Fusion of Multibiometric in Security Management System

S. S. Chowhan
School of Computational Sceinces
S. R. T. M. University,
Vishnupuri, Nanded, India
drschowhan@gmail.com

M. H. Kondekar
Sinhgad School of Computer Studies
Solapur, (M.H) India
mhkondekar@gmail.com

M. R. Mahamune .
School of Computational Sciences
S. R. T. M. University,
Vishnupuri, Nanded, (M.H) India
mohnish.mahamune@gmail.com

***Abstract*—** Nowadays personal identification or verification has become one of the most prominent issues in security management. In order to restrict access to secure systems multibiometric refers to authentication techniques that rely on measurable physiological and individual traits that can be automatically verified. In other words, all individuals ones have personal traits that can be used for distinctive identification purposes, including a face, fingerprint, Iris, palm print, retina and voice etc. Multibiometric systems, are projected to be more reliable due to the presence of multiple, legitimate bits of evidence. In this paper, we describe fusion techniques and performance of a multibiometric in pattern recognition and security systems. Some of the experimental results are performed on fusing on fingerprint and Iris.

Keywords*-Biometric; Fingerprint; Iris; Fusion Technique**; pattern recognition;security*

*****

I. INTRODUCTION

Biometrics system is associated to personal identity or verifies a person's identity. A variety of such systems have been implemented and used successfully over the years, including ones based on ear, DNA, fingerprints, irises, face expression, hand geometry, and voice recognition, among others. The key issues of biometrics system are accuracy, efficiency, stability, robustness, applicability, and universality [1]. In recent years biometric identity cards have been issued in some countries based on Iris, fingerprint and face technologies to improve border security control. However, biometrics provided a simple and operative tool for personal authentication or identification, use of these biometrics traits in a ubiquitous and unchecked manner has become hazardous. These concerns mostly center on the security of biometric data and the privacy of individuals whose biometric data is captured [2]. Fusion of fingerprint and iris has accelerated the security process throughout the world such as ATMs, Computer Network, Bank accounts, smart cards and financial services. Iris technology had made excellent performance especially in airports and border crossing security. John Duagman had first proposed an algorithm for iris recognition. His algorithm is based on Iris Codes. Integro-differential operators are used to detect the inner and outer part of the iris. The images are normalized by converting it from Cartesian to polar transform and rectangular representation of the region of interest is generated which is known as rubber sheet model. For feature extraction, Gabor wavelets are used to generate the Iris codes, finally Hamming Distance was used for matching purpose [3]. R. P. Wildes, *et. al.* have stated an automated iris recognition as a biometrically based technology for personal identification and verification. They have used an isotropic band-pass decomposition derived from the application of Laplacian of Gaussian filters to the image data also used the first derivative of image intensity to find the location of edges corresponding to the border of the iris (inner & outer boundaries of Iris) [4]. S. Lim, *et. al.*, represented the feature extraction method where 2D Haar

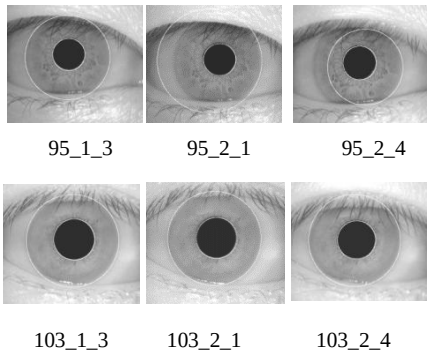

Figure 1. CASIA Images of different clasess

wavelet had used and quantized at the 4th-level high-frequency information to form an 87-binary code length as feature vector. For classification purpose authors had applied an LVQ neural network [5]. The fingerprint recognition algorithms can be broadly classified into minutiae-based and FilterBank-based algorithms. The minutiae-based matching algorithms first extract the local minutiae such as ridge endings and ridge bifurcations from the thinning image or the gray scale image, and then match their relative placement in a given fingerprint with the stored template. A number of matching techniques are available in the literature including point-based matching [6].
String-based matching. Although the minutiae-based matching is widely used in fingerprint verification [7] .
Fingerprints have local parallel ridges and valleys, and well defined local frequency and orientation. Properly tuned Gabor filters can remove noise, preserve the true ridge and valley structures, and provide information contained in a particular orientation in the image. Before filtering the fingerprint image, it is normalized to the region of interest in each sector separately to a constant mean and variance [3]. Normalization

