RESEARCH ARTICLE OPEN ACCESS

Performance Enhancement of Multimodal Biometrics Using Cryptosystem

Muskaan [1], Tarun Gulati [2]
Research scholar [1], Associate Professor [2]
Department of ECE
MMEC, Mullana
Haryana – India

ABSTRACT
Multimodal biometrics means the unification of two or more uni modal biometrics so as to make the system more reliable and secure. Such systems promise better security. This study is a blend of iris and fingerprint recognition technique and their fusion at feature level. Our work comprises of two main sections: feature extraction of both modalities and fusing them before matching and finally application of an encryption technique to enhance the security of the fused template.
Keywords:- Multimodal ,Unimodal ,Fusion ,Security

.

I. INTRODUCTION

Biometrics is defined as the identification or verification of a human being through measurement of repeatable physiological or behavioural characteristics. Use of multi biometrics systems is being increased rapidly because of the various advantages such as low error rate, better accuracy, larger population coverage as compared to the single biometric system. Multi biometric systems use more than one trait for a person's recognition. Because of better accurate results, multi modal systems are becoming more popular than the uni modal systems. Consider an example where a person is unable to provide his fingerprint due to a cut in his finger, then the other biometric (used in conjunction) can be used for identification. Voice identification cannot be performed well if the environment is noisy or if the user is suffering from some illness in throat. For these reasons multimodal has become a better approach for the security, identification and verification purpose. Here, we have used two traits: fingerprint and iris. Features are extracted from these two modalities and fusion is performed on them before the application of any matching algorithm. Further security is enhanced using cryptosystem. Fusion at feature level is used here. The different levels of fusion are:

Levels of Fusion

The biometric modalities can be fused at any four levels:

Before Matching Fusion: Integration of information before the application of any matching algorithm.

Sensor Level: This level acquires the information from the user. Raw data is fused at an early stage so it has lot of information as compared to the other fusion levels.
Feature level: It processes the acquired biometric data and extracts a feature set to represent it. Here, the feature set are fused together. These features are then combined to form a new feature vector.

After Matching Fusion: Integration of information after the matcher stage.

Match Score Level Fusion: It is executed by calculating the mean score from both the biometrics scores produced after matching. These scores contain the richest information about the input.
Rank Level Fusion: When output of each biometric matcher is a subset of possible matches stored in decreasing order of confidence.
Decision Level Fusion: Final outputs of multiple classifiers are combined. Integration at this level takes place when each biometric matcher individually decides on the best match based on the input presented to it.

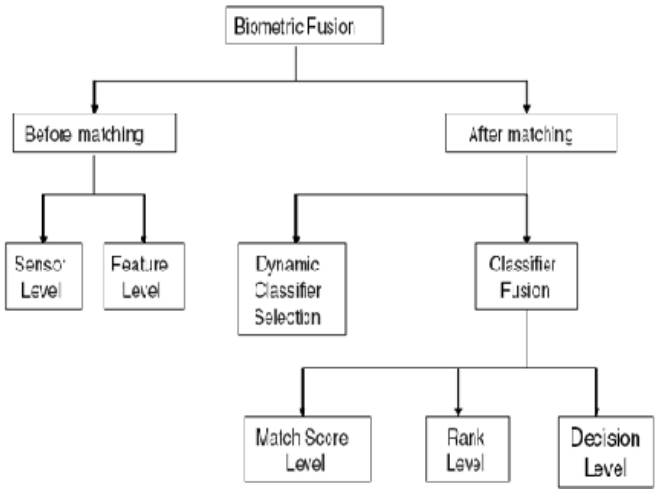

Fig.1 Levels of Fusion

Before matching technique is a better approach than those involving fusion after matching as it reduces the system complexity. So fusion at feature level is expected to give better recognition results.

