Appeared in Proc. of 3rd Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), pp. 354-359, Sweden, June 6-8, 2001.

Information Fusion in Biometrics

Arun Ross[1], Anil Jain[1] and Jian-Zhong Qian[2]

[1] Michigan State University, East Lansing, MI, USA 48824
{rossarun,jain}@cse.msu.edu
[2] Siemens Corporate Research, Princeton, NJ, USA 08540
qian@scr.siemens.com

Abstract. User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multimodal biometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. These systems also help achieve an increase in performance that may not be possible by using a single biometric indicator. This paper addresses the problem of *information fusion* in verification systems. Experimental results on combining three biometric modalities (face, fingerprint and hand geometry) are also presented.

1 Introduction

The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant confidence score (or matching score) computed by the matching module may not be reliable. Simply put, the matching score generated by a noisy input has a large variance. This problem can be alleviated by installing multiple sensors that capture different biometric traits. Such systems, known as *multimodal biometric systems* [1], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are able to meet the stringent performance requirements imposed by various applications. Moreover, it will be extremely difficult for an intruder to violate the integrity of a system requiring multiple biometric indicators. However, an integration scheme is required to fuse the information churned out by the individual modalities. In this work we address the problem of *information fusion* by first building a multimodal biometric system and then devising various schemes to integrate these modalities. The proposed system uses the fingerprint, face, and hand geometry features of an individual for verification purposes.

2 Fusion in Biometrics

Figure 1 illustrates the various levels of fusion that are possible when combining multiple biometric systems: (a) fusion at the feature extraction level, where features extracted using mutiple sensors are concatenated, (b) fusion at the confidence level, where matching scores reported by multiple matchers are combined [2], and (c) fusion at the abstract level, where the accept/reject decisions of multiple systems are consolidated [3].

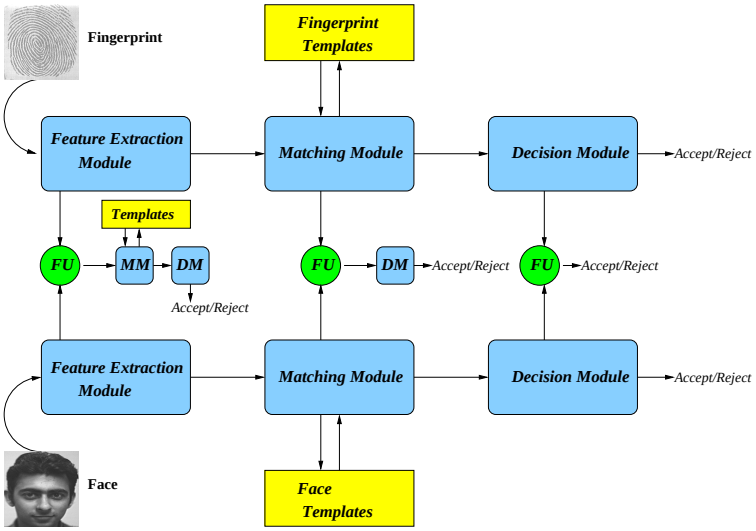


Fig. 1. A bimodal biometric system showing the three levels of fusion; FU: Fusion Module, MM: Matching Module, DM: Decision Module.

Fusion in the context of biometrics can take the following forms: (i) Single biometric multiple classifier fusion, where multiple classifiers on a single biometric indicator are combined [4]. (ii) Single biometric multiple matcher fusion, where scores generated by multiple matching strategies (on the same representation) are combined [2]. (iii) Multiple biometric fusion, where multiple biometrics are utilized [5], [6], [7].

An important aspect that has to be dealt with is the normalization of the scores obtained from the different domain experts [8]. Normalization typically involves mapping the scores obtained from multiple domains into a common framework before combining them. This could be viewed as a two-step process in which the distributions of scores for each domain is first estimated using robust statistical techniques and these distributions are then scaled or translated into a common domain.

3 Experiments

A brief description of the three biometric indicators used in our multimodal verification system is given below. Our experiments deal with combining information at the representation and confidence levels, and not at the abstract level. There is very little information available at the abstract level, and a simple voting scheme would be expected to do well at this level [3].

(a) Face Image (b) Fingerprint Image (c) Hand Image

Fig. 2. The three biometric indicators used in our experiments.

