.9, No.3, pp.65, 2012.

[6] A.A. Ross, K. Nandakumar, and A.K. Jain, "Handbook of multibiometrics (international series on biometrics). Secaucus", 2006.

[7] A. Mishra, "Multimodal biometrics it is: need for future systems", *International Journal of Computer Applications*, Vol.3, No.4, pp.28-33, 2010.

[8] M.M. Monwar and M.L. Gavrilova, "Multimodal biometric system using rank-level fusion approach", *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, Vol.39, No.4, pp.867-878, 2009.

[9] A. Jain and A. Ross, "Fingerprint mosaicking", In: *Proc. of International Conf. On Acoustics, Speech, and Signal Processing (ICASSP)*, Vol.4, pp. IV-4064, 2002.

[10] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics", In: *Proc. of International Conf. On Biometric technology for human identification II*, Vol. 5779, pp.196-204, 2005.

[11] K. Chang, K.W. Bowyer, S. Sarkar, and B. Victor, "Comparison and combination of ear and face images in appearance-based biometrics", *IEEE Transactions on pattern analysis and machine intelligence*, Vol.25, No.9, pp.1160-1165, 2003.

[12] M.D. Dhameliya, and J.P. Chaudhari, "A multimodal biometric recognition system based on fusion of palmprint and fingerprint", *International Journal of Engineering Trends and Technology (IJETT)*, Vol.4, No.5, pp.1908-1911, 2013.

[13] G.W. Mwaura, W. Mwangi, and C. Otieno, "Multimodal Biometric System:-Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level", *International Journal of Scientific & Technology Research*, Vol.6, No.4, pp.41-49, 2017.

[14] G.L. Marcialis and F. Roli, "Fingerprint verification by fusion of optical and capacitive sensors", *Pattern Recognition Letters*, Vol.25, No.11, pp.1315-1322, 2004.

[15] A. Ross and A. Jain, "Information fusion in biometrics", *Pattern recognition letters*, Vol.24, No.13, pp.2115-2125, 2003.

[16] T. Kinnunen, V. Hautamäki, and P. Fränti, "Fusion of spectral feature sets for accurate speaker identification", In: *Proc. of 9th International Conf. On speech and computer*, 2004.

[17] O. Al-Hamdani, A. Chekima, J. Dargham, S.H. Salleh, F. Noman, H. Hussain, A. Ariff, and A.M. Noor, "Multimodal biometrics based on identification and verification system", *Journal of Biometrics & Biostatistics*, Vol.4, No.2, pp.1-8, 2013.

[18] M.S.M. Asaari, S.A. Suandi, and B.A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger-based biometrics", *Expert Systems with Applications*, Vol.41, No.7, pp.3367-3382, 2014.

[19] M.S. Aslan, Z. Hailat, T.K. Alafif, and X.W. Chen, "Multi-channel multi-modal feature learning for face recognition", *Pattern Recognition Letters*, Vol.85, pp.79-83, 2017.

[20] N. Radha and A. Kavitha, "Rank level fusion using fingerprint and iris biometrics", *Indian Journal of Computer Science and Engineering*, Vol.2, No.6, pp.917-923, 2012.

[21] A. Jagadeesan, T. Thillaikkarsai, and K. Duraiswamy, "Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature", *International Journal of Computer Applications*, Vol.2, No.6, pp.16-26, 2010.

[22] V. Sireesha, and S.R.K. Reddy, "Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities", *International Journal of Intelligent Engineering and Systems*, Vol.9, No.3, pp.21-35, 2016.