Performance Enhancement in Multimodal Biometrics for Authentication

Dharun Surath K.S.
PG Scholar
Department of Computer Science and Engineering
PSG College of Technology Coimbatore - 641004

R. Venkatesan, PhD
Professor
Department of Computer Science and Engineering
PSG College of Technology Coimbatore - 641004

ABSTRACT
The biometric system used for person identification is based on the physical modality such as fingerprint, iris, face, etc for providing security to the information. Normally, when a single modality is used for authentication or for encryption there might be a security issue if the hacker or intruder identifies the single modality. To overcome this issue, the proposed work uses multimodal system which combines fingerprint and iris biometrics for improving the security of the information. This Multimodal Biometrics in Information Security is done by extracting the feature points from the fingerprint and iris of the individual, followed by performing fusion of the biometric features and encrypting the fused matrix using Advanced Encryption Standards (AES) which could be used as a key for the authentication of an individual. In this paper, a new fusion technique namely modified-Canonical Correlation Analysis (m-CCA) has been proposed for fusion. The proposed method's performance is evaluated by constructing the confusion matrix and extracting the Genuine Acceptance Rate (GAR), which is observed to be performing better.

General Terms
Pattern Recognition, Security, Encryption

Keywords
Multi-modal Biometrics, Minutiae, Fingerprint, Iris, Feature Extraction, Encryption, AES, GAR, FRR

1. INTRODUCTION
The biometric system commonly uses a unimodal which is a single biometric template for authenticating the user. But in Multimodal Biometric system, more than one biometric templates such as a fingerprint, face, iris or ears are used in the authentication of the user. Normally the unimodal system deals with various challenges such as lack of secrecy, spoofing attacks on stored data, extent of user's comfort and freedom while dealing with the system, non-universality of samples, etc. Here, the Multimodal Biometric System overcomes these problems. Some of the advantages of the multimodal biometric system:

- Availability of multiple biometric templates makes the authentication more reliable.
- A multimodal biometric system increases security and secrecy of user information.
- A multimodal biometric system performs fusion strategies to combine decisions which are the features from each subsystem and then comes up with a conclusion. This increases the accuracy of the system.
- If any of the biometric identifier template fail to work for known or unknown reasons, the system still the security can be provided by employing the other identifier templates.
- Multimodal systems can help in detecting spoofing of the modal due to the liveliness of the modal.

1.1 Fusion
Fusion is defined as the set of methods, tools and means of using data from two or more different images to improve the quality of the information in the image. Fusion can be achieved in two different ways. The first method is information fusion prior to matching and the second method is fusion after matching. Fusion prior to matching can be achieved in two different ways: 1. Sensor level fusion 2. Feature level fusion. Sensor level fusion is applicable only if the data is captured from multiple source of sensors which are of different or same compatibility. Feature level fusion is achieved by combination of different homogeneous or heterogeneous feature sets extracted from multiple biometric sources. Fusion after matching can be achieved in three different ways: *1. Matching score level fusion 2. Rank level fusion 3.Decision level fusion*. *Matching score level fusion* provides richest set of information based on the score. *Rank level fusion* fuses the data based on the consolidated ranks output by the individual subsystems. Rank level fusion provides less information when compared to match score level fusion. *Decision level fusion* is carried out at decision level where the decisions output by the individual matcher are available consolidated for the fusion. The final decisions are evaluated with the help of some rules like "AND" or "OR", majority voting, Bayesian decision fusion etc.

1.2 Advanced Encryption Standard (AES)
The Advanced Encryption Standard (AES) used in the proposed work is based on substitution and permutation principles and input is processed in blocks. The algorithm supports 128 block length and supports key lengths of 128, 192, and 256 bits. The AES calculation is extremely hard to break and is well reasonable to security related applications, when the input is a text. But when the input is an image then its high computations, hardware requirements makes the processes slower.

