(Appeared in Pattern Recognition Letters, Vol. 24, Issue 13, pp. 2115-2125, September, 2003)

Information Fusion in Biometrics

Arun Ross and Anil Jain *

Department of Computer Science and Engineering,
Michigan State University,
East Lansing, MI, USA 48824

Abstract

User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, non-universality of the biometric trait 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. Multibiometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. These systems help achieve an increase in performance that may not be possible using a single biometric indicator. Further, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. However, an effective fusion scheme is necessary to combine the information presented by multiple domain experts. This paper addresses the problem of *information fusion* in biometric verification systems by combining information at the matching score level. Experimental results on combining three biometric modalities (face, fingerprint and hand geometry) are presented.

Key words: Biometrics, Multimodal, Fingerprints, Face, Hand geometry, Verification, Decision tree, Linear discriminant analysis, Sum rule

1 Introduction

A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. Examples of such appli-

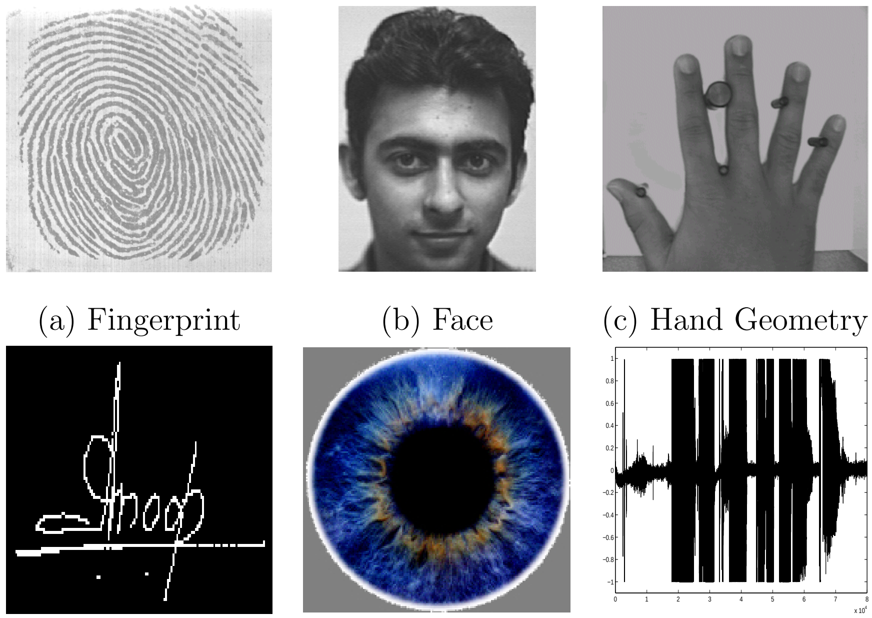
* Corresponding author. Tel: +1-517-355-9319; Fax: +1-517-432-1061
Email addresses: rossarun@cse.msu.edu (Arun Ross), jain@cse.msu.edu (Anil Jain).

cations include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust verification schemes, these systems are vulnerable to the wiles of an impostor. Credit card fraud for example, costs the industry millions of dollars annually, primarily due to the lack of effective customer verification techniques [1].

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to applications. However, security can be easily breached in these applications when a password is divulged to an unauthorized user or a badge is stolen by an impostor. The emergence of *biometrics* has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person (Figure 1). Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature or voiceprint to verify a person's identity [2]. They have an edge over traditional security methods in that they cannot be easily stolen or shared.

A simple biometric system has a sensor module, a feature extraction module and a matching module. 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 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 addressed by installing multiple sensors that capture different biometric traits. Such systems, known as *multimodal biometric systems* [3], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications [4]. Multimodal systems address the problem of non-universality: it is possible for a subset of users to not possess a particular biometric. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a 'live' user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities.

In this paper we deal with 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.



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

(d) Signature (e) Iris (f) Voice

Fig. 1. Examples of some of the biometric traits associated with an individual.

2 A Biometric System

A biometric-based authentication system operates in two modes:

(1) Enrollment Mode: In the enrollment mode a user's biometric data is acquired using a biometric reader and stored in a database. The stored template is labeled with a user identity (e.g., name, identification number, etc.) to facilitate authentication.
(2) Authentication Mode: In the authentication mode, a user's biometric data is once again acquired and the system uses this to either *identify* who the user is, or *verify* the claimed identity of the user. While *identification* involves comparing the acquired biometric information against templates corresponding to all users in the database, *verification* involves comparison with only those templates corresponding to the claimed identity. Thus, identification and verification are two distinct problems having their own inherent complexities.

A simple biometric system has four important components:

(1) *Sensor module* which acquires the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a

user.

(2) *Feature extraction module* in which the acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint image would be extracted in the feature extraction module of a fingerprint system.
(3) *Matching module* in which the feature values are compared against those in the template by generating a matching score . For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.
(4) *Decision-making Module* in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module.

