Can Multibiometrics Improve Performance?

Lin Hong
Visionics Corp.
Jersey City, NJ 07302
lin@faceit.com

Anil Jain
Dept. of Comp. Science & Engg.
Michigan State University
East Lansing, MI 48823
jain@cse.msu.edu

Sharath Pankanti
IBM T J Watson Research Ctr
Yorktown Heights, NY 10598
sharat@watson.ibm.com

Abstract

While it is widely acknowledged that the performance improvement in current biometrics-based personal authentication systems is necessary, it is not clear what mechanisms could be used to improve the performance. In this paper, we formulate the problem of multiple biometrics integration and examine whether the improvement in performance could be achieved from integrating multiple biometrics. For two practical and commonly used situations of multibiometric integration, we analyze the performance gains. We also demonstrate empirically that integration of multiple biometrics does indeed result in a consistent and significant performance improvement.

1 Introduction

Biometrics deals with automatically identifying individuals based on their distinctive physiological or behavioral characteristics. It is widely acknowledged that only biometric identifiers come close to actually authenticating the person instead of their possessions (e.g., a passport) or their exclusive knowledge (e.g., passwords). Unlike the possession-based and knowledge-based identity authentication schemes, the biometric identifiers cannot be misplaced, forgotten, guessed, or be easily forged. Despite these inherent advantages of using biometrics-based personal authentication, their wide scale deployment has been hindered due to several reasons.

One of the primary limitations of the biometric identifiers is their less than desired accuracy performance in several application domains. Note that the presentation of a correct (incorrect) password in a password-based authentication system *always correctly* results in acceptance (denial) of an identity authentication claim. On the other hand, even if a legitimate biometric identifier is presented to a biometric-based authentication system, the correct authentication may not be guaranteed due to sensor noise and limitations of feature extractor and matcher. Similarly, there is a possibility that an impostor will be incorrectly accepted by a biometrics-based authentication system. An improvement in the accuracy performance of a biometrics based personal identification system is, therefore, highly desirable.

How can the performance of a biometrics-based identification system be improved? There comes a stage in the development of any biometric authentication system where it becomes increasingly difficult to achieve significantly better performance from a given biometric identifier and the need to explore other sources for improvement becomes a practical necessity. The *integration* approach to improve performance can take any number of different forms. One could combine a biometrics scheme with non-biometrics (possession or knowledge) based schemes. For instance, combining a possession-based (e.g., smart card) authentication with biometric authentication will relieve the burden of higher performance from the biometrics component without increasing the risk of an impostor acceptance. However, these solutions re-introduce the problems inherent in the possession- and knowledge-based techniques for personal identification which is not desirable. This implies that for the desired performance improvement, we may need to rely on integrating multiple biometrics.

Multiple biometrics can alleviate several practical problems in the biometrics-based personal identification. For instance, although a biometric identifier is supposed to be *universal* (each person in the target population should possess it), in practice, no biometric identifier is truly universal. Similarly, the biometric identifiers are not always sensed/measured by a practical biometric identification system. That is, some small fraction of the target population may possess biometric identifiers which are not easily quantifiable by the given biometric system. For instance, a small fraction of the population may possess fingerprints which are not easily captured by the representations (features) adopted by a given system. Consequently, the authentication system can not handle this fraction of population based on that particular biometric identifier. Further, different biometrics may not be acceptable to different sections of the target population. In highly secure systems, reinforcement of evidence from multiple independent biometric identifiers offers increasingly irrefutable proof of the identity of the authorized person. The assumptions of universality, collectability, acceptability, and integrity are more realistically accommodated when the personal authentication is based on information from several biometric identifiers.

The purpose of this paper is to examine whether the performance of a biometrics system could indeed be improved by integrating multiple biometrics. An analysis of the entire domain of multibiometrics is beyond the scope of this paper; we will restrict our study to typical cases of multiple biometrics integration and show that the integration of multiple biometric is indeed admissible. The rest of the paper is organized as follows: First, we formulate the problem of multiple biometrics integration and state the assumptions underlying the integration. Next, we present how information from multiple biometrics can be combined at various levels using a number of different methods. For two typical cases of integration, we prove that integration schemes can indeed result in an improvement in performance. We further illustrate the advantages of integrating multiple sources of information by presenting empirical results of a system which integrates face and fingerprint.