2. RELATED WORKS
Rupesh Wagh, Saurabh Darokar, Shubham Khobragade [1] have proposed the fusion of fingerprint and iris biometric template. Initially in his work, the features of the fingerprint and iris are extracted and the fusion of the biometric template is carried on by Principal Component Analysis (PCA). The performed fusion matrix is then encrypted and stored in the database. Here encryption is followed by certain steps such as Encryption Using Chaotic Map, Encryption using Feature

Level Fusion of Biometrics Cryptography, Encryption using Multimodal biometrics with Cryptography and finally Encryption method using selective method. The acceptance and rejection ratios are computed as the performance evaluation of the experiment and the time elapsed for the unimodal and the multimodal are compared.

Sheena S and Sheena Mathew [2] have proposed biometric system that uses the fingerprint and iris. In the proposed work, feature points of fingerprint is extracted using minutiae point extraction methods and the feature points of iris is done by Edge-detection using Sobel filters, Contrasting, Iris localization using Hough Transform. The fingerprint features are encrypted by MD5 Hashing and the result is used as a key for the encryption of the iris features and are stored in the CASIA database. Similarly the decryption is also done with the template and the authentication is done by hamming distance between the decrypted template from the database and the image template scanned.

Basma Ammour, Toufik Bouden, Souad Amira-Biad [3] have proposed a biometric system that fuses the iris from CASIA database and face from ORL database. The feature points of iris is extracted and Hough Transform is done. Similarly the face features are extracted with PCA and other methods and finally the fusion of the modal are done by score level fusion. Finally the different fusion rule such as min, max and sum are calculated for the system and compared.

Ms.Anuradha, Dr. Somesh Kumar, Dr.Anuranjan Misra, Dr.K.Rama Krishna [4] has proposed the Advanced Encryption Standard (AES) for encrypting the images through a series of steps like converting the image to grey scale, Substitution of bytes, Shifting the rows, mixing the column, adding the round key and finally the left shift by nth bit where the nth bit is the round number. Finally, the correlation coefficient of the images at each stage are analyzed.

Shradha D.Jamdar, Yogesh Golhar [5] has proposed the work on the fusion of Face, Iris and ears. The proposed work involves in the creation of the database followed by preprocessing the image, PCA transformation, Creating the GUI and finally matching. The 100 datasets are stored in the database and trained using SVM and classification is carried out for the datasets. The accuracy of the modal is tested and compared.

In the above discussed existing works, multimodal used are fused using Principal Component Analysis (PCA) followed by different types of encryption such as MD5 hashing, AES encryption are done. In fusion, PCA fusion technique is performed for the two modal and encryption is carried out where the accuracy is to be improved for enhancing the security and privacy of the information stored in online databases. In order to improve the accuracy, in this paper, the modified-Canonical Correlation Analysis (m-CCA) has been proposed and performance compared with the other fusion method.

3. PROPOSED SYSTEM

The main objective of the proposed work is to secure the information stored in the online databases with the help of a key generated using the Multimodal biometrics fusion technique. In this work, the multimodal which are the fingerprint and the iris of a unique person is used for the generation of the key. Normally, for encryption and decryption of the information which are to be stored online, a key is used for the process. If a key used for the encryption of the information stored in the online database is a common key, then the hacker can easily decrypt the information using the weak key which leads to the loss of information. So to prevent this, the enhancement of the security with the help of the key is proposed in this work. So, the information can be secured.

The Figure 1 is the implementation of the Multimodal Biometric System in Information security. The working scheme of the system is the feature points of the fingerprint and the iris are extracted using Minutiae based fingerprint recognition and Gabor filter by removing the noises initially. Followed by it, the extracted features are fused using the Canonical Correlation Analysis (CCA) fusion technique. In this proposed work, the fusion of features extracted from fingerprint and iris is enhanced from the previous fusion techniques for better accuracy of the biometric modal of individual unique person, which helps in improving the privacy and security of the information stored and the fused matrix extracted after CCA fusion is encrypted using Advanced Encryption Standard (AES) encryption technique. Hence the encrypted matrix generated after AES encryption can be used as a key for the encryption of the information stored in online databases.

