Multi-Modal Biometric System using Iris, Face and Fingerprint Images for High-Security Application

Nelapalli Damodaram
Dept of CSE
Besant Theosophical College

D. Venkata Siva Reddy
HOD of CSE
Besant Theosophical College

Abstract:- **Biometric systems are normally used for individual's recognition's based on the biological characters of individuals such as ears, veins, signatures, voices, typing styles, odors, gaits, and etc. the Uni-model Biometric systems does not provide better security and recognition accuracy so the multi-model biometric system are introduced, but the multi-model biometric system consist of some drawbacks such as intra class variations, Spoof attacks, non-universality, and distinctiveness. To overcome the drawbacks and improving the performance of Multi-model biometrics and future level fusion based biometric. In this document fingerprint, iris and face biological characters based on highly secured (using Advanced Encryption Standard (AES)) FIF-AES-MM multi-model biometric system is introduced. In this FIF-AES-MM system, sharpening filter is used for image enhancement which provide efficient input image for Authentication. The Empirical Mode Decomposition (BEMD) and minutiae extraction algorithms are used for feature value extraction. BEMD method is used for Face and Irish feature value extraction. Minutiae extraction meteorology is used for fingerprint Feature value extraction. The Feature level fusion (FLF) methodology is used for combining the features and Correlation methodology is used for matching, finally the FIF-AES-MM system performances are measured. The execution parametric quantity such as accuracy, execution time, error rate, Recall (R), False negative (FN), False Positive (FP), Precision (P), True Positive (TP) and True Negative (TN). The FIF-AES-MM system provides better accuracy 90%, 80, and 70%.**

Keywords: Advanced Encryption Standard, Biometric systems, Bi-dimensional Empirical Mode Decomposition, Feature level fusion and Minutiae.

INTRODUCTION:

Biometric system is a biometric identification management system for traditional individual authentication. Now a days Biometric systems are used in the various places such us bank, Mobile phone, House, government security areas and etc. In the bio-metrics system, security of the biological database is the major drawback. To improve the database security and improve the performance of fusion based multi-modal biometric motivate to done this work. Basically, Biometric identification systems working on the principle of measuring and checking the biological characters of individuals (such as hands, fingers, feet, irises, faces, retinas, teeth, ears, veins, signatures, voices, typing styles, odors, gaits, and DNA). In Biometric identification, individual features values are extracted and stored, which is called as a biometric database or biometric templates. For checking, this database or templates are used to identify the individuals. Biometric identification systems are classified into two different types such as Uni-modal and multi-modal. Uni-modal Biometric identification systems consists of only one biometric characteristic of the individual recognition. Biometric identification systems using a combination of two or more biological characters to identify an individual are called multi-modal BS. The most important reason behind the multi-modal biometric system is to increase the recognition rate.

Uni-modal BIS has some drawback such as high spoofing rate, uniqueness, high error rate, non-universality, and noise. To overcome the Uni-modal limitations, now a day's multi-modal Biometric identification systems are recommended, which improves the accuracy and population coverage. This technique work for combining multiple features from each modality to provide the enhanced authentication results. To overcome the limitations in Biometric identification systems , a number of studies and algorithms have been introduced. Fusion-based multi-modal Biometric identification systems techniques are introduced, which is a hopeful solution for feature combining . According to Paliwal and Sanderson various levels of image fusion are categories into two types such as fusion next classification and fusion earlier classification.

II. PROPOSED SYSTEM

Multi-model BS is high-performance security systems. To develop the security and classification accuracy in this paper a new FIF-AES-MM method is introduced. The FIF-AES-MM System involves three major parts such as training testing and matching.

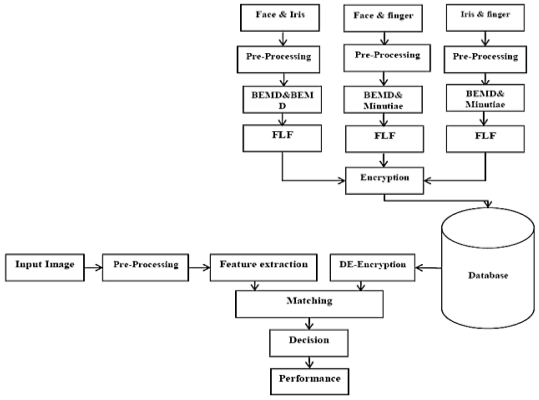


FIG - 1: THE FIS – AES – MM SYSTEM

In the FIF-AES-MM Training section consists of six major steps like image acquisition, image enhancement, Feature extraction, fusion, database training and AES encryption. Three different combinations of inputs are taken to the training such as Face & Iris, Face & finger and iris & finger. The input images are improved by the help of Sharpening filter. The enhanced features values are extracted by the BEMD and Minutiae techniques, the feature values are added by the fusion technique. The feature values are encrypted by the AES technique and it is kept in the databank

In the testing section Image Acquisition is 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 and Minutiae techniques, the feature values are fused by the fusion method. Finally, the fused feature values are given to the matching. The FIF-AES-MM matching section is the most important process, which is processed by two input feature values such as database feature values and input image feature values. The database encrypted data's are decrypted by the AES decryption process and it is given to the matching. Matching technique predicts the decision of individuals.

