International Journal of Information Technology and Knowledge Management
January-June 2012, Volume 5, No. 1, pp. 211-214

MAKING BIOMETRIC SYSTEM MORE ROBUST WITH MULTIBIOMETRICS

Darshan Lal[1], Bharat Bhushan[2] and Chander Kant[3]

ABSTRACT: A biometric system is a pattern recognition system that makes a personal verification and identification by establishing the authenticity on the basis of a particular physiological or behavioral characteristic possessed by the user. Biometrics provides a better solution for increased security requirements and privacy protection than traditional recognition methods such as passwords and PINs. Biometric systems that use a single biometric trait to establish identity are unimodal biometric systems. Various limitations imposed by these biometric systems are noisy data, non-universality, intra-class variations, inter-class similarities and spoof attacks. These limitations can be addressed by deploying multimodal biometric systems that consolidate the evidence presented by multiple biometric sources of information. This paper discusses the various sources of biometric information that can be integrated, different levels of fusion that are possible, and factors affecting design issues.

Keywords: Biometrics, multimodal, face, fingerprint, iris, signature, fusion, matching score.

1. INTRODUCTION

Multimodal biometric systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence [1]. These systems are able to meet the stringent performance requirements imposed by various applications. Unimodal biometric systems have to contend with a variety of problems [2] that are discussed below.

(i) Noisy Data: A fingerprint with a scar (Figure 1) [1] and a voice altered by cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors (for example, accumulation of dirt on a fingerprint sensor) and unfavorable ambient conditions (for example, poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

(ii) Inter-class similarities or Distinctiveness: While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities (overlap) in the feature sets [3] used to represent these traits. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

(iii) Non-universality: The biometric system may not be able to acquire meaningful biometric data from a subset of individuals resulting in a failure-to-enroll (FTE) error. For example, a fingerprint biometric system may be unable to extract features from the fingerprints of certain individuals due to the poor quality of the ridges (Figure 1) [1].

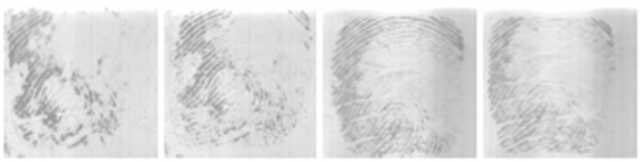


Figure 1: An Example of "Failure to Enroll" for Fingerprint Recognition System: Four Different Impressions of a Subject's Finger Exhibiting Poor Quality Ridges Due to Extreme Finger Dryness. A Given Fingerprint System Might Not Be Able to Enroll this Subject Since Minutiae and Ridge Information Cannot be Reliably Extracted.

(iv) Spoof attacks: An impostor may attempt to spoof the biometric trait of a legitimately enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits like fingerprints are also susceptible to spoof attacks.

(v) Interoperability issues: Most biometric systems operate under the assumption that the biometric data to be compared are obtained using the same sensor and, hence, are restricted in their ability to match or compare biometric data originating from different sensors. For example, fingerprints obtained using multiple sensor technologies cannot be reliably compared [4] [5] due to variations in sensor technology, image resolution, sensing area, distortion effects, etc.

Multimodal biometric systems address noisy data problem by providing multiple sensors and multiple traits. Intra-class variations and inter-class similarities can be avoided with multiple samples and multiple instances of

[1] Research Scholar, Department of Comp. Sc. Singhania University, Rajasthan, India, E-mail: darshanynr18@gmail.com.
[2] Professor & HOD, Deptt. of Computer Science, Khalsa College, Yamuna Nagar, E-mail: bharat_dhiman@sify.com.
[3] Asst. Professor, Deptt. of Comp. Sc. & Appl, K.U. Kurukshetra, E-mail: ckverma@rediffmail.com.

same trait. These systems also provide sufficient population coverage with multiple traits to address the problem of non-universality. 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 present at the point of data acquisition [6]. They also impart fault tolerance to biometric applications so that they continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction or deliberate user manipulation.

2. LEVELS OF FUSION

A generic biometric system consists of four modules namely sensor module, feature extraction module, matcher module and decision module. In a multibiometric system fusion can be performed depending upon the type of information available in any of these modules. According to Sanderson and Paliwal [16] various levels of fusion can be classified into two broad categories: fusion before matching and fusion after matching (Figure 2) [3].