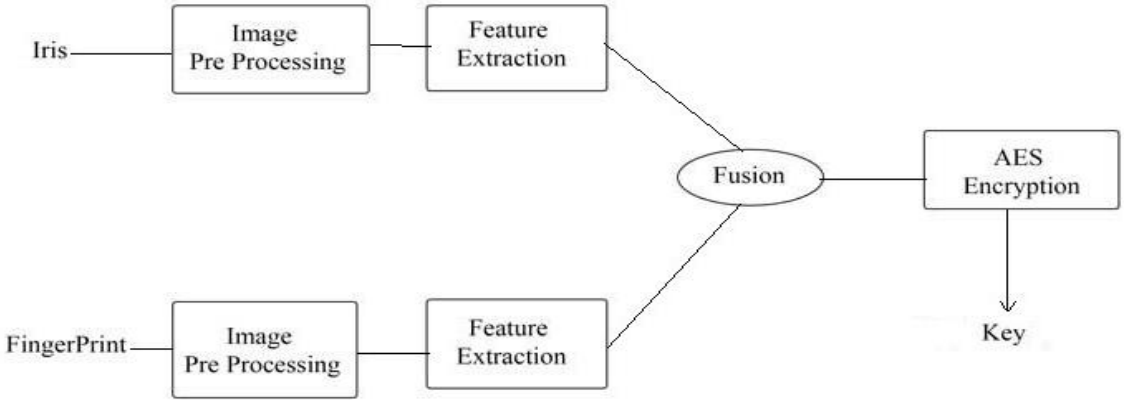

Fig 1: Data Flow Design of Multimodal Biometric System

4. EXPERIMENT DESIGN AND ENVIRONMENT

4.1 Minutiae based Fingerprint Recognition

Th Fingerprint recognition systems are based on minutiae matching, but liable minutiae matching algorithm requires more accurate minutiae extraction. Therefore, minutiae extraction is an extremely important step in the whole system, especially in low-quality images where noise may hide the real minutiae. The common minutiae extraction methods are:

binarization based method and direct gray scale extraction. In this proposed work, I have used binarization based method which is explained below.

4.1.1 Binarization

The image with only two intensity values is called the binary image. This image usually shows only black or white and black is represented by 0 and white is represented by 1. Hence, it can separate the ridge line from the background of fingerprints. The basic principle of binarization is to compare the pixel intensity with the threshold, and setting the pixel whose intensity is less than threshold to 0 and the other to 1. Therefore, the threshold is particularly important for binarization. Thresholds are divided into global thresholds and local thresholds, where global thresholds means that defining a single threshold for the whole image and local thresholds means changing the threshold locally by adapting the average local intensity, respectively.

4.1.2 Thinning

Thinning is the process that the ridge line thickness is reduced to one pixel width by deleting pixels at edge of ridge lines. The basic principle of thinning is to build deletion templates, and then compare the binary images with templates to determine whether pixels at the certain point should be deleted or not. The thinning of fingerprint image is based on the binary image and the quality of the binary image have significant influence on the thinned image. The Figure 2 shows the original finger print image and the thinned finger print image.

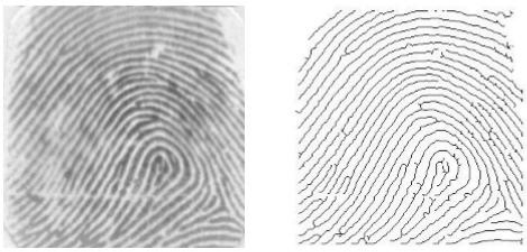

Fig 2: Original image (left) and the thinned image (right)

4.1.3 Minutiae Extraction

In biometrics, minutiae are major features of a fingerprint, using which comparisons of one print with another can be made. Minutiae includes the ridge ending and ridge bifurcation. Ridge ending is the abrupt end of a ridge which are the minutiae of finger print. Ridge bifurcation is a single ridge that divides into two ridges. Ridges are selected from the thinned finger print matrix by using a three cross three dimension matrix which looks for 1s in the diagonals index [0,0] and [1,1] which is ridge end and 1s at [1,0],[0,1],[1,1] and [2,2] which indicates ridge bifurcation. The three dimension matrix is traversed throughout the entire fingerprint image.