A.IMAGE ACQUISITION

In this FIF-AES-MM system, three types of biological characters are taken to identify the individual's biological characters such as fingerprint, iris and face that are show in fig 2. Face, iris Images are captured using the digital mobile camera and the Fingerprint are capture from the fingerprint sensors.

FIG.2. IMAGE ACQUISITION

(I) IMAGE ENHANCEMENT

A High-Pass Filter (HPF) is used for image enhancement to make a picture sharpening. These filters emphasize fine details in the picture and the graphic attribute of a picture is enormously degraded if the high frequencies are attenuated. In contrast improving the high-frequency components of an image are leads to an improvement in the Imaged quality of image.

(II) FEATURE EXTRACTION

Enhanced image features are extracted in this section, Empirical mode decomposition (EMD) feature Value extraction technique is used for Face and iris feature extraction, Minutiae method is used for Finger feature extraction.

(III) EMPIRICAL MODE DECOMPOSITION FEATURE EXTRACTION

BEMD is a propelled rendition of Empirical Mode Decomposition. BEMD has been relevant in different fields. Be that as it may, in the Field of outward appearance verification framework just a few have been utilized. BEMD breaks down convoluted information into a limited measure of segments named as IMFs (Intrinsic Mode Functions). An IMF ought to pursue the two conditions: i) measure of extrema and zero intersections should either be equivalent to zero, ii) mean estimation of envelope guard by neighborhood maxima and nearby minima ought to be zero. The IMFs are gotten by a procedure named as moving procedure. This procedure extricates the nearby extrema for every IMF. BEMD is a reasonable FE system for non-straight and non-stationary information's.

(IV) ALGORITHM

The difference among BEMD and EMD are local extrema detection and surface interpolation of the envelopes. The BEMD principle is mathematical equation is denoted in Eq(1).

$$Ori(x,y)= \sum_{t=0}^{t} Bi(x,y) + res(x,y) \text{-------(1)}$$

Where Ori the original signal before decomposition. i is the Th Bi-dimensional IMF component formed by the sifting procedure and e is the residue. The IMF elements are formed by the shifting procedure where the nearest windows are used to detect the local extrema.

The steps for BEMD are as follows:

1. Initialize residue, r_0 and index, l=1.
2. Now, initialise h_0=rj-1 and i=1.
3. Detect the local maxima, e_{max} (t) and local minima, e_{min}(t) of the picture in step 2.
4. Find the upper envelope and lower envelope with respect to that of local maxima quantity and local minima quantity.
5. Calculate the average envelope m (t) = (e_{max} (t) +e_{min} (t))/2.
6. Update the value of h as h_i=h_i-1-x_i-1 and i as i=i+1.
7. Perform iteration on the residual picture m (t).
8. The iteration results in many decomposition signals.
9. The iteration continues until the number of extrema in the residue r_i is less than 2

(V) MINUTIAE

The minutiae angles and minutiae location are derived from the minutiae extraction. The terminations which lie at the outer boundaries regions are not considered as Crossing Number (CN) and Minutiae Points (MP), is used to regain the MP in thumb-print picture. CN is defined as half of the sum of differences among intensity values of two side by side pixels. If CN is one, two and three or greater than three then MP are classified as Bifurcation (Bifn), Termination, and Normal ridge respectively, are show in fig 4(Crossing Number and Type of Minutiae).