The performance of a biometric system can be measured by reporting its False Accept Rate (FAR) and False Reject Rate (FRR) at various thresholds. These two factors are brought together in a Receiver Operating Characteristic (ROC) curve that plots the FRR against the FAR at different thresholds. (Alternately, the genuine accept rate, which equals 1-FRR, may be plotted against the FAR). The FAR and FRR are computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match. A genuine matching score is obtained when two feature vectors corresponding to the *same* individual are compared, and an impostor matching score is obtained when feature vectors from two *different* individuals are compared.

3 Fusion in Biometrics

The layout of a bimodal system is shown in Figure 2. The purpose of this diagram is to illustrate the various levels of fusion for combining two (or more) biometric systems. The three possible levels of fusion are: (a) fusion at the feature extraction level, (b) fusion at the matching score level, (c) fusion at the decision level.

(1) Fusion at the feature extraction level: The data obtained from each sensor is used to compute a feature vector. As the features extracted from one biometric trait are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniques may be employed to extract useful features from the larger set of features.
(2) Fusion at the matching score level: Each system provides a matching score indicating the proximity of the feature vector with the template vector.

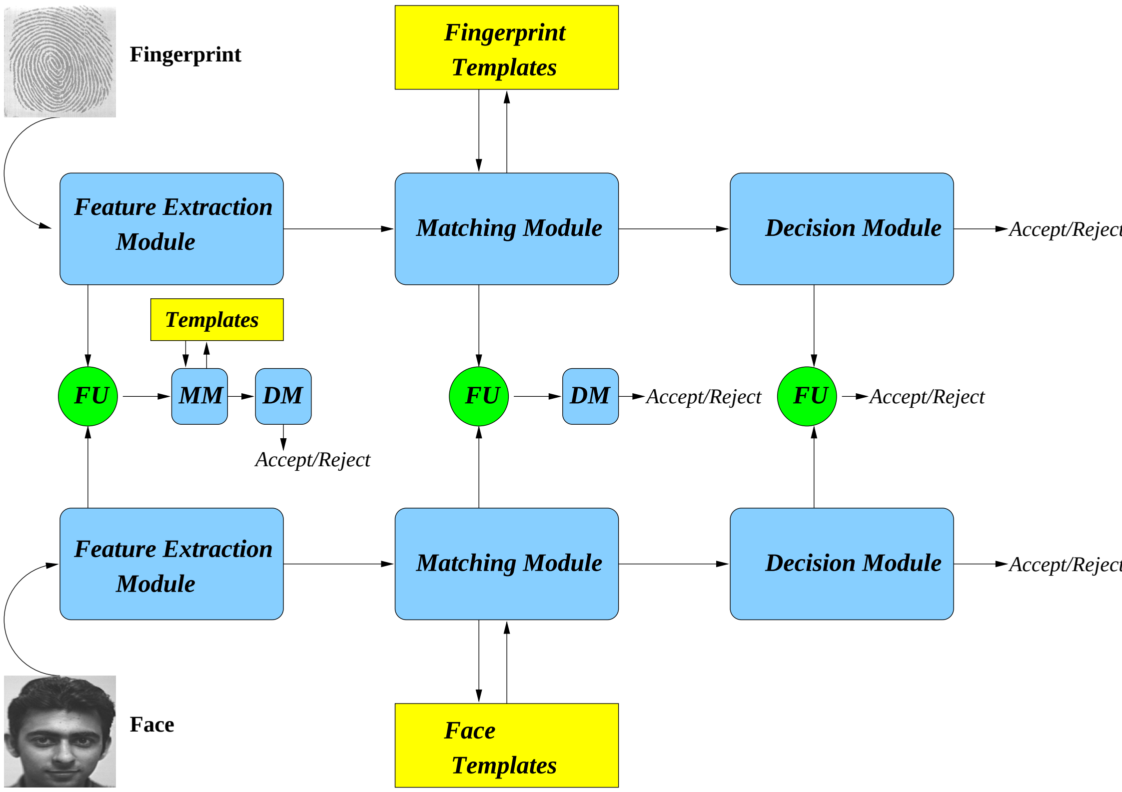


Fig. 2. A bimodal biometric system showing the three levels of fusion; FU: Fusion Module, MM: Matching Module, DM: Decision Module.

These scores can be combined to assert the veracity of the claimed identity. Techniques such as 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 [5].

(3) Fusion at the decision level: Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes - accept or reject. A majority vote scheme, such as that employed in [6] can be used to make the final decision.

Fusion in the context of biometrics can take the following forms:

(1) Single biometric multiple representation.
(2) Single biometric multiple matchers.
(3) Multiple biometric fusion.

