This CVPR2013 Workshop paper is the Open Access version, provided by the Computer Vision Foundation.
The authoritative version of this paper is available in IEEE Xplore.

On Controlling Genuine Reject Rate in Multi-stage Biometric Verification

Md S. Hossain
Louisiana Tech University
Ruston, LA 71270
msh040@latech.edu

Kiran S. Balagani
New York Institute of Technology
Old Westbury, NY 11568
kbalagan@nyit.edu

Vir V. Phoha
Louisiana Tech University
Ruston, LA 71270
phoha@latech.edu

Abstract

An important problem in multi-stage biometric verification is to select an appropriate reject region. A reject region says which samples to be rejected. Rejecting impostor samples does not incur any cost in terms of user inconvenience, however, erroneously rejecting genuine samples leads to both user and administrator inconvenience. The problem becomes severe in the applications that involve a huge number of biometric transactions. Such applications necessitate the reject rate of genuine samples to be controlled. However, to date, no work has studied on controlling genuine reject rate (GRR) in multi-stage biometric verification. In this paper, we focused on controlling GRR and to this end, developed a rejection method called symmetric rejection method.

Our rejection method adds the following benefits to multi-stage biometric verification: (1) it enables the system administrator to control GRR, (2) it allows to calculate the reject region without estimation of score distributions, and (3) it does not use any assumption on the functional form of score distributions. We performed experiments on (1) two fingerprint datasets of 6000 users and (2) two face datasets of 3000 users. For fingerprint data, we achieved 18.96 percent to 70.89 percent reduction in EER by rejecting 1.5 percent to 9.4 percent genuine scores and for face data, we achieved 3.27 percent to 85.83 percent reduction in EER by rejecting 0.3 percent to 14.4 percent genuine scores.

1. Introduction

In an n-stage biometric verification system (*e.g.*, [11], [10], [2], [3], [16], and [12]), if the verifier in stage i is not confident enough to decide whether the sample is genuine or impostor, the sample is *rejected* and a new sample is submitted to the verifier in stage $i+1$ to get a more confident decision. If all the verifiers in stages 1 through $n-1$ fail to give a genuine or impostor decision, the verifier in stage n (last stage) gives the final decision. The option to reject the 'confusing' samples by the verifiers in stages 1 through $n-1$ is called *reject option* (see [5], [7], [17], [15], and [4]), which builds the skeleton of a multi-stage biometric verification system.

Reject option is exercised by selecting a reject region that says which samples to be rejected. Typically, a reject region consists of two reject thresholds A and C such that $A < C$. The sample is rejected if the corresponding score (in studies [11] and [10]) or corresponding probability ratio (in studies [3], [16], and [12]) falls inside the reject region AC. Based on the location and width of the reject region, different reject regions can reject different number of scores and yield different error rates. This phenomenon poses the challenge– how to select an appropriate reject region?

A reject region rejects both genuine and impostor scores. Rejecting impostor scores incurs no cost in terms of user inconvenience. However, erroneously rejecting genuine scores leads to both user and administrator inconvenience. The problem becomes severe in the applications that involve a huge number of users or biometric transactions. In such applications, selecting an *inappropriate* reject region (that yields huge genuine score rejection) can render the verifier impractical. Therefore, it is necessary to control the reject rate of genuine scores in each stage of multi-stage biometric verification.

However, to the best of our knowledge, no work has studied on controlling genuine (score) reject rate in multi-stage biometric verification. Rejection methods proposed in [11], [10], and [2] use the *whole* confusion region as the reject region. Using the whole confusion region as the reject region has two major drawbacks: 1) it rejects a large number of genuine scores, which causes severe user and administrator inconvenience and 2) by rejecting all scores inside the confusion region, it treats every score inside the confusion region in the same manner, however, the probability of a score being genuine or impostor is not same in every part of the confusion region. Rejection methods proposed in [3] and [16] calculate the reject region based on sequential probability ratio test (see [18]) and rejection method in [12] calculates the reject region based on minimum log-likelihood

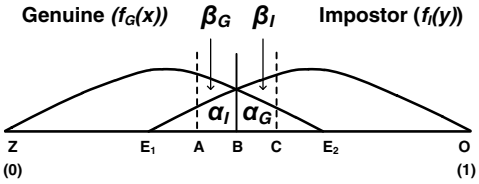


Figure 1. Illustration of symmetric rejection. AC is the symmetric reject region, ZE_2 is the genuine score region, E_1O is the impostor score region, E_1E_2 is the confusion region, and B is the threshold where EER occurs before exercising reject option.

ratio. Rejection methods in [3], [16], and [12] have the following two drawbacks: 1) they assume that biometric samples are independent, which may not be true in practice (see [13] and [6]) and 2) they calculate reject region by estimating score distributions, which is an expensive and difficult task (see [8] and [14]).

