Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Multimodal Biometrics by Feature Level Fusion: A Review

Sumeet Kaur
Department of Computer Science and Engineering
Punjabi University Regional Centre of Information Technology and Management, India

Priyanka Sharma
Department of Computer Science and Engineering
PEC University of Technology, Chandigarh, India

Abstract: ***This review paper introduces the concepts of multimodal biometrics that integrates two or more biometric identifiers and takes advantage of the capabilities of each biometric to provide greater performance and higher reliability. It also discusses various levels of fusion, the importance of fusion at the feature level and a comparative study using different algorithms for performance analysis.***

Keywords: Biometrics, multimodal, fusion, PCA, LDA, ICA

I. INTRODUCTION

As more and more technologies emerge, the impact of secure database systems on these technologies will be significant. An aid to control the suspicious login of the database and suspicious session is a must. Authentication is required when it is necessary to know if a person is who they claim to be. In relation to biometrics, incorporating multiple sources of data for authentication purposes is known as multi-modal biometric authentication.

Traditionally, user authentication was performed based on passwords (something you know) or tokens such as smartcards (something you have). These techniques are, however, less secure since passwords can be forgotten or guessed and the tokens can be lost or stolen. In contrast, Biometrics provides a convenient means of authentication as it is based on something you are that cannot be lost or forgotten [9]. A reliable authentication system is required in order to combat the epidemic growth in identity theft and to meet the increased security requirements in a variety of applications ranging from international border crossings to securing information in databases [1]. Biometric recognition is the study of establishing the identity of a person using his/her anatomical and behavioral traits. Various biometric traits are used in biometric recognition such as fingerprint, face, iris, hand geometry, voice, palm-print, handwritten signatures and gait [8].

A multimodal biometric system is one that utilizes information from multiple cues (multiple modalities or multiple processing techniques or both) to authenticate a user. Thus, a multi-biometric system integrates two or more biometric identifiers and takes advantage of the capabilities of each biometric to provide even greater performance and higher reliability. Ross and Jain stated that the unimodal biometric systems suffers from a variety of problems like noisy sensor data, non-universality, restricted degree of freedom, intra-class variations, spoof attacks and unacceptable error rates. Some of these problems of single trait biometric systems can be overcome by designing multimodal biometric systems which provides multiple evidence of the same feature [2].

II. LEVELS OF FUSION

The fusion of information can occur at the different logical modules of a biometric system. Various levels of fusion in multimodal biometric systems namely sensor level, feature level, match score level and decision level are explained below [3]:

A. Sensor Level Fusion

This fusion strategy requires the raw data to be acquired from multiple sensors which can be further processed and integrated to generate new data from which features can be extracted. This fusion level can be performed only if the sources are either samples of the same biometric trait obtained from multiple compatible sensors or multiple instances of the same biometric trait obtained using a single sensor. The block diagram of sensor level fusion is shown in Fig 1:

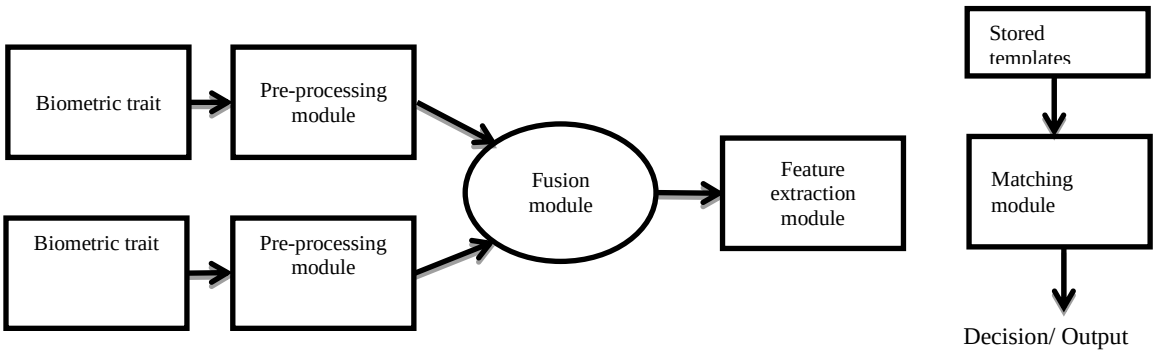

Fig. 1 Sensor level fusion

B. Feature level

The feature set is extracted from the multiple sources of information and is further concatenated into a joint feature vector. This new high dimensional feature vector represents an individual. Various feature selection or transformation procedures may be adopted to reduce the dimensionality of this resultant high dimensional feature set. Then this vector is compared to an enrollment template (which itself is a joint feature vector stored in a database) and classification is performed accordingly. The block diagram representing the flow of feature level fusion is shown in Fig. 2:

