IJITKM Volume 7 • Number 2 • Jan– June 2014 pp. 20-25 (ISSN 0973-4414)

Secure Identity using Multimodal Biometrics

Meenu Mittal[1], Bhumika Garg[2]
[1]M.Tech. Scholar, Modern Institute of Engineering & Technology, Ambala
[2]Assistant Professor, Modern Institute of Engineering & Technology, Ambala
meenumittal12@gmail.com

Abstract
Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Multimodal biometric systems elegantly address several of these problems present in unimodal systems. By combining multiple sources of information, such as palm print and hand geometry, face and fingerprints, face and ear biometric, these systems improve matching performance, increase population coverage, deter spoofing, and facilitate indexing. Various fusion levels and scenarios are possible in multimodal systems. This paper discusses different levels of fusion, various scenarios that are possible in multimodal biometric systems and also analyses accuracy and performance of different multimodal biometric traits (palm print and hand geometry, face and fingerprints, face and ear biometric) with respect to Enrolment, Feature extraction, Matching and Decision making.

1. Introduction

Most biometric systems deployed in real-world applications are unimodal[1], i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint or face). These systems have to contend with a variety of problems such as:

a) **Noise in sensed data**: fingerprint images with a scar or a voice sample altered by cold are examples of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system).
b) **Intra-class variations**: These variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication (e.g., optical versus solid-state fingerprint sensors).
c) **Inter-class similarities**: In a biometric system comprising of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users [2].
d) **Non-universality:** The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges.
e) **Spoof attacks**: This type of attack is especially relevant when behavioral traits such as signature or voice are used. However, physical traits such as fingerprints are also susceptible to spoof attacks.

Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [3]. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [4]. These systems are able to meet the stringent performance requirements imposed by various applications.
They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition. This paper is organized as follows. In the next section we would talk about Fusion Levels which would be continued with Fusion scenarios in the section three. We will conclude the paper with describing our future works.

2. Levels of Fusion

A generic biometric system has 4 important modules:

1. The sensor module which captures the trait in the form of raw biometric data;
2. The feature extraction module which processes the data to extract a feature set that is a compact representation of the trait;
3. The matching module which employs a classifier to compare the extracted feature set with the templates residing in the database to generate matching scores;
4. The decision module which uses the matching scores to either determine an identity or validate a claimed identity.

In multimodal biometric system information reconciliation can occur in any of the aforementioned modules (see Figure 1).

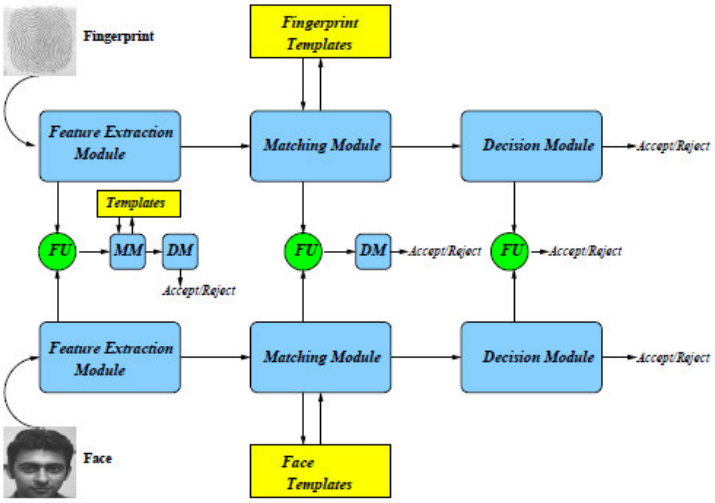

Figure 1: Levels of fusion in a bimodal biometric system; FU: Fusion Module, MM: Matching Module, DM: Decision Module

