RESEARCH ARTICLE OPEN ACCESS

Fusion Techniques in Multi Biometric Systems

Puja S Prasad [1], Prof G N Purohit [2], Dr.Sourabh Mukherjee [3]
Department of Computer Science [1] & [3]
AIM&ACT [2]
Banasthali Vidyapith Banasthali University, Rajasthan
India

ABSTRACT
Biometric fusion uses multiple biometric inputs to enhance the performance of the system or to make more robust system. Biometric fusion improves system accuracy, efficiency, applicability, and robustness that is not completely provided by uni modal system. While fusion can be very effective, it should not be regarded as a universal remedy, since it adds costs complexity to data collection and whole system architecture**.**

Keywords :— Multimodal Biometric, fusion , matching score, threshold

I. INTRODUCTION

Biometric systems is an authentication system that verify a person’s identity based on his anatomical and behavioural characteristics such as palm print, vein pattern, fingerprint, face and iris. A method of identifying or verifying the identity of an individual person or subject based on the physiological and behavioral characteristics is called biometric recognition. Multimodal biometrics reduces the limitation of unimodal system by using multiple instances of same biometric or fusing two or more biometric. A multi-biometric system is one in which multiple categories of data are collected and used for various purposes like fusion and many more other purposes.

II. MULTI-BIOMETRIC SYSTEMS

Multi biometric systems address the issue of non-universality i.e., limited population coverage. For example, if a person’s poor quality of fingerprints prevents him from enrolling in the system; then the use of other biometric traits such as iris, face, voice etc. will help the system acquire meaningful biometric data and enrol the user. It is extremely difficult to spoof multiple biometric traits of a ones legitimate user. If each subsystem determines the probability of the particular trait being a spoof, it is possible to find out the probability of the user being an imposter by using an appropriate fusion technology., a challenge response mechanism can be included that asks user to present the random subset of traits at the point of cquisition. This would ensure that the system is interacting with a live user.

Multi biometric systems effectively address the problem arising because of noisy data. When the information acquired from one biometric trait is corrupted by noise, it is possible to use information acquired from the other biometric trait. Some systems also take into considerations the quality of acquired input biometric signals during the fusion process. Estimating the quality of acquired biometric data is in itself a challenging problem. However, if done appropriately, multi biometric systems gain significant benefits.

III. CATEGORIES OF FUSION

One of the fundamental issues in the development of a multi biometric system is to determine the type of information that should be fused. The biometrics image fusion extracts information from each source image and obtains the effective representation in the final fused image. The aim of image fusion technique is to fuse the detailed information which obtains from both the source images. By convention, multi-resolutions images are used for image fusion, which are obtained from different sources. Multi-resolution analysis of images provides useful information for several computer vision and image analysis applications. The multi-resolution image used to represent the signals where decomposition is performed for obtaining finer detail. Multi resolution image decomposition gives an approximation image and three other images viz. ,horizontal, vertical and diagonal images of coarse detail. The Multi-resolution techniques are mostly used for image fusion using wavelet transform and decomposition Depending on the type of information that is fused, the fusion scheme can be classified as sensor level, feature level, score level and decision level fusion.

