ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Multimodal Biometric System Using Fusions

Sona Aggarwal*
Research Scholar: Computer Science & Engg.
Haryana College of Technology & Management
Kaithal, India
sonaaggarwal56@yahoo.com

Neeraj Jindal*
Research Scholar: Electronics & Communication Engg.
Bhai Maha Singh College of Engineering
Muktsar, India
er.neerajjindal@yahoo.com

Abstract: A biometric system which relies only on a single biometric trait is often not able to meet the desired performance. The Multi-modal system is used where more than one biometric trait is used to identify a person. The study of methods for uniquely recognize based upon one or more intrinsic physical or behavioral. In this paper we present the use of multimodal biometric system to get the higher degree of security.

Keywords: Multimodal Biometric**;** Fusion Strategies and Template Security; Fusions**;**

I. INTRODUCTION

Biometrics system deals with the distinctive physiological or behavioral characteristics of human being. Biometrics system provides different types of techniques that capture a person's identity. Multimodal biometric system provides the technique that combine two or more traits which cannot be easily copied, forgotten or stolen by any intruder. It uses identifiers that capture two or more traits which match with the stored template. And after this process if the person passes all the stages then he/she can continue his/her work.

II. MULTIMODAL BIOMETRIC

The Multimodal biometric systems are providing identification and human security over last few decades. Due to this reason multimodal biometrics systems are adapted to many fields of applications. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a Specific task. Multimodal biometric systems are those which utilize, or are capability of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system is essentially a pattern recognition system. This system measure and analyzes human body Physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics. The biometric identifiers cannot be misplaced. In spite of inherent advantages, unimodal biometric solutions also have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing.

This limitation occurs in several application domains, example is face recognition [1]. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks. Inspite of using unimodal biometric system that have poor performance and accuracy, we study and propose a new approach to the multimodal biometric system. This new Multimodal biometric systems perform better than unimodal biometric systems and are popular even more complex. Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrolment, verification or identification. The reason to combine different modalities is to improve recognition rate [2].

III. BIOMETRIC LEVELS

Feature extraction level: The lowest level of abstraction is when combing the raw data from the sensors, which means that it is only possible to combine multiple samples of the same biometric attribute (i.e. fingerprint with fingerprint), but not samples from another biometric input (i.e. iris with fingerprint sample). In this level we are working with feature extraction where features vectors (extracted from the input sample) are combined. If two different samples are of the same types (two samples of the right index finger), then it is possible to combine and create a new and more reliable feature vector from the two vectors. However, if the samples are of different types (fingerprint and gait-data), the feature vectors can be concatenated into a new and more detailed feature vector.

a. Comparison level: Combining in the comparison level means that each biometric sample computes the comparison score (indicating the proximity of the feature vector with the template vector) independently and where the scores are combined into one single score using mathematical algorithms (logistic regression may be used to combine the scores reported by the two sensors. These techniques attempt to minimize the FRR for a given FAR (Jain et al., 1999b) \cite{art11}). An alternative way at this level of abstraction is to match at the rank level. Different biometric systems return the top n candidates, that is an ordered list of n elements which best matches the input sample.

