Performance Analysis for Integrating Biometrics

Lianfen Qian*, and Hanqi Zhuang**

*Department of Mathematics (lqian@fau.edu)
**Department of Electrical Engineering (zhang@fau.edu)
Florida Atlantic University
Boca Raton, FL 33431

Abstract

Due to the performance limitation of using a single biometric, many researchers have been investigating ways to integrate multiple biometrics for the purpose of authentication. To this end, there have been numerous articles on promoting multiple biometric identifiers. It is thus important to know when integrating improves the performance and when it does not. This research focuses on integrating biometrics at the decision level. In this article, the formulas are first derived for the probabilities of a False Accept and a False Reject when \( n \) Biometric tests are combined. The conditions are then obtained for performance improvement and degradation of combining two biometric identifiers. To the end, some other interesting results of integrating biometric solutions are also presented.

I. Introduction

Biometric personal authentication has the potential to provide security solutions for purposes, such as, homeland security, the prevention of identity theft, and other government and commercial applications [1]. Due to the performance limitation of using a single biometric, many researchers have been investigating ways to integrate multiple biometrics for the purpose of authentication. Integrating (or fusing) multiple biometrics can be done in different levels, i.e., sensor level, feature level, measurement level and abstract or decision level [2]. Jain and his coworkers commented that integrating at early stages may lead to a better authentication performance [2]. They also mentioned that there are difficulties in integrating multiple biometrics in the early stages, for instance, in the feature level. One major difficulty of doing so is that one may not have all the means to obtain different types of feature as vendors may not provide accessible features or templates to the end users. Thus decision level fusion becomes a choice for many field engineers. This practice raises a couple of important questions: will integrating multiple biometric solutions at the decision level always improve the system authentication performance? If not, under which conditions will it provide a better solution?

In the literature, there have been numerous articles that argued affirmatively to the question [3-19]. Daugman, in his online short note [20, 21], made the following statement:

There is common and intuitive assumption that the combination of different tests must improve performance, because "surely more information is better than less information." On the other hand, a different intuition suggests that if a strong test is combined with a weaker test, the resulting decision environment is in a sense averaged, and the combined performance will lie somewhere between that of the two tests conducted individually (and hence will be degraded from the performance that would be obtained by relying solely on the stronger test).

Daugman, with mathematic derivations, showed that a strong biometric is better alone than in combination with a weaker one [20]. This note extends Daugman’s results to more general setting: Integrating \( n \) biometrics. The authentication performance is judged in this article by a cost that combines False Accept Rate and False Reject Rate. The formulas are first derived for the probabilities of a False Accept and a False Reject when \( n \) Biometric tests are combined. The conditions are then obtained for performance improvement of combining two independent biometric identifiers. It is confirmed that the authentication performance may be improved when two similar biometrics are combined. On the other hand, the overall performance will certainly degrade when two biometrics with a large power discrepancy are combined. Finally, some other interesting results of integrating biometrics are also presented.

II. Decision Level Fusion

There are two common errors a biometric system can make: A False Acceptance and a False Reject. A false acceptance identifies an impostor to be a genuine user. A False Reject rejects a genuine user as an impostor.
Let us consider \( n \) hypothetical biometric tests in a biometric authentication system, where \( n \) is an integer. There are two possible integration approaches to combine the outcomes of the \( n \) Biometric tests to form an “enhanced” decision. Here Daugman’ definitions for these two ways given in [20] are adopted. That is:

**Rule A (OR Rule):** Accept if at least one of the \( n \) tests is passed.

**Remark 1:** Daugman defines “OR Rule” as “accept if either test 1 or test 2 is passed.” This definition is not precise as it does not include the case of both tests passed. However, the derivation and the results obtain in [20] are correct.