3.1 Single Biometric Multiple Representation

This type of fusion involves using multiple representations on a single biometric indicator. Typically, each representation has its own classifier. The similarity scores reported by these classifiers are then consolidated. Cappelli et al. [7]

describe a fingerprint *classification* system [1] that combines a structural classifier with a KL transform-based classifier by integrating the scores generated by the two classifiers. This is done by first mapping the scores (which are distance measures) into a common domain via a double sigmoid function and then taking a weighted average in the new domain. Jain et al. [8] also use multiple classifiers for fingerprint indexing. Their technique uses a K nearest neighbor classifier and a set of 10 neural network classifiers to classify fingerprints. General strategies for combining multiple classifiers have been suggested in [9]. All the approaches presented there (the highest rank method, the Borda count method and logistic regression) attempt to reduce or rerank a given set of classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present.

The fusion in this approach takes place at the matching stage, after the classifiers report a similarity score for each class. Prabhakar and Jain [10] show that selecting classifiers based on some "goodness" statistic may be necessary to avoid performance degradation when using classifier combination techniques. It should also be possible to combine (concatenate) the feature vectors extracted by the individual classifiers.

3.2 Single Biometric Multiple Matchers

It is also possible to incorporate multiple matching strategies in the matching module of a biometric system and combine the scores generated by these strategies. Jain et al. [5] use the logistic function to map the matching scores obtained from two different fingerprint matching algorithms into a single score. The authors demonstrate that such an integration strategy improves the overall performance of a fingerprint verification system.

This type of fusion also takes place at the matching stage of a biometric system. Although there are multiple matchers in this case, all matchers operate on the same representation of the biometric data.

3.3 Multiple Biometric Fusion

Multibiometric fusion refers to the fusion of multiple biometric indicators. Such systems seek to improve the speed and reliability (accuracy) of a biometric system [4] by integrating matching scores obtained from multiple biometric

[1] The system classifies a fingerprint into one of five classes - Arch, Left loop, Right loop, Whorl and Tented arch. Thus it is not a biometric system by itself, as it does not perform person identification or verification.

sources. A variety of fusion schemes have been described in the literature to combine these various scores. These include majority voting, sum and product rules, k-NN classifiers, SVMs, decision trees, Bayesian methods, etc. (see for example [11–16]).

An important aspect that has to be addressed in fusion at the matching score level is the normalization of the scores obtained from the different domain experts [17]. Normalization typically involves mapping the scores obtained from multiple domains into a common domain 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 [18] and these distributions are then scaled or translated into a common domain.

Besides the techniques described above, other types of fusion are also possible in biometrics. (i) A fingerprint biometric system may store multiple templates of a user's fingerprint (same finger) in its database. When a fingerprint impression is presented to the system for verification, it is compared against each of the templates, and the matching score generated by these multiple matchings are integrated. (ii) A system may store a single template of a user's finger, but acquire multiple impressions of the finger during verification. (iii) Another possibility would be to acquire and use impressions of multiple fingers for every user. These possibilities have been discussed in [19].

4 Experiments

A brief description of the three biometric indicators used in our experiments is given below.

4.1 Face Verification

Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in the database. The feature extraction process is often preceded by a face detection process during which the location and spatial extent of the face is determined within the given image. This is a difficult process given the high degree of variability associated with human faces (color, texture, expression, pose, etc.). The problem is further compounded by the presence of complex backgrounds and variable lighting conditions (Figure 3). A variety of techniques have been described in the literature to locate the spatial coordinates of a face within an image [20–22]. Once the boundary of the face is established, we use the eigenface approach to extract features from the face [23,24]. 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 eigenface coefficients of the template and the detected face.

Fig. 3. The problem of face detection is compounded by the effects of complex lighting and cluttered background.

4.2 Fingerprint Verification

A fingerprint refers to the flowing pattern of ridges and furrows located on the tip of a finger. Traditionally, these patterns have been extracted by creating an inked impression of the fingertip on paper. But the electronic era has ushered in a range of compact sensors that provide digital images of these patterns (Figure 4). In real-time verification systems, the images acquired by these sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points (ridge endings and ridge bifurcations) that are present in every fingerprint (Figure 5). The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. For this experiment, the techniques described in [25] were used in the feature extraction and matching stages of the fingerprint verification system.

4.3 Hand Geometry

Hand geometry, as the name suggests, refers to the geometric structure of the hand. This structure includes width of the fingers at various locations, width of the palm, thickness of the palm, length of the fingers, etc. Although these metrics do not vary significantly across the population, they can nevertheless be used to verify the identity of an individual. Hand geometry measurement is non-intrusive and the verification involves a simple processing of the resulting

Fig. 4. A compact solid-state sensor and a sample fingerprint acquired by the sensor. The sensor is about the size of a postage stamp.