In this paper, we focused on controlling the genuine reject rate (GRR) in multi-stage biometric verification. To this end, we developed a rejection method, referred to as "Symmetric Rejection Method", to determine the reject region. Symmetric rejection method enables the system administrator to 1) control the genuine reject rate at each stage and 2) determine the reject region without estimation of genuine and impostor score densities.

We evaluated the performance of symmetric rejection method by experimenting on two biometric modalities: fingerprint and face, where each modality contains two different training sets and testing sets. In experiments, symmetric rejection method shows significant promise in reducing error rates.

Rest of the paper is organized as follows. In Section 2, we describe the proposed symmetric rejection method. In Section 3, we describe experiments and corresponding results. Finally, we conclude in Section 4 giving our future research direction.

2. Symmetric Rejection Method

Let X be the genuine score set and Y be the impostor score set generated by the verifier V for user U. Let $f_G(x)$ and $f_I(y)$ be the distributions estimated from scores in X and Y respectively. Without loss of generality, we assume that 1) verifier V outputs dissimilarity scores (and hence genuine scores are typically expected to have smaller values than impostor scores) and 2) the scores lie in the interval $[0, 1]$. Fig. 1 illustrates $f_G(x)$ and $f_I(y)$ on the scoreline $[0, 1]$. In the scoreline, ZE_2 is the genuine score region, E_1O is the impostor score region, E_1E_2 is the confusion region where $f_G(x)$ and $f_I(y)$ overlap, and B is the threshold where EER occurs before exercising reject option.

Below, we introduce some notation to describe the symmetric rejection method. Let PQ be a region in the scoreline. Then

- $N_{G,PQ}$ is the number of genuine scores in PQ.
- $N_{I,PQ}$ is the number of impostor scores in PQ.
- $N_{G,Total}$ is the total number of genuine scores.
- $N_{I,Total}$ is the total number of impostor scores.
- $P_{G,PQ}$ is the proportion of genuine scores in PQ, calculated by $\frac{N_{G,PQ}}{N_{G,Total}}$.
- $P_{I,PQ}$ is the proportion of impostor scores in PQ, calculated by $\frac{N_{I,PQ}}{N_{I,Total}}$.

Symmetric rejection method: Select a reject region AC (see Fig. 1) in the scoreline $[0, 1]$ such that–

$$P_{G,BC} = P_{I,AB} \tag{1}$$

where $A \in [E_1, B)$ and $C \in (B, E_2]$. That is, the proportion of genuine scores in BC is equal to the proportion of impostor scores in AB. AC is called the symmetric reject region. Here B is the threshold where EER occurs before exercising reject option and E_1E_2 is the confusion region.

Below, we introduce some symbols corresponding to symmetric rejection:

$$\begin{array}{|ccc|}\hline \alpha_G = P_{G,BC} & \beta_G = P_{G,AB} & \lambda_G = P_{G,BE_2} \\ \alpha_I = P_{I,AB} & \beta_I = P_{I,BC} & \lambda_I = P_{I,E_1B} \\ \hline \end{array}$$

Then, the probability of a genuine score being rejected, genuine reject rate (GRR) can be computed as follows:

$$\text{GRR} = P_{G,AC} = \alpha_G + \beta_G. \tag{2}$$

Note that GRR is a function of α_G. When the value of α_G is zero, β_G is also zero. Therefore, no scores are rejected and GRR is zero (which is minimum). When the value of α_G is equal to λ_G, β_G is equal to P_{G,E_1B}. Therefore, all scores inside the confusion region are rejected and GRR is equal to $\lambda_G + P_{G,E_1B}$ (which is maximum). Hence we can control GRR by setting the value of α_G. Algorithm 1 shows how to calculate symmetric rejection region AC for a given α_G that gives GRR equal to $\alpha_G + \beta_G$.

