

Improving Personal Identification Accuracy Using Multisensor Fusion for Building Access Control Applications

Lisa Osadciw, Pramod Varshney, and Kalyan Veeramachaneni

laosadci,varshney,kveerama@syr.edu

Department of Electrical Engineering and Computer Science
Syracuse University
Syracuse, NY 13244

Abstract - *This paper discusses a multimodal biometric sensor fusion approach for controlling building access. The motivation behind using multimodal biometrics is to improve universality and accuracy of the system. A Bayesian framework is implemented to fuse the decisions received from multiple biometric sensors. The system's accuracy improves for a subset of decision fusion rules. The optimal rule is a function of the error cost and a priori probability of an intruder. This Bayesian framework formalizes the design of a system that can adaptively increase or reduce the security level. This is important to systems designed for varying security needs and user access requirements. The additional biometric modes and variable error costs give the system adaptability improving system acceptability. This paper presents the framework using three different biometric systems: voice, face, and hand biometric systems.*

1 Introduction

The personal safety of the population in public and private buildings has always been a concern but since September 11 is receiving more attention. A variety of pilot projects in the area of access control based on a single biometric have been completed recently [1,2]. The unsatisfactory results from these projects highlight the need to improve biometric verification accuracy to address both customer and user needs. Issues that need to be addressed in a building accessibility system include performance, acceptability, and circumvention. Acceptability, referring to the population's acceptance of biometrics in daily life, is best addressed by society's leaders and is beyond the scope of this paper. However, system accuracy and circumvention are dependent on the biometric technology as well as the system design. This is the focus of this paper.

In this building access application, a set of employees are identified as requiring certain access needs. Different employees may require more access than others and thus a

mechanism to adapt the security level to the individual needs to be available. The employees are enrolled in the system through the assignment of a security level and biometric feature collection. In the system under consideration, the enrollment data is stored on a card that the employee carries. This addresses some privacy concerns raised by having a central biometric database. As the employee attempts to gain access, the biometric features are collected at the building entrance and matched against the features stored on the card. This is a one-to-one matching process that verifies the employee's identification. The matching process is faster since a large database is not searched.

The system then makes 1 of 4 possible decisions during the matching process. The possible decisions are

1. the genuine employee is accepted,
2. the genuine employee is rejected,
3. the imposter is accepted,
4. the imposter is rejected.

The accuracy of the decision is specified in terms of the rate with which the system makes decisions 2 and 3, which are erroneous. The error described in 2 is referred to as false rejection rate (FRR). The error in 3 is the false acceptance rate (FAR). These quantities are specified in terms of conditional probabilities.

Another system error is failure to enroll an employee. This occurs if the biometric is not unique for an individual or can not be collected. In fingerprint systems, poor finger pressure, gloves, injuries, and paint can prevent reasonable capture. In voice biometrics, a cold or simply being out-of-breath may prevent adequate capture of the biometric feature. In iris biometrics, distractions as well as glasses may prevent biometric capture [2]. This is such a common problem that many systems routinely use decision fusion by

employing a best out of 3 captures to achieve reasonable FRR performance [1].

Other approaches employing fusion for personal identification have been investigated with success [3,4]. These approaches have explored using different types of sensors to collect the same biometric feature. An example is the fusion of fingerprints collected using both an optical sensor and ultrasound sensor. Others have studied system performance for multimodal biometric fusion such as face and voice. All have demonstrated performance improvement. In a system for the general population, it is paramount that a multimodal system employing fusion be available so that tailoring of the biometric collection and matching process can be accomplished to address the employee's unique characteristics as well as access needs.

This paper focuses on reducing decision errors, FAR and FRR, through fusing multimodal biometrics in a Bayesian framework. A related performance measure is genuine acceptance rate (GAR) is defined as (in probability)

$$G_{AR} = 1 - F_{RR}. \quad (1)$$

In detection theory [5], FAR, FRR and GAR are commonly known as the false alarm rate, miss rate and detection rate, respectively. This paper will present performance improvement in terms of these parameters.