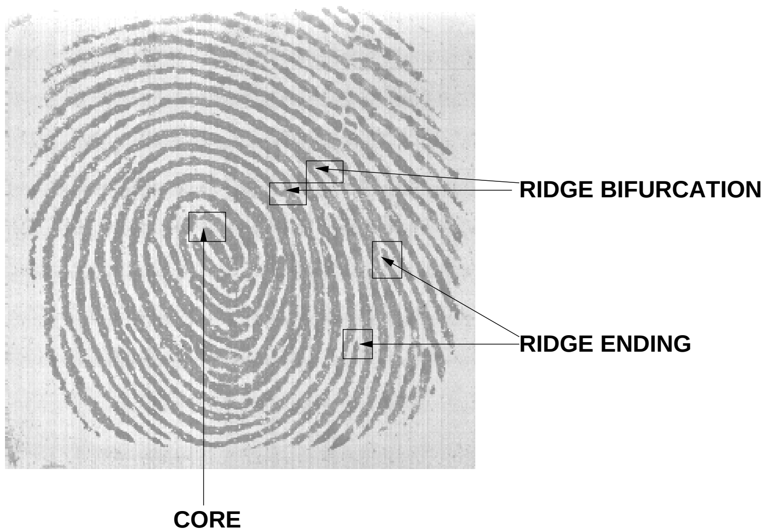
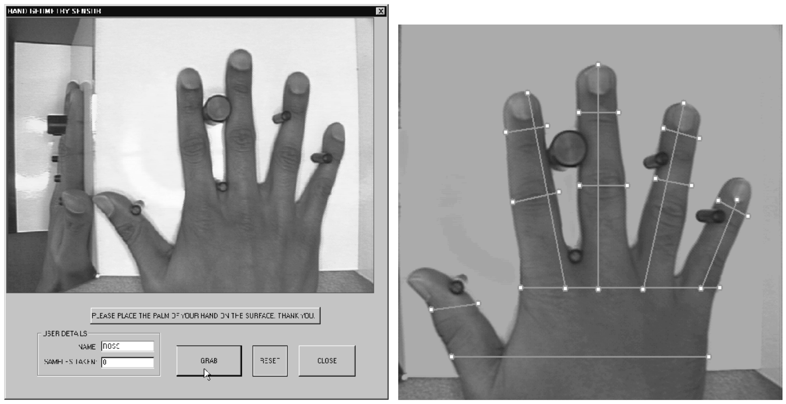


Fig. 5. A fingerprint image with the core and four minutiae points labeled.

features. Figure 6 shows the hand geometry system that was used in our experiments. The system computes 14 feature values comprising of the lengths of the fingers, widths of the fingers and widths of the palm at various locations [26].

4.4 Combining the three modalities

The database for our experiments consisted of matching scores obtained from three different modalities - face, fingerprint and hand geometry. However, data



(a) GUI for capturing hand geometry. The five pegs aid in proper placement of the hand on the platen.

(b) 14 hand features corresponding to various length and width measurements.

Fig. 6. A Hand Geometry System. The sensor provides both the top and side views of the subject's hand. Features are extracted using the image of the top-view only.

pertaining to all three modalities were not available for a single set of users. The mutual non-dependence of the biometric indicators allows us to assign the biometric data of one user to another.

The database itself was constructed as follows: The fingerprint and face data were obtained from user set I consisting of 50 users. Each user was asked to provide five face images and five fingerprint impressions (of the same finger). This data was used to generate 500 (50×10) genuine scores and $12,250$ ($50 \times 5 \times 49$ - each feature set of a user was compared against one feature set each of all other users) impostor scores for each modality. The hand geometry data was collected separately from user set II also consisting of 50 users [2]. This resulted in 500 genuine scores and $12,250$ impostor scores for this modality also. Each user in set I was randomly paired with a user in set II. Thus corresponding genuine and impostor scores for all three modalities were available for testing. All scores were mapped to the range $[0, 100]$. Since the face and hand scores were not similarity scores (they were distance scores), they were converted to similarity scores by simply subtracting them from 100. A similarity score x represents the proximity of two feature sets as computed by a classifier. A *score vector* represents the scores of multiple classifiers. Thus, the vector (x_1, x_2, x_3) is a score vector, where x_1, x_2 and x_3 correspond to the (similarity) scores obtained from the classifers corresponding to the face, fingerprint and hand geometry systems, respectively.

[2] Some users from set I were present in set II.

The scatter plot of the genuine and impostor scores is shown in Figure 7. The plot indicates that the two classes are reasonably separated in 3-dimensional space; therefore, a relatively simple classifier should perform well on this dataset. The ROC curves depicting the performance of the individual modalities are shown in Figure 8.