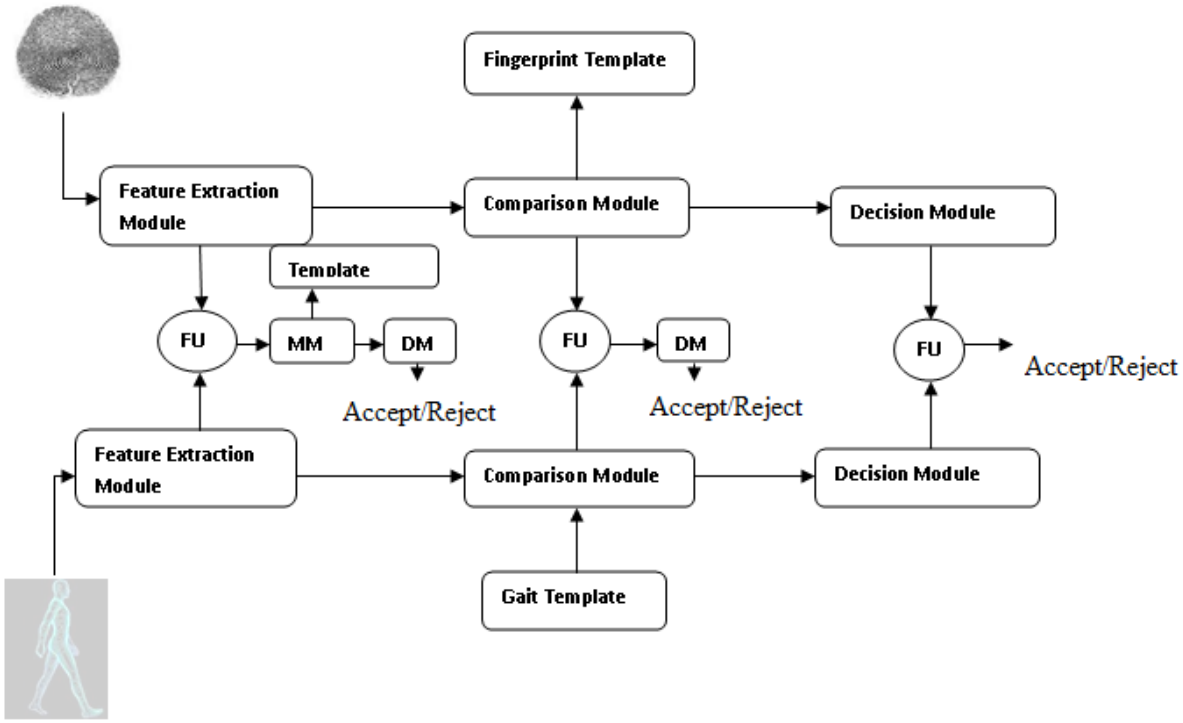

Figure 1: The three levels for multi-modal biometric system

b. Decision-making level: In the decision-making level each system has its own threshold and individually makes their final decision. What will happen in the fusion process is that by joining the several decisions into one single decision, the system can accept or reject, such as by majority voting or Boolean AND/OR laws.

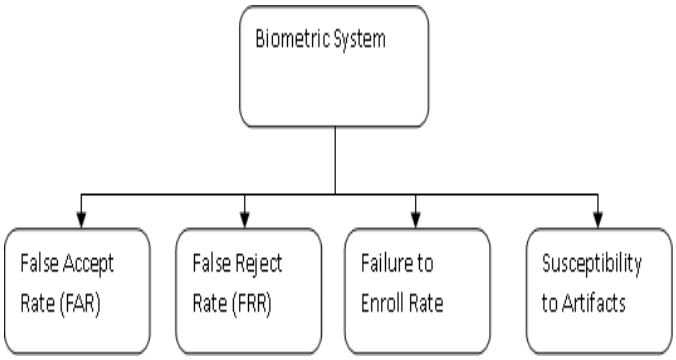

Figure 2: Various rates of the biometric system

IV. THE AIM OF MULTI BIOMETRICS

Generally the match score fusion approach is the method which is mostly used. The reason for that is that match scores are easy to access and there are many ways of combining them, from simple to complex implementations. In addition, match scores present rich information about the input. But match scores are not always to be obtained from all biometric systems. On the other hand they suffer from some commercial systems, which only provide the final authentication decision. Therefore it will be impossible to gain this kind of information.

V. VARIOUS RATES OF BIOMETRIC SYSTEM

a. False accept Rate (FAR)
b. False Reject Rate (FRR)
c. Failure To Enroll Rate (FTR)
d. Susceptibility to Artifacts

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example a system with voice and finger print recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities [3].

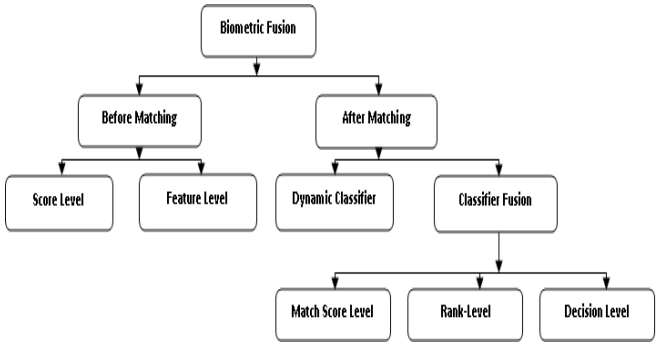

Figure 4: Fusions at different levels

VI. FUSIONS

a. Sensor Level Fusion
b. Feature Level Fusion
c. Score Level Fusion
d. Rank Level Fusion
e. Decision Level Fusion