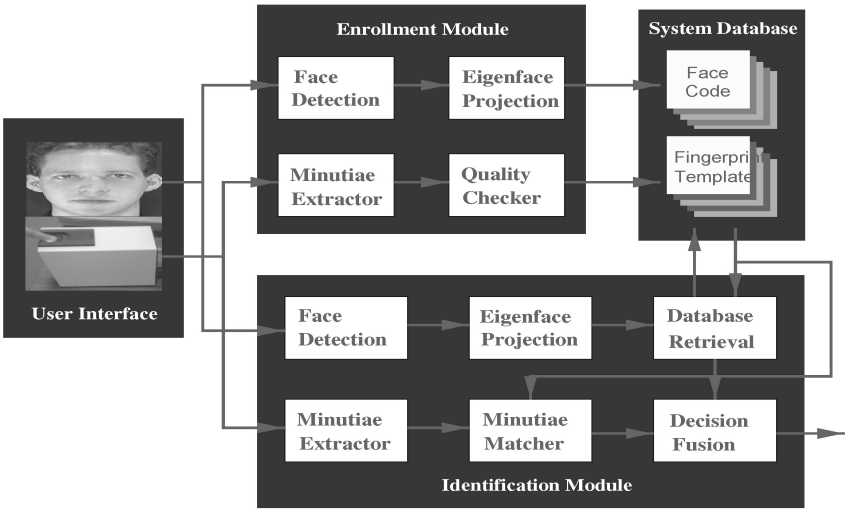

Figure 2: System architecture of the prototype integrated biometric identification system

a) **Fusion at the data or feature level:** Either the data itself or the feature sets originating from multiple sensors/sources are fused.
b) **Fusion at the match score level**: The scores generated by multiple classifiers pertaining to different modalities are combined.
c) **Fusion at the decision level**: The final output of multiple classifiers is consolidated via techniques such as majority voting [5].

Biometric systems that integrate information at an early stage of processing are believed to be more effective than those systems which perform integration at a later stage. Since the feature set contains richer information about the input biometric data than the matching score or the output decision of a matcher, fusion at the feature level is expected to provide better recognition results. However, fusion at this level is difficult to achieve in practice because of the following reasons

(i) The feature sets of the various modalities may not be compatible (e.g., Eigen-coefficients of face and minutiae set of finger)

(ii) Most commercial biometric systems do not provide access to the feature sets (nor the raw data) which they use in their products. Fusion at the decision level is considered to be rigid due to the availability of limited information. Thus, fusion at the match score level is usually preferred, as it is relatively easy to access and combine the scores presented by the different modalities.

3. Fusion Scenarios

Due to intraclass variations in the biometric characteristics, the identity can be established only with certain confidence. A decision made by a biometric system is either a "genuine individual" type of decision or an "impostor" type of decision, [6]. For each type of decision, there are two possible outcomes, true or false. Therefore, there are a total of four possible outcomes:

1) A genuine individual is accepted,
2) A genuine individual is rejected,
3) An impostor is rejected, and
4) An impostor is accepted.

Outcomes 1 and 3 are correct, whereas outcomes 2 and 4 are incorrect. The confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates:

1) False acceptance rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and
2) false reject rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor.

FAR and FRR are dual of each other. A small FRR usually leads to a larger FAR, while a smaller FAR usually implies a larger FRR. Generally, the system performance requirement is specified in terms of FAR .A FAR of zero means that no impostor is accepted as a genuine individual. In order to build a biometric system that is able to operate efficiently in identification mode and achieve desirable accuracy, an integration scheme which combines two or more different biometric approaches may be necessary.

3.1 Face and Fingerprint

Face recognition is fast but not extremely reliable, while fingerprint verification is reliable but inefficient in Database retrieval. A prototype biometric system which integrates faces and fingerprints overcome the limitations of face recognition systems as well as fingerprint verification systems. The integrated prototype system operates in the identification mode with an admissible response time shown in Figure 2.