Single biometric systems have variable FAR and FRR operating points. The system designer exercises a trade-off between FAR and FRR since both can not be reduced simultaneously. Since security is usually of prime consideration, a low FAR is needed. This results in a high FRR causing a variety of problems in the building access application. These problems include long transaction times and extensive user training. These issues may lead to employees circumventing the system to avoid the daily frustration of using it.

The results from current pilot programs clearly indicate that a high FRR leads to low user acceptance. In fact, some current pilot programs offer the user an option to simply enter a PIN, personal identification number. PIN use has been shown to increase when the FRR is too high. In the recent Personal Identification Pilot Study (PIPS) [2] conducted by the Army Research Laboratory at Adelphi, 60% of the users felt that the iris biometric took too long to collect. The single sensor performance was not matching the manufacturer's rate so the PIPS system uses a 1 out of 2 approach requiring biometrics for both the left and right eyes. This reduced the FRR from 6 to 7% down to 5%. However, the transaction time increased from 15 seconds to 30 seconds.

This paper proposes a Bayesian approach to fusion in order to support system security adaptability as well as addressing user issues. A suite of biometric sensors have been chosen so that multiple biometrics can be obtained simultaneously addressing the transaction time issue. It is possible to collect voice, face and hand biometrics simultaneously using low cost digital cameras and microphones. In our approach, each biometric sensor makes a decision based on its own biometric and match processing. These decisions are combined using the optimum fusion rule for the assigned error cost and a priori probability of an imposter in the Bayesian framework. Performance of different fusion rules is evaluated using the biometric sensor performance data available in [4]. The study using the 3 biometric sensors provides the insight necessary to the design of a building security system that uses multimodal biometrics.

2 Sensor level decision making

The problem of personal identification can be formulated as a hypothesis testing problem where the two hypothesis are

H_0 : the person is an imposter

H_1 : the person is genuine.

The conditional probability density functions are $p(u_i|H_1)$ and $p(u_i|H_0)$ where u_i is the output of the i^{th} biometric sensor given the genuine person and the imposter respectively. The decision made by the sensor i is

$$u_i = \begin{cases} 0, & \text{person is an imposter} \\ 1, & \text{person is genuine} \end{cases}$$

This decision is made based on the following likelihood ratio test

$$\frac{p(y_i|H_1)}{p(y_i|H_0)} \underset{u_i = 0}{\overset{u_i = 1}{\geq}} \lambda_i \quad (2)$$

where λ_i is an appropriate threshold. The threshold is assumed to be set internally in the biometric sensor to meet the sensor's design performance criteria.

We define the errors, FAR and FRR, for a sensor as

$$F_{AR_i} = P(u_i = 1 | H_0)$$

and

$$F_{RR_i} = P(u_i = 0 | H_1).$$

The performance of a detector is often represented in terms of receiver operating characteristics (ROC) which is a plot of GAR versus FAR. Different values of FAR yield different operating points on the ROC. It should be pointed out that the optimum decision rule can be designed using various performance criteria (e.g. minimum probability of error). In this paper, we do not consider the design of individual biometric sensor decision rules. We assume that they have been designed and their ROC's are available to us. Based on this information, we study the fusion of the biometric sensor decisions and derive optimum decision fusion rules.

3 Biometric sensors

Three biometric sensors are considered in this paper: a face recognition system by Visionics, a hand biometric system by Recognition Systems, and a voice recognition system by OTG using the SecurPBX demonstration system [1]. Figure 1 contains the three ROCs constructed based from data available in [1]. The biometric sensors selected have comparable performance so that a single sensor does not perform better in both FAR and FRR.