II. RELATED STUDY

K.Sasidhar [1] converged on fact that multimodal biometric systems perform well than unimodal biometric systems and are popular even more complex also at the same time. His paper also epitomes the notion of accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off- The-Shelf (COTS) products.Sagar et. al. [13] discussed that Security concerns regarding the stored biometric data is impeding the widespread public acceptance of biometric technology. A number of bio-crypto algorithms have been proposed but they have a bounded practical usage due to the trade-off between recognition performance and security of the template. This involves the improved recognition performance as well as the security of a fingerprint based biometric cryptosystem, called finger print fuzzy vault. Minutiae descriptors capture the orientation and frequency information in a minutia's neighbourhood, in the vault construction using the fuzzy commitment approach. Hence as a result, the fingerprint matching performance is improved with some improvement in security as well with the use of minutiae descriptors.

Zhifang Wang, Erfu Wang, Shuangshuang Wang and Qun Ding[24] proposed multimodal biometric algorithm for face and iris. Firstly the features of face are extracted using eigenface method and then features of iris are extracted using 2D even Gabor filter. Z score normalization was used to eliminate the difference of the order of magnitude and the distribution between face features and iris features. The normalized features are combined in series and take Euclidean distance as a classifier. Their experiments show that the algorithm proposed improves the performance of two unimodal biometrics combined.

Yuliang He, Jie Tian, Xiping Luo, Tang hui Zhang[25] proposed an algorithm for fingerprint enhancement based on orientation fields. Three aspects were considered: introduction of ridge information into the minutiae matching process in a simple but effective way; Use of variable size bounding box and the use of simple alignment method.

K.Geetha and V.Radhakrishnan [26] discussed various issues related to multimodal biometric system. Using the various Biometric traits in conjunction improves the system performance. Fingerprints and palm prints are used here. Features are extracted from them and then they are fused together. Classification of the fused features are done using support vector machine (SVM).

III. PROPOSED METHODOLOGY

Fig. 2 shows the block diagram of the proposed multimodal biometric recognition system. Iris and fingerprint images are taken as the input. Features are extracted from both of them using various techniques. Fusion is done at this stage which is known as feature level fusion. To achieve security, encryption is done on the fused template. Based on this, a final decision is made.

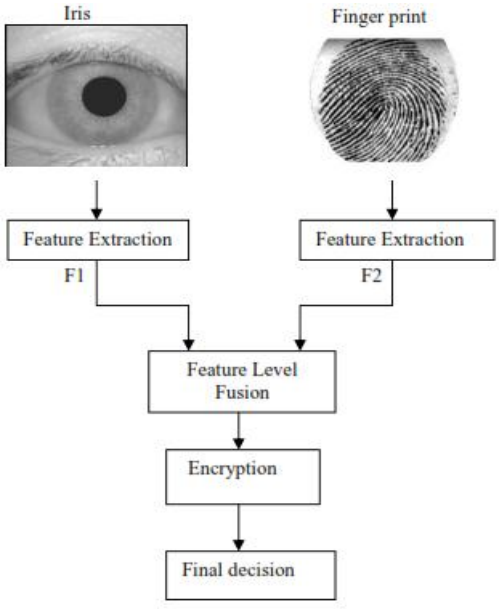

Fig.2 Block diagram of proposed system

The proposed methodology can be explained using following steps:

1) Fingerprints and iris biometric sample will be enrolled using different sensors.
2) Features will be extracted differently from both the biometrics.
3) Fusion of these extracted features will take place here i.e. fusion at feature level.
4) Generated template will be stored in the database.
5) Above stored template will be protected via cancellable biometric.
6) Security will be further increased by encrypting the template using cryptography.

Biometrics Used: The two biometric traits used here are Iris and Fingerprint.

1) Iris Recognition System: It is one of the most accurate biometric technology as compared to the other technologies used commercially. It consists of mainly three stages: first stage is the analysis of iris which involves the normalisation and localization of iris. Second stage comprises of the feature extraction and the encoding. Third stage is the recognition stage which consists of the identification and verification.