In Algorithm 1, note that symmetric reject region AC is calculated directly from genuine and impostor scores (see steps 14-15), without estimating score densities.

Note–In algorithm 1, we use a function $funcOriginalEER(G, I)$ which calculates the EER before exercising reject option given array of genuine scores G and array of impostor scores I. Because the calculation of EER before exercising reject option is trivial, we did not give details of this function.

Algorithm 1 Algorithm to find a symmetric reject region.

Input: $G[1:M]$: array of M genuine scores,
$I[1:N]$: array of N impostor scores, and
α_G: proportion of genuine scores that can be erroneously rejected by region BC in Fig. 1.
Output: Symmetric reject region AC

1: $EER_{original} \leftarrow funcOriginalEER(G, I)$; /*$funcOriginalEER(G, I)$ is a function which calculates the EER before exercising reject option. Variable $EER_{original}$ stores the calculated EER.*/
2: $\lambda_G \leftarrow EER_{original}$;/*From Fig 1, $\lambda_G = P_{G,BE_2}$, which is EER before exercising reject option.*/
3: $\lambda_I \leftarrow EER_{original}$;/*From Fig 1, $\lambda_I = P_{I,E_1B}$, which is EER before exercising reject option.*/
4: $G_{sorted}[1:M] \leftarrow$ sorted $G[1:M]$;
5: $I_{sorted}[1:N] \leftarrow$ sorted $I[1:N]$;
6: $Gen_{BE_2} \leftarrow (M * \lambda_G)$; /*Calculate the number of genuine scores in BE_2.*/
7: $Imp_{E_1B} \leftarrow (N * \lambda_G)$; /*Calculate the number of impostor scores in E_1B.*/
8: $GenIndexCut = M - Gen_{BE_2}$; /* Genuine scores stored in $G_{sorted}[1 : GenIndexCut]$ are declared as genuine before exercising reject option.*/
9: $ImpIndexCut = Imp_{E_1B} + 1$; /* Impostor scores stored in $I_{sorted}[ImpIndexCut : N]$ are declared as impostor before exercising reject option.*/
10: $Gen_{BC} = M * \alpha_G$; /*Calculate the number of genuine scores in BC.*/
11: $Imp_{AB} = N * \alpha_G$; /*Calculate the number of impostor scores in AB.*/
12: $IndexRight = GenIndexCut + Gen_{BC}$; /*Variable $IndexRight$ stores the index of the right threshold C in G_{sorted}.*/
13: $IndexLeft = ImpIndexCut - Imp_{AB}$; /*Variable $IndexLeft$ stores the index of the left threshold A in I_{sorted}.*/
14: $A \leftarrow I_{sorted}[IndexLeft]$; /*Get the value of A.*/
15: $C \leftarrow G_{sorted}[IndexRight]$; /*Get the value of C.*/
16: **return** AC;

3. Performance Evaluation with Fingerprint and Face Biometrics

We evaluated the performance of symmetric rejection method on a public database, namely, NIST-BSSR1 [1], [9]. NIST-BSSR1 database consists of three datasets– 1) NIST-Fingerprint-Face, 2) NIST-Fingerprint, and 3) NIST-Face. We experimented on NIST-Fingerprint and NIST-Face datasets. NIST-Fingerprint is comprised of fingerprint scores from one system run on images of 6000 individuals. For each individual, the set contains one score from the comparison of two left index fingerprints and another from two right index fingerprints. NIST-Face is comprised of scores from two face systems (C and G) run on images from 3000 individuals. For each individual, the set contains one score from the comparison of face X with a later face, Y, and a score from face X and another later face, Z. The two datasets used in our study are summarized in Table 1.

We did experiment separately for left index fingerprints, right index fingerprints, face scores from matcher C, and face scores from matcher G. Recall, we assume that the verifier or matcher outputs dissimilarity scores which lie in the interval $[0, 1]$. However, the scores in NIST-Fingerprint and NIST-Face datasets are similarity scores and lie in different interval. Hence, to keep consistency in the experiments, we converted the similarity scores into dissimilarity scores and normalized the scores so that they lie in the interval $[0, 1]$. We used min-max normalization in our experiments.

