Multimodal Biometric Fusion System for Authentication using Fingerprint and Iris

Mohamed Basheer. K.P
Research Scholar, Department of Computer Science, Jamal Mohamed College, Tiruchiarappalli

Abstract: In the real world applications, unimodal biometric systems often face limitations because of sensitivity to noise, intra class invariability, data quality, and other factors. Improving the performance of individual matchers in the aforementioned situation may not be effective. Multi biometric systems are used to overcome this problem by providing multiple pieces of evidence of the same identity. This system provides effective fusion scheme that combines information provided by the multiple domain experts based on score-level fusion method, thereby increasing the efficiency which is not possible in unimodal system. In this paper, we have proposed the development of a fingerprint and iris fusion system which provide higher security than the individual unimodal system.

Keywords: Multimodal biometrics, fingerprint recognition, iris recognition

I.INTRODUCTION

Each biometric feature has its own strengths and weaknesses and the choice typically depends on the application. The better biometric characteristic has five qualities: robustness, distinctiveness, availability, accessibility and acceptability. Fingerprints are unique and it is most widely used to identify the person. Its matching accuracy was very high [10]. Iris is the ideal part of the eye in human body. It contains many distinctive features such as furrows, ridges and rings etc [11]. Iris technology provides greater unique identification. According to the above features fingerprint and iris are taken to develop the proposed system. A Multi-biometric system combines characteristics from different biometric traits. A reliable and successful multimodal biometric system needs an effective fusion scheme to combine biometric characteristics derived from one or modalities. It also improves the template security by combining the feature sets from different biometric sources using appropriate fusion scheme.

The concept of multimodal biometric system has been proposed by Ross and Jain [1] where apart from fusion strategies various levels of integration are also presented. In [2] fusion of iris and face biometrics has been proposed. The score level fusion in multimodal biometrics system is proposed in [3]. A novel fusion at feature level for face and palmprint has been presented in [4]. The purpose is to investigate whether the integration of face and palmprint biometrics can achieve higher performance that may not be possible using a single biometric indicator alone. Both Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are considered in this feature vector fusion context. It is found that the performance has improved significantly.

Dass, Nandakumar& Jain (2005) have proposed an approach to score level fusion in multimodal biometrics systems [6]. Experimental results have been presented on face, fingerprint and hand geometry using product rule and coupla method. It is found that both fusion rules show better performance than individual recognizers. Common theoretical framework [7] for combining classifiers using sum rule, median rule, max and min rule are analyzed by Kittler et al. (1998) under the most restrictive assumptions and have observed that sum rule outperforms other classifiers combination schemes.

The proposed work is designed to provide improved performance over the unimodal systems. The major advantage of the framework is that since both modalities utilized the same matcher module the memory footprint of the system is reduced. The framework is demonstrated through the development of a fingerprint and iris based multimodal biometric identification system with score level fusion. Feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These

individual scores are finally combined into a total score which is passed to the decision module.

III.FINGERPRINT RECOGNITION

Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries.

1. Fingerprint Enhancement

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system would be robust with respect to the quality of the fingerprint images, it would be essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module.

The pre processing steps included are:

a. Normalization:

Normalization allows standardizing the distorted levels of variation in the gray scale values among ridges and valleys. Histogram equalization, as normalization method, is a process to enhance the contrast of images by transforming its intensity values.

Figure 1: Normalization

b.Segmentation

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutiae in the bound region are confusing with those spurious minutiae that are generated when the ridges are out of the sensor. The method of block direction estimation is used here.