**Rule B (AND Rule):** Accept only if all tests are passed.

**Notation**

Let us introduce the following notation:

\[
\begin{align*}
FA_i &= \text{a False Accept using Biometric } i \text{ alone.} \\
FR_i &= \text{a False Reject using Biometric } i \text{ alone.} \\
P_r(FA) &= P(FA) = \text{the probability of a False Accept using Biometric } i \text{ alone.} \\
P_r(FR) &= P(FR) = \text{the probability of a False Reject using Biometric } i \text{ alone.} \\
P_a(FA) &= P_a(FA) = \text{the probability of a False Accept using rule A.} \\
P_a(FR) &= P_a(FR) = \text{the probability of a False Reject using rule A.} \\
P_b(FA) &= P_b(FA) = \text{the probability of a False Accept using rule B.} \\
P_b(FR) &= P_b(FR) = \text{the probability of a False Reject using rule B.} \\
A &= \text{the complement event of any event } A. \\
\end{align*}
\]

**Theorem 1.** Assume that \( n \) Biometric tests are combined.

1. If “OR Rule” is used, one has:
   \[
   P_a(FA) = 1 - P(FA_1 \cap FA_2 \cap \cdots \cap FA_n) \\
   \geq P(FA), \quad \text{for } i = 1, \ldots, n.
   \]
   and
   \[
   P_a(FR) = P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
   \leq P_a(FR), \quad \text{for } i = 1, \ldots, n.
   \]

2. If “AND Rule” is used, one obtains similar formulas as follows:
   \[
   P_b(FA) = P(FA_1 \cap FA_2 \cap \cdots \cap FA_n) \\
   \leq P_a(FA), \quad \text{for } i = 1, \ldots, n
   \]
   and
   \[
   P_b(FR) = 1 - P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
   \geq P(R), \quad \text{for } i = 1, \ldots, n.
   \]

**Remark 2:** From this theorem, for a random attack system (all impostors are equally dangerous and all authorized users are equally important) and assuming users are willing to offer multiple biometric identifiers without complaints, one observes that combining \( n \) biometrics results in one of the two false rates increases and the other decrease comparing with each of the individual tests. For “OR Rule”, the probability of False Accept (positive or match) is higher than that of using any one of the biometrics only; while for “AND Rule”, is lower. On the other hand, the probability of False Reject is decreased for “OR Rule” and increased for “AND Rule”. Thus, if a system is designed to be more secure to imposters (or the cost of a False Accept is higher than the cost of a False Reject), it may take “AND Rule” but bear with rejecting more genuine users. As the same token, if a system is intended to be more convenient to genuine users (the cost is higher for a False Reject than that of a False Accept) and afford to bear accepting more imposters, then it may adapt “OR Rule”. Examples for the former are high security devices concerning break-ins and for the latter are forensic systems to catch criminals [22].

**Proof of Theorem 1:** 1. If “OR Rule” is used to combine \( n \) tests, a False Accept happens if at least one of the \( n \) tests is passed.

Using De Morgan theorem, we have:

\[
\begin{align*}
P_a(FA) &= P(FA_1 \cup FA_2 \cup \cdots \cup FA_n) \\
&= 1 - P(FA_1 \cap FA_2 \cap \cdots \cap FA_n) \\
&= 1 - P_a(FA) \\
&\geq 1 - P_a(FA) \\
&= 1 - P_a(FR) \\
&= P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
&= P_a(FR), \quad \text{for } i = 1, \ldots, n.
\end{align*}
\]

and a False Reject happens if all \( n \) tests produce False Rejects,

\[
\begin{align*}
P_a(FR) &= P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
&\leq P_a(FR) \\
&\leq P_a(FR) \quad \text{for } i = 1, \ldots, n.
\end{align*}
\]

2. Similarly, if “AND Rule” is used to combine \( n \) tests, a False Accept happens if all \( n \) tests produce a False Accept. We have:

\[
\begin{align*}
P_b(FA) &= P(FA_1 \cap FA_2 \cap \cdots \cap FA_n) \\
&\leq P_a(FA) \quad \text{for } i = 1, \ldots, n.
\end{align*}
\]

and a False Reject happens if at least one of the \( n \) tests is passed.

By De Morgan theorem, we have:

\[
\begin{align*}
P_a(FR) &= P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
&= 1 - P_a(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \\
&= 1 - P_a(FR) \\
&\geq 1 - P_a(FR) \\
&= P_b(FR) \quad \text{for } i = 1, \ldots, n.
\end{align*}
\]

This completes the proof of Theorem 1.