For each experiment, scores from the first half users were used in training and scores from the rest half users were used in testing. We experimented with 20 different symmetric regions (ACs), obtained from the training set of genuine and impostor scores. We applied each symmetric reject region AC on the testing set and calculated corresponding equal error rates (EERs) and genuine reject rates (GRRs).

How we selected 20 ACs: We selected 20 different symmetric regions (ACs) by varying the value of α_G, from zero to λ_G. Recall that when the value of α_G is zero, no scores are rejected, which is the minimum rejection, and when the value of α_G is equal to λ_G, all scores in the confusion region are rejected, which is the maximum rejection. We set the initial value of α_G to zero. Then we increment the value α_G 20 times, each time by $\frac{\lambda_G}{20}$.

Performance metrics: We evaluated the symmetric rejection method using EER versus GRR trade-off curves that plot GRRs on the x-axis and corresponding EERs on the y-axis. Moreover, we plotted percentage reduction in EER versus GRR curves to show the performance improvement in terms of reduction in equal error rate.

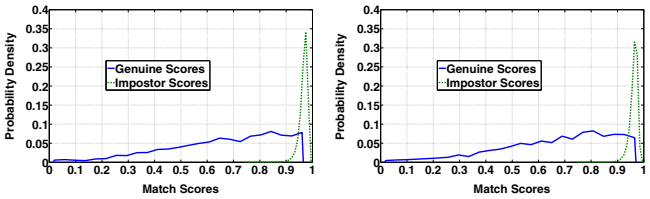
For comparative study, besides applying each symmetric reject region AC on the testing set, we apply each symmetric reject region AC on the training set. We consider the EER-GRR trade-off curve obtained from the training set as the expected trade-off curve and see how much the EER-GRR curve obtained from the testing set deviate from the expected one. Low deviation indicates high promise of the symmetric rejection method in the tested biometric modality.

3.1. Results of Fingerprint Dataset

Fig. 2 and Fig. 3 show the distributions of genuine and impostor scores for left index finger and right index finger respectively. Distributions in Fig. 2a and Fig. 3a represent training sets and distributions in Fig. 2b and Fig. 3b repre-

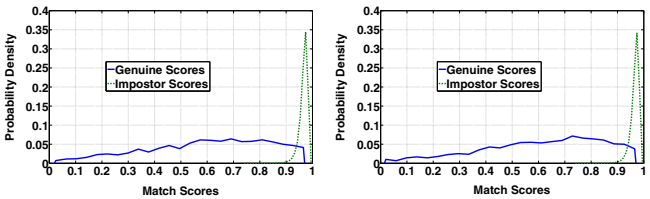
	NIST-Fingerprint		NIST-FACE	
	Left Index	Right Index	Matcher C	Matcher G
No. of users	6000	6000	3000	3000
Total genuine scores	6000*1	6000*1	3000*2	3000*2
Total impostor scores	6000*5999	6000*5999	3000*5998	3000*5998

Table 1. Summary of NIST-Fingerprint and NIST-Face datasets.



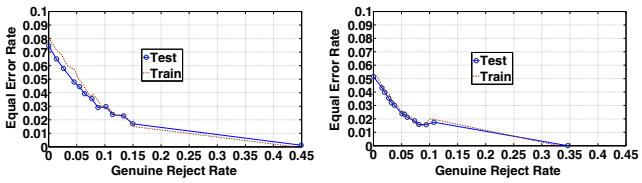
(a) Training set (b) Testing set

Figure 2. Distribution of genuine and impostor scores for left index finger. (a) Distribution for training dataset. (b) Distribution for testing dataset.



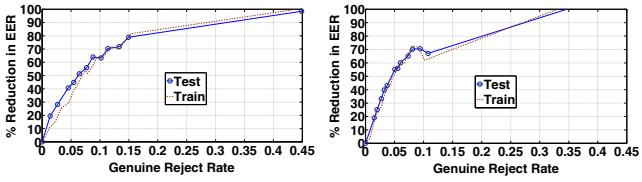
(a) Training set (b) Testing set

Figure 3. Distribution of genuine and impostor scores for right index finger. (a) Distribution for training dataset. (b) Distribution for testing dataset.