1. Face Verification:
   Grayscale images of a subject's face were obtained using a Panasonic video camera. The eigenface approach was used to extract features from the face image [9]. In this approach a set of orthonormal vectors (or images) that span a lower dimensional subspace is first computed using the principal component analysis (PCA) technique. The feature vector of a face image is the projection of the (original face) image on the (reduced) eigenspace. Matching involves computing the Euclidean distance between the coefficients of the eigenface in the template and the eigenface for the detected face.
2. Fingerprint Verification:
   Fingerprint images were acquired using a Digital Biometrics sensor at a resolution of 500 dpi. The features correspond to the position and orientation of certain critical points, known as minutiae, that are present in every fingerprint. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template [11].
3. Hand Geometry Verification:
   Images of a subject's right hand were captured using a Pulnix TMC-7EX camera. The feature extraction system computes 14 feature values comprising of the lengths of the fingers, widths of the fingers and widths of the palm at various locations of the hand [10]. The Euclidean distance metric was used to compare feature vectors, and generate a matching score.

The database for our experiments consisted of matching scores obtained from the face, fingerprint and hand geometry systems. However, data pertaining to

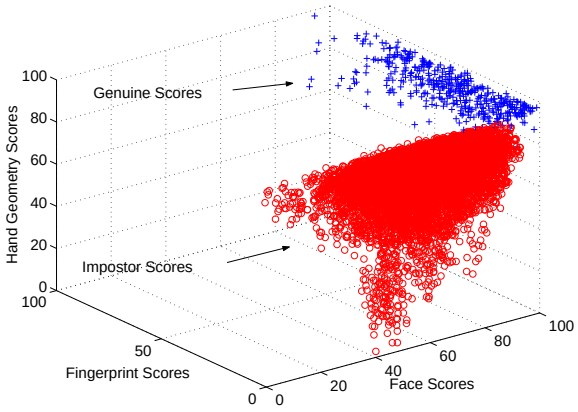
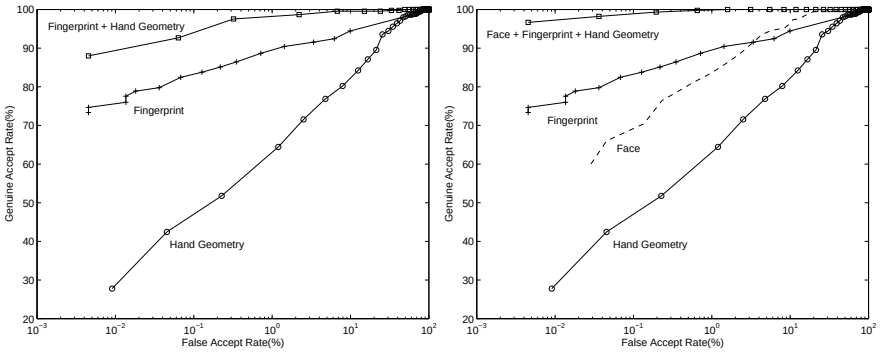


Fig. 3. Scatter Plot showing the genuine and impostor scores. The points correspond to 450 genuine scores (+) and 11,025 impostor scores (o).

all three modalities were not available for a single set of users. The mutual independence of these three biometric indicators allows us to collect the biometric data individually and then augment them. The fingerprint and face data were obtained from user set I consisting of 50 users. Each user was asked to provide 9 face images and 9 fingerprint impressions (of the same finger). The hand geometry data was collected separately from user set II also consisting of 50 users (some users from set I were present in set II). Each user in set I was randomly paired with a user in set II. 450 genuine scores and 22,050 impostor scores were generated for each of the three modalities. All scores were mapped to the range $[0, 100]$. A score vector - (x_1, x_2, x_3) - represents the scores of multiple matchers, with x_1, x_2 and x_3 corresponding to the scores obtained from the 3 modalities. The three-dimensional scatter plot of the genuine and impostor scores is shown in Figure 3. The plot indicates that the two distributions are reasonably well separated in 3-dimensional space; therefore, a relatively simple classifier should perform well on this dataset.

1. **Sum Rule:**
   The sum rule method of integration takes the weighted average of the individual score values. This strategy was applied to all possible combinations of the three modalities. Equal weights were assigned to each modality as the bias of each matcher was not available. Figure 4(a) shows the performance of the sum rule using only two modalities, and Figure 4(b) shows the performance using all three modalities.
2. **Decision Tree:**
   The $C5.0$ program was used to generate a decision tree from the training set of genuine and impostor score vectors. The training set consisted of 11,025 impostor score vectors and 225 genuine score vectors. The test set consisted of the same number of independent impostor and genuine score vectors. Table 1(a) shows the performance of the $C5.0$ decision tree on one such test set.