Following are the steps used for iris recognition:

- Take the input image
- Convert colour image to gray scale.
- Remove the noise using Gaussian mask.
- Detect the edges of the image using Prewitt operator.
- Detect the iris using Hough transform.
- Store the centre and the radii of the circle thus detected from the previous step.
- Detect the presence of ellipses surrounding the circle.
- Geometrically match each of the detected circle enclosed in an ellipse.
- Rule out the pair of eyes based on geometrical considerations from the above step.

2) Fingerprint Recognition system: Fingerprint is the impression of friction ridges on all or any part of the finger. Finger print is composed of ridges and furrows. They show quiet similarity and hence fingerprints are not identified by their ridges and furrows. Following Steps are used for the enhancement and feature extraction of fingerprints:

- Clahe is used to enhance the image's contrast.
- FFT is used to segment the image block wise.
- Segmentation is done to separate the actual fingerprint from the background area.
- Ridge Orientation estimation is done to estimate the orientation of the image.
- Ridge frequency estimation is done to approximate the ridge frequency for fingerprint image by dividing it into blocks of 8x8 pixels.
- Filtering is done to remove the noise and preserve ridge structure.
- Minutiae Extraction is done because minutia points are the most unique points of the fingerprints. It reduces the complex fingerprint recognition problem.

IV. RESULTS & DISCUSSIONS

Better features are extracted using various techniques which results in improved performance of the system.

Table 1 Feature extraction of finger and iris

S.No.	TECHNIQUE USED	PREVIOUS	PROPOSED
1.	Contrast Stretching	Histogram equilization	CLAHE
2.	Block Segmentation	Segmentation	FFT
3.	Quantization level	N.A.	4^{th} Level

Clahe (contrast limited adaptive histogram equilization) is used for enhancing the contrast of the fingerprint image as shown in the figure below. It eliminates the artificially induced boundaries.

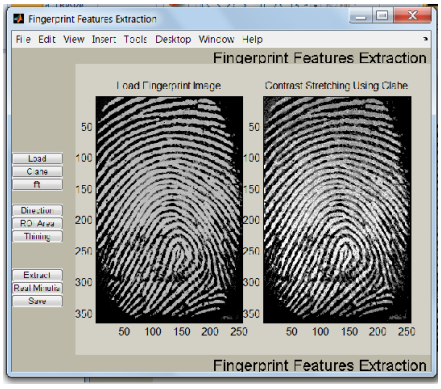

Fig.3 Image contrast increased using Clahe

FFT (fast fourier transform) is used to segment the finger print image block wise . FFT improves the image by connecting some falsely broken on the ridges and it also removes some spurious connections between the ridges.

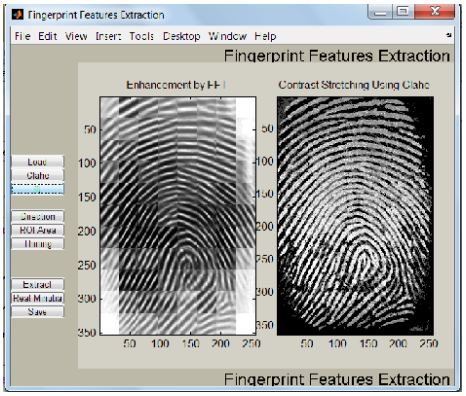

Fig. 4 Blockwise segmentation using FFT

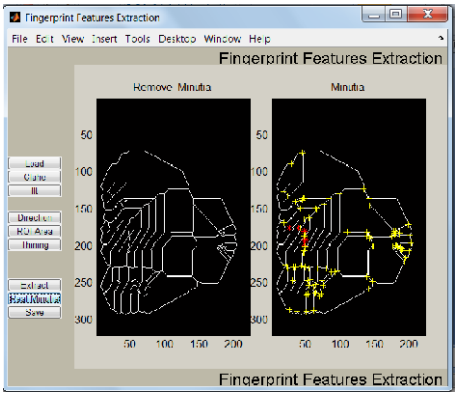

Fig. 5 Extracted minutia points

Figures above show the steps for the enhancement of fingerprint. Fig. 3 shows the improved contrast of the input image using CLAHE. Fig.4 shows the application of FFT on the input image which segments it into blocks and fig. 5 shows the extracted minutia points by removing false minutia points.