(a) Left index finger (b) Right index finger

Figure 4. EER-GRR trade-off curve obtained by symmetric rejection method on NIST-Fingerprint dataset.



(a) Left index finger (b) Right index finger

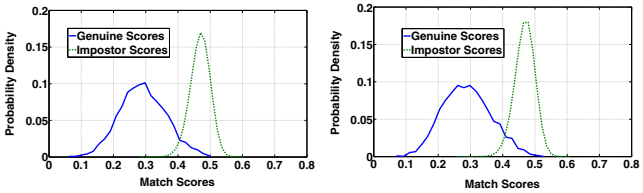
Figure 5. Percentage reduction in EER vs. GRR curve obtained by symmetric rejection method on NIST-Fingerprint dataset.

sent testing sets. We observe that 1) for both left and right index fingers, distributions of training and testing sets are almost same, which indicates that the training sets are good representatives of the testing sets and 2) proportion of genuine and impostor scores in the confusion regions for left index finger is higher than that for right index finger.

Fig. 4 shows the EER-GRR trade-off curves, when symmetric rejection was applied on NIST-Fingerprint dataset. Fig. 4a shows the results for left index finger and Fig. 4b shows the results for right index finger. In each figure we plotted two curves: one curve is generated from testing score distribution and the other curve is generated from training score distribution. Our observations from Fig. 4 are listed below.

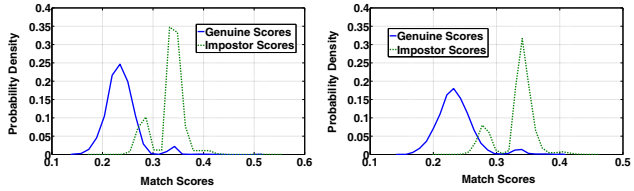
- *Observation 1:* EER-GRR trade-off curves obtained from training data and testing data are almost same for both left and right index fingers. These results reflect that the training data are representatives of test data.
- *Observation 2:* EER decreases monotonically with the increase of GRR (except for GRR value 0.11 in right index finger dataset). For testing data of left index finger, EER decreases from 0.075 to 0.017, when GRR increases from 0 to 0.15. For testing data of right index finger, EER decreases from 0.052 to 0.0156, when GRR increases from 0 to 0.09.
- *Observation 3:* The last stepsize of GRR is very high in all cases (for example, in case of left index finger, the last step of GRR is from 0.15 to 0.45). This is because of how we chose the symmetric reject regions (ACs). Recall, we selected 20 different (ACs), by varying the value of α_G, from zero to λ_G. We incremented α_G by equal step size of $\frac{\lambda_G}{20}$. However, because the tail of the impostor score distribution is monotonically increasing, in each step, the increment of β_G is higher than the previous step. As a consequence, in each step, the increment of GRR ($\alpha_G + \beta_G$) is higher than the previous step. Therefore, in the last step the increment of GRR is very high.

Performance improvement: Fig. 5 shows that the percentage reduction in EER achieved with symmetric rejection in comparison to the EER without reject option. For left index finger, symmetric rejection achieved from 19.51 percent to 78.92 percent reduction in EER, when GRR varies from 0.0138 to 0.149 (*i.e.*, with 1.38 percent to 14.9 percent genuine score rejection). For right index finger, symmetric rejection achieved from 18.96 percent to 70.89 percent reduction in EER, when GRR varies from 0.015 to



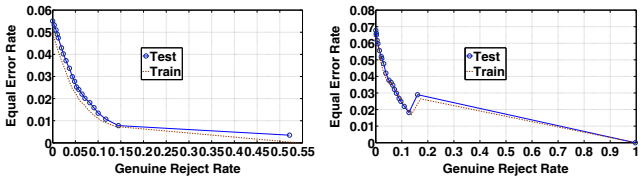
(a) Training set (b) Testing set

Figure 6. Distribution of genuine and impostor scores for face matcher C. (a) Distribution for training dataset. (b) Distribution for testing dataset.