2 Performance Characterization

For an effective understanding of the advantages of a multibiometrics approach to a given application, it is necessary to correctly define the terms "performance" and "performance improvement". A number of criteria including the accuracy, cost, and speed of the system may be used to assess its performance. As the higher speed processors are becoming available at cheaper prices and as the cost of the biometric sensors is dramatically decreasing, we believe that the accuracy performance of biometrics systems will become the predominant focus of the system design. For simplicity, we will assume that the cost and the speed of the system do not play any significant role in its performance assessment.

A biometric system can commit two types of errors. A *false acceptance* (positive or match) refers to identifying an impostor to be a genuine user. A *false reject* (negative or non-match) refers to rejecting a genuine user as an impostor. It should be noted that the error rates of the system are necessary but not sufficient ingredients for evaluating the system performance; the performance depends not only on the error rates but also on the value placed by the system application on false match/mismatch, and the expected frequency/nature of the attacks on the system. It is to be noted that the costs of a false match and a false mismatch are often not identical and are significantly different depending on the application domain. For instance, high security access applications are concerned about break-ins and hence require smaller FA; forensic applications desire to catch a criminal even at the expense of examining a large number of false accepts and hence operate their matcher at a high FA [1]. In a system with different levels of security, it is conceivable that not all errors cost the same (e.g., mistaking an individual A as impostor versus mistaking B as an impostor, etc.) – again, for simplicity, we assume that each false positive poses the same amount of risk (all impostors are equally dangerous), every false negative presents identical liability (all authorized users are equally important), and the system is under random attack. Further, we conservatively assume that an impostor can get away with impunity when system detects an impostor attack (no scarecrow effect) and the frequency of impostor attack is the same as the frequency of authorized usage. Finally, we will assume that offering multiple biometric identifiers presents a negligible inconvenience to the user.

Formally, a biometrics system, $\mathcal{B}$, matches an input, $\mathbf{\Phi^i}$, against a template, $\mathbf{\Phi^t}$, obtains a similarity (or distance) assessment based on a (typically) scalar value (score) to determine which category, w_1 or w_2, the input $\mathbf{\Phi^i}$ belongs to, where w_1 indicates that $\mathbf{\Phi^i}$ is *a genuine user*, and w_2 indicates that $\mathbf{\Phi^i}$ is *an impostor*. It can be formulated as follows:

$$\mathbf{X} \in \begin{cases} w_1, & if\ \mathbf{X} \in \mathbf{R}, \\ w_2, & otherwise, \end{cases} \tag{1}$$

where $\mathbf{X} = \mathcal{F}(\mathbf{\Phi^i}, \mathbf{\Phi^t})$ is a random variable indicating the *similarity* between $\mathbf{\Phi^i}$ and $\mathbf{\Phi^t}$ and $\mathbf{R}$ is a set which consists of similarity values representing genuine users. The *false reject rate*, $FR(\mathbf{R})$, and the *false acceptance rate*, $FA(\mathbf{R})$, which are functions of the set $\mathbf{R}$ are defined as

$$FR(\mathbf{R}) = 1 - \int_{\mathbf{R}} f(\mathbf{X}|w_1)d\mathbf{X}, \tag{2}$$

$$FA(\mathbf{R}) = \int_{\mathbf{R}} f(\mathbf{X}|w_2)d\mathbf{X}, \tag{3}$$

where $f(\mathbf{X}|w_1)$ and $f(\mathbf{X}|w_2)$ represent the conditional probability density functions of genuine users and impostors, respectively. The total risk, $E(\mathbf{R})$, is defined as

$$E(\mathbf{R}) = \mathcal{C}_{FR} * FR(\mathbf{R}) + \mathcal{C}_{FA} * FA(\mathbf{R}), \tag{4}$$