(a) (b)

Fig. 4. ROC curves using the sum rule: (a) Combining fingerprint and hand geometry scores, (b) Combining fingerprint, face and hand geometry scores.

3. **Linear Discriminant Function:**
   Linear discriminant analysis of the training set helps in transforming the 3-dimensional score vectors into a new subspace that maximizes the between-class separation. The test set vectors are classified by using the minimum Mahalanobis distance rule (with the assumption that the two classes have unequal covariance matrices). Table 1(b) shows the confusion matrix resulting from using this quadratic decision rule on the test set.

	Genuine	Impostor
Genuine	203	22
Impostor	4	11,021

(a) $C5.0$ Decision Tree.

	Genuine	Impostor
Genuine	225	0
Impostor	72	10,953

(b) Linear Discriminant classifier.

Table 1. Confusion matrices showing the performance of the (a) $C5.0$ Decision Tree, and (b) Linear Discriminant classifier, on an independent test set.

The experimental results show that the sum rule performs better than the decision tree and linear discriminant classifiers. The FAR of the tree classifier is 0.036% (±0.03%) and the FRR is 9.63% (±0.03%). The FAR of the linear discriminant classifier is 0.47% (±0.3%) and it's FRR is 0.00%. The low FRR value in this case is a consequence of overfitting the genuine class which has fewer samples in both test and training sets. The sum rule that combines all three scores has a corresponding FAR of 0.03% and a FRR of 1.78% suggesting better performance than the other two classifiers. It has to be noted that it is not possible to fix the FRR (and then compute the FAR) in the case of the decision tree and linear discriminant classifiers.

We also investigated the integration of multiple biometric modalities at the representation level. The face and fingerprint feature vectors were augmented to create a higher dimensional feature vector. A texture-based feature set, as opposed to a minutiae-based set, was used to represent fingerprints in this case [12]. The normalized feature vector was used to represent the identity of a person. Initial experiments show that this augmented feature vector performs better than combining scores at the confidence level (sum rule). We are conducting more extensive experiments to examine fusion at the representation level.

4 Conclusion

This paper provides initial results obtained on a multimodal biometric system that uses face, fingerprint and hand geometry features for verification. All the three fusion schemes (at the confidence level) considered here provide better verification performance than the individual biometrics. It would be instructive to study other datasets involving a larger number of users with additional biometric indicators. Towards this end, we are in the process of collecting data corresponding to four biometric indicators - fingerprint, face, voice and hand geometry - from a larger number of users.

References

1. L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," in *Proceedings AutoID'99*, (Summit(NJ), USA), pp. 59–64, Oct 1999.
2. A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for a high security fingerprint verification system," *Pattern Recognition Letters*, vol. 20, pp. 1371–1379, 1999.
3. 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, Aug 1996.
4. R. Cappelli, D. Maio, and D. Maltoni, "Combining fingerprint classifiers," in *First International Workshop on Multiple Classifier Systems*, pp. 351–361, Jun 2000.
5. J. Kittler, M. Hatef, R. P. Duin, and J. G. Matas, "On combining classifiers," *IEEE Transactions on PAMI*, pp. 226–239, Mar 1998.
6. E. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using bayesian statistics," in *First International Conference on AVBPA*, (Crans-Montana, Switzerland), pp. 291–300, Mar 1997.
7. S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of face and speech data for person identity verification," Research Paper IDIAP-RR 99-03, IDIAP, CP 592, 1920 Martigny, Switzerland, Jan 1999.
8. R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Transactions on PAMI*, vol. 12, pp. 955–966, Oct 1995.
9. M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.
10. A. K. Jain, A. Ross, and S. Pankanti, "A prototype hand geometry-based verification system," in *Second International Conference on Audio and Video-based Biometric Person Authentication*, (Washington, D.C., USA), pp. 166–171, Mar 1999.
11. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints," in *Proceedings of the IEEE*, vol. 85, pp. 1365–1388, 1997.
12. A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features," to appear in the *Proceedings of ICIP 2001*, (Greece), Oct 2001.