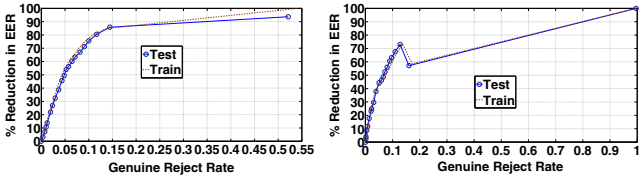
(a) Training set (b) Testing set

Figure 7. Distribution of genuine and impostor scores for face matcher G. (a) Distribution for training dataset. (b) Distribution for testing dataset.



(a) Matcher C (b) Matcher G

Figure 8. EER-GRR trade-off curve obtained by symmetric rejection method on NIST-Face dataset.



(a) Matcher C (b) Matcher G

Figure 9. Percentage reduction in EER vs. GRR curve obtained by symmetric rejection method on NIST-Face dataset.

0.094 (*i.e.*, with 1.5 percent to 9.4 percent genuine score rejection). These results indicate that symmetric rejection is promising because percentage reduction in EER is very high where the corresponding percentage genuine score rejection is very low.

3.2. Results of Face Dataset

Fig. 6 and Fig. 7 show the distributions of genuine and impostor scores obtained by face matcher C and face matcher G. Distributions in Fig. 6a and Fig. 7a represent training sets and distributions in Fig. 6b and Fig. 7b represent testing sets. We observe that 1) for both matchers C and G, distributions of training and testing sets are almost same, which indicates that the training sets are good representatives of the testing sets, 2) proportion of genuine and impostor scores in the confusion regions for matcher C is less than that for matcher G, and 3) both genuine and impostor score distributions for matcher G are multi-modal.

Fig. 8 shows the EER-GRR trade-off curves, when symmetric rejection was applied on NIST-Face dataset. Fig. 8a shows the results for matcher C and Fig. 8b shows the results for matcher G. In each figure we plotted two curves: one curve is generated from testing score distribution and the other curve is generated from training score distribution. Our observations from Fig. 8 are listed below.

- *Observation 1:* EER-GRR trade-off curves obtained from training data and testing data are almost same for both matchers C and G. These results reflect that the training data are representatives of the testing data.
- *Observation 2:* EER decreases monotonically with the increase of GRR (except for GRR value 0.16 in matcher G dataset). For testing data obtained by matcher C, EER decreases from 0.055 to 0.007, when GRR increases from 0 to 0.144. For testing data obtained by matcher G, EER decreases from 0.067 to 0.018, when GRR increases from 0 to 0.127.
- *Observation 3:* The last stepsize of GRR is very high. The reason is same as in fingerprint.

Performance improvement: Fig. 9 shows that the percentage reduction in EER achieved with symmetric rejection in comparison to the EER without reject option. For matcher C, symmetric rejection achieved from 3.27 percent to 85.83 percent reduction in EER, when GRR varies from 0.003 to 0.144 (*i.e.*, with 0.3 percent to 14.4 percent genuine score rejection). For matcher G, symmetric rejection achieved from 2.52 percent to 73.04 percent reduction in EER, when GRR varies from 0.002 to 0.127 (*i.e.*, with 0.2 percent to 12.7 percent genuine score rejection). Similar to fingerprint, these results indicate that symmetric rejection is promising in face biometric modality.

4. Conclusion

In this paper, we developed a rejection method, called symmetric rejection method, which rejects equal proportion of genuine scores and impostor scores. Assuming dissimilarity scores, symmetric rejection method takes the EER-threshold (the threshold where equal error rate occurs before exercising reject option) as the center, and rejects a certain proportion of genuine scores from the right side of the EER-threshold, and at the same time, rejects the same proportion of impostor scores from the left side of the EER-threshold (and vice versa for similarity scores).

The symmetric rejection method advances the state-of-art as follows: 1) it enables to control the proportion of genuine scores to be rejected and 2) it enables to calculate the reject region directly from scores (see Algorithm 1, steps 14-15), without estimation of score distributions. Moreover, because symmetric rejection method does not use any assumption on the score distributions, it is applicable to all kinds of biometric modalities. As a consequence, in case of *multi-modal* multi-stage biometric verification systems, where different stages use different biometric modalities, symmetric rejection method appears to be more appropriate than conventional rejection methods, which depend on particular data-distributions.