is performed to remove the effects of sensor noise and gray level distortion due to finger pressure differences [8].

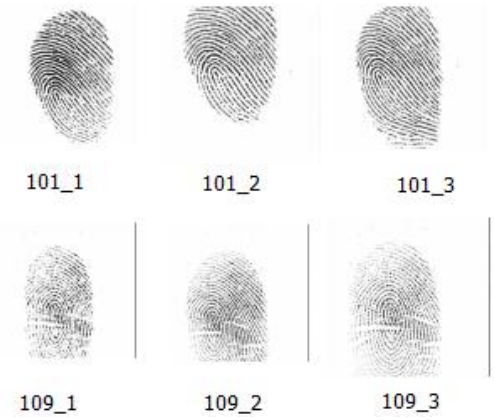

Figure 2. Fusion of Multibiometric

$$G(x, y, f, \theta) = \exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\delta_{x'}^2} + \frac{y'^2}{\delta_{y'}^2}\right]\right\}\cos(2\pi f x') \quad (1)$$

Here f is the frequency of the sinusoidal function along the direction θ, δ_x and δ_y are the space constants of the Gaussian envelope along the x and y axis, respectively, θ denotes the orientation of Gabor filter. For the defined filter δ_x equals to δ_y. In our experiment, the central frequencies used are 8, 10, 12, 14, and 16 for each f filtering is performed at $\theta = 0, \frac{\pi}{4}, \frac{2\pi}{4}, \frac{3\pi}{4}$

II. FUSION OF FINGERPRINT AND IRIS

The implementation of biometrics entails either the establishment of an identity or tracing a person's identity. Biometric passport data (e.g., irises, fingers, faces) can be used in order to verify a passenger's identity. The proposed Passenger Name Record (PNR) system contains all the information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person [20].

Most biometric is essentially a pattern-recognition that makes a personal identification by determining the authentication of user. Some of the biometric traits of an individual are hand geometry, fingerprint, face, iris, retina, palm print, and voice [9]. Biometric systems based on single biometric traits are referred as unimodal systems. These unimodal biometric traits have some limitation. However, a single physical or behavioral characteristic of an individual can sometimes fail to be sufficient for recognition [10]. In order to enhance the accuracy in biometric recognition a fusing is done i: e multibiometric systems. Where multibiometric found to be very useful and exhibit robust performance over the unimodal biometric systems in terms of several constraints [11]. The main aim of multibiometric is to fuse various biometric traits at different information fusion levels to achieve an increased recognition rate with fusion [12]. Fusion in biometry refers to the process of combining two or more biometric modalities. Fingerprint and iris are commonly used biometric for fusion. Here, we represent the fusion of these two biometrics as shown Fig.3.

In the field of statistical pattern recognition fusion of biometric is a special case for pattern classification, by combing multiple classifiers for recognition purpose [13].

Fusion can be made into two categories: pre-fusion and post fusion. Such type of categories are required when the amount of information is available for fusion. It reduces drastically once the matcher has been invoked

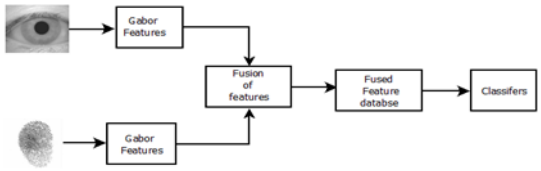

Figure 3. Fusion of Multibiometric

Pre-classification fusion schemes typically require the development of new matching techniques (since the matchers used by the individual sources may no longer be relevant) thereby introducing additional challenges. Pre-classification schemes include fusion at the sensor (or raw data) and the feature levels while post-classification schemes include fusion at the match score, rank and decision levels [14].