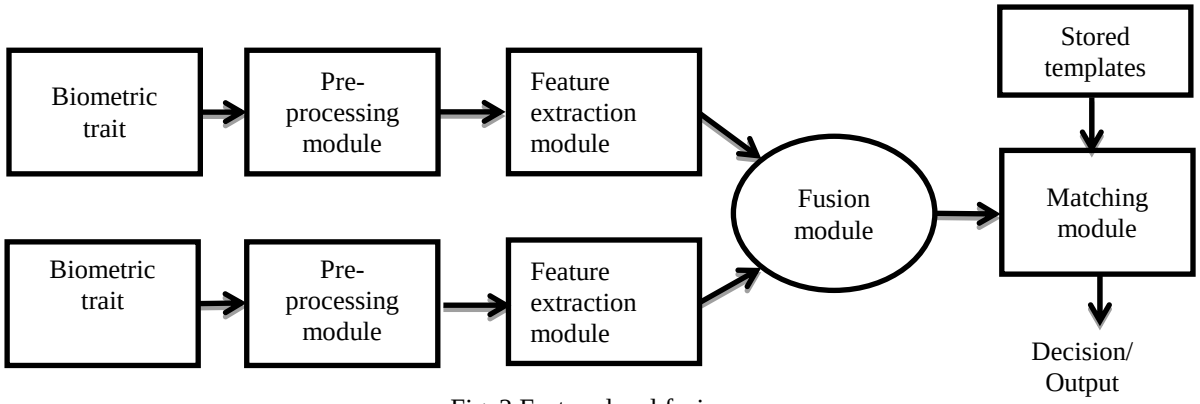

Fig. 2 Feature level fusion

C. Match score level

Match score is a measure of the similarity between the input biometric and template biometric feature vectors. This type of fusion creates the feature vectors independently for each modality and then each individual set is compared to the enrollment templates which are stored separately for each biometric trait during enrollment module. Based on the similarity of feature vector and the template, each subsystem calculates its own match score value. These individual scores are finally combined to obtain a total score, which is then passed to the decision module, after which recognition is performed. The general flow of information in a match score level fusion scheme is shown in Fig. 3:

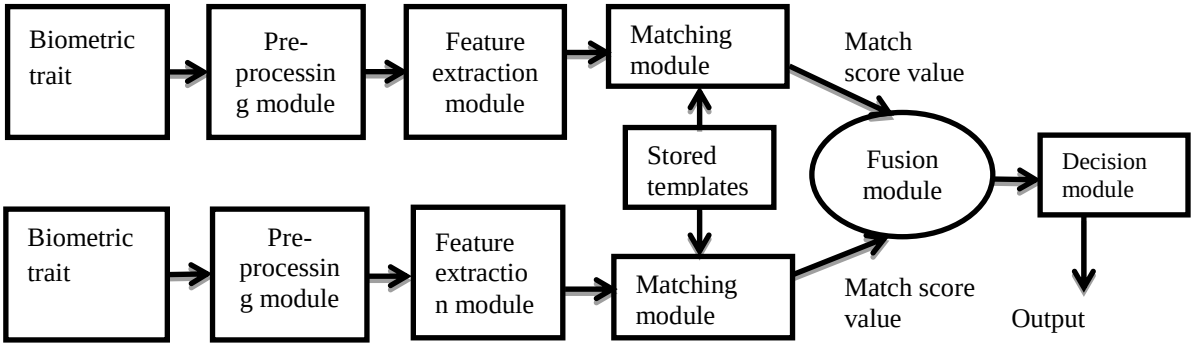

Fig. 3 Match score level fusion

D. Rank level

This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity. Thus, fusion entails consolidating the multiple ranks associated with an identity and determining a new rank that would aid in establishing the final decision.

E. Decision level

In a multi biometric system, fusion is carried out at this level when only the decisions output by the individual biometric matchers are available. Here, a separate authentication decision is computed for each biometric trait (i.e., accept or reject in a verification system, or the identity of a user in an identification system) which is then combined to result in a final vote. Different strategies are available to combine the distinct decisions of individual modality to a final authentication decision. They are majority voting technique, Boolean conjunctions, AND rule, OR rule, Bayesian decision fusion, the Dempster-Shafer theory of evidence and behavior knowledge space. Fusion at this level is considered to be rigid compared to the other fusion schemes due to the availability of limited information. The bolock diagram is shown in Fig. 11.