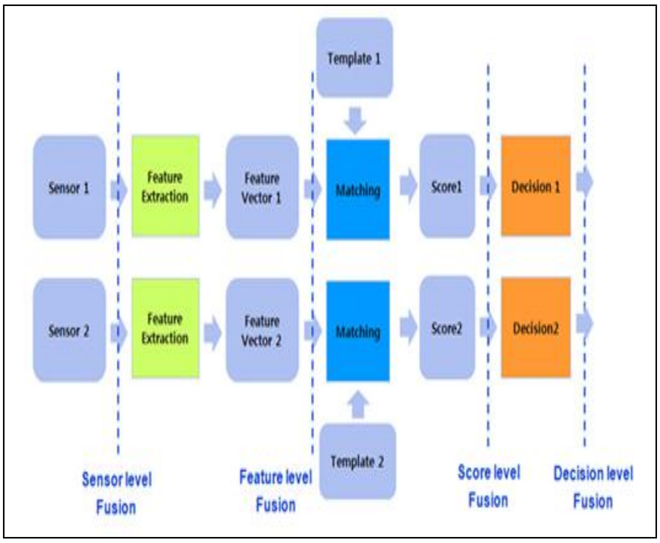

Fig 1. Levels of Fusion

The raw biometric data (e.g., face image in the case of face biometric) has the highest information content, which gets reduced by subsequent processing (e.g., after extraction of PCA features). In the verification mode, the final decision label contains only a single bit of information (match or non-match). However, the different stages of biometric data processing are expected to decrease the intra-user variability and the amount of noise that is contained in the available information. Further, in many practical multi biometric systems, higher levels of information such as the raw images or feature sets are either not easy. On the other hand, in most of the multi biometric systems, it is relatively easy to access and combine the match scores generated by different biometric matchers.

The types of data or methods of processing used constitute the categories of fusion:

- Multi-sample: In this type of fusion multiple samples (images) acquired from the same source, such as multiple images of a single fingerprint, images of the same face, or recordings of a speaker.
- Multi-instance: fusion of multiple instances of the same type of biometric, such as fingerprints from different fingers, or images of both irises.
- Multi-modal: fusion of multiple types of biometrics, such as a combination of a subject's fingerprints, face, irises, and voice.
- Metadata: fusion of biometric inputs with other information, such as gender, height, or age. Demographic information is sometimes described as soft biometrics. There are different levels of fusion

A. *Fusion before matching*

Fusion before to matching can be achieved in two different ways:

1. Sensor level fusion

2. Feature level fusion

In Sensor level fusion multiple samples are combined to form single sample and this type of fusion applicable only if the multiple sources represent samples of the single biometric trait obtained either using a single sensor or different compatible sensors.

In Feature level fusion is achieved by combining different feature sets extracted from multiple

biometric sources. Feature sets could be either homogeneous or heterogeneous. This means sample is taken from different biometric traits or from same biometric traits that have one or more instances.

B. *Fusion after matching*

1.Score-level fusion

2.Decision level fusion

3.Rank level fusion

Matching module compares the extracted feature set with the stored templates using a classifier or matching algorithm in order to generate matching scores; in the decision module the matching scores are used either to identify an enrolled user or verify a user's identity. Generally, a multi-biometric system based on the matching score level fusion works as follows: each subsystem of the multi-biometric system exploits one biometric trait to produce a matching score. Then these matching scores are normalized and integrated to obtain the final matching score or final decision for personal authentication. Match scores generated from different matchers might not be homogeneous. We have discussed various normalization schemes which transform the match scores into a comparable domain. After the match scores are normalized, different classifier combination rules such as sum, max and min can be used for fusion. In classifier-based fusion, the vector of match scores generated by multiple matchers is input to the trained classifier. The trained classifier classifies the vector into one of the two classes, genuine or imposter.

In matching score fusion we actually fuses this matching score before it go in decision module . A system makes a match or non‐match decision based on a score threshold; genuine or imposter refer to whether the samples actually came from the same individual or from different individual.

In score level fusion multiple samples, instances, or modalities are compared, and the resulting similarity scores (or probabilities) are combined to form a single matching score. Score-level fusion can also be used to combine the results of multiple algorithms when a single sample is searched. Let X be an individual arriving at a biometric system, and let {x1, x2, . . . , xn}represent the gallery of enrolled passengers. By comparing X with enrollee xi,a matching score si is generated, representing the degree of similarity between the biometric feature(s) of X and xi. Provided one of these matching scores is above or below a certain pre-determined threshold, the decision is made to grant or deny access to an individual.