where $\mathcal{C}_{FR}$ and $\mathcal{C}_{FA}$ are the cost of the false negatives and cost of authorizing an impostor, respectively. When $\mathcal{C}_{FR} = \mathcal{C}_{FA} = 1$, the risk is equivalent to the total error. The minimum total risk, $E(\mathbf{R}_{min})$, is defined as

$$E(\mathbf{R}_{min}) = Min_{\mathbf{R}}\{\mathcal{C}_{FR} * FR(\mathbf{R}) + \mathcal{C}_{FA} * FA(\mathbf{R})\}. \quad (5)$$

Let us now formulate a multibiometrics scenario. For simplicity, we will consider integration of only two biometrics[1]. Let $\mathcal{B}_i$, $i = 1, 2$, be two biometrics systems each of which uses a different biometrics indicator. Let $\mathbf{X}_i$ denote the corresponding similarity random variables and $f_i(\mathbf{X}_i|w_1)$ and $f_i(\mathbf{X}_i|w_2)$ represent the conditional probability density functions of genuines and impostors, respectively. The false reject rate, false acceptance rate, total risk, and minimum total risk of $\mathcal{B}_i$, $i = 1, 2$, are

$$\begin{aligned} FR_i(\mathbf{R}_i) &= 1 - \int_{\mathbf{R}_i} f_i(\mathbf{X}_i|w_1)d\mathbf{X}_i, && (6)\\ FA_i(\mathbf{R}_i) &= \int_{\mathbf{R}_i} f_i(\mathbf{X}_i|w_2)d\mathbf{X}_i, && (7)\\ E_i(\mathbf{R}_i) &= \mathcal{C}_{FR} * FR_i(\mathbf{R}_i) + \\ &\quad \mathcal{C}_{FA} * FA_i(\mathbf{R}_i), && (8)\\ E_i(\mathbf{R}_{min_i}) &= Min_{\mathbf{R}_i}\{\mathcal{C}_{FR} * FR_i(\mathbf{R}_i) + \\ &\quad \mathcal{C}_{FA} * FA_i(\mathbf{R}_i)\}. && (9) \end{aligned}$$

3 Architecture for Integration

Information contained in multiple biometrics could be integrated using a number of different methods, at various levels, and in different contexts (see for instance, Figure 1). Here, we will only discuss the integration based on the extent of the information shared among multiple biometric identifiers.

The output from multiple biometric sensors could be used to create a more reliable and/or extensive (spatially, temporally, or both) input acquisition [4]. The representations extracted from many biometric sensors could be collated and the decisions could be made based on the joint feature vector. The integration at sensor or representation level assumes a strong interaction among the input measurements and such integration schemes are referred to as *tightly coupled integrations* [3]. The *loosely coupled systems*, on the other hand, assume a very little or no interaction among the inputs (e.g., face and finger) and integration occurs at the output of relatively autonomous agents, each agent independently assessing the input from its own perspective. We will restrict ourselves to loosely coupled systems.

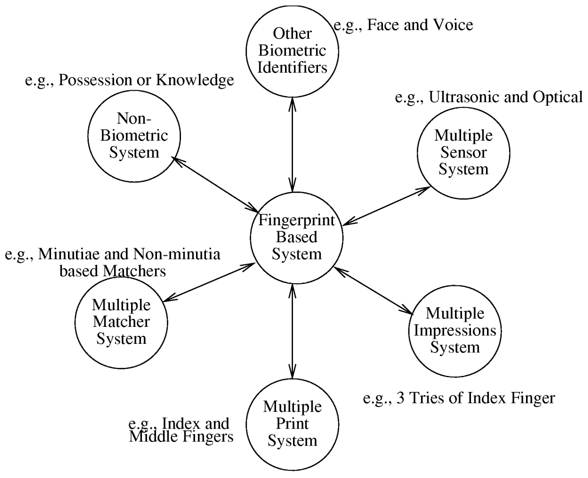
Other Biometric Identifiers
e.g., Face and Voice
e.g., Possession or Knowledge
Non-Biometric System
e.g., Ultrasonic and Optical
Multiple Sensor System
Fingerprint Based System
e.g., Minutiae and Non-minutia based Matchers
Multiple Matcher System
Multiple Impressions System
e.g., 3 Tries of Index Finger
e.g., Index and Middle Fingers
Multiple Print System

Figure 1: Multiple choices for integration in a fingerprint based system.