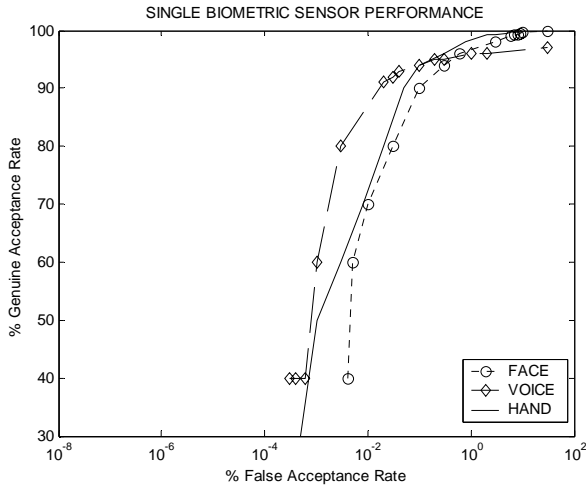


Figure 1. Experimentally Determined Operating Curves for 3 Biometric Sensors [1]

As mentioned earlier, human factor issues can affect the performance of a single sensor and are not accounted for in the operating curves. For face recognition, glasses, hair styles, facial hair, and tans can reduce the system accuracy. In a hand recognition system, jewelry such as rings and hand injuries cause errors. The voice recognition system was found to have a failure to acquire rate of 2.5%. Higher FRR than reported in Figure 1 also resulted for individuals with colds and/or being out-of-breath and are not accounted. All of these issues lead to other system design issues such as user training, recalibration, and biometric feature aging that are not addressed in this paper. It is interesting to note that all three of the systems in this study allow the customer to accept an individual if only 1 out of 3 matching attempts succeeds. This indicates that in actual use human factors issues result in unacceptable FRR levels.

Another major factor in any biometric building security system is the transaction time or time required to collect the biometric data. The following transaction times were experimentally determined in Table I [1]. The face and voice have the longest transaction times but these biometrics can be collected simultaneously reducing the total mean transaction time from 37 seconds to 22 seconds. If all three biometrics are collected simultaneously, the transaction time reduces to 14 seconds. This may require more training for the users, however. As previously mentioned, users are sensitive to the time required to collect the biometric data.

TABLE I. Transaction Time

System	Mean (s)	Median (s)	Minimum (s)
Face	15	14	10
Hand	10	8	4
Voice	12	11	10

4 Optimum decision level fusion

Decision level fusion creates a global decision based on the local decisions of the biometric sensors. Although this paper focuses on three biometric sensors, the results can be generalized to any set of biometric sensors. The system designer's goal is lowering both FAR and FRR by combining the sensor decisions. This error reduction must be significant enough to justify the added cost, complexity, and transaction time required by a multiple sensor system.

The optimum decision fusion rule is obtained using the Bayesian framework. Specifically, a weighted sum of the two types of error probabilities is minimized where the

weights are the costs associated with the two types of errors. The total cost to be minimized is

$$E = C_{FA}F_{AR} + C_{FR}F_{RR} \quad (3)$$

where C_{FA} is the cost of falsely accepting an imposter individual, C_{FR} is the cost of falsely rejecting the genuine individual, F_{AR} is the global FAR, and F_{RR} is the global FRR. This can be rewritten in terms of one cost using

$$C_{FR} = 2 - C_{FA} \quad (4)$$

giving

$$E = C_{FA}F_{AR} + (2 - C_{FA})F_{RR}. \quad (5)$$

The optimum fusion rule minimizes this cost by selecting the rule that combines single biometric sensor decisions into a combined decision. The single sensor observations and corresponding decisions are assumed to be independent. Costs have been included in the expression (3) to allow the system designer to weight the FAR more heavily reflecting the customer's need for an increased level of security. Varying these costs affect the fusion rule selection.

The optimum fusion rule allowing access to a building for N sensors is [6,7]

$$\sum_{i=1}^N \left[u_i \log \left(\frac{1 - F_{RR_i}}{F_{AR_i}} \right) + (1 - u_i) \log \left(\frac{F_{RR_i}}{1 - F_{AR_i}} \right) \right]$$

$$\begin{aligned} u_g &= 1 \\ &\geq \log \left(\frac{C_{FA}}{2 - C_{FA}} \right) \\ u_g &= 0 \end{aligned} \quad (6)$$

where u_i is the local sensor decision (1 to accept identity or 0 to reject), u_g is the global decision, and N is the number

of sensors. There is a total of 2^{2^N} possible fusion rules for the sensors considering all possible combinations of the sensor decisions. The system designer selects a set of individual sensor operating points as well as error costs. Then based on these selections, the optimum fusion rule is obtained. The designer can modify the optimum rule by varying the cost and/or sensor operating point. Figure 2 illustrates the fusion process.