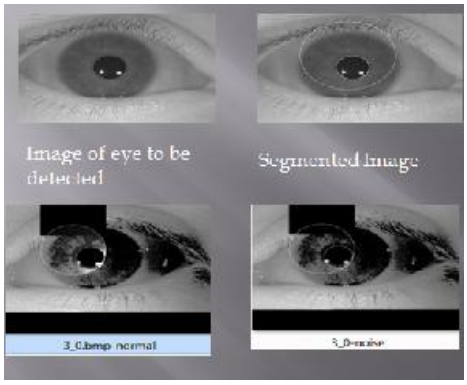

Fig. 6 Segmentation of iris and removal of polar noise

Fig. 6 shows the input image of eye on which the feature extraction is to be performed and the segmented image.4th level of quantization is used which results in the removal of polar noise which also shown in figure above.

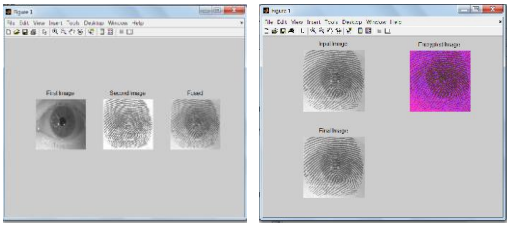

Fig. 7 Fusion& Encryption

Fusion of the two biometric traits is shown in the figure above. Fusion of the features of iris and fingerprints is done into a single multi-biometric template that is secured using fuzzy vault and fuzzy commitment. The fuzzy vault is basically is used for fingerprint modality where as for Iris modality fuzzy commitment is used. Fusion is followed by the encryption of the multimodal biometric. Here, selective encryption is used which gives helpful results for the data to be secured. The fused template is encoded using the encryption algorithm and a new template is generated. A security key is applied to the fused output. Hence, a new template is created which is stored in the database for the person's identification at the time of verification process.

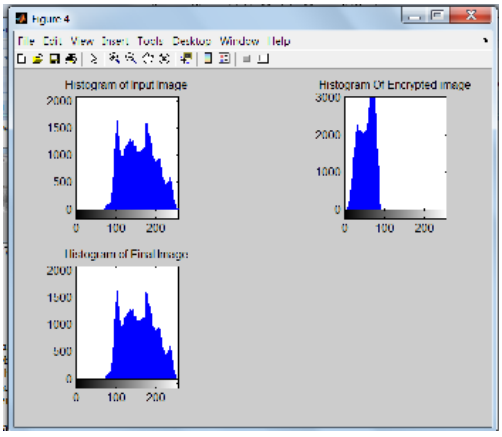

Fig.8 Histogram of the fused and encrypted image

V. CONCLUSIONS & FUTURE SCOPE

Multimodal biometrics systems provide a more secure environment and better accuracy. Features are extracted from both the biometric traits and then the fusion is performed at this stage which is also called as feature level fusion. The proposed technique is based on improving the performance of individual biometrics at feature extraction level and then fuses them together before matching. This is believed to be a better approach as compared to the one that involves fusion after matching. Cancellable biometrics is used to provide security. It hides the original template from the intruders. Further the security is raised using cryptography on the template obtained from the cancellable biometrics.

The proposed model is effective for segmentation of iris with less loss of features. This technique can be further enhanced in the future for iris image capture from the moving face.

REFRENCES

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article Biometric Template Security, Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI48824, USA.