The loosely coupled systems are not only simpler to implement, they are more feasible in commonly confronted integration scenarios. A typical scenario for integration is two biometric systems (often proprietary) independently acquiring inputs and making an autonomous assessment of the "match" based on their respective identifiers; while the decisions or scores of individual biometric systems are available for integration, the features used by one biometric system are not accessible to the other biometric system. In this paper, we will analyze two scenarios for integration based on scores or decisions provided by two different biometrics systems. In both the cases, we demonstrate that the integration schemes result in a performance improvement.

4 Score Level Integration

In this section, we will consider score level integration of two biometric systems. As mentioned earlier, we will assume that $\mathbf{X}_i$, $i = 1, 2$, are statistically independent. As a result, the joint conditional probability density functions for genuine users and impostors, $f(\mathbf{X}_1, \mathbf{X}_2|w_1)$ and $f(\mathbf{X}_1, \mathbf{X}_2|w_2)$, can be simplified as

$$\begin{aligned} f(\mathbf{X}_1, \mathbf{X}_2|w_1) &= f_1(\mathbf{X}_1|w_1)f_2(\mathbf{X}_2|w_1), && (10)\\ f(\mathbf{X}_1, \mathbf{X}_2|w_2) &= f_1(\mathbf{X}_1|w_2)f_2(\mathbf{X}_2|w_2). && (11) \end{aligned}$$

The decision rule can be written as

$$(\mathbf{X}_1, \mathbf{X}_2) \in \begin{cases} w_1, & if\ (\mathbf{X}_1, \mathbf{X}_2) \in \mathbf{R}_{min}, \\ w_2, & otherwise, \end{cases} \quad (12)$$

where

$$\mathbf{R}_{min} = \{(\mathbf{X}_1, \mathbf{X}_2)| \frac{\mathcal{C}_{FR} * f(\mathbf{X}_1, \mathbf{X}_2|w_1)}{\mathcal{C}_{FA} * f(\mathbf{X}_1, \mathbf{X}_2|w_2)} \geq 1\}, \quad (13)$$

[1] By induction, the results could be extended to integration of multiple biometrics.

which can reach a minimum total risk,

$$\begin{aligned} E(\mathbf{R}_{min}) &= \mathcal{C}_{FR}\left\{1-\int\int_{\mathbf{R}_{min}} f(\mathbf{X}_1,\mathbf{X}_2|w_1)d\mathbf{X}_1 d\mathbf{X}_2\right\} \\ &+ \mathcal{C}_{FA}\int\int_{\mathbf{R}_{min}} f(\mathbf{X}_1,\mathbf{X}_2|w_2)d\mathbf{X}_1 d\mathbf{X}_2. \quad (14) \end{aligned}$$

Given the above formulation, we would like to prove that

$$E(\mathbf{R}_{min}) \le E_i(\mathbf{R}_{min_i}), i=1,2, \qquad (15)$$

for demonstrating performance improvement due to multibiometrics.