First, the fusion of the face and voice biometric sensor decisions are analyzed. There are 16 potential rules possible as depicted in Table II. Most of these rules do not improve performance [6] so that only the monotonic fusion rules need to be considered. The most commonly used rules are

f_2 (AND rule) and f_8 (OR rule). The NAND rule or f_9 is the worst performing rule and rarely be of interest. The f_1 rule simply allows no one in the building. This rule might be useful during emergencies but not as a general operating rule. Similarly, the f_{16} rule allows everyone in which may be used during open house events, etc., but again not for general usage. The system can be switched into single sensor operation by using the f_4 and f_6 rules.

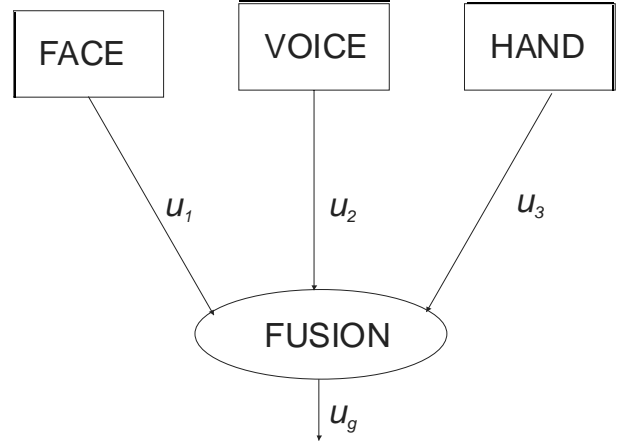


Figure 2. Illustration of Fusion of Three Biometric Sensors

TABLE II. Two Sensor Fusion Rules

u_1	u_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

u_1	u_2	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

In order to gain insight into the performance enhancements resulting from fusion, we present the global FAR and FRR as functions of the individual sensor FAR and FRR for

the AND and OR rules. The combined errors for the AND rule are

$$F_{AR} = F_{AR_1} F_{AR_2} \quad (7)$$

and

$$F_{RR} = F_{RR_1} + F_{RR_2} - F_{RR_1} F_{RR_2}. \quad (8)$$

This rule improves FAR while degrading the FRR. The degradation can be significant if the two sensors do not have a comparable degree of accuracy. The OR rule reverses this effect giving

$$F_{AR} = F_{AR_1} + F_{AR_2} - F_{AR_1} F_{AR_2} \quad (9)$$

and

$$F_{RR} = F_{RR_1} F_{RR_2}. \quad (10)$$

The ROCs for these two rules provide a comparison of the rules' performance. The OR rule ROC curve is steeper with lower FRR for the same high FAR values in Figure 3. Thus FAR does not improve but FRR does. Conversely, the AND rule ROC curve is flatter than for the OR rule indicating better FAR performance. An insight gained from this study is that the performance of one of the errors is constrained by the weakest sensor with only 2 biometric sensors. FAR or FRR can be improved through the fusion rule but both can still not be reduced simultaneously.

Thus, a third biometric sensor with comparable accuracy is introduced into the suite. The problem of analyzing all possible rules becomes more complex since there are potentially 256 fusion rules. Once again, however, most of these rules can be ignored since only 20 rules are monotonic. The ROC curves for 4 of these rules are presented in Figure 4. These curves clearly illustrate potential improvement in both error types. For added insight, a comparison is made between the ROCs for the AND rule and is given in Figure 5 as the number of sensors increases. For improvement in both error types, the ROC must shift from from the lower right to the upper left as shown for 1 to 3 sensors.

5 Impact of cost on rule selection

The system designer increases the impact of a particular type of error by changing the FAR cost in (5). The local decisions are first weighted by the accuracy of the sensor's current operating point and then compared with a threshold in (6). If the costs are equal, the threshold is 0. The threshold increases as the cost of FAR increases changing the optimal fusion rule to reduce the global FAR. The rule

selection process also accounts for the inherent accuracy of the sensor. This results in a table of optimal fusion rules as a function of FAR costs.