i. Sensor-level fusion: The raw biometric data (e.g., a face image) acquired from an individual represents the richest source of information although it is expected to be contaminated by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor level fusion refers to the consolidation of (a) raw data obtained using multiple sensors, or (b) multiple snapshots of a biometric using a single sensor. Dieck mann et. al[5] have proposed an abstract level fusion scheme: "2-from-3 approach", which integrate face, lip motion, and voice based on the principle that human user multiple clues to identify a person.

ii. Feature-level fusion: In feature-level fusion, the feature sets originating from multiple biometric algorithms are consolidated into a single feature set by the application of appropriate feature normalization, transformation and reduction schemes. The primary benefit of feature- level fusion is the detection of correlated feature values generated by different biometric algorithms and, in the process, identifying a salient set of features that can improve recognition accuracy. Eliciting this feature set typically requires the use of dimensionality reduction methods and, therefore, feature-level fusion assumes the availability of a large number of training data. Also, the feature sets being fused are typically expected to reside in commensurate vector space in order to permit the application of a suitable matching technique upon consolidating the feature sets.

iii. Score-level fusion: In score-level fusion the match scores output by multiple biometric matchers are combined to generate a new match score (a scalar) that can be subsequently used by the verification or identification modules for rendering an identity decision. Fusion at this level is the most commonly discussed approach in the biometric literature primarily due to the ease of accessing and processing match scores (compared to the raw biometric data or the feature set extracted from the data). Fusion methods at this level can be broadly classified into three categories: density-based schemes [6], transformation-based schemes [9] and classifier based schemes.

iv. Rank-level fusion: When a biometric system operates in the identification mode, the output of the system can be viewed as a ranking of the enrolled identities. In this case, the output indicates the set of possible matching identities sorted in decreasing order of confidence. The goal of rank level fusion schemes is to consolidate the ranks output by the individual biometric subsystems in order to derive a consensus rank for each identity. Ranks provide more insight into the decision- making process of the matcher compared to just the identity of the best match, but they reveal less information than match scores. However, unlike match scores, the rankings output by multiple biometric systems are comparable. As a result, no normalization is needed and this makes rank level fusion schemes simpler to implement compared to the score level fusion techniques [10].

v. Decision-level fusion: Many commercial off-the-shelf (COTS) biometric matchers provide access only to the final recognition decision [4]. When such COTS matchers are used to build a multi biometric system, only decision level fusion is feasible. Methods proposed in the literature for decision level fusion include "AND" and "OR" rules [7], majority voting weighted majority voting, Bayesian decision fusion the Dumpster-Shafer theory of evidence and behavior knowledge space [8].

VII. FUSION STRATEGIES AND TEMPLATE SECURITY

Multibiometric Verification:

Fusion techniques for obtaining score for making decision can be divided into the following three categories:

a. Transformation-based score fusion:

The match scores obtained after fusion are first normalized (transformed) to a common domain and then combined by using product, sum, max or min rules [**14**]. Choice of the normalization scheme and combination weights is data-dependent and requires extensive empirical evaluation [**15**].

b. Classifier-based score fusion:

Scores obtained from multiple matchers are treated as a feature vector and a classifier is constructed to discriminate genuine and impostor scores [**14]**. When biometric score fusion is considered as a classification problem, the following issues pose challenges.

a) Unbalanced training set: The number of genuine match scores available for training is $O(N)$, but the number of impostor scores is $O(N2)$, where N is the number of users in the database.

b) Cost of misclassification: Depending on the biometric application, the cost of accepting an impostor may be very different from the cost of rejecting a genuine user. For example, a biometric system deployed in a security application typically is required to have a false accept rate (FAR) of less than 0:1%. Therefore, the fusion strategy needs to minimize the false reject rate (FRR) at the specified FAR values rather than minimizing the total error rate (sum of FAR and FRR) [**15**].