[2] A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[3] T. Gulati, M. Pal, "Interpreting Low Resolution CT Scan Images Using Interpolation Functions," International Journal of Computer Applications, Vol 74– No.3, July 2013, pp. 50-57.

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," in Proceedings of the IEEE International Symposium on Information Theory, p. 408, Piscataway, NJ, USA, June-July 2002.

[5] Binsu C. Kovoor, Supriya M.H. and K. Poulose Jacob, "Effectiveness of feature detection operators on the performance of iris biometric recognition system", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007.

[7] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in Proceedings of the 7thMultimedia and SecurityWorkshop (MMand Sec '05), pp. 111–116, New York, NY, USA, August 2006.

[8] T. Gulati, H.P.Sinha, "Interpreting Low Resolution MRI Images Using Polynomial Based Interpolation," International Journal of Engineering Trends and Technology (IJETT) – Volume 10 Number 13 - Apr 2014, pp. 626-631.[9] Debnath Bhattacharya, Rahul Ranjan, Farkhod Alisherov A. and Minkyu Choi," Biometric Authentication: A Review", International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.

[10] RajkumarYadav, Rahul Rishi &SudhirBatra, "A New Steganography Method for Gray Level Images using Parity Checker",International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010

[11] RajkumarYadav et al. / International Journal on Computer Science and Engineering (IJCSE)

[12] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.

[13] Abhishek Sagar,Karthik Nandakumar, Anil K.Jain,"Multi biometric cryptosystems based on feature level fusion" ,Department of Computer Science and Engineering,Michigan State University, 3115 Engineering Building, East Lansing, MI48824, USA.

[14] Wayman, J. L., "A path forward for multi-biometrics,"ICASSP '06.

[15] R.N. Kankrale, Prof. S. D. Sapkal, " Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems", Department of Information Technology SRES.

[16] A. Ross and A.K. Jain, "Information fusion in biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125,2003.

[17] A.Ross, K.Nandakumar, and A.K. Jain, Handbook of Multibiometrics, Springer-Verlag edition, 2006.

[18] L.Lan and C.Y Suen, ―Application of majority voting to pattern recognition,‖ IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, vol. 27, no.5, pp. 553–568, 1997.

[19] G Hemantha Kumar and Mohammad Imran," Research avenues in multimodal biometrics", IJCA, RTIPPR, 2010.

[20] J.Heo, S.Kong, B.Abidi, and M.Abidi, ―Fusion of visible and thermal signatures with eyeglass removal forrobust face recognition,‖ in IEEE workshop on Object Tracking and Classification Beyond the visible spectrum in conjunction with (CVPR-2004), Washington, DC, USA, 2004, pp. 94–99.

[21] Poonam, Santosh Kumar Mishra, "Encryption of secutiy of multimodal biometric using Encryption method", IJAGET, vol-2, issue-09, September 2014.

[22] Sulochna Sonkamble, DR. Ravindra Thool, Balwant Sonkamble,"Survey of biometic recognition systems and their applications",JATIT,2005.

[23] Renu Bhatia,'Biometrics and face recognition techniques',IJARCSSE, vol-3, issue-5, May 2013.

[24] Zhifang Wang, Erfu Wang, Shuangshuang Wang and Qun Ding (Key Laboratory of Electronics Engineering, College of Heilongjiang Province,School of Electronic Engineering, Heilongjiang University, Harbin, China) : "Multimodal Biometric System Using Face-Iris Fusion Feature, Journal of Computers, Vol. 6, No. 5, May 2011

[25] Yuliang He, Jie Tian, Xiping Luo, Tang hui Zhang,"Image enhancement and minutiae matching in fingerprint verification".Pattern recognition letters 24 (2003) 1349-1360.

[26] K.Geetha,V.Radhakrishnan,"Multimodal biometric system: A feature level fusion approach".IJCA, Volume 71-No.4,May 2013.