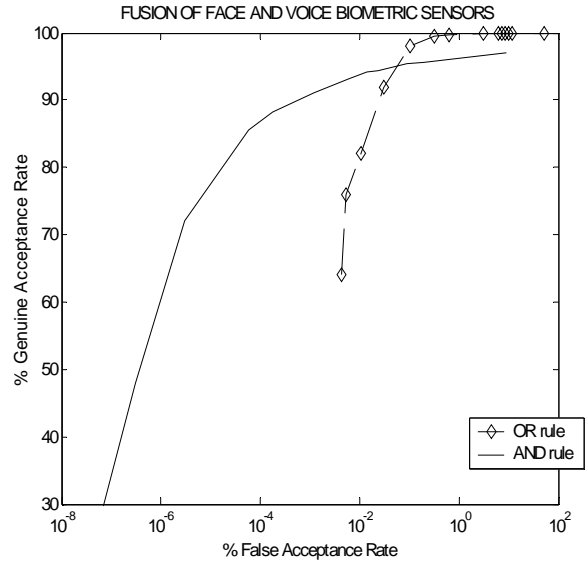


Figure 3. The ROC for Two Biometric Sensors

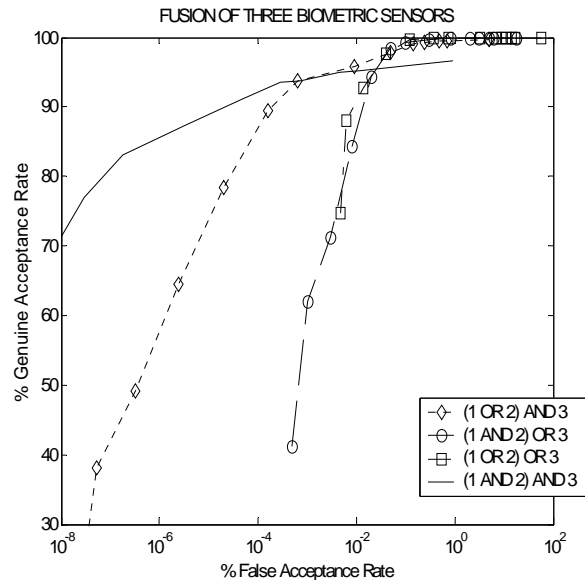


Figure 4. ROC Curves for Three Sensors

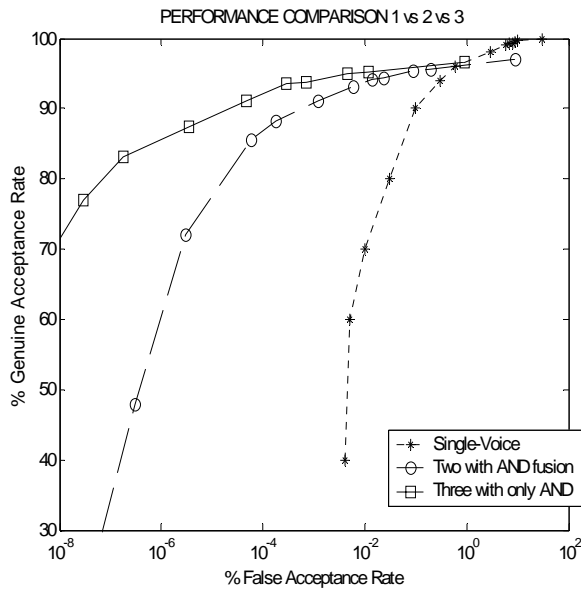


Figure 5. ROC Comparison for AND Rule

Insight into this process is gained by first considering the two sensor problem operating with the same FAR and FRR. It should be mentioned that this is not possible unless the sensors are identical. Logic leads one to conclude that if the FAR is more costly, the AND rule is optimal. If the FRR is more costly, the OR rule is optimal. Table III shows the optimal fusion rules from an analysis that considered all 6 of the monotonic rules for two sensors. There is a very small range of costs for which allowing everyone and rejecting everyone is optimal. The OR and AND rules transition at a cost equal to 1, i.e., when both errors are equally costly as expected.