Without a loss of generality, let us assume that $E_1(\mathbf{R}_{min_1}) \ge E_2(\mathbf{R}_{min_2})$. For a given value of $\mathbf{X}_1$, x_1, the above decision rule can be reformulated as

$$(x_1,\mathbf{X}_2) \in \begin{cases} w_1, & if\ \frac{\mathcal{C}_{FR}*f(x_1,\mathbf{X}_2|w_1)}{\mathcal{C}_{FA}*f(x_1,\mathbf{X}_2|w_2)} \ge 1, \\ w_2, & otherwise, \end{cases} \qquad (16)$$

which has the following minimum risk

$$\begin{aligned} E(R_{min}|x_1) &= \mathcal{C}_{FR}\left\{1-\int_{\mathbf{R}_{min}} f(x_1,\mathbf{X}_2)|w_1)d\mathbf{X}_2\right\} \\ &+ \mathcal{C}_{FA}\int_{\mathbf{R}_{min}} f(x_1,\mathbf{X}_2)|w_2)d\mathbf{X}_2. \quad (17) \end{aligned}$$

Inequality

$$\frac{\mathcal{C}_{FR}*f(x_1,\mathbf{X}_2|w_1)}{\mathcal{C}_{FA}*f(x_1,\mathbf{X}_2|w_2)} \ge 1 \qquad (18)$$

is equivalent to inequality

$$\frac{\mathcal{C}_{FR}*f_1(x_1|w_1)f_2(\mathbf{X}_2|w_1)}{\mathcal{C}_{FA}*f_1(x_1|w_2)f_2(\mathbf{X}_2|w_2)} \ge 1, \qquad (19)$$

which is further equivalent to inequality

$$\begin{aligned} &\frac{\mathcal{C}_{FR}*f_2(\mathbf{X}_2|w_1)}{\mathcal{C}_{FA}*f_2(\mathbf{X}_2|w_2)} \ge \\ &\quad \frac{f_1(x_1|w_2)/(f_1(x_1|w_1)+f_1(x_1|w_2))}{f_1(x_1|w_1)/(f_1(x_1|w_1)+f_1(x_1|w_2))}. \quad (20) \end{aligned}$$

Since $f_1(x_1|w_1)/(f_1(x_1|w_1) + f_1(x_1|w_2))$ and $f_1(x_1|w_2)/(f_1(x_1|w_1)+f_1(x_1|w_2))$ are the probabilities indicating x_1 is a genuine user and an impostor, respectively and $\mathbf{X}_2$ is statistically independent of $\mathbf{X}_1$, $f_1(x_1|w_1)/(f_1(x_1|w_1) + f_1(x_1|w_2))$ and $f_1(x_1|w_2)/(f_1(x_1|w_1)+f_1(x_1|w_2))$ essentially are priors of random variable $(x_1, \mathbf{X}_2)$. Thus, the reformulated decision rule is exactly the Bayesian rule. The Bayesian rule guarantees that the resulting total error due to its application is no greater than the total error due to any other decision (including the decision which could have resulted in $E(R_{min_2})$ at point x_1. Therefore, $E(R_{min}|x_1) \le E_2(\mathbf{R}_{min_2})$ at point x_1. Since this inequality holds for all values of $\mathbf{X}_1$, $E(\mathbf{R}_{min}) \le E_2(\mathbf{R}_{min_2})$. Note that the equality holds only in the following situations: $f_i(\mathbf{X}_i|w_1) = f_i(\mathbf{X}_i|w_2)$ or both $\mathbf{X}_1$, $\mathbf{X}_2$ can take only a few (say, two) discrete values.

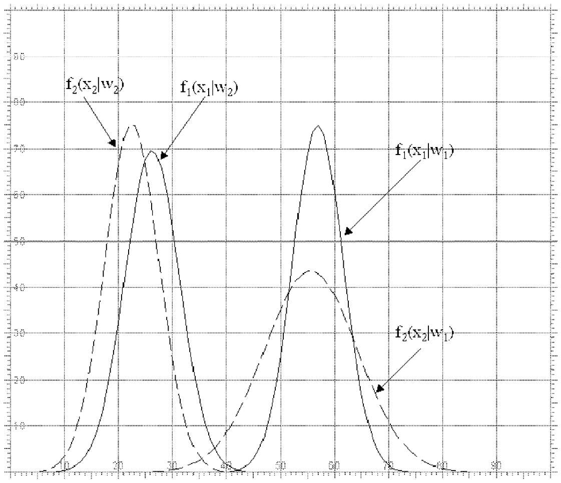

Figure 2: The (simulated) genuine and impostor distributions of two different biometrics.