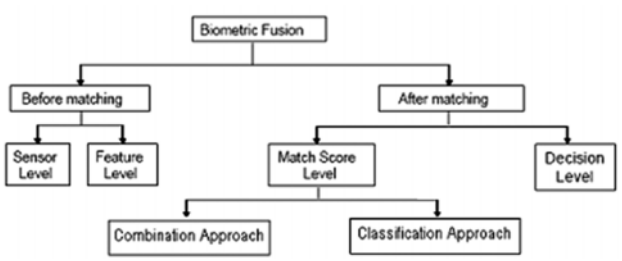


Figure 2: Biometric Fusion Classification.

This classification is based upon the fact that once the matcher of a biometric system is invoked, the amount of information available to the system drastically decreases [4].

(1) Fusion Prior to Matching

This scheme includes fusion at the sensor and feature extraction levels (Figure 3).

(1.1) Sensor Level Fusion

It refers to fusion of raw biometric data of the same trait obtained from multiple compatible sensors or fusion of multiple samples of the same trait obtained using a single sensor [17].

(1.2) Feature Level Fusion

It refers to fusion of different feature sets extracted from multiple biometric sources. When the feature sets are homogeneous (e.g., multiple measurements of a person's hand geometry), a single resultant feature set is calculated as a weighted average of the individual feature sets. When the feature sets are non homogeneous (e.g., feature sets of different biometric modalities like face and hand geometry) [18], we can concatenate them to form a single feature set. Concatenation is not possible when the feature sets are incompatible (e.g., fingerprint minutiae and eigen-face coefficients).

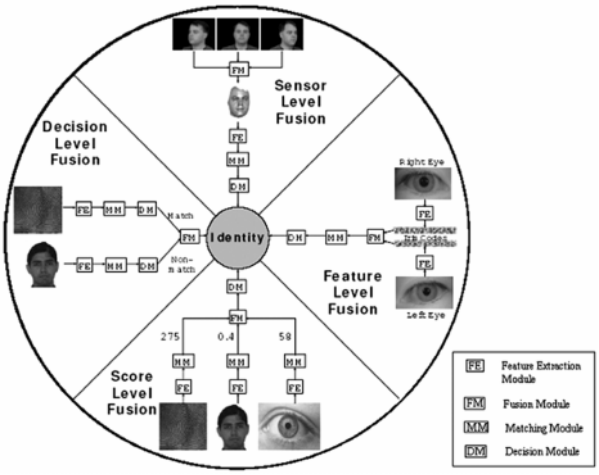


Figure 3: Fusion at Various Levels in a Biometric System.

(2) Fusion After Matching

This scheme includes fusion at the match score and decision levels (Figure 3).

(2.1) Match Score Level Fusion

It refers to the fusion of match scores generated by multiple biometric matchers. The resulting score is then used by the verification or identification modules for rendering an identity decision [19][20]. It is further classified into combination and classification approach. In combination approach, individual matching scores are combined to generate a single scalar score, which is then used to make the final decision. In classification approach, a feature vector is constructed using the matching scores output by individual matchers. This feature vector is then classified into one of two classes: Accept (genuine user) or Reject (imposter) [21].

(2.2) Decision Level Fusion

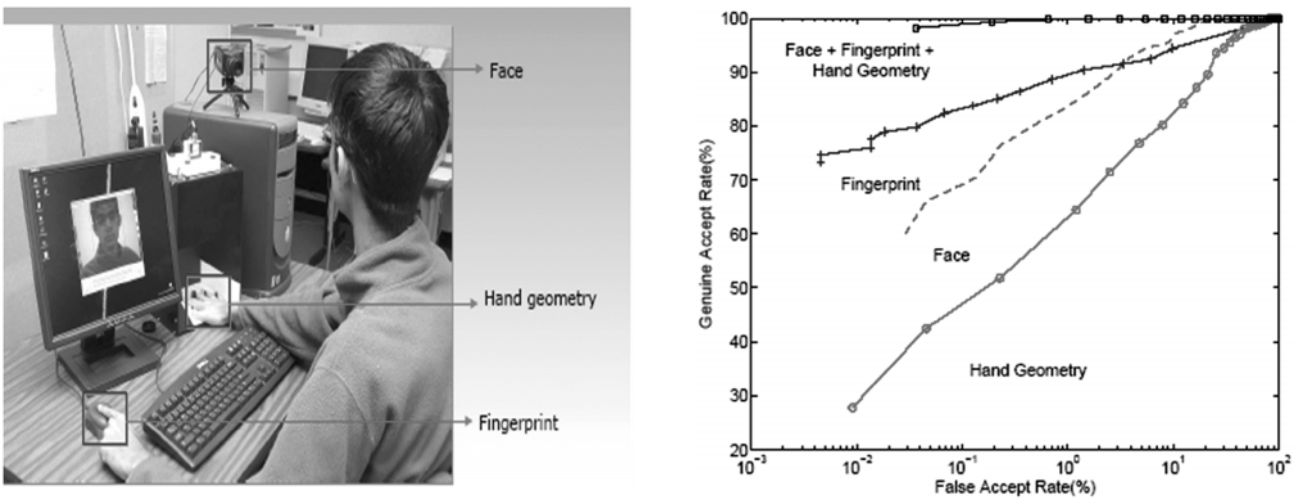
At this level the final decisions output by the individual systems are consolidated by using various techniques [22].