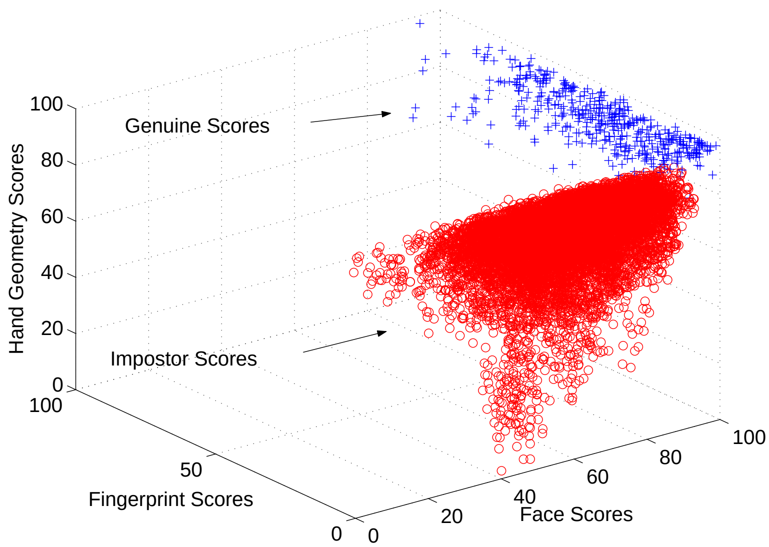


Fig. 7. Scatter Plot showing the genuine and impostor scores in 3-D space. The points correspond to 500 genuine scores (+) and 12, 250 impostor scores (o).

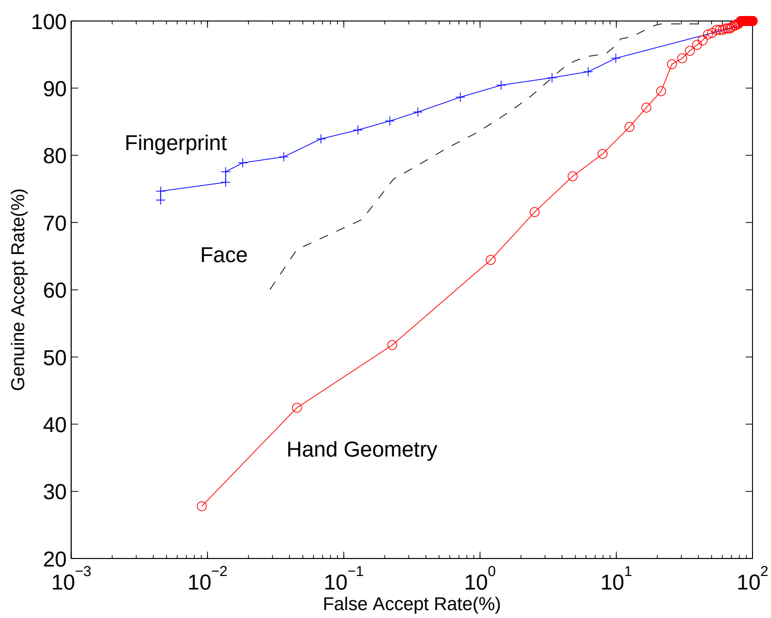
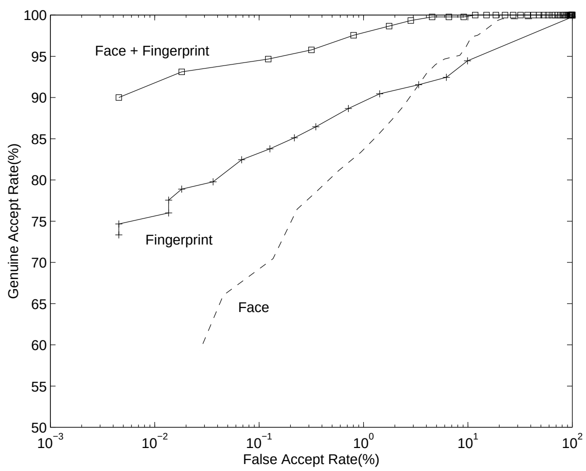


Fig. 8. ROC curves showing the performance of each of the three individual modalities.

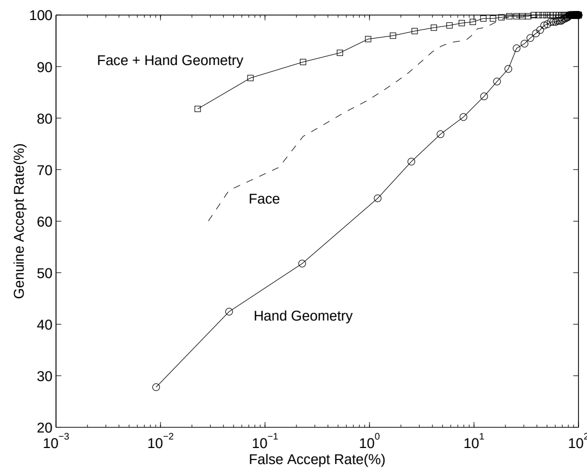
4.4.1 Sum Rule

The simplest form of combination would be to take the weighted average of the scores from the multiple modalities. This strategy was applied to all possible combinations of the three modalities. Equal weights were assigned to each modality as the bias of each classifier was not computed. Figure 9 and Figure 10 show the performance of the sum rule on the three modalities.