**Corollary 1:** If the \( n \) Biometric tests are independent and combined, then one has
\[ P_A(FA) = 1 - \prod_{i=1}^{n}(1 - P_i(FA)) \]
\[ P_A(FR) = \prod_{i=1}^{n} P_i(FR) \]
\[ P_b(FA) = \prod_{i=1}^{n} P_i(FA) \]
\[ P_b(FR) = 1 - \prod_{i=1}^{n}(1 - P_i(FR)). \]

Proof: If “OR Rule” is used to combine \( n \) tests, a False Accept happens if at least one of the \( n \) tests is passed. By the results from Theorem 1.1 and the independent assumption of the \( n \) Biometric tests, a further simplification is obtained as follows:

\[ P_A(FA) = 1 - P\left(F_A \cap F_{A_1} \cap \cdots \cap F_{A_n}\right) \]
\[ = 1 - \prod_{i=1}^{n} P_i(FA) \]
\[ = 1 - \prod_{i=1}^{n}(1 - P_i(FA)) \]

and

\[ P_A(FR) = P(FR_1 \cap FR_2 \cap \cdots \cap FR_n) \]
\[ = \prod_{i=1}^{n} P_i(FR). \]

Similarly, if “AND Rule” is used to combine \( n \) tests, a False Accept happens if all \( n \) tests produce a False Accept. By the results from Theorem 1.2 and the independent assumption of the \( n \) tests, one has

\[ P_b(FA) = P(FA_1 \cap FA_2 \cap \cdots \cap FA_n) \]
\[ = \prod_{i=1}^{n} P_i(FA) \]

and

\[ P_b(FR) = 1 - P\left(\overline{F_R} \cap \overline{F_{R_1}} \cap \cdots \cap \overline{F_{R_n}}\right) \]
\[ = 1 - \prod_{i=1}^{n} P_i(\overline{FR}) \]
\[ = 1 - \prod_{i=1}^{n}(1 - P_i(\overline{FR})) \]

This completes the proof of Corollary 1.

**Corollary 2:** When \( n = 2 \), then we have

\[ P_A(FA) = P_1(FA) + P_2(FA) - P_1(FA) \cdot P_2(FA) \]
\[ P_A(FR) = P_1(FR) \cdot P_2(FR) \]
\[ P_b(FA) = P_1(FA) \cdot P_2(FA) \]
\[ P_b(FR) = P_1(FA) + P_2(FA) - P_1(FA) \cdot P_2(FA) \]

which is the Daugman’s results given in [20].

### III. Performance Criteria for Combining Two Independent Biometrics

Now let us turn to discuss the performance criteria by considering the costs of a False Accept and a False Reject. For simplicity, the case of \( n = 2 \) is considered. Let \( C_{FA} \) and \( C_{FR} \) be the costs of a False Accept and a False Reject, respectively. Then, the average costs (total risks in Hong at el. [22]) are

\[ R_A = C_{FA}P_A(FA) + C_{FR}P_A(FR) \]

and

\[ R_B = C_{FA}P_b(FA) + C_{FR}P_b(FR) \]

for decision “Rule A” and “Rule B”, respectively.

For notation simplicity, from now on, \( P_A(FA) \) and \( P_A(FR) \) are denoted by \( FA \) and \( FR \), respectively. When the decision rule is clearly stated, \( FA \) and \( FR \) may be used as the corresponding probabilities for the integrated system.

For a biometric system using only a single biometric identifier, we adapt the same notation for total risk. That is, \( R_i \) is used as the total risk when using \( ith \) biometric alone. If the cost of the two types of errors are same, i.e., \( C_{FA} = C_{FR} \), then minimizing the total risk is the same as minimizing the sum of the two types of error rates.

At the decision level fusion, for \( n = 2 \), Hong at el. [22] show that there exists a decision integration scenario such that the integrated system is better than single biometric alone based. Daugman gave example that when combining two biometric solutions with large difference in power can worsen the system. The natural question is when it is worth to combine and when it is not. Mathematically, what is the necessary and sufficient condition for improvement when integrating multiple biometrics?

Assume that two independent biometrics are to be integrated under same costs for the two types of errors, the following three scenarios are considered:

- One biometric identifier is stronger than the other.
- Two biometrics have similar power such as two fingerprints.
- The probability of False Accept of the first biometric is the same as the probability of False Reject of the second biometric, and vice versa [22].