4.2 Iris Feature Extraction

The another biometric modal used is the eye where the iris template from the CASIA database is used in the extraction of the feature by following certain steps such as initially the segmentation of the iris and the pupil followed by it identifying and removing the noise, normalization of the entire segmented region and finally extracting the feature using Gabor filter and Hough transform which are performed. The Figure 3 represents how the iris feature region is extracted from the eyes into a rectangular region.

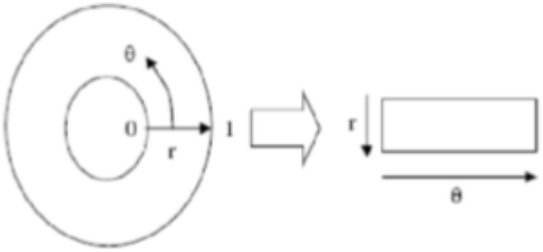

Fig. 1. Iris Normalization and feature extraction

4.3 Proposed m-CCA Fusion

The Canonical Correlation Analysis (CCA) fusion technique is used in the fusion of the feature points of fingerprint and iris. The proposed work is a feature level fusion technique used for biometric feature fusion. Initially in the proposed work, the covariance for the two feature matrix extracted are computed and using the covariance, Eigen values and corresponding Eigen vector are computed. The computed Eigen vector is projected in a matrix and the dimension reduced vector is generated. This is Dimensionality reduction done with the help of Principal Component Analysis (PCA). After this dimensionality reduction, the fusion between the dimension reduced vector is done using modified – Canonical Correlation Analysis (m-CCA) which is proposed in this experiment where normally Canonical Correlation Analysis is performed in the existing methods. In m-CCA, the canonical correlation between the PCA matrices are performed followed by it, the fusion is performed by average of the features extracted from the modal. The performance of the proposed work is computed using the accuracy by Genuine Acceptance Rate (GAR) which is the correct identification of the person based on the fingerprint and iris template of the person. The below formula is used for finding the GAR.

$$GAR = (tp+tn) / (tp+tn+fp+fn)$$

Here, True positive (TP) is the outcome from a prediction p where the actual value is also p. False positive (FP) is the actual value is n for a prediction n. True Negative (TN) is the outcome from a prediction n where actual value is p. False Negative (FN) is the actual value p for a predicted value n.

4.4 AES Encryption

Advanced Encryption Standard (AES) is a basic encryption method commonly used for encrypting the information stored online. In this experiment, AES is done using 128 bit encryption key which uses 10 round of encryption by substitution and permutation of the input fused matrix. The input to the AES encryption are the fused matrix and the 16 bit key. The encrypted image which is generated is in the size of 12*12 square matrix which can be used as a key for the encryption of the encryption of the online information stored in databases.

5. EXPERIMENTAL RESULTS

In this experiment, the fingerprint and the iris feature points are extracted and the comparison between the different fusion techniques are done for the same set of modal of unique persons. The Figure 4 shows the different techniques for fusion such are the PCA, CCA and the proposed m-CCA which are compared and tested for 70 modal and the recognition rate is analyzed by Initially taking one set of fused matrix from each individual person followed by 2, 3 and so on till 7 set of fused matrix. Each set consists of a training and a testing fused matrix.

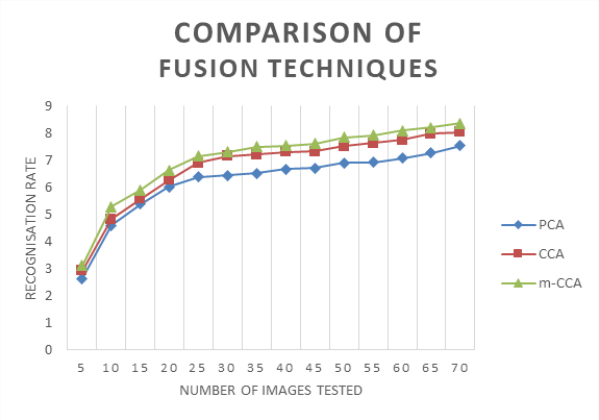

Fig. 2. Comparison of Fusion Techniques

5.1 HYPOTHESIS TESTING FOR PROPOSED m-CCA FUSION

Initially 70 unique datasets are taken and Normal Distribution Curve is generated. For fitting in the normal curve, mean and Standard Deviation are computed for the datasets. After fitting the datasets in the normal curve the Null hypothesis and Alternative hypothesis are decided which are:

Null Hypothesis (H0): The accuracy of the recognition rate does not increase by m-CCA fusion.