Decision-level fusion is used in the same cases as score-level fusion, but the scores are turned into match/non-match decisions before fusion. In decision level fusion, each classifier applies a threshold on the match score and renders its decision regarding the presence (=1) or absence (=0) of a genuine individual. The decisions from multiple classifiers are then fused in order to generate the final decision.

As score level fusion has many advantages as compared to other level fusion strategies. Fusion at matching score level is likely to provide better recognition performance as it contains more contented information which is both feasible and practical. Three main categories of score level fusion, namely, density-based, transformation based and classifer-based are commonly used..Density-based schemes require a large number of training samples in order to estimate the joint conditional densities. When the available training data is limited, it is appropriate to use transformation-based schemes .

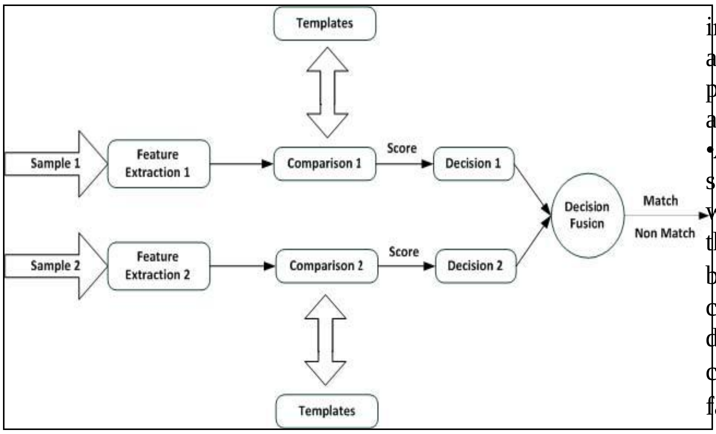

Fig 2.Match score fusion

Rank level fusion consolidates the ranks output by the individual subsystems in order to derive a agreement rank of each identity. In multimodal biometric system, rank level fusion can be used to combine the biometrics matching scores from the different biometric modalities (for example face, fingerprint, palmprint and iris).

It can also be used for performance improvement in unimodal biometric system by combining multiple classifier output that use different classifiers (K nearest neighbor, neural network, support vector machine, decision tree, etc.), different training set, different architectures (different number of layers or transfer function in neural network) or different parameter values (different kernels in support vector machine or different K in K nearest neighbor). Rank level fusion provides less information with compare to match score level fusion.

1.2 Purposes for fusion

Fusion has been used successfully for years in large ‐ scale automated fingerprint identification systems (AFIS), which combine multi ‐ finger data and multiple methods of processing; indeed, it is fair to say that multi ‐ instance and multi ‐ algorithm fusion are what have made very large ‐ scale fingerprint systems practical. Today, various forms of fusion are used in a number of different types of biometric systems.

Fusion can be used to address a number of issues faced by the designers, implementers, and operators of biometric systems:

• ***Accuracy:*** Fusion can be used very efficiently to improve overall accuracy. Biometric system accuracy is generally stated in terms of maximizing the True Accept Rate (TAR) while minimizing the False Accept Rate (FAR): maximizing the ability to recognize those subjects who have already been enrolled, without incorrectly identifying them as other subjects.

• ***Efficiency:*** Fusion can be used to increase efficiency, or to allow tradeoffs between efficiency

and accuracy. System efficiency can be stated in terms of throughput (processing time),computational requirements, and financial cost.

• ***Robustness:*** The inherent redundancy in a fused system increases the system's robustness. Robustness refers to the ability of a system to continue to function as accurately as possible despite problems such as poor sample (image) quality and data integrity errors.

•***Applicability:*** Applicability relates to the appropriateness of a system for a task: the need to

work with legacy data often dictates the biometric modalities that can be used. A multimodal system is more applicable to a broad variety of uses than a uni ‐ modal system, because it can be used in conjunction with multiple sources of legacy data. For example, a multimodal fingerprint and face system can conduct both fingerprint ‐ only background checks and face ‐ only watchlist checks.