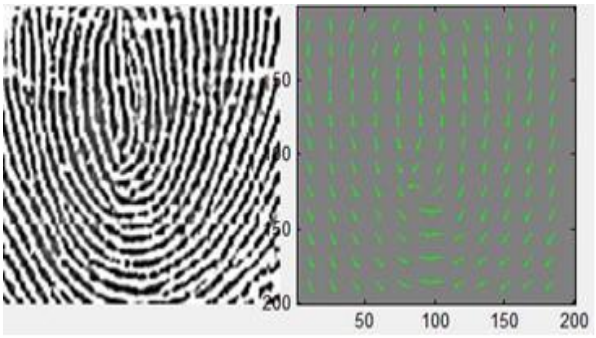

Figure 2: Segmentation

2. Minutia Extraction

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3 x3window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. Using the properties of the CN, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation, and if the value of the CN is two then it corresponds to normal ridge pixel.

$CN=0.5\sum_{t=1}^{8} (P_i-P_{i+1)},\ P9=P1$

Where*Pi* is the pixel value in the neighborhood of *P*

3. False Minutiae Removal

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Following steps are used in order to remove false minutiae:

1. If the distance between one bifurcation and one

termination is less than D and the two minutiae are in the same ridge. Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.
4. If two terminations are located in a short ridge with length less than D, remove the two terminations.

Once all the spurious and false minutiae has been removed following information is recorded to carry out the process of matching:

1. Termination in x and y direction.
2. Bifurcation in x and y direction.
3. Orientation of each termination and bifurcation.

III.IRIS RECOGNITION

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the ridges of an individual's eyes. Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits; the False Reject Rate (FRR) of these systems can be rather high. Iris recognition analyzes features like rings, furrows, and freckles existing in the colored tissue surrounding the pupil. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates.

Following are the various steps during image preprocessing stage:

1. Iris Segmentation: This involves first employing Canny Edge Detection to generate an edge map.

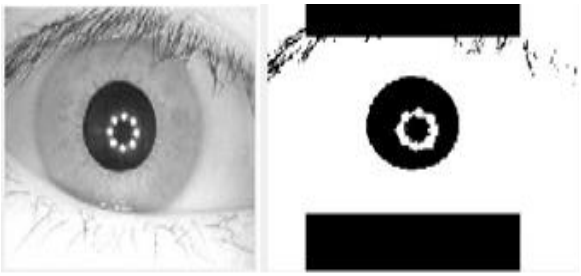

Figure 3: Iris Segmentation

2. Iris Localization: In the work, in order to increase the overall speed of the system, circle detection algorithm is used.

Circle detection in the work contributes to:

a. It has good recognition performance and speed
b. The algorithm is able to very accurately detect even partially occluded circles.
c. The algorithm needs a very small amount of memory.
d. The algorithm creates low processing burden than other methods.
e. It is simple and efficient method.

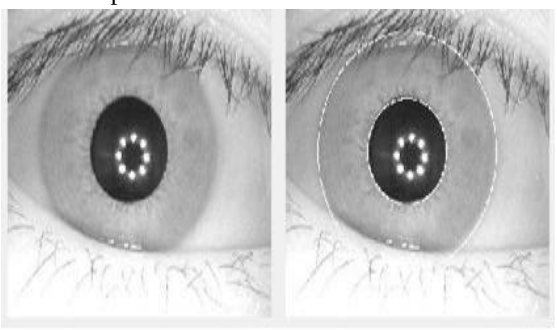

Figure 4: Iris Localization

4. Iris Normalization:

After successfully extracting the iris part from the eye image, in order to allow comparisons between different irises, transform the extracted iris region so that it has a fixed dimension, and hence removing the dimensional inconsistencies between eye images due to the stretching of the iris caused by the pupil dilation from varying levels of illumination. Therefore, this normalization process will produce irises with same fixed dimensions so that two photographs for the same iris under different lighting conditions will have the same characteristic features.