It is generally believed that a fusion scheme applied as early as possible in the recognition system is more effective. For example, an integration at the feature level typically results in a better

improvement than at the matching score level. This is because the feature representation conveys the richest information about the biometric data than the matching score, while the decision labels contain the least amount of information about the decision being made. However, it is difficult to achieve integration at the feature level because the relationship between the feature sets of different biometric systems may not be known and the feature representations may not be compatible (for example, it is difficult to combine the minutiae points of a fingerprint image with the eigen-coefficients of a face image). Furthermore, most commercial biometric systems do not provide access to the feature sets, which they use in their products. In such cases, integrations at the matching score or decision levels are the only options. Next to the feature sets, the matching scores output by the different matchers contain the richest information about the input pattern and also it is relatively easy to access and combine the scores. Therefore, fusion at the match score level is the most common approach in multimodal biometric systems [21].

4. EXAMPLE OF A MULTIMODAL BIOMETRIC SYSTEM

Multimodal biometric systems alleviate some of the problems observed in unimodal biometric systems. They can consolidate information at various levels, the most popular is fusion at the matching score level where the scores generated by individual matchers are combined. In literature, a number of multimodal systems have been discussed. In figure 4 a multibiometric login system is shown. It combines three biometric traits of a person (face, hand geometry and fingerprint). In this system fusion is performed at the match score level. Integration strategies adopted depends upon the fusion level. Fusion at the match score level has been well studied in the literature [23][24][25]. Robust and efficient normalization techniques are necessary to transform the scores of multiple matchers into a common domain prior to consolidating them [26]. Ross and Jain have shown [27] that simple sum rule can be used effectively to enhance performance of the multimodal biometric system shown below in figure. Figure shows the ROC curve depicting the performance gain when simple sum rule is used to combine the matching scores of face, fingerprint and hand geometry.



(a) (b)

Figure 4: (a) A Multimodal Biometric Login System (b) Performance Gain using the Sum Rule Combining the Three (Face, Fingerprint, Hand Geometry) Modalities [2].

5. FACTORS AFFECTING DESIGN OF MULTIMODAL SYSTEMS

A variety of factors should be considered when designing a multimodal biometric system.

They include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple biometric sources should be integrated; the methodology adopted to integrate the information; and the cost versus matching performance trade-off [21]. They are more expensive and require more storage space and computation methods than unimodal systems. They generally require more time for enrollment and recognition causing some inconvenience to the user. Finally, if a proper integrating technique is not used to consolidate the multiple evidences, the system performance can degrade [28].

6. CONCLUSION

Multimodal biometric systems are expected to play a vital role in establishing identity in the coming years. They improve the matching accuracy of a biometric system while

increasing population coverage, reducing the failure to enroll/failure to capture rates and providing resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources. Integration at the match score level is generally preferred due to the presence of sufficient information content and the ease in accessing and combining matching scores. Mere using multiple biometrics does not imply better system performance rather degrade the performance of individual modalities when used in poorly designed system.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, 14 pp. 4-20, Jan 2004.

[2] Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview, Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO)", (Vienna, Austria), pp. 1221-1224, September 2004.

[3] Arun Ross, "An Introduction to Multibiometrics", EUSIPCO, 2007.

[4] A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multibiometrics", New York: Springer, 2006.