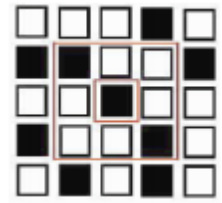
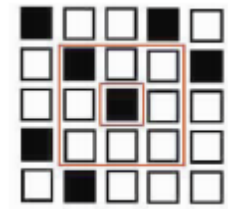
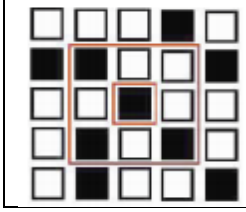
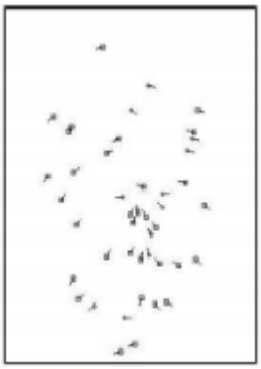
	**Crossing Number =2 Normal ridge point**
	**Crossing Number =1 Termination point**
	**Crossing Number =2 Bifurcation Point**

FIG 3. CROSSING NUMBER AND TYPE OF MINUTIAE

To evaluate the Bifn space, the benefit of the fact that termination and Bifn are dual in nature. The end in a picture corresponds to the Bifn in its position picture hence by applying the aforesaid set of regulation to the position picture; we get the Bifn space.Fig 3 shows the original picture and the extracted MP. Square contour show the position of diamond shape show the position of Bifn as in Fig 4 (b).

FIG.4.FINGER PRINT (A) THUMB-PRINT GRAY-SCALE



(B) THUMB-PRINT MINUTIAE POINTS

B. FUSION

The feature extracted values are joined by the Fusion process, which combines two or more distinct entities into new whole entities. FLF has the richer information about the biometric features. This FLF is performed before matching and it combines the biometric information such as face, iris, finger print. The response time of the feature level fusion is less than the score level fusion. FLF concatenates the extracted features. The dimensionality of the fused feature vector is maximized by feature set concatenation. The steps which is performed in the FLF is given as follows,

1. Normalization of feature vector
2. Fusing the feature vector

I .NORMALIZATION OF FEATURE VECTOR

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

II .FUSING THE FEATURE VECTOR

The final fused vector is achieved by concatenating the feature vector from face, iris and fingerprint. The Fused vector is shown in the following equation (6).

$Fused_{vector}=[f_1,f_2,\ldots.f_n.i_1,i_2,\ldots.i_n,fp_1,fp_2\ldots..fp_n]$----------(6)

where,$f_1,f_2,\ldots..f_n,i_1,i_2,\ldots i_n$, and $fp_1,fp_2,\ldots.fp_n$ are defined the normalized vectors of face, iris and fingerprint respectively. These fused vectors are stored in the database and it is used for identification of individuals.

C. AES ENCRYPTION

AES is a symmetric square figure. The convention configuration gives the non-denial, respectability, secrecy, and confirmation with AES strategy. The cryptography calculation with encryption strategy comprises of both Training and Testing. Both Training and Testing share the basic key an incentive for encryption and unscrambling. Training and Testing share normal key esteem. The cryptography calculation investigates some protected method to give scrambled and unscrambled key in the Testing. To convey the way to the Testing, the compelling key dispersion is required. The pair of keys for encryption is utilized. Each client has a solitary pair of keys. General society key is gotten to by anybody. The private key is a mystery key, which isn't known by any others. The AES calculation requires less computational handling time and encode quicker. The development in key size, just as square size and security, get improved. AES depends on the message recuperation, which incorporates a message and the mark. AES is quicker and stores information in a packed organization.

III. RESULT AND DISCUSSION

The FIF-AES-MM method was successfully implemented by using the fingerprint, iris and face bio-metrics data sets. The FIF-AES-MM system was analyzed with the help of MATLAB simulator software version 2017b. The entire work is done by using I7 system with 8 GB RAM. This FIF-AES-MM system developed with the biometric features of face, iris and fingerprint to enhance the security of the desired system. Here, the database for face, iris and fingerprint are MIT CBCL , MMU and Casia V5 respectively. The performance of the FIF-AES-MM method was measured by the terms of Recall, Precision, False Measure, Sensitivity, specificity, Accuracy, False Rejection Ratio, False acceptance ratio and geometric mean. The FIF-AES-MM method consists of three different combinations of biological characteristics are taken such as Face & Iris, Face & finger and iris & finger. For identifying the individual FIF-AES-MM method need any one combination of individuals. The FIF-AES-MM system entirely consists of 90 database images. In that each biological characters consists of 30 image which are separated as 20 images for database training and 10 images for testing. Totally training consists of 60 images (which separated 20 images for Face, 20 images for finger and 20 images for iris) and training consists of 30 images (which separated 10 images for Face, 10 images for Iris, and 10 images for finger) The database generation and testing is defined below.