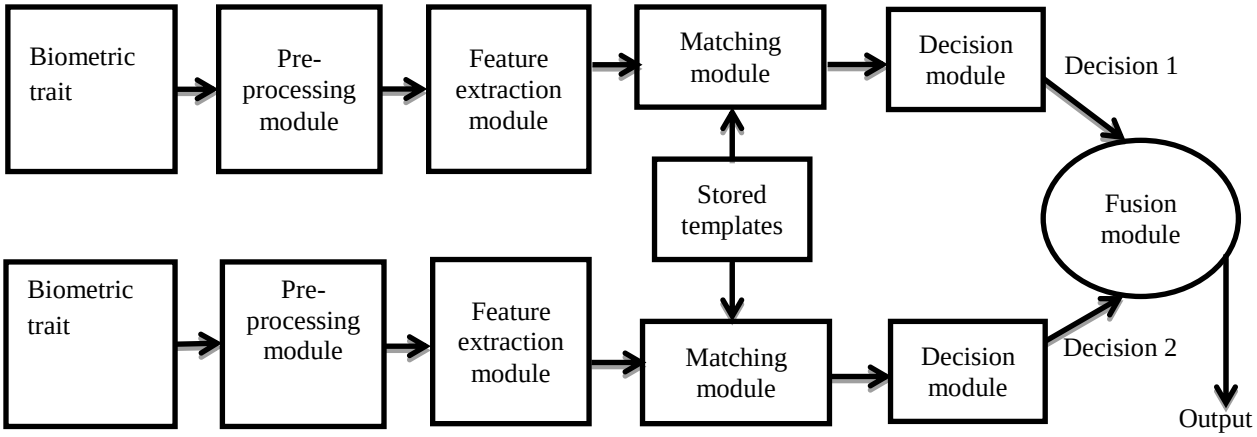

Fig. 4 Decision level fusion

Fusion at the match score, rank and decision levels have been extensively studied in the literature. Rattani et al. presented the multimodal biometric system based on the integration of face and a fingerprint traits at feature extraction level. It suggested to attempt a multimodal data fusion as early as possible in the processing pipeline. The experimental results demonstrate that fusing information from independent/ uncorrelated sources (face and fingerprint) at the feature level fusion increases the performance as compared to score level. Fusion at the match score, rank and decision levels have been extensively studied in the literature.

Fusion at the feature level, however, is a relatively understudied problem. [4]. Fusion at this level is difficult to achieve in practice because multiple modalities may have incompatible feature set or the feature space may be unknown, concatenated feature vector may lead to the problem of curse of dimensionality, a more complex matcher may be required for concatenated feature vector and concatenated feature vector may contain noisy or redundant data thus leading to decrease in the performance of the classifier. But fusion at feature level is expected to provide better authentication results than the match score or the final decision level as its feature set contains richer information about the raw biometric data. Mark Abernethy stated that the data fusion investigation demonstrated that multi-modal biometric authentication systems provide additional accuracy improvement compared to uni-modal biometric authentication systems. Also the fusion at feature level demonstrated improved accuracy compared with confidence score level and decision level data fusion methods [7].

III. FEATURE EXTRACTION ALGORITHMS

Feature extraction process is used for extracting the geometrical features from various images. There are many types of algorithms used for extraction process. This paper discusses the use of three appearance-based statistical methods, namely Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA). Delac et al. had presented an independent and comparative study of three most popular appearance based face recognition algorithms (PCA, ICA and LDA) in completely equal working conditions and across all implementations (all algorithm-metric combinations). It was found that no algorithm-metric combination is the state-of-the-art at this time, and the space of algorithm comparisons needs further research [10]. Some of these appearance based face recognition algorithms are discussed below.

A. Principal component analysis (PCA)

Bokade and Sapkal proposed an authentication for a multimodal biometric system identification using two traits i.e., face and palm print at feature extraction level. The training database consisted of face and palm print images. Principal Component Analysis method is used to extract the features from face and palm prints separately. The feature normalization and feature concatenation scheme followed by a dimensionality reduction procedure is adopted to form the feature matrix [5].