Alternative Hypothesis (Ha): The accuracy of the recognition rate increases by m-CCA fusion.

After fitting in normal curve and hypothesis are decided, the Z-Score which is the standardized representation of the normal curve is computed. From Z-Score value, the p-value which is the Decision Rule for the distribution is computed with the significance level of 0.01 (1%).

From the computed result, it is observed that

0.2366(p-value) < 0.01 (Significance Level)

So, here the null hypothesis is rejected which implies that the accuracy of the recognition rate does not increase by m-CCA fusion is false. Hence, the accuracy of the recognition rate increases by m-CCA fusion.

6. CONCLUSION

The multimodal biometric system helps in improving the security of the information stored in the online databases through the fusion of the finger print and the iris template extracted from the person who is being authenticated to access the data. The multimodal used is more secure than unimodal since intruders or hackers need template of two biometrics. The performance analysis of the system is improved from the existing methods of the fusion by using the proposed methodology of m-CCA fusion between the multimodals. The recognition rate of the proposed work has been improved and further encryption of the fused model helped in generating a unique password or identification for a person to secure the information. This experiment is a little bit time consuming during the feature extraction, fusion and followed by encryption but after key generation, the time consumption is based on the application which uses a secure key which is generated. In addition, the accuracy of the modals can be improved by storing the fingerprint and the iris template in a database which helps in retaining the original features of the modals without compression or loss of feature information.

7. ACKNOWLEDGMENTS

Our thanks to the PSG College of Technology for the support and guidance of the resources for the project implementation.

8. REFERENCES

[1] "Multimodal Biometrics Features with Fusion Level Encryption", Rupesh Wagh, Saurabh Darokar, Shubham Khobragade – IJESC 2017, Volume 7, Issue No.3.

[2] "Multimodal Biometric Authentication: Secured Encryption of Iris Using Fingerprint ID", Sheena S and Sheena Mathew - International Journal on Cryptography and Information Security (IJCIS), Vol. 6, No. 3/4, December 2016.

[3] "Multimodal Biometric Identification System based on the Face and Iris", BasmaAmmour, ToufikBouden, Souad Amira-Biad - The 5th International Conference on Electrical Engineering – Boumerdes (ICEE-B) October 29-31, 2017.

[4] "Improved Rapid AES for Secure Digital Images", Ms.Anuradha, Dr. Somesh Kumar, Dr.Anuranjan Misra, Dr.K.Rama Krishna - International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).

[5] "Implementation of Unimodal to Multimodal Biometric Feature Level Fusion of Combining Face Iris and Ear in Multi-Modal Biometric System", Shradha D.Jamdar, Yogesh Golhar - International Conference on Trends in Electronics and Informatics ICEI 2017.

[6] "Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition", Mohammad Haghighat, Mohamed Abdel-Mottaleb, Wadee Alhalabi - IEEE transactions on information forensics and security, vol. 09, no. 12, month 2016.

[7] "Multimodal Biometric Identification System based on the Face and Iris", Basma Ammour, Toufik Bouden, Souad Amira-Biad - The 5th International Conference on Electrical Engineering, October 29-31, 2017.

[8] "Multimodal Biometric Identification System using Fusion Level of Matching Score Level in Single Modal to Multi-Modal Biometric System", Chetan Jamdar, Amol Boke - International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).

[9] "Application to Three-Dimensional Canonical Correlation Analysis for Feature Fusion in Image Recognition", Xiaogang Gong, Jiliu Zhou, Huilin Wu, Gang Lei and Xiaohua Li, Journal of Computers, vol. 6, no. 11, November 2015.

[10] "Cryptographic Key Generation from Multimodal Template using Fuzzy Extractor", Taranpreet Kaur, Manvjeet Kaur - Tenth International Conference on Contemporary Computing (IC3), 10-12 August 2017.