To obtain an idea of the extent of improvement due to integration, we ran simulation tests for synthetically generated impostor and genuine probability density functions under Gaussian assumption as shown in Figure 2. For example, a simulation test with $E_i(\mathbf{R}_{min_i})$ of $\mathcal{B}_1$ and $\mathcal{B}_2$ equal to 0.002 and 0.02, respectively, and $\mathcal{C}_{FA} = \mathcal{C}_{FR} = 1$, $E(\mathbf{R}_{min})$ is 0.00012 (a 16 times improvement) as per the integration scheme prescribed by Eq. (12)!

5 Decision Level Fusion

In this section, we will assume that only decisions made by the individual biometric systems are available for integration. Noting that the argument of the risk function ($\mathbf{R}$) now parameterizes the operating point, the total risk in a decision fusion scenario is

$$\begin{aligned} E(\mathbf{R}) &= \mathcal{C}_{FR}*FR(\mathbf{R})+\mathcal{C}_{FA}*FA(\mathbf{R}), \quad (21) \\ E_i(\mathbf{R}_i) &= \mathcal{C}_{FR}*FR_i(\mathbf{R}_i)+\mathcal{C}_{FA}*FA_i(\mathbf{R}_i)(22) \end{aligned}$$

There are two possible integration approaches: AND and OR. We need to show in both these approaches that there exists a decision integration scenario for which

$$E(\mathbf{R}) < E_i(\mathbf{R}_i), \forall i. \qquad (23)$$

5.1 OR Rule

Consider an OR integration scenario where a user is required to offer the biometric identifier associated with $\mathcal{B}_1$ and if $\mathcal{B}_1$ rejects the user, the user is given a second chance to verify the identity with $\mathcal{B}_2$.

The error rates of the integrated system are:

$$\begin{aligned} FA(\mathbf{R}) &= FA_1(\mathbf{R}_1) + FA_2(\mathbf{R}_2) \\ &\quad -FA_1(\mathbf{R}_1) * FA_2(\mathbf{R}_2), \qquad (24) \\ FR(\mathbf{R}) &= FR_1(\mathbf{R}_1) * FR_2(\mathbf{R}_2). \qquad (25) \end{aligned}$$

Substituting Eqs. (24) and (25) in Eq. (21) and dropping $(\mathbf{R})$ for brevity, the requirement for improvement due to integration implies that

$$\mathcal{C}_{FR} * FR_1 * (1 - FR_2) > \mathcal{C}_{FA} * FA_2 * (1 - FA_1) \quad (26)$$
$$\mathcal{C}_{FR} * FR_2 * (1 - FR_1) > \mathcal{C}_{FA} * FA_1 * (1 - FA_2) \quad (27)$$

Given a matcher $\mathcal{B}_2$ operating at (FA_2, FR_2), is there a matcher $\mathcal{B}_1$ with some operating point (FA_1, FR_1) which will result in an improvement in performance?

Rewriting inequalities represented by Eqs. (26) and (27), we obtain

$$\begin{aligned} FR_1 &> -\frac{k * FA_2}{1 - FR_2} * FA_1 + k * \frac{FA_2}{1 - FR_2}, \quad (28) \\ FR_1 &< -\frac{k * (1 - FA_2)}{FR_2} * FA1 + 1, \qquad (29) \end{aligned}$$

where $k = \frac{\mathcal{C}_{FA}}{\mathcal{C}_{FB}}$. It is easy to see that inequality (28) represents a linear boundary B represented by the following equation (see Figure 3)

$$FR_1 = -\frac{k * FA_2}{1 - FR_2} * FA_1 + k * \frac{FA_2}{1 - FR_2}, \qquad (30)$$

which divides the (FA, FR) plane into two regions. The region admissible by inequality (28) is represented by the area above line B. Similarly, the region admissible by inequality (29) is represented by area below line A which is represented by