Generally, there are two major tasks in face recognition:

1. Locating faces in input images and
2. Recognizing the located faces.

The eigenface approach is used for the following reasons:

- In the context of personal identification, the background, transformations, and illumination can be controlled,
- Eigenface approach has a compact representation—a facial image can be concisely represented by a feature vector with a few elements,
- It is feasible to index an eigenface-based template database using different indexing techniques such that the retrieval can be conducted efficiently [8],
- The eigenface approach is a generalized template matching approach which was demonstrated to be more accurate than the attribute-based approach in one study [7].

Face-recognition techniques that can be used are principle component analysis (PCA) , linear discriminant analysis (LDA) [8], singular value decomposition (SVD) , and a variety of neural network-based techniques.

The eigenface-based face recognition consists of the following stages

3.1.1Ttraining Stage

In training stage a set of N training face images are collected and each face is represented as a point in the M dimensional eigenspace

3.1.2 Operational Stage

In Operational stage each test image is first projected onto the M-dimensional eigenspace; the M dimensional face representation is then deemed as a feature vector and fed to a classifier to establish the identity of the individual. A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. It is formed by the accumulation of dead, cornified cells that constantly slough as scales from the exposed surface. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. The two most

prominent ridge characteristics, called minutiae, are ridge ending and ridge bifurcation. Fingerprint verification consists of two main stages [9]:1 minutiae extraction and 2) minutiae matching. Minutiae extraction mainly consists of three steps: 1) orientation field (ridge flow) estimation, in which the orientation field of input fingerprint images is estimated and the region of interest is located, 2 ridge extraction, in which ridges are extracted and thinned, and

3.1.3 Minutiae Detection and Postprocessing

In this stage minutiae are extracted from the thinned ridge maps and refined. The minutiae matching determine whether two minutiae patterns are from the same finger or not. The minutiae matching will be done into two stages: 1) Alignment stage, where transformations such as translation, rotation, and scaling between an input and a template in the database are estimated, and the input minutiae are aligned with the template minutiae according to the estimated parameters; and 2) Matching stage, where both the input minutiae and the template minutiae are converted to "strings" in the polar coordinate system, and an "elastic" string matching algorithm is used to match the resulting strings, and finally, the normalized number of corresponding minutiae pairs is reported. This approach incorporates a **decision fusion** module to improve the identification performance by integrating multiple cues with different confidence measures.

3.2. Face and Ear:

Face recognition is the most promising biometrics. It has many practical applications, such as bankcard identification, access control, mug shots searching, security monitoring, and surveillance systems. But face is not a rigid body, easily changes with makeup, hairstyle, facial expressions and the variation in lighting, pose and acquisition time. All of these may reduce the robustness of system. As a new member of non-intrusive biometric recognition technology, ear recognition system has its own advantages[10]: a) ears do not change significantly from the moment in which people reach adult age; b) ears' surface is so small to allow working with reduced spatial resolution images; c) ears have a uniform distribution of color; d) they do not change their appearance with the expression of the subject; e) the effective recognition angle range of about 60° In the horizontal direction when using both ears at one time, which means that it would be twice as face recognition.

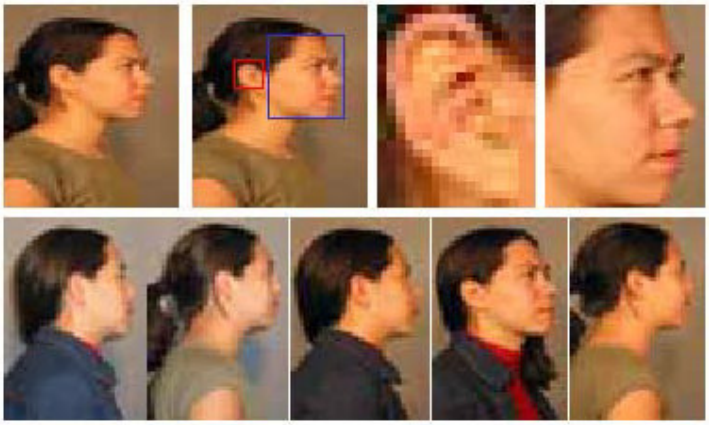

Fig. 3 Procedures of extracting ear and face images (upper), and image variations used in the experiement (Lower)