FIG.5 FACE IMAGE (A) FACE INPUT IMAGE

(B) FACE PRE-PROCESSED IMAGE

FIG.6.FINGER PRINT (A) FINGERPRINT INPUT IMAGE

(B) FINGERPRINT PRE-PROCESSED IMAGE

In the training, three different combinations of three databases are generated such as Face & Iris, Face & finger and iris & finger. For example Face & finger database generation is explained, as well as all another database are also generated. Here, we are taking 20 face images and 20 fingerprint images, all the images are separately per-processed with the help of high pass filter. For example one face and finger print input image and pre-processed image is show in the fig 6 and fig7.The filter applied face images are feature extracted by the help of BEMD feature extraction, finger print images are extracted by the help of minutiae FE which is show in the fig 7.

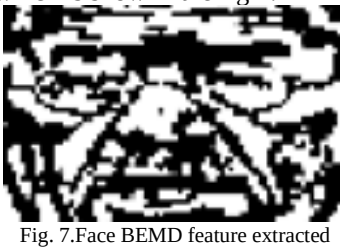
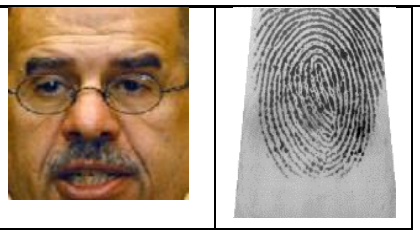
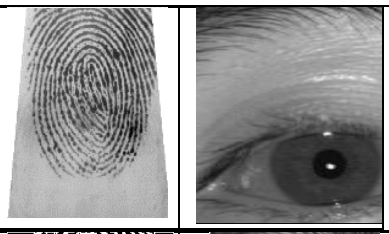
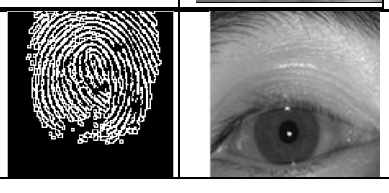
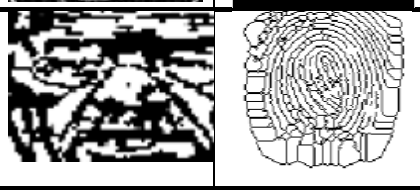
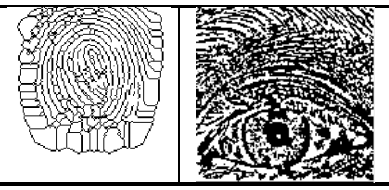


Fig. 7.Face BEMD feature extracted

Fig.8. Fingerprint minutiae feature extracted

The extracted Face BEMD features and Fingerprint minutiae features are fused by the FLF for example it is show in below fig 9.The fused Face & finger feature values are encrypted by the help of AES encryption which is stored as database image. This AES encryption improves the database security. The database structure is show in the fig 10.In the testing section three different combination of individuals are tested by the same Face & Iris, Face & finger and iris & finger combination. In that same database different images of trained person are taken to the testing. The procedure of database loading (up to fusion) is same for testing, but it also

TABLE.1. FIF-AES-MM METHOD INPUT IMAGES, PER-PROCESSED IMAGE AND FEATURE EXTRACTED IMAGES COMPARISON

	Face-finger	**Face-Iris**	**Finger- Iris**
Input images			
Pre-processed images			
Feature extracted images			

IV. PERFORMANCE MEASUREMENT CALCULATIONS

A. RECALL:

Recall (R) is the amount of True Positives (tp) divided by the amount of tp and the amount of False Negatives (fn).Recall mathematical equations is show in Eq (7);

R=tp/tp+fn------(7)

B. PRECISION:

Precision (P) is the amount of tp divided by the amount of tp and False Positives (fp). It is also named the Positive Predictive (PP) Value. Precision mathematical equations is show in Eq (8):

P=tp+tn/tp+tn+fp+fn-----(8)

C. FALSE MEASURE:

A measure that combines P and R is the harmonic mean of precision and recall, the traditional F-measure or balanced F-score: False Measure (FM) mathematical equations is show in Eq (9):

FM= 2.R.P/R+p-------(9)

D. SENSITIVITY:

consists of database loading and AES decryption process. Finally the input test image and database decrypted images are matched by correlation function. If the person is identified or unidentified means the helping window is appeared which is show in fig 11.The correlated values are identify by the classes which is show in fig 12. Finally the performances are calculated by using the eq. 2 to 10.In the below tabulation 1 show, the three different combinations (such as Face-finger, Face-Iris and Finger- Iris) of FIF-AES-MM system input images, per-processed image and feature extracted images are shows

Sensitivity (Se) is a basic property of the image processing. Sensitivity is also named as tp rate. Mathematically, Sensitivity equations is show in Eq (10):

Se=tp/tp+fn-------(10)