$$FR_1 = -\frac{k * (1 - FA_2)}{FR_2} * FA1 + 1. \qquad (31)$$

Note that the lines A and B always pass through (0, 1) and (1, 0), respectively; they have X- and Y-intercepts of $(\frac{FR_2}{k*(1-FA_2)}, 1)$ and $(1, k * \frac{FA_2}{1-FR_2})$, respectively. In order that intersection of the regions admissible by both inequalities (28) and (29) is non-empty, it is necessary that either (i) the X-intercept of line A be greater than 1; (ii) the Y-intercept of line B be less than 1, or (iii) both. This implies that at least one of the following two conditions needs to be satisfied in order for the performance of the integrated system using OR decision fusion rule to improve:

$$k * FA_2 + FR_2 > k, \qquad (32)$$
$$k * FA_2 + FR_2 < 1. \qquad (33)$$

For instance, integration of two matchers with (FA, FR) values of $(0.0001, 0.001)$ and $(0.001, 0.0001)$ using an OR-rule decision fusion reduces the total risk (i) from 0.0011 to approx. 0.0002 (for $k = 1$); (ii) from 0.00101 to approx. 0.00002 (for $k = 0.1$)!!

5.2 AND Rule

Consider an AND integration scenario where a user is required to offer the biometric identifiers associated with both $\mathcal{B}_1$ and $\mathcal{B}_2$, and the user is accepted if both the identifiers are acceptable by their respective biometric systems.

The error rates of the integrated system are:

$$\begin{aligned} FR(\mathbf{R}) &= FR_1(\mathbf{R}_1) + FR_2(\mathbf{R}_2) \\ &\quad -FR_1(\mathbf{R}_1) * FR_2(\mathbf{R}_2), \qquad (34) \\ FA(\mathbf{R}) &= FA_1(\mathbf{R}_1) * FA_2(\mathbf{R}_2). \qquad (35) \end{aligned}$$

Following the logic similar to that used in Section 5.1, it can be proven that at least one of the following two conditions needs to be satisfied in order for the performance to improve

$$k * FA_2 + FR_2 > 1, \qquad (36)$$
$$k * FA_2 + FR_2 < k, \qquad (37)$$

where $k = \frac{\mathcal{C}_{FA}}{\mathcal{C}_{FB}}$ and the feasible operating points (FA_1, FR_1) of such a matcher are prescribed by a region enclosed (Region 1 in Figure 3) by the lines defined by

$$\begin{aligned} FR_1 &< -\frac{k * FA_2}{1 - FR_2} * FA_1 + k * \frac{FA_2}{1 - FR_2}, \quad (38) \\ FR_1 &> -\frac{k * (1 - FA_2)}{FR_2} * FA1 + 1. \qquad (39) \end{aligned}$$

6 Empirical Results

Empirical demonstrations of improvement in performance due to integration of multiple biometrics abound in the literature [2, 8, 7, 6, 5, 4, 3]. Here, we summarize results from one case study in integration which is based on our work reported elsewhere [2]. This system implements a score-based decision fusion framework which integrates two biometrics (face and fingerprint) for an online identification application. The integrated system first retrieves the top 5 matches for an identity using face recognition. Then fingerprint verification is applied to each of the resulting top 5 matches and a final decision is made by the decision fusion scheme. Experimental results using a small database of 64 individuals demonstrate that the multibiometrics system performs better than the identification performed by either finger or face alone (see Table 1 and Fig. 4).