3.2.1 Profile face and ear:

The special relationship of face and ear in physiological location makes the multimodal based on them reasonable. Let us consider a passive multimodal biometric system based on eigenfaces and eigenears. The best concept is that only need to capture a single image, from which the ear and profile is extracted. Performance of the verifications is obtained based on successful hits by calculating the distance within the prescribed threshold. In case of multimodal biometric system, if the system recognizes any one of the ear or face of a particular person successfully, we consider the correct identification of the subject. Applied the FSLDA algorithm for feature extraction and classification, and then integrated the multimodal biometric ear and profile face at the decision level. The recognition rate of single ear is 94.05% and the recognition rate of single profile face is 88.10%. For the fusion scheme, the best performance is achieved by the Sum rule and Median rule at 97.62% accuracy. After that, many experiments were conducted based on different algorithms and different fusion schemes, for instance, tried to combine profile and ear at feature level and got the best recognition rate of

97.37% with CCA (Canonical Correlation Analysis) [11] method at end. Got a rather better result of 98.68% when adopted KCCA (Kernel CCA) [12], that is an exciting achievement proves that multimodal biometric based on profile and ear very promising again.
Besides, face and ears' special relationship of physiological location would help to reduce the cost of the hybrid system. Overall, multi-modal biometrics system based on face and ear could fully utilize their connection relationship of physiological location. It would significantly improve recognition accuracy, robustness and provide a new way for non-intrusive recognition. This approach integrates ear and profile face at the decision level.

3.3 Palm print and Hand Geometry:
The palmprint and hand geometry images can be extracted from a hand image in a single shot at the same time. Unlike other multi biometrics systems (e.g., face and fingerprint, voice and face , etc.), a user does not have to undergo the inconvenience of passing through multiple sensors. Furthermore, the fraud associated with fake hand, in hand geometry based verification system, can be alleviated with the integration of palmprint features. The block diagram of the proposed verification system is shown in figure 4. Hand images of every user are used to automatically extract the palmprint and hand geometry features. This is achieved by first thresholding the images acquired from the digital camera. The resultant binary image is used to estimate the orientation of hand since in absence of pegs user does not necessarily align their hand in a preferred direction. The rotated binary image is used to compute hand geometry features. This image also serves to estimate the center of palmprint from the residue of morphological erosion with a known structuring element (SE). This center point is used to extract the palmprint image of a fixed size, from the rotated gray level hand images. Each of these palmprint images are used to extract salient features. Thus the palmprint and hand geometry features of an individual are obtained from the same hand image. Two schemes for the fusion of features, fusion at the **decision level** and at the **representation level**, were considered. The normalization is used to reduce the possible imperfections in the image due to sensor noise and non-uniform illumination. The method for normalization employed in this work is the same as suggested in [13].