A. *Level of Fusion*

- *Sensor level fusion*: The Data coming from different sensors can be fused, so that the resulting information are in some sense better than they would be possible when these sources were individually used [15]. The term better in that case can mean more accurate, more complete, or more dependable.
- *Feature level fusion:* By combining different feature vectors extracted from multiple biometric sources. When the feature sets are homogeneous a single resultant feature vector can be calculated as a weighted average of the individual feature vectors [16].
- *Matching-score level:* which is based on the combining matching scores, after separate feature extraction and comparison between train data and test data [17].
- *Rank level:* This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity (a higher rank indicating a good match). Thus, fusion entails consolidating the multiple ranks associated with an identity and determining a new rank that would aid in establishing the final decision. Techniques such as the Borda count may be used to make the final decision [18].
- *Decision level:* When each matcher outputs its own class label (i.e., accept or reject in a verification system, or the identity of a user in an identification system), a single class label can be obtained by employing techniques such as majority voting or behavior knowledge space [19].

 ISSN: 2321-8169
1363– 1366

III. FEATURE EXTRACTION

Iris has a particularly interesting structure and provides rich texture information. Here we have implemented principal component analysis method which captures local underlying information from an image. This is method is applied to extract the features ROI. In this experiment the size of the feature vector is more than 9000. This is dimension is too high for computation purpose. SVD is a method for identifying and ordering the dimensions along which the feature exhibit the most variation. The most variation are identified the best approximation of the original data points using less dimensions. This generates 1D feature vector that is defined as

Figure 4. 20 Persons Iris Feature Vector

Figure 5. 20 Persons Fingerprint Feature Vector

Experiments are conducted on FVC Database. Four distinct databases, provided by the organizers, constitute the benchmark: DB1, DB2, DB3 and DB4. Each database is 150 fingers wide and 12 samples per finger in depth (1800 fingerprint images). Each database is partitioned in two disjoint subsets A and B: Image size is 388x374 (142 Kpixels) set A (100x8) and set B(10x8) 500dpi. Feature of fingerprint and Iris are fused in 1D feature vector whose size 1X100 for experimental purpose we have selected 80 features of Iris and 20 from fingerprint. We have implemented the FMM algorithm using MATLAB 7.0 and ran on Intel (R) Core Duo core, 1.66 GHz, 980 MHz, 512MB of RAM. Different Data sets are used to perform experiments and Individual comparison is made with Neural Network classifier used for recognition.

The topology of artificial neural network is as shown in figure 6.

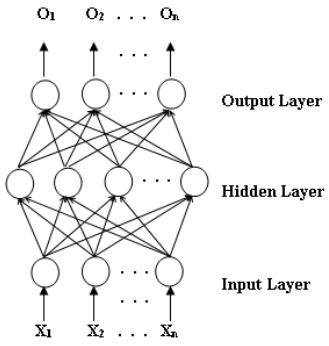

Figure 6. Feed forward Neural Network Architecture with Input layer, Hidden layer and Output layer

TABLE I. ARTIFICIAL NEURAL NETWORK APPROACH

Classifier	Artificial Neural Network Approach		
	Database	*Train time in Seconds*	*Recall time seconds*
Neural Network	Iris CASIA V1	0.930394	34.789102
	FVC	0.730662	29.123098
	Fused Database (Fingerprint + Iris)	0.986655	33.990632

TABLE II. RECOGNITION RATE OF ANN

Methodology	*Database*	*Recognition rate (%)*
Neural Network	Iris CASIA V1	97.37
	FVC	98.78
	Fused Database (Fingerprint + Iris)	96.72

ACKNOWLEDGMENTS

The authors would like to acknowledge support from school of computational sciences of Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India. They are also grateful for staff members from school who have supported for assistance with literature and data.