TABLE III. Optimal Fusion Rules for Same Operating Point

($FAR_1=FRR_1=FAR_2=FRR_2=10\%$)

OPTIMAL FUSION RULE	RANGE OF COSTS
ALLONES	0-0.0024
OR	0.0024-1
AND	1-1.976
ALL ZEROS	1.976-2

A typical set of sensor operating points for the multimodal situation is summarized in Table IV. As indicated by the operating points, sensor 1 dominates FRR and has a poor FAR. Sensor 2 has better FAR values so the designer should use this to improve performance especially if FAR is more costly. This is accomplished through the AND rule as indicated by (7). The table indicates that the AND rule remains optimal for FAR costs down to .7752. Conversely, FRR has to become much more costly with FAR around .6172 before the OR rule becomes optimal. It is interesting to notice the small region of cost values for which sensor 1 should simply be ignored. The optimum fusion rule for FAR costs between .6172 and .7752 relies on only one sensor. Figure 6 presents the total error as a function of FAR cost. The lines cross at the points where the optimum rule switches.

Sensor 1 has a significantly lower FRR than sensor 2 but much higher FAR in Table V. Thus, the OR rule remains optimal even for cost values up to 1.3916. This prevents the FAR to be reduced unnecessarily by the AND rule as shown by comparing (7) and (9). It is interesting to see that once again there is a range of cost values for which sensor 2 decisions are used. This is a larger range of values. Thus, the operating points of the sensors should be carefully chosen in order to improve system accuracy. Figure 7 presents the total error for the fusion rules as a function of FAR cost for Table V.

A selected set of fusion rules are analyzed for three sensors in Table VI. This is a much more complicated situation. It is interesting to note that the two middle rules can be used interchangeably for certain cost values. This table does not summarize the entire set of rules but provides insight concerning the advantages of using three sensors. There are also cost regions where it is best to ignore 1 or 2 of the sensors as shown in the previous tables.

TABLE IV. Optimal Fusion Rules If One Sensor Dominates FRR

($FAR_1=9\%$ $FRR_1=0.6\%$ $FAR_2=1\%$ $FRR_2=4\%$)

OPTIMAL FUSION RULE	RANGES OF COSTS
ALL ONES	0-0.0005326
OR	0.0005326--0.6172
f_6	0.6172-0.7752
AND	0.7752--1.9982
ALL ZEROS	1.9982-2.0000

TABLE V. Optimal Fusion Rules If One Sensor Dominates FAR

($FAR_1=3\%$ $FRR_1=2\%$ $FAR_2=0.04\%$ $FRR_2=7\%$)

OPTIMAL FUSION RULE	RANGE OF COSTS
ALL ONES	0-0.0028
OR	0.0028-1.3916
f_6	1.3916-1.9592
AND	1.9592-2.0
ALL ZEROS	2.0

6 Conclusions

It is difficult to address all the human factor and performance issues using a single biometric modality. A multimodal biometric approach with an associated error cost gives the system designer flexibility to design a robust system and security adaptable system for a variety of building access applications. This paper presented a Bayesian framework from which optimal fusion rules are selected based on the biometric sensor operating points and FAR costs. It was also demonstrated in the paper that the biometric sensor operating point should be carefully chosen in order to achieve accuracy improvement through fusion.

The error cost included in the optimization process provides the system designer a tool for reducing FAR and thus increasing system security in real-time. The cost is incorporated at the fusion center. The designer can change the cost as the real-time situation changes. This may cause the optimum fusion rule to switch changing the system performance.

Thus, a system based on multimodal biometrics is more robust and adaptable. For users that experience problems with certain biometric acquisitions, the operating points and costs may be adapted. This allows the system to maintain the same level of security while servicing more of the population. The security level may be adapted during operation by simply changing the error cost. The multimodal biometric fusion using a Bayesian framework allows the system to better adapt to the changing security needs of the building as well as address the human factor issues of the general population.