We evaluated the performance of symmetric rejection method by experimenting on two biometric modalities: fingerprint and face, where fingerprint dataset contains scores from two different fingers: left index finger and right index finger and face dataset contains scores generated by two different matchers: C and G. We used a public-domain database, namely, NIST-BSSR1 [1] to create the training and testing sets. Experimental results show that for all testing sets, the symmetric rejection method performs very well in terms of EER-GRR trade-off curves. For fingerprint data, we achieved 18.96 percent to 70.89 percent reduction in EER by rejecting only 1.5 percent to 9.4 percent genuine scores. For face data, we achieved 3.27 percent to 85.83 percent reduction in EER by rejecting only 0.3 percent to 14.4 percent genuine scores.

As future work, we will study how symmetric rejection method works in other biometric modalities. Further, we will study its usability in non-biometric data, for example, how it performs in anomaly detection problem. We are also interested, in our future work, to study the optimality of symmetric rejection method.

5. Acknowledgment of Support

This work was supported in part by DARPA Active Authentication grant FA8750-12-2-0201 and P-KSFI grant LEQSF (2007-12)-ENHPKSFI-PRS-03. The views, findings, recommendations, and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the sponsoring agencies or the U.S. Government.

References

[1] http://www.nist.gov/itl/iad/ig/biometricscores.cfm.

[2] Z. Akhtar, G. Fumera, G. Marcialis, and F. Roli. Evaluation of serial and parallel multibiometric systems under spoofing attacks. In *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*, pages 283 –288, sept. 2012.

[3] L. Allano, B. Dorizzi, and S. Garcia-Salicetti. Tuning cost and performance in multi-biometric systems: A novel and consistent view of fusion strategies based on the sequential probability ratio test (sprt). *Pattern Recogn. Lett.*, 31(9):884–890, July 2010.

[4] P. L. Bartlett and M. H. Wegkamp. Classification with a reject option using a hinge loss. *J. Mach. Learn. Res.*, 9:1823–1840, June 2008.

[5] C. K. Chow. On optimum recognition error and reject tradeoff. *Information Theory, IEEE Transactions on*, 16(1):41–46, jan 1970.

[6] S. Dass, Y. Zhu, and A. Jain. Validating a biometric authentication system: Sample size requirements. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 28(12):1902 –1319, dec. 2006.

[7] G. Fumera, F. Roli, and G. Giacinto. Reject option with multiple thresholds. *Pattern Recognition*, 33:2099–2101, 2000.

[8] M. Girolami and C. He. Probability density estimation from optimally condensed data samples. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(10):1253–1264, Oct. 2003.

[9] A. Kumar and S. Shekhar. Personal identification using multibiometrics rank-level fusion. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 41(5):743–752, 2011.

[10] G. Marcialis, P. Mastinu, and F. Roli. Serial fusion of multimodal biometric systems. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010 IEEE Workshop on*, pages 1 –7, sept. 2010.

[11] G. L. Marcialis, F. Roli, and L. Didaci. Personal identity verification by serial fusion of fingerprint and face matchers. *Pattern Recognition*, 42(11):2807 – 2817, 2009.

[12] T. Murakami, K. Takahashi, and K. Matsuura. Towards optimal countermeasures against wolves and lambs in biometrics. In *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*, pages 69 –76, sept. 2012.

[13] K. Nandakumar, Y. Chen, S. C. Dass, and A. Jain. Likelihood ratio-based biometric score fusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30:342–347, 2008.

[14] S. Prabhakar and A. K. Jain. Decision-level fusion in fingerprint verification. *Pattern Recognition*, 35:861–874, 2001.

[15] C. M. Santos-Pereira and A. M. Pires. On optimal reject rules and roc curves. *Pattern Recogn. Lett.*, 26:943–952, May 2005.

[16] K. Takahashi, M. Mimura, Y. Isobe, and Y. Seto. A secure and user-friendly multimodal biometric system. *Proceedings of the SPIE*, 5404:12–19, 2004.

[17] F. Tortorella. An optimal reject rule for binary classifiers. In *Proceedings of the Joint IAPR International Workshops on Advances in Pattern Recognition*, pages 611–620, London, UK, 2000. Springer-Verlag.

[18] A. Wald. *Sequential Analysis*. John Wiley and Sons, 1st edition, 1947.