c) Selection of classifier: Given a variety of admissible classifiers, selecting and training a classifier that gives

the optimal performance (minimum FRR at a specified FAR) on a given data set is not easy.

c. Density-based score fusion:

Density-based score fusion approach is based on the likelihood ratio test and it requires explicit estimation of genuine and impostor match score densities [**13**]. The density based approach has the advantage that it directly achieves optimal performance at any desired operating point (FAR), provided the score densities can be estimated accurately. In fact, a comparison of eight biometric fusion techniques conducted by NIST [**11**] with data from 187000 subjects concluded that \Product of Likelihood Ratios was consistently most accurate, but most complex to implement" and\ complexity in this implementation is in the modeling of distributions, rather than fusion per se". The statement in [**15**] about the complexity of density estimation was based on the use of kernel density estimator (KDE). The selection of kernel bandwidth and density estimation at the tails proved to be the very complex steps in estimating the score densities using KDE in [**12**].

From these three approaches, density based fusion is a more principled approach because it achieves optimal fusion performance if the score densities are estimated accurately. Hence, we follow the density-based score fusion approach in this thesis. We investigate two different techniques for accurately estimating the genuine and impostor match score densities, namely, the Gaussian mixture model (GMM) and the non-parametric kernel density estimator (KDE).We show that:

a) GMM is quite effective in modeling the genuine and impostor score densities and is simpler to implement than KDE.
b) Fusion based on the resulting density estimates achieves consistently high performance on three multibiometrics databases involving fingerprint, face, iris, and speech modalities.
c) Biometric sample quality can be easily incorporated in the likelihood ratio based fusion framework.

VIII.CONCLUSION

In this paper various issues related to multimodal biometrics system have been presented. By combining multiple biometric traits, the performance of biometric system can be improved. Various applications of multimodal biometrics system and different levels of fusion are discussed. The multimodal biometrics is very popular in these days due to its performance and advance level of security. Though some complexity also exists in multimodal system which reduces its acceptability in many areas.

IX. REFERENCES

[1]. R. Brunelli and T.Poggio. Face recognition: Features versus templates. IEEE Trans. Pattern Analysis and machine intelligence, 15 (10) : 1042-1052. 1993.

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

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

[4]. M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"

[5]. U. Dieckmann, P. Plankensteiner, and T.Wagner Sesam :A biometric person identification system using sensor fusion, pattern Recognition letters, 18(9) : 827-833, 1992.

[6]. J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226- 239, Mar. 1998.

[7]. L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.

[8]. R. Auckenthaler, M. Carey, and H. Lloyd-Thomas, "Score Normalization for Text- Independent Speaker Verification Systems," Digital Signal Processing, vol. 10, pp. 42-54, 2000.

[9]. G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheeps, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker

[10]. Recognition Evaluation," Proc. ICSLD 98, Nov. 1998.

[11]. P.J. Huber, Robust Statistics. Wiley, 1981.

[12]. M. Cheung, K. Yiu, M. Mak, and S. Kung, "Multi-Sample Fusion with Constrained Feature Transformation for Robust Speaker Verification", In Eighth International Conference on Spoken Language Processing (ICSLP), pages 1813- 1816, Jeju Island, Korea, October 2004.

[13]. Sheetal Chaudhary, Rajender Nath, "A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face", in IEEE Xplore, International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, pp. 596-600, 27 - 28 october, ARTCom 2009.

[14]. S. C. Dass, K. Nandakumar, and A. K. Jain, "A principled approach to score level fusion in multimodal biometric systems," in Proc. 5th Int. Conf. Audio- and Video-Based Biometric Person Authentication, Rye Brook, NY, pp. 1049–1058, Jul. 20–22, 2005.

[15]. T. Kinnunen, V. Hautamaki, and P. Franti, "Fusion of Spectral Feature Sets for Accurate Speaker Identification", In Ninth Conference on Speech and Computer, pages 361-365, Saint-Petersburg, Russia, September 2004.

[16]. J. Kittler and M. Sadeghi, "Physics-based Decorrelation of Image Data for Decision Level Fusion in Face Verification", In Fifth International Workshop on Multiple Classifier Systems, pages 354-363, Cagliari, Italy, June 2004.