(a) Combining face and fingerprint scores

Threshold	Genuine Accept Rate(%)	False Accept Rate(%)
38	100.00	11.75
41	99.77	4.54
42	99.33	2.83
43	98.66	1.75
44	97.55	0.80
45	95.77	0.31
46	94.66	0.12
47	93.11	0.01
49	87.55	0.00



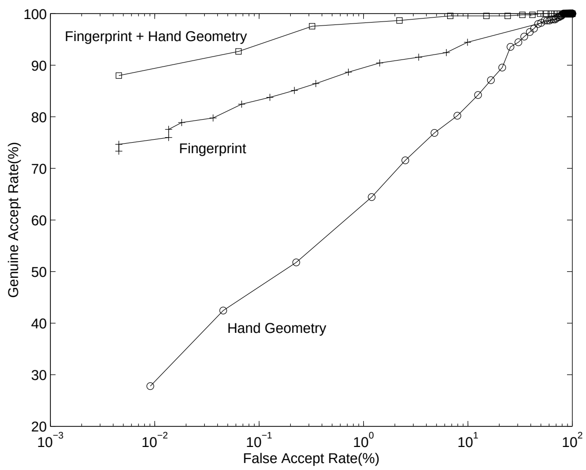
(b) Combining face and hand geometry scores

Threshold	Genuine Accept Rate(%)	False Accept Rate(%)
72	100.00	37.31
79	99.33	12.28
82	98.00	5.83
83	97.55	4.13
86	95.33	0.97
87	92.66	0.52
88	90.88	0.23
90	81.77	0.02
91	76.22	0.00

Fig. 9. ROC curves showing an improvement in performance when scores are combined using the sum rule.

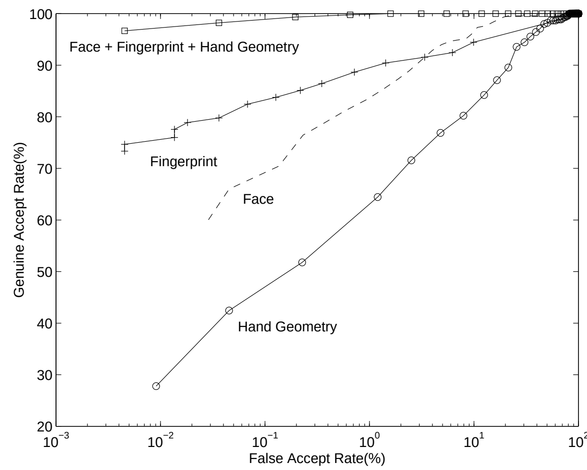
4.4.2 Decision Trees

A decision tree derives a sequence of *if-then-else* rules using the training set in order to assign a class label to the input data. It does this by finding out an attribute (feature) that maximizes information gain at a particular node. The $C5.0$ program [27] was used to generate a tree from the training set



(a) Combining fingerprint and hand geometry scores

Threshold	Genuine Accept Rate(%)	False Accept Rate(%)
41	100.00	49.19
43	99.77	33.28
46	99.55	6.77
47	98.66	2.20
48	97.55	0.32
51	84.00	0.00



(b) Combining face, fingerprint and hand geometry scores

Threshold	Genuine Accept Rate(%)	False Accept Rate(%)
57	100.00	1.59
58	99.77	0.65
59	99.33	0.19
60	98.22	0.03
62	95.55	0.00

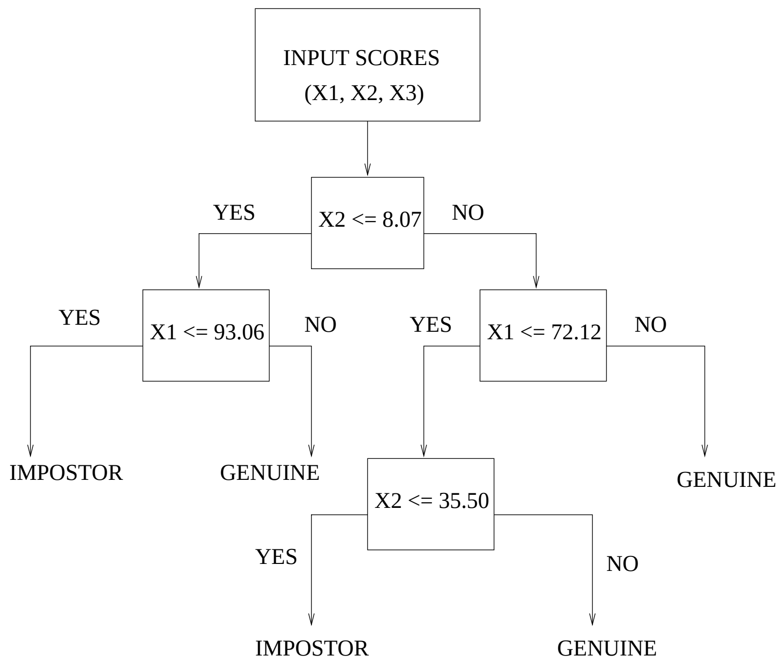
Fig. 10. ROC curves showing an improvement in performance when scores are combined using the sum rule.