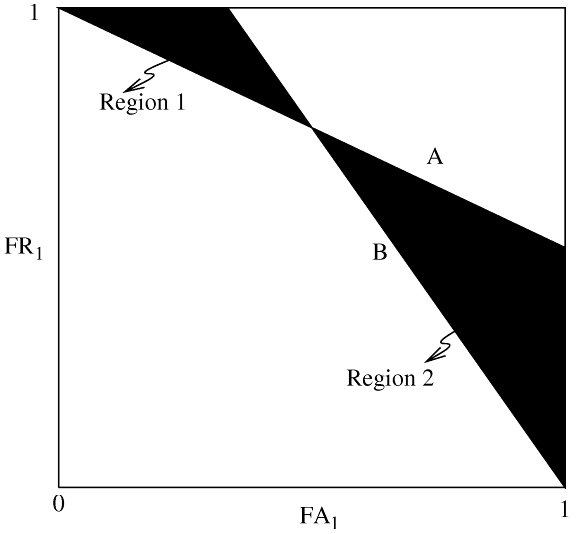

Figure 3: Boundaries of admissibility in a decision fusion system. $FA_2 = 0.5$, $FR_2 = 0.7$, $k = 0.85$. Region 1 is admissible under AND fusion rule; Region 2 is admissible under OR fusion rule. Atypical error rates are used for clearly illustrating admissible regions.

Table 1: False reject rates on the test set with different values of False Acceptance Rates. FR1, FR2, and FR3 denote face, fingerprint, and integrated false reject rates, respectively.

FA (%)	FR1 (%) (face)	FR2 (%) (fingerprint)	FR3 (%) (integrated)
1.0	15.8	3.9	1.8
0.1	42.2	6.9	4.4
0.01	61.2	10.6	6.6
0.001	64.1	14.9	9.8

7 Conclusions

One of the most common barriers against wide-scale adoption of biometrics-based personal identification systems is their less than satisfactory performance [1]. Consequently, improving the system performance is a significant research challenge. In this paper, we formulate the multibiometrics problem. In two commonly used scenarios, we prove that it is possible to improve performance by integrating multiple biometrics. These results are further supported by empirical evidence from our earlier work on integrating face and fingerprint.

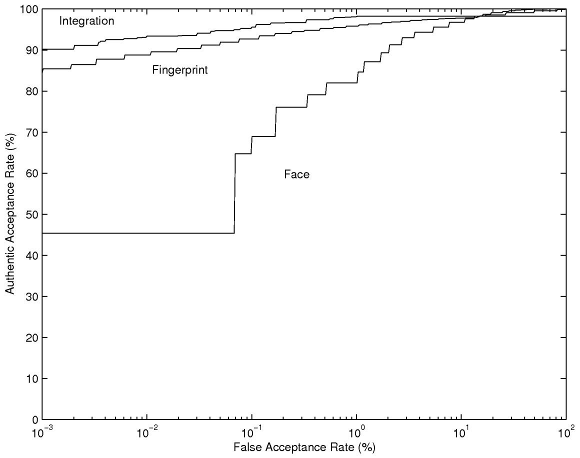

Figure 4: Receiver Operating Characteristics curves for a multibiometrics system.

References

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

[2] L. Hong and A. K. Jain. Integrating Faces and Fingerprints, *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 20, No. 12, pp. 1295-1307, December 1998.

[3] J. Clark and A. Yuille. *Data Fusion for Sensory Information Processing Systems.* Kluwer Academic Publishers, Boston, 1990.

[4] R. R. Brooks and S. S. Iyengar. *Multi-sensor Fusion: Fundamentals and Applications with Software.* Prentice-Hall, Upper Saddle River, New Jersey, 1997.

[5] U. Dieckmann, P. Plankensteiner and T. Wagner. Sesam: A biometric person identification system using sensor fusion. *Pattern Recognition Letters*, Vol. 18, No. 9, pp. 827–833, 1997.

[6] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer. Expert conciliation for multi modal person authentication systems by Bayesian statistics. In *Proc. 1st Int. Conf. on Audio Video-Based Personal Authentication*, pp. 327–334, Crans-Montana, Switzerland, 1997.

[7] R. Brunelli and D. Falavigna. Personal identification using multiple cues. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 17(10):955–966, 1995.

[8] J. Kittler, Y. Li, J. Matas, and M. U. Sanchez. Combining evidence in multimodal personal identity recognition systems. In *Proc. 1st Int. Conf. on Audio Video-Based Personal Authentication*, pp. 327–334, Crans-Montana, Switzerland, 1997.