E. SPECIFICITY:

The specificity (SP) provides, how likely the test is to come back negative characteristic. Specificity also called the tn rate. Mathematically, Specificity equations is show in Eq (11):

SP=tn/tn+fp---------(11)

F. ACCURACY:

By using the Specificity and Sensitivity, the

Accuracy of the image is calculated. Accurately represent the quantity of the image. Mathematically it is show in equation (12):

$$Accuracy = tp_{+} tn/tp + p + tn + n \text{-------}\text{----(12)}$$

G. GMEAN:

The FM is the harmonic mean of tp, tn, fp and fn. Mathematically, G-mean is show in equation (13):

$$Tp_{rate}=tp/p$$
$$tn_{rate}=tn/p$$
$$G\text{-}mean=root(tp_{rate})*tn_{rate}\text{--------(13)}$$

H. FALSE ACCEPTANCE RATIO (FAR):

FAR, is the measure of the likelihood that the Biometric Security System (BSS) will incorrectly accept an unauthorized user. FAR equation is show in equation (14):

FAR=fp/fp+fn---------(14)

I.FALSE REJECTION RATIO (FRR):

FRR, is the measure of the likelihood that the BSS will incorrectly reject an access attempt by an authorized user. FRR mean is equation show in equation (15):

FRR=fp/tp+fn-------(15)

TAB.2. FIF-AES-MM METHOD PERFORMANCE

	tp	tn	fp	**fn**	**FAR**	**FRR**
Face-finger	1	6	3	0	7	3
Face-Iris	1	7	2	0	8	2
Finger-Iris	1	8	1	0	9	1

In tabulation 2. Shows the FIF-AES-MM method Face-finger, Face-Iris and Finger- Iris. In that true positive value of the three combinations are same true negative rating of the three combinations is much lesser. False positive rate of the Face-finger is 3, Face-Iris is 2 and Finger- Iris is 1, the false negative rate of the FIF-AES-MM system is zero. FAR rating and FRR of FIF-AES-MM method is also much better. The performance plot of the tp, tn, fp, fn, FRR and FAR is show in fig13.

TAB.3. FIF-AES-MM METHOD PERFORMANCE

Performance	**Accuracy**	**Sensitivity**	**Specificity**	**Precision**	**Recall**	**False Measure**	**G-mean**
Face-finger	0.7000	1.0000	0.6667	0.2500	1.0000	0.4000	0.8165
Face-Iris	0.8000	1.0000	0.7778	0.3333	1.0000	0.5000	0.8819
Finger-Iris	0.9000	1.0000	0.8889	0.5000	1.0000	0.6667	0.942

The tabulation 3 shows the performance of FIF-AES-MM method Sensitivity, Recall, Specificity, Accuracy, Precision, False Measure and Gmean. In that Accuracy of the FIF-AES-MM Face-finger is 70%, Face-iris is 80% and the Finger- Iris is 90%. Compared to the existing systems FIF-AES-MM methods provides better performance in all terms. The tabulation 2 graphical representation is show in the fig 14.

V. CONCLUSION

In the FIF-AES-MM method was carried out successfully by using fingerprint, iris and Face bio-metrics database. AES cryptography method is used for security purpose, which provide High security in the multi-modal bio-metrics system. BEMD method is used for Face Irish FE and Minutiae methods are used for thumb-print feature extraction. FLF technique is used for fusion purpose which improve the Classification performance. Correlation based matching method is used for classification purpose, which provide High performance with less time. From the performance analysis the FIF-AES-MM method has providing high accuracy with encryption, particularly the fingerprint and iris providing 90% of accuracy. All the three simulations are providing 100% of sensitivity and Recall. Precision (25%, 33%, 50%) and the False-measure (40%, 50%, 66%) of the system is also less. to the existing techniques, FIF-AES-MM method provides much better results and very good security.

REFERENCES

[1] Radha, N., and A. Kavitha. "Rank level fusion using fingerprint and iris biometrics." Indian Journal of Computer Science and Engineering 2, no. 6 (2012): 917-923

[2] Sanjekar, P. S., and J. B. Patil. "An overview of multimodal biometrics." Signal & Image Processing 4, no. 1 (2013): 57.

[3] Mishra, Ashish. "Multimodal biometrics it is: need for future systems." International Journal of Computer Applications 3, no. 4 (2010): 28-33.

[4] Abdolahi, Mohamad, MajidMohamadi, and Mehdi Jafari. "Multimodal biometric system fusion using fingerprint and iris with fuzzy logic." International Journal of Soft Computing and Engineering 2, no. 6 (2013): 504-510.