REFERENCES

[1] C. John and S. Blaul, Implementing Biometric Security, Wiley , 2003.

[2] A. K. Jain, R. Challappa, S. C. darper, Nasir Memon, P. J. Philips and Anthony Vetro, IEEE Signal Processing PP. 146- 152, Nov. 2007.

[3] J. G. Daugman, "High confidence Visual Recognitions of Persons by a statistical Independence," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148–1161, 1993.

[4] R. P. Wildes, et. al., "A System for Automated Iris Recognition," in Proc. Second IEEE workshop Application of Computer Vision, pp. 121-128, 1994.

[5] S. Lim, *et. al.*, "Efficient Iris Recognition through Improvement of Feature Vector and Classifier," *ETRI J.*, vol. 23, no. 2, pp. 61-70, 2001.

[6] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints", Proceedings of the IEEE, Vol. 85, No. 9, pp. 1365 - 1388, 1997.

[7] A. K. Hrechak and I. A. Mchugh, "Automated fingerprint recognition using structural matching", Pattern Recognition, vol. 23, no. 8, pp. 893 - 904, 1990.

[8] J. G. Daugman, "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two - dimensional visual cortical filters" , J.Opt. Soc. Amer. A. vol. 2, pp. 1160-1169, 1985.

[9] Slobodan Ribaric, Ivan Fratric "A Biometric Identification System Based on Eigenpalm and Eigenfinger Features," IEEE Transactions ON Pattern Analysis and Machine Intelligence, vol. 27, No. 11, pp. 1698-1709, November 2005.

[10] Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing, "Feature Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature" IIT, Kanpur,

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

[12] Ujwalla Gawande, Mukesh Zaveri, and Avichal Kapur, "A Novel Algorithm for Feature Level Fusion Using SVM Classifier for

Multibiometrics-Based Person Identification, " Applied Computational Intelligence and Soft Computing, Volume 2013, 17th June, 2013.

[13] Austin Hicklin, Brad Ulery, Craig watson, "A Brief Introduction to Biometric fusion, " NIST, Interagency Report, 16th June, 2006.

[14] Arun Ross, " An introduction to Multibiometrics," Proc. 15th European Signal Processing conference (EUSIPCO), Poland, September, 2007.

[15] Houda Benadiouche and Mohamed Touashria, "Comparative study of Multimodal Biometric Recognition by fusion of Iris and Fingerprint," Hindawi Publishing Corporation, The scientific World Journal, http://dx.doi.org/10.1155/2014/829369, 29th January, 2014.

[16] A. Ross, A. Jain, "Information fusion in biometrics, " Elsevier, Pattern recognition letters 24 (2003) 2115-2125.

[17] Vincenzo Conti, Carmelo Militello, Filippo Sorbello and Salvatore Vitabile, "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems," IEEE Trans. Systems, Man, and cybernetics—Part C: Applications and reviews, vol. 40, no. 4, July. 2010, pp. 384-395.

[18] A. Ross, A. Jain, Handbook of Multibiometrics. New York: Springer-Verlag, 2006.

[19] Md. Maruf Monwar, and Marina L. Gavrilova, "Multimodal Biometric System Using Rank-Level Fusion Approach, " IEEE Trans. Systems, Man, and Cybernetics—Part B: Cybernetics, vol. 39, no. 4, August 2009, pp. 867-878.

[20] G. Nouskalis, "Biometrics, e-Identity, and the Balance between Security and Privacy: Case Study of the Passenger Name Record (PNR) System," Special Issue: Biometrics Applications: Technology, Ethics, and Health Hazards, The Scientific World Journal (2011) 11, 474–477 ISSN 1537-744X; DOI 10.1100/tsw.2011.48