TABLE VI. Optimal Fusion Rules for Three Biometric Sensors

($FAR_1=6\%$ $FRR_1=1\%$ $FAR_2=0.1\%$ $FRR_2=6\%$ $FAR_3=0.8\%$ $FRR_3=2\%$)

OPTIMAL FUSION RULE	RANGE OF COSTS
ONLY OR	$2.57 \cdot 10^{-5}$ -0.03917
(1 AND 2) OR 3	$2.57 \cdot 10^{-5}$ -0.14535
	0.3355-1.9836
	1.9934-1.99836
(1 OR 2) AND 3	0.33557-1.9836
	1.9934-1.99836
ONLY AND	1.99836-2

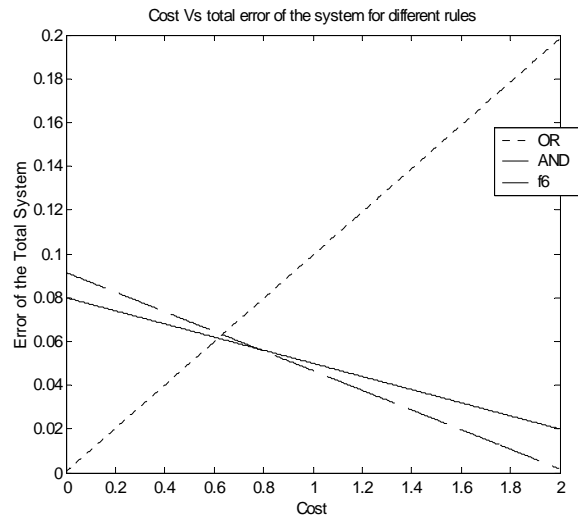


Figure 6. Cost Vs Total Error for the operating point in Table IV

- [7] Pramod K. Varshney , Distributed Detection and Data Fusion, Springer, New York,1997.

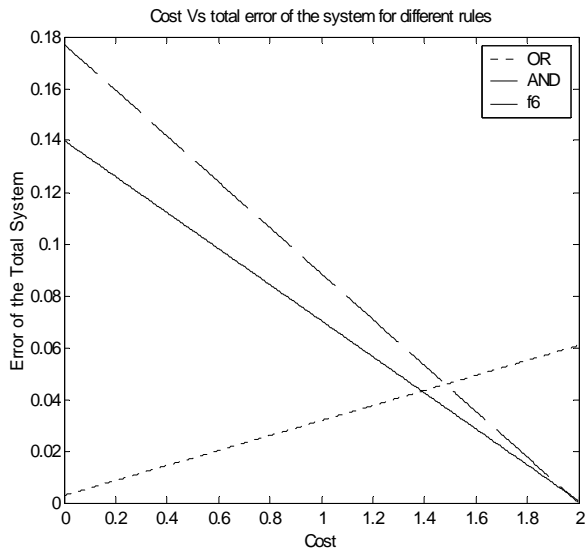


Figure 7. Cost Vs Total Error for the operating point in Table V

7 References

- [1] Tony Mansfield, Gavin Kelly, David Chandler, and Jan Kane, Biometric Product Testing Final Report, Computing, National Physical Laboratory, Crown Copyright, UK, March, 2001.
- [2] Steven King, "Personal Identification Pilot Study," The Biometrics Consortium Conference 2002, Arlington Virginia, February, 2002.
- [3] Lin Hong and Anil Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, Dec., 1998, pp. 1295 - 1307.
- [4] Salil Prabhakar and Anil Jain, "Decision-level Fusion in Fingerprint Verification", Pattern Recognition, vol. 35, 2002, pp. 861-874.
- [5] Steven M. Kay, Fundamentals of Statistical Signal Processing: Detection Theory, Vol. II, Prentice-Hall, Inc., 1998.
- [6] Ramanarayanan Viswanathan and Pramod K. Varshney, "Distributed Detection With Multiple Sensors: Part I - Fundamentals", Proceedings of the IEEE, Vol. 85, No. 1, Jan., 1997, pp. 54 - 63.