**Theorem 2:** Let \( F_1 = max(FA_1, FR_1) \) and \( F_2 = min(FA_2, FR_2) \).

1. If \( F_1 \leq F_2 \), then the integrated system using two biometric identifiers performs no worse than biometric 2 but no better than biometric 1. Hence, there is no improvement in performance of integrating.
2. If \( FA_1 = FA_2 \leq 0.5 \) and \( FR_1 = FR_2 \leq 0.5 \) and \( F_1 > F_2 \), then the integrated system improves under one of the decision rules and degrades under the other decision rule. More specifically,
   a. If \( FR_1 > FA_1 \), then using “OR Rule” can improve the performance but “AND Rule” degrading the system.
b. If \( FR_1 < FA_1 \), then using “AND Rule” can improve the performance but “OR Rule” degrading the system.

**Remark 3:** The assumption of the false error rates less than or equal to 0.5 in Theorem 2.2 is only for mathematic derivation. In practice, the assumption is unnecessary. This is because that if the error rates are bigger than 0.5 = 50%, the biometric is a very poor identifier, not worth to use anyway.

**Remark 4:** 1. The condition \( F_1 < F_2 \) indicates that biometric 1 is stronger than biometric 2 in both types of errors. Hence using only the biometric 1 will be better than using combined biometric system. 2. The conditions \( FA_1 = FA_2 \) and \( FR_1 = FR_2 \) indicate two similar biometrics such as two fingerprints, two eyes, etc.

**Remark 5:** One of Daugman’s examples in [20] is to combine two-eye iris test results. It is suspected that his statement “with AND Rule, it may reducing FR rate” should be “with OR Rule...” by Theorem 2.2.a.

**Proof of Theorem 2:** 1. “OR Rule” is proven first. In order to improve the performance in terms of total risk, one needs to have

\[
R < \min(R_1, R_2).
\]

By Theorem 1.1, improving the performance of biometric 1, or \( R < R_1 \) is equivalent to require

\[
FA_1 *(1 - FA_1) < FR_1 *(1 - FR_2). \tag{1}
\]

and of biometric 2 or \( R < R_2 \), is equivalent to require

\[
FA_2 *(1 - FA_2) < FR_2 *(1 - FR_1). \tag{2}
\]

Thus, in order to show that there is an improvement when integrating two independent biometrics, both (1) and (2) need to hold. The condition \( F_1 \leq F_2 \) implies that

\[
FR_1 *(1 - FR_1)\leq F_1 *(1 - F_1) \leq FA_1 *(1 - FA_1)
\]

which implies that inequality (1) does not hold or equivalently \( R \geq R_1 \). That is, biometric 1 performs no worse than the integrated one. Hence, the integrated system performs no better than biometric 1 used alone. But inequality (2) holds with equality since

\[
FR_2 *(1 - FR_2)\leq F_2 *(1 - F_2) \leq FA_2 *(1 - FA_2).
\]

Thus Theorem 2.1 is true for “OR Rule.”

Now the case of “AND Rule” is studied. By Theorem 1.2, one has

\[
R < R_1 \text{ is equivalent to }
FR_1 *(1 - FR_1) < FA_1 *(1 - FA_2) \tag{3}
\]

and

\[
FR_1 *(1 - FR_1) < FA_1 *(1 - FA_2).
\]

In order to improve the performance, both (3) and (4) need to hold. Notice that under the condition of Theorem 2.1, one has

\[
FA_2 *(1 - FA_1) \geq F_1 *(1 - F_1) \geq F_1 *(1 - F_1) \geq FR_1 *(1 - FR_2)
\]

which indicates that (4) holds with equality hence the integrated system is no worse than biometric 2. However

\[
FA_2 *(1 - FA_1) \leq F_2 *(1 - F_2) \leq F_2 *(1 - F_2) \leq FR_2 *(1 - FR_1)
\]

contrads with (3), indicating that biometric 1 is no worse than the integrated one. This completes the proof of Theorem 2.1.

To prove Theorem 2.2, it is first noticed that under the conditions of Theorem 2.2, one has either Theorem 2.2.a: \( FR_1 > FA_1 \) or Theorem 2.2.b: \( FR_1 < FA_1 \). Secondly, let us utilize the strictly increasing property of the function \( f(x) = x(1-x) \) over domain \((0,0.5)\).

Consider Theorem 2.2.a first. For “OR Rule”, the integrated system improving the performance is equivalent to require \( R < \min(R_1, R_2) \), which is equivalent to

\[
FR_1 *(1 - FR_1) > FA_1 *(1 - FA_1) \tag{5}
\]

Combining the condition \( FR_1 > FA_1 \) and the strictly increasing property of \( f(x) = x(1-x) \) over \((0,0.5)\), the above inequality holds. Hence “OR Rule” improves the performance.