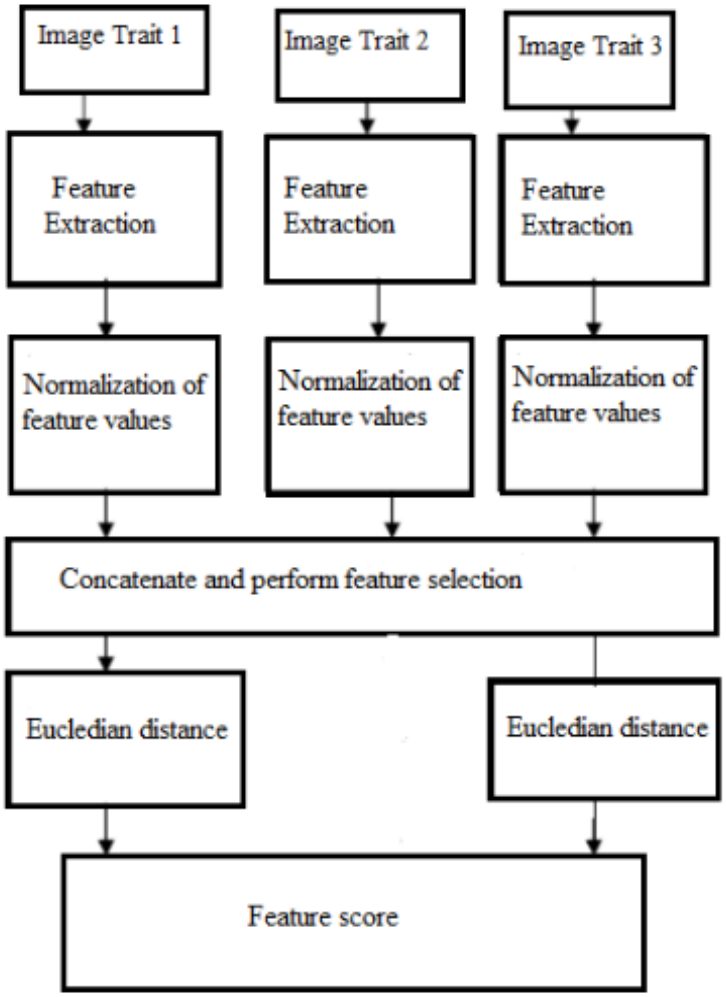

Fig. 5 Block diagram of PCA algorithm

B. Linear discriminant analysis (LDA)

This algorithm is used to find a linear combination of features which characterizes or separates two or more classes of objects or events. It is a parametric approach in supervised learning category of various pattern recognition algorithms. Initially this algorithm was used for dimensionality reduction and feature extraction but later on it is moved for classification purpose also. It can easily handle the cases where the within-class frequencies are unequal and their performances had been examined on randomly generated test data. Thus it maximizes the ratio of between-class variance to the within-class variance in any particular data set thereby guaranteeing maximal separability.

Linear discriminant analysis has a close relation with Principal Component Analysis (PCA). Both these methods are used for dimensionality reduction process. LDA have been proven better algorithm when compared with PCA. The prime difference between LDA and PCA is that PCA does more of feature classification and LDA does data classification. In working with PCA, the location of the original data set changes when transformed to a totally different space whereas LDA doesn't change the location but only tries to provide more class separability and draw a decision region between the given classes.

IV. DISCUSSION AND CONCLUSION

Multibiometric systems, which integrate information from multiple biometric traits, are gaining popularity because they are able to overcome limitations of unimodal biometrics. Until recently, most research in multi-modal biometrics have concentrated on combining data at decision or score levels. It has been proposed in the literature that fusion at the feature level has been an understudied subject and also it uses data closest to the raw data, and therefore is richer in feature information (compared with the other levels). Thus; provide more and robust verification process. Also, no algorithm-metric combination is the state-of-the-art at this time, and space of algorithm comparisons needs further research. The intention of this study is to fuse multi-modal biometric data at the feature level and compare them by using different algorithms for performance analysis.

References

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", in *Journal on Advances in Signal Processing*, Michigan State University, pp. 1-17, 2007.

[2] A. K. Jain and A. Ross, "Multibiometric Systems," *Communications of the ACM*, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34–40, 2004.

[3] A. Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", Proc. of SPIE Conference on Biometric Technology for Human Identification II, Orlando, USA, pp. 196-204, March 2005.

[4] A. Rattani, D. R. Kisku, M. Bicego and M. Tistarelli, "Feature Level Fusion of Face and Fingerprint Biometrics", Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on; 10/2007

[5] Gayatri Umakant Bokade and Ashok. M. Sapkal, "Feature Level Fusion of Palm and Face for Secure Recognition, Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004. Recognition" , International Journal of Computer and Electrical Engineering, Vol.4, No.2, April 2012.

[6] Kresimir Delac, Mislav Grgic and Panos Liatsis "Appearance-based Statistical Methods for Face Recognition", 47th International Symposium ELMAR-2005, 08-10 June 2005, Zadar, Croatia.

[7] Mark Abernethy, "User Authentication Incorporating Feature Level Data Fusion of Multiple Biometric Characteristics" Doctor of Philosophy Murdoch University, January 2011.

[8] Vani Perumal, Dr.Jagannathan Ramaswamy, "An Innovative Scheme For Effectual Fingerprint Data compression using Bezier Curve Representation", in International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009

[9] Abhishek Nagar, "Biometric Template Security", Ph.D. Thesis, 2012.

[10] Kresimir Delac, Mislav Grgic and Sonja Grgic, "A COMPARATIVE STUDY OF PCA,ICA AND LDA".