• ***Universality:*** Universality refers to whether all people can use a given biometric system. Some people cannot provide usable biometric samples, for reasons such as amputations, injury, or disease. Multi ‐ modal and multi ‐ instance systems can provide alternatives so that all people can use a system.

III. CONCLUSIONS

Various types of information can be combined. In this paper we have discussed the various levels of fusion that are used in fusing information in multi biometric systems. Sensor level fusion combines the information at raw level and is not very complicated. Although raw data is the rich in information, it is there is high probablity that raw data is contaminated by noise.

Feature level fusion involves fusion of the feature sets originating from multiple information sources (from multiple feature extractors). Compared to the raw data, noise is suppressed in feature-level representation.

Moreover, feature transformation algorithms can be applied to the augmented feature sets which enable the detection/removal of correlated feature values improving recognition accuracy.

Match scores contain the richest information after the raw data and feature sets obtained from raw data. Moreover, it is easy to access and combine the match scores from different biometric matchers. Therefore, fusion at score level is the most common approach in multi biometric systems.In rank level fusion each classifier associates a rank with every enrolled identity. Hence, rank level fusion is appropriate for systems operating in the identification mode. In decision level fusion, information is combined at abstract level. However, decision level fusion is the only viable approach for combining outputs from the commercial matchers which provide only the final recognition result.

REFERENCES

[1] C. SANDERSON, K.K. PALIWAL, INFORMATION FUSION AND PERSON VERIFICATION USING SPEECH AND FACE INFORMATION, RESEARCH PAPER IDIAP-RR 02-33, IDIAP, SEPTEMBER 2002.

[2] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric IEEE Trans. Circuits Systems Video Technol. 14 (1) (2004) 4–20 (special issue on image- and video-based biometrics).

[3] Hassan Soliman et al. "Feature Level Fusion of Palm Veins and Signature Biometrics" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 01 28

[4] Mohammad H. Mahoor, 2008, "A Multimodal Approach for Face Modelling and Recognition", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, September, pp: 431- 440.

[5] Harbi AlMahafzah, Mohammad Imran and H.S. Sheshadri "Multibiometric: Feature level fusion" IJCSI, Vol. 9, Issue 4, No 3, July 2012

[6] S. Perumal Sankar, Dinakardas C. N., " Multimodal biometric Authentication System Based on High level feature fusion approach" ISSN 1450- 216X Vol. 84 No. 1 (2012), pp. 55-63.

[7] Kevin W. Bowyer, K.I. Chang "Multi-modal Biometrics"

[8] Pradeep K. Atrey, M. Anwar Hossain "Multimodal fusion for multimedia analysis" Multimedia systems (2010) 16:345-379

[9] P.D.Garje, Prof. S.S. Agrawal "Multimodal Identification System" (IOSRJECE) ISSN: 2278-2834 Volume 2, Issue 6 (Sep-Oct 2012)

[10] Pradeep K. Atrey, M. Anwar Hossain , Abdulmotaleb El Saddik, Mohan S. Kankanhalli " Multimodal fusion for Multimedia analysis: a survey" Multimedia Systems (2010) 16:345-379.

[11] R. BRUNELLI, D. FALAVIGNA, "Person identification using multiple cues," IEEE Transactions on Pattern Analysis and Machine Intelligence 1995.

[12] J. KITTLER, R. P.W. DUIN, "The combining classifier: to train or not to train," in Proceedings of the International Conference on Pattern Recognition, vol. 16, no. 2, pp. 765–770, 2002.

[13] L. HONG and A. K. JAIN, "Integrating faces and fingerprints for personal identification," IEEE Trans. PAMI, vol. 20, no. 12, pp. 1295-1307, 1998.

[14] S. BEN-YACOUB, Y. ABDELJAOUED, and E. MAYORAZ, "Fusion of face and speech data for person identity verification," IEEE Tran Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.