of genuine and impostor score vectors. The training set consisted of $11,125$ impostor score vectors and 250 genuine score vectors. The test set consisted of the same number of impostor and genuine score vectors. Cross-validation was done by considering 10 such partitions of the training and test sets. Figure 11 shows the construction and performance of the $C5.0$ decision tree on one such training and test set.

4.4.3 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. Figure 12 shows the plot of the score vectors using the first and the second discriminant variables.

The test set vectors are classified by using the minimum Mahalanobis distance rule (after first calculating the centroids of the two classes in the new feature



Evaluation on training data :

	Genuine	Impostor
Genuine Class	239	11
Impostor Class	2	11,123

Evaluation on test data :

	Genuine	Impostor
Genuine Class	226	24
Impostor Class	4	11,121

Fig. 11. Construction and Performance of the $C5.0$ Decision Tree on one specific partition of the training and test sets. The performance is indicated by confusion matrices.

space, and then measuring the Mahalanobis distance). We assume that the two classes have unequal covariance matrices. Table 1 shows the confusion matrices resulting from using this rule on different partitioning of the data into training and test sets.

4.4.4 Discussion

The experiments described above suggest that the sum rule performs better than the decision tree and linear discriminant classifiers. The FAR of the tree classifier is 0.036% ($\pm$0.03%) and the FRR is 9.63% ($\pm$0.03%). The FAR of

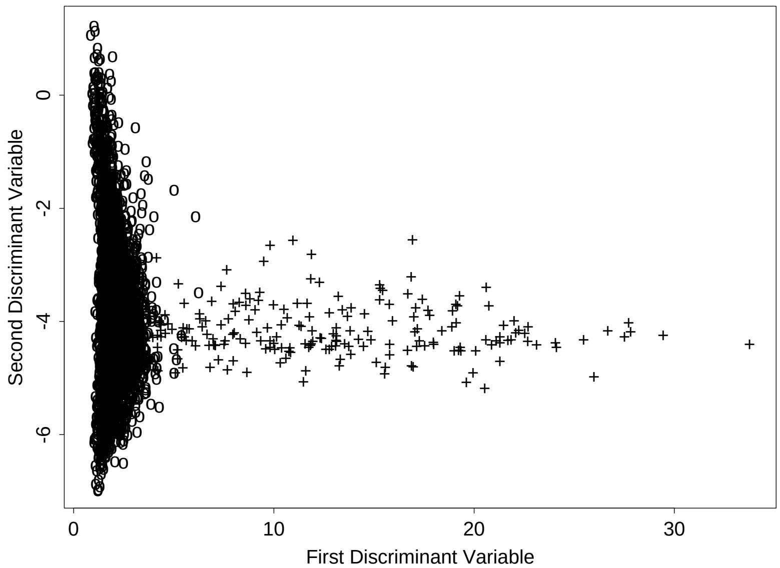


Fig. 12. Linear Discriminant Analysis of the score vectors. The score vectors have been plotted in a 2-dimensional space representing the first and the second discriminant variables. There are 250 genuine score vectors(+) and $11,125$ impostor score vectors (o).

Trial 1:

	Genuine	Impostor
Genuine Class	250	0
Impostor Class	54	$11,071$

Trial 2:

	Genuine	Impostor
Genuine Class	250	0
Impostor Class	50	$11,075$

Trial 3:

	Genuine	Impostor
Genuine Class	250	0
Impostor Class	72	$11,053$

Table 1
Performance of the linear discriminant classifier on three different trials as indicated by the confusion matrices. In each trial the training and test sets were partitioned differently.

the linear discriminant classifier is 0.47% (±0.3%) and it's FRR is 0.00%. The FRR value in this case is a consequence of overfitting the genuine class as it has fewer samples in both the 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.

5 Conclusion and Future Work

This paper provides initial results obtained on a multimodal biometric system that uses face, fingerprint and hand geometry features for biometric verification purposes. Our experiments indicate that the sum rule performs better than the decision tree and linear discriminant classifiers. The benefits of multibiometrics may become even more evident in the case of a larger database of users. We are, therefore, in the process of collecting data corresponding to four biometric indicators - fingerprint, face, voice and hand geometry - from a larger user set (100).