[5] Arun Ross and Anil K. Jain, "Biometric Sensor Interoperability: A Case Study in Fingerprints", In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW), LNCS 3087, Springer, 2004.

[6] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, 1, No. 2, June 2006.

[7] A. Kong, J. Heo, B. Abidi, J. Paik, and M. Abidi., "Recent Advances in Visual and Infrared Face Recognition - A Review", Computer Vision and Image Understanding, 97(1): pp. 103-135, January 2005.

[8] X. Chen, P. J. Flynn, and K. W. Bowyer., "IR and Visible Light Face Recognition", Computer Vision and Image Understanding, 99(3): pp. 332-358, September 2005.

[9] D. A. Socolinsky, A. Selinger, and J. D. Neuheisel., "Face Recognition with Visible and Thermal Infrared Imagery", Computer Vision and Image Understanding, 91(1-2): pp. 72-114, July-August 2003.

[10] R. K. Rowe and K. A. Nixon., "Fingerprint Enhancement Using a Multispectral Sensor", In Proceedings of SPIE Conference on Biometric Technology for Human Identification II, 5779, pp. 81-93, March 2005.

[11] X. Lu, Y. Wang, and A. K. Jain., "Combining Classifiers for Face Recognition", In IEEE International Conference on Multimedia and Expo (ICME), 3, pp. 13-16, Baltimore, USA, July 2003.

[12] A. Ross, A. K. Jain, and J. Reisman., "A Hybrid Fingerprint Matcher", Pattern Recognition, 36(7): pp. 1661-1673, July 2003.

[13] J. Jang, K. R. Park, J. Son, and Y. Lee., "Multi-Unit Iris Recognition System by Image Check Algorithm", In Proceedings of International Conference on Biometric Authentication (ICBA), pp. 450-457, Hong Kong, July 2004.

[14] A. O'Toole, H. Bulthoff, N. Troje, and T. Vetter., "Face Recognition across Large Viewpoint Changes", In Proceedings of the International Workshop on Automatic Face- and Gesture-Recognition (IWAFGR), pp. 326-331, Zurich, Switzerland, June 1995.

[15] R. Brunelli and D. Falavigna, "Person Identification using Multiple Cues," IEEE Transactions on PAMI, 12, pp. 955-966, Oct 1995.

[16] C. Sanderson and K. K. Paliwal., "Information Fusion and Person Verification Using Speech and Face Information", Research Paper IDIAP-RR 02-33, IDIAP, September 2002.

[17] G. L. Marcialis and F. Roli., "Fingerprint Verification by Fusion of Optical and Capacitive Sensors", Pattern Recognition Letters, 25(11): pp. 1315-1322, August 2004.

[18] A. Ross and R. Govindarajan., "Feature Level Fusion Using Hand and Face Biometrics", In Proceedings of SPIE Conference on Biometric Technology for Human Identification II, 5779, pp. 196–204, Orlando, USA, March 2005.

[19] A. K. Jain, S. Prabhakar, and S. Chen, "Combining Multiple Matchers for a High Security Fingerprint Verification System", Pattern Recognition Letters, 20, pp. 1371-1379, 1999.

[20] 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, Jul. 20-22, 2005, pp. 1049–1058.

[21] A. K. Jain and A. Ross., "Multibiometric Systems", Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1): pp. 34-40, January 2004.

[22] S. Prabhakar and A. K. Jain, "Decision-Level Fusion in Fingerprint Verification", Pattern Recognition, 35, No. 4, pp. 861-874, 2002.

[23] Jain, A.K., Hong, L., Kulkarni, Y., 1999d., "A Multimodal Biometric System using Fingerprint, Face and Speech", In: Second Internat. Conf. on AVBPA, Washington, DC, USA. pp. 182-187.

[24] L. Hong and A. K. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on PAMI, 20, pp. 1295-1307, Dec 1998.

[25] R. W. Frischholz and U. Dieckmann, "Bioid: A Multimodal Biometric Identification System", IEEE Computer, 33, No. 2, pp. 64-68, 2000.

[26] A. K. Jain, K. Nandakumar, and A. Ross., "Score Normalization in Multimodal Biometric Systems", Pattern Recognition, 38(12): pp. 2270-2285, December 2005.

[27] A. Ross and A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, 24, pp. 2115-2125, Sep 2003.

[28] L. Hong, A. K. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?", In Proc. AutoID, Summit, NJ, Oct. 1999, pp. 59-64.