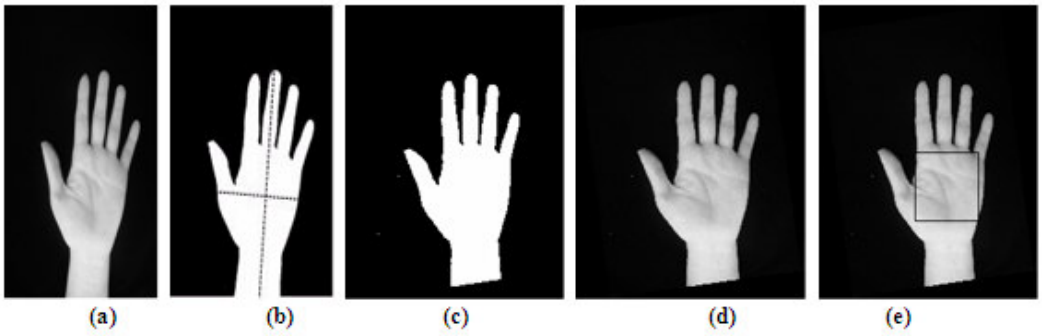

Figure 4: Extraction of two biometric modalities from the hand image, (a) captured image from the digital camera, (b) binarized image and ellipse fitting to compute the orientation (c) binary image after rotation, (d) gray scale image after rotation (e) ROI, i. e., palmprint, extracted from the center of image in (c) after erosion.

Three levels of information fusion schemes have been suggested;
(i) Fusion at representation level, where the feature vectors of multiple biometric are concatenated to form a combined feature vector,
(ii) Fusion at decision level, where the decision scores of multiple biometric system are combined to generate a final decision score
(iii) Fusion at abstract level [14], where multiple decisions from multiple biometric systems are consolidated [14].

The first two fusion schemes are more relevant for a bimodal biometric system and were considered for better performance. The similarity measure between v1 (feature vector from the user) andv2 (stored identity as claimed) is used as the matching score.

4. Conclusion
Due to the Identity management entering the enterprise now as a widely accepted utility, the identity management depends significantly on biometrics technology. With respect to the tremendous advances Biometrics has achieved during the past few years, it can be referred to as the most cost effective and secure

means of authentication in use now. To overcome the limitation of a single biometrics, information from multiple biometrics can be integrated to achieve more reliable and robust performance. Different biometric modalities are discussed and each combination provides some degree of performance. Future efforts should be focused to develop algorithms that can adaptively select the best set of biometric modalities from the available set to ensure the desired level of performance and security.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[2] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," IEEE Trans. on Patt. Anal. and Mach. Intell., vol. 19, pp. 786–796, July 1997.

[3] A. Ross and A. K. Jain, "Information fusion in biometrics," Pattern Recognition Letters, vol. 24, pp. 2115–2125, Sep 2003.

[4] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?," in Proc. of Int'l Conf. on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain), pp. 168–171, 2000.

[5] Y. Zuev and S. Ivanon, "The voting as a way to increase the decision reliability," in Foundations of Information/ Decision Fusion with Applications to Engineering Problems, (Washington D.C., USA), pp. 206–210, August 1996.

[6] E. Newham, The Biometric Report. New York: SJB Services, 1995

[7] R. Brunelli and T. Poggio, "Face Recognition: Features Versus Templates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 15, no. 10, pp. 1,042–1,052, Oct. 1993

[8] D.L. Swets and J. Weng, "Using Discriminant Eigenfeatures for Image Retrieval," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 831–836, Aug. 1996.

[9] N. Ratha, K. Karu, S. Chen, and A.K. Jain, "A Real-Time Matching System for Large Fingerprint Database," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 799–813, Aug.1996.

[10] K. Chang, K. W. Bowyer, Sarkar, et al., "Comparison and Combination of Ear and Face Images in Appearance-Based Biometrics," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp.1160-1165, September 2003.

[11] Xiaona Xu, Zhichun Mu, "Multimodal recognition using ear and face profile based on CCA," Application Research of Computers, vol. 24, no.11, pp. 312-314, November 2007.

[12] Xiaona Xu, Zhichun Mu, "Feature Fusion Method Based on KCCA for Ear and Profile Face Based Multimodal Recognition," Proceedings of the IEEE International Conference on Automation and Logistics, Jinan, China, pp. 620-623, August 2007.

[13] N. Otsu, "A threshold selection method from gray-scale histogram," IEEE Trans. Syst., Man, Cybern., vol. 8, pp. 62-66, 1978.

[14] S. Baskan, M. M. Balut, and V. Atalay, "Projection based method for segmentation of human face and its evaluation," Pattern Recognition Lett., vol. 23, pp. 1623-1629, 2002.