Future experiments include developing user specific weights for the individual modalities. Different users tend to adopt differently to individual biometric indicators. For example, some users may find it easier to interact with a fingerprint sensor than with a hand image sensor. Consequently, their chances of being rejected by a stand-alone hand geometry biometric system may be high. Therefore, it would be appropriate to associate different weights to the individual modalities based on the user's preference or the system's performance for that user. These weights can be learnt over time by examining the stored template of the user, the query set provided by the user, and the matching scores for each of the individual modalities. By doing so, each user is tightly coupled with that subset of biometric traits that distinguishes her very well from the rest of the users. User specific weights also help address the problem of non-universality of biometric traits by giving less weightage to those traits that are not easily extracted. We are also working on designing techniques to automatically update the biometric templates of a user.

References

[1] P. Wallich, How to steal millions in chump change, Scientific American (Aug 1999).

[2] A. K. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

[3] L. Hong, A. K. Jain, S. Pankanti, Can multibiometrics improve performance?, in: Proceedings AutoID'99, Summit(NJ), USA, 1999, pp. 59–64.

[4] L. Hong, A. K. Jain, Integrating faces and fingerprints for personal identification, IEEE Transactions on PAMI 20 (12) (1998) 1295–1307.

[5] A. K. Jain, S. Prabhakar, S. Chen, Combining multiple matchers for a high security fingerprint verification system, Pattern Recognition Letters 20 (1999) 1371–1379.

[6] Y. Zuev, 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, 1996, pp. 206–210.

[7] R. Cappelli, D. Maio, D. Maltoni, Combining fingerprint classifiers, in: First International Workshop on Multiple Classifier Systems, 2000, pp. 351–361.

[8] A. K. Jain, S. Prabhakar, L. Hong, A multichannel approach to fingerprint classification, IEEE Transactions on PAMI 21 (4) (1999) 348–359.

[9] T. K. Ho, J. J. Hull, S. N. Srihari, Decision combination in multiple classifier systems, IEEE Transactions on PAMI 16 (1) (1994) 66–75.

[10] S. Prabhakar, A. K. Jain, Decision-level fusion in fingerprint verification, Pattern Recognition 35 (4) (2002) 861–874.

[11] U. Dieckmann, P. Plankensteiner, T. Wagner, Sesam: A biometric person identification system using sensor fusion, Pattern Recognition Letters 18 (9) (1997) 827–833.

[12] J. Kittler, M. Hatef, R. P. Duin, J. G. Matas, On combining classifiers, IEEE Transactions on PAMI 20 (3) (1998) 226–239.

[13] E. Bigun, J. Bigun, B. Duc, S. Fischer, Expert conciliation for multimodal person authentication systems using Bayesian Statistics, in: First International Conference on AVBPA, Crans-Montana, Switzerland, 1997, pp. 291–300.

[14] A. K. Jain, L. Hong, Y. Kulkarni, A multimodal biometric system using fingerprint, face and speech, in: Second International Conference on AVBPA, Washington D.C., USA, 1999, pp. 182–187.

[15] P. Verlinde, G. Cholet, Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application, in: Second International Conference on AVBPA, Washington D.C., USA, 1999, pp. 188–193.

[16] S. Ben-Yacoub, Y. Abdeljaoued, 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).

[17] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Transactions on PAMI 12 (10) (1995) 955–966.

[18] F. Hampel, P. Rousseeuw, E. Ronchetti, W. Stahel, Robust Statistics: The Approach Based on Influence Functions, John Wiley & Sons, 1986.

[19] A. K. Jain, S. Prabhakar, A. Ross, Fingerprint matching: Data acquisition and performance evaluation, Technical Report MSU-TR:99-14, Michigan State University (1999).

[20] H. Rowley, S. Baluja, T. Kanade, Neural network-based face detection, IEEE Transactions on PAMI 20 (1) (1998) 23–38.

[21] G. Burel, C. Carel, Detection and localization of faces on digital images, Pattern Recognition Letters 15 (1994) 963–967.

[22] G. Yang, T. Huang, Human face detection in a complex background, Pattern Recognition 27 (1) (1994) 53–63.

[23] M. Kirby, L. Sirovich, Application of the Karhunen-Loeve procedure for the characterization of human faces, IEEE Transactions on PAMI 12 (1) (1990) 103–108.

[24] M. Turk, A. Pentland, Eigenfaces for recognition, Journal of Cognitive Neuroscience 3 (1) (1991) 71–86.

[25] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, An identity authentication system using fingerprints, Proceedings of the IEEE 85 (9) (1997) 1365–1388.

[26] A. K. Jain, A. Ross, S. Pankanti, A prototype hand geometry-based verification system, in: Second International Conference on Audio and Video-based Biometric Person Authentication (AVBPA), Washington, D.C., USA, 1999, pp. 166–171.

[27] R. J. Quinlan, C4.5: Programs for Machine Learning, The Morgan Kaufmann Series in Machine Learning, Morgan Kaufmann Publishers, 1992.