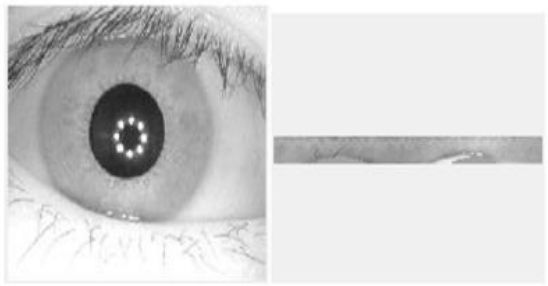

Figure 5: Iris Normalization

4. Iris Feature Extraction:

This is the most key component of an iris recognition system and determines the system's performance to a large extent. Iris recognition produces the correct result by extracting features of the input images and matching these features with known patterns in the feature database.

Features are the attributes or values extracted to get the unique characteristics from the image. Features from the iris image are extracted using Haar Wavelet decomposition process. In the wavelet decomposition the image is decomposed into four coefficient i.e., horizontal, diagonal, vertical and approximation. The approximation coefficients are further decomposed into four coefficients. The sequences of steps are repeated for five levels and the last level coefficients are combined to form a vector. The combined vector is binarized to allow easy comparisons between the iris codes for database and query image.

$FV(i)$ □ 0

$IC(i)$ □□□

□0 $FV(i)$ □ 0

The binarized feature vectors are passed to the matching module to allow comparisons.

IV. MATCHING

The comparison is done between iris codes and fingerprint codes generated for database and query images using hamming distance approach. In this approach the difference between the bits of two codes of both are counted and the number is divided by the total number of comparisons.

V.FUSION

No individual trait can provide 100% accuracy. Thus to overcome the problems faced by individual traits, a novel combination is proposed for the recognition system. The integrated system also provide anti spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. Scores generated from individual traits are combined at matching score level using weighted sum of score technique.

VI. RESULTS

The database consists of four iris images (50×4) and four fingerprint images (50×4) per person with total of 50 persons. For the purpose allowing comparisons two levels of experiments are performed. At first level iris and fingerprints algorithms are tested individually. At this level the individual accuracy for iris and fingerprint is found to be 95.16% and 91.94% respectively as shown in Table 1. However in order to increase the accuracy of the biometric system as a whole the individual results are combined at matching score level. At second level of experiment the matching scores from the individual traits are combined and final accuracy graph is plotted as shown in Figure 1. Table 1 shows the accuracy and error rates obtained from the individual and combined system. The overall performance of the system has increased showing an accuracy of 94.07% with FAR of 1.46% and FRR of 6.87% respectively.

Trait	Algorithm	Accuracy (%)	FAR (%)	FRR (%)
Iris	Haar Wavelet	95.16	4.85	6.43
Fingerprint	Minutiae Matching	91.94	3.17	12.69
Fusion	Haar + Minutiae	94.07	1.46	6.87

Table 1: Figures showing individual and combined accuracy

VII. CONCLUSION

The paper proposes a multimodal biometrics authentication system using a combination of iris and fingerprints using a single hamming distance matcher in order to overcome the difficulties posed by unimodal systems which make use of individual traits. The system is giving an overall accuracy of 94.07% with FAR and FRR of 1.46% and 6.87%.

REFERENCES

[1] A. Ross, & A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, 24(13), 2003, 2115-2125.

[2] W. Yunhong, T. Tan, & A. K. Jain, Combining

Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on AVBPA, Guildford, UK, 2003, 805-813.

[3] S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA), Rye Brook, NY, 2005.

[4] G. Feng, K. Dong, D. Hu, & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, International Conference on Bioinformatics and its Applications, Hong Kong, China, 2004, 701-707.

[5] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, On combining classifiers, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), pp. 226–239, 1998

[6] HunnyMehrotra, AjitaRattani, Phalguni Gupta, Fusion of iris and fingerprint biometric for recognition, Indian Institute of Technology Kanpur, India – 208016

[7] Phalguni Gupta, AjitaRattani, HunnyMehrotra, Anil Kumar Kaushik, Multimodal Biometrics System for Efficient Human Recognition, Indian Institute of Technology Kanpur, India – 208016.