Now consider “AND Rule”. Improving the performance is equivalent to require

\[
FR_1 *(1 - FR_1) < FA_1 *(1 - FA_1) \tag{6}
\]

which is possible over \((0,0.5)\) since \( FR_1 > FA_1 \) and \( f(x) = x(1-x) \) is strictly increasing.

To prove Theorem 2.2.b, “AND Rule” is first considered. Improving in performance is equivalent to require \( R < \min(R_1, R_2) \), which is equivalent to

\[
FR_1 *(1 - FR_1) < FA_1 *(1 - FA_1) \tag{7}
\]

Combining the condition \( FR_1 < FA_1 \) and the strictly increasing property of \( f(x) = x(1-x) \) over \((0,0.5)\), the above inequality holds. That “OR Rule” does not improve the performance follows from

\[
FR_1 *(1 - FR_1) \leq FA_1 *(1 - FA_1) \tag{8}
\]

Thus the proof of Theorem 2 is completed.

**Corollary 3:** Assume that \( FA_i = FR_i, i = 1,2 \). Then the integrated biometric system does not have a better authentication performance as defined.

**Proof:** The condition implies that \( F_i = FA_i \) and \( F_2 = FA_2 \). Thus, there are three possibilities:

1. \( F_1 = FA_1 < FA_2 = F_2 \).
2. \( F_1 = FA_1 = FA_2 = F_2 \).
3. \( F_1 = FA_1 > FA_2 = F_2 \).

Theorem 2.1 implies that cases 1 and 2 can not improve the performance. For case 3, one may consider biometric 2 as biometric 1 in Theorem 2.1, thus it cannot improve the overall system performance either.

**Example 1:** In one of the examples given in [20], \( FA_1 = FR_1 = 0.001 \) and \( FA_2 = FR_1 = 0.01 \). Then \( F_1 = 0.001 < 0.01 = F_2 \).

**Example 2:** If \( FA_1 = FR_1 = FA_2 = FR_2 = 0.01 \), then \( F_1 = F_2 = 0.01 \). Then, \( R_1 = R_2 = R_1 = R_2 = 0.02 \).
Remark 6: Theorem 2 provides the conditions under which the integrated system can or cannot improve the performance. But it does not cover all possibilities. The following example from Hong et al. [22] serves one of the possibilities. Note that the authors mistakenly gave this example as the one to show the improvement offered by integrating two independent biometric solutions.

Example 3: [22] Let \( FA_1 = FR_2 \neq FA_2 = FR_1 \). Then one has \( R = R_1 = R_2 = 11000/10^2 = 0.0011 \). But \( F_1 = 0.001 > F_2 = 0.0001 \).

Through this example, the following more generally result can be inferred.

Theorem 3: If \( FA_1 = FR_2 \) and \( FA_2 = FR_1 \), then the integrated system performs equally well as the one using a single biometric identifier alone.

Remark 7: There is no need for integration in the case stated in Theorem 3. One shall just use one of the biometric identifiers.

Proof of Theorem 3: The result for “OR Rule” is only proven here. It is similar for “AND Rule”. Using Corollary 2, one has

\[
FA = FA_1 + FA_2 - FA_1 * FA_2
\]

\[
FR = FR_1 + FR_2 - FR_1 * FR_2
\]

Therefore,

\[
R = FA + FR = FA_1 + FA_2 - FR_1 + FR_2 = R_1 = R_2.
\]

Hong’s example given in [22] is a special case of Theorem 3 since \( FA_1 = FR_2 = 0.0001 \) and \( FA_2 = FR_1 = 0.001 \).

IV. Conclusions

In this article, the conditions under which integrating multiple biometrics will improve or will degrade the overall system performance have been investigated. The general formulas have been derived for the probabilities of a False Accept and a False Reject when \( n \) Biometric tests are combined. Furthermore, some necessary and sufficient conditions have been obtained for improving performance of combing two independent biometric identifiers. It has been confirmed that the authentication performance can be improved when two similar biometrics are combined. On the other hand, the overall performance will certainly degrade when two independent biometrics with a large power discrepancy are combined. Some other interesting results of integrating biometrics have also been presented.

References


