

Robustness of Multi Biometric Authentication Systems against Spoofing

Mahdi Hariri (Corresponding author)

Electrical Engineering Department

Iran University of Science and Technology (IUST)

Narmak, Hengam Ave

Tehran 16846, Iran

E-mail: mahdi_hariri@iust.ac.ir

Shahriar B. Shokouhi

Electrical Engineering Department

Iran University of Science and Technology (IUST)

Tehran 16846, Iran

Tel: 98-21-7322-5614 E-mail: bshokouhi@iust.ac.ir

Received: October 2, 2011

Accepted: November 14, 2011

Published: January 1, 2012

doi:10.5539/cis.v5n1p77

URL: <http://dx.doi.org/10.5539/cis.v5n1p77>

Abstract

Nowadays biometric authentication systems have been more developed, especially in secure and financial systems; so cracking a biometric authentication system is now a growing concern. But their security has not received enough attention. Imitating a biometric trait of a genuine user to deceive a system, spoofing, is the most important attacking method. Multi biometric systems have been developed to overcome some weaknesses of single biometric systems because the forger needs to imitate more than one trait. No research has further investigated the vulnerability of multimodal systems against spoof attack. We empirically examine the robustness of five fixed rules combining similarity scores of face and fingerprint traits in a bimodal system. By producing different spoof scores, the robustness of fixed combination rules is examined against various possibilities of spoofing. Robustness of a multi biometric system depends on the combination rule, the spoof trait and the intensity of spoofing. Min rule shows the most robustness when face is spoofed especially in very secure systems but when the fingerprint is faked the max rule shows the least vulnerability against possibilities of spoofing.

Keywords: Vulnerability, Multi biometric, Spoof attack possibilities, Fixed combination rules

1. Introduction

Automatic personal identification has received its position as an urgent need in many social activities. Nowadays biometric authentication systems have been presented as the best identification methods, using biometric traits of a person (Prabhakar & Jain, 2002). Variety of biometric modalities and their special benefits has resulted in their development in many social activities especially in secure and financial systems such as international airports and bank accounts. At first spoofing a biometric system seemed hard and impossible that their robustness was not taken into consideration. But development of technology and general application of biometric authentication systems encourage fraudulent imposters and terrorists to crack the protected systems, especially in secure and financial applications. Spoofing attack is the major and the most common threat to biometric systems.

Based on the research of Rodriguez (Rodrigues, Ling, & Govindaraju, 2009) "the hypothesis that an imposter may spoof a biometric trait is not considered in any proposed fusion method thus far". Multi biometric systems have been proposed to alleviate some problems of unimodal systems such as vulnerability against spoofing toward improving their performance and accuracy (Bubeck & Sanchez, 2003).

These systems attempt to fuse the information obtained from different biometric traits, matchers and snapshots (Bergamini, Oliveira, Koerich, & Sabourin, 2009; Hong, Jain, & Pankanti, 1999). Several studies have shown

that better performance can be expected if various information from multiple biometric traits is fused (Ulery, Hicklin, Watson, Fellner, & Hallinan, 2006). Fusion can be done at all main levels of a biometric system: sensor level, feature extraction level, (ISO & IEC19792, 2009) (3) matching score level and (4) decision making level. Fusion in matching score level is generally preferred, because access to matching scores and combining them seem feasible and applicable (Dass, Nandakumar, & Jain, 2005; Kang & Park, 2009; Ulery *et al.*, 2006). We integrate the matching scores of face and fingerprint biometric matchers in score level to produce bimodal multi biometric systems.

Rodrigues mentioned that successful spoofing of only one matcher in a multi biometric system may increase the vulnerability of the system to be cracked. This note in security field needs more investigation which has not more examined in the mentioned research. Since the relationships between the robustness of multi modal authentication systems and the intensity of spoofing their traits have not been discussed yet, this problem motivated us to investigate the vulnerability of multi biometric systems against the various qualities of spoofing. In (Hariri & Shokouhi, 2011) for the first time we examined the vulnerability of multimodal biometric systems against various intensities of spoofing. We proposed the simulation success rate of a biometric trait as the possibility of spoofing and introduced it with 'k' parameter. Investigating the robustness of biometric systems from this point of view has not been considered thus far.

Many multi biometric systems have been presented by different combination methods and strategies in order to reach more precise operation and recognition rates. Some of these studies (Fox, Gross, Cohn, & Reilly, 2007; He *et al.*, 2010; Monwar & Gavrilova, 2008; Wang & Han, 2008) involve robustness and security of authentication systems. In most studies, the researchers have considered the security from the viewpoint of attempt to decrease both FAR and FRR error rates by applying various identification methods and increasing the number of traits (from 2 to 3); without any major study on importance of robustness for a biometric system against attacks.

In this paper we practically try to examine the robustness of multimodal systems against spoofing. Performance evaluation is conducted on five fixed score level fusion techniques: sum rule, product rule, Bayesian rule, minimum (min) rule and maximum (max) fusion rule. These rules are called fixed rules because they do not have the training phase. Because the data base of spoof traits does not exist, we simulate the spoof scores of applying fake samples to a biometric matcher. We use similarity scores of a true multimodal dataset for this aim.

The rest of the paper is organized as follows. In Section 2, we introduce the spoof attack, and propose a novel method for simulation of matching scores with various possibilities of spoofing a biometric matcher. Section 3 is dedicated to the methodology of experiment, fusion in score level and criterion for comparing the vulnerability of experimental systems. Observations and results are stated in section 4 and finally, we will present the conclusion of this research in section 5.

2. Spoof Attack

Absolute security does not exist. Given funding, opportunity and the proper technology, every secure system can be compromised. A generic biometric system can be attacked from 8 points which are depicted in Figure 1 (Ratha, Connell, & Bolle, 2001).

Spoofing attack behaves as a direct attack to the sensor level of a system (A.K. Jain, Nandakumar, & Nagar, 2008). These threats, corresponding to type 1 in Figure 1, are applied to the sensor trying to gain access to the system by impersonating a real user. When a fraudulent imposter attempts to apply a fake physiological biometric trait (e.g., fingerprint, iris, face) of a legitimately registered user to the sensor of an authentication system in order to circumvent the system, this process is known as spoofing, like gummy finger, high quality iris or face image; and when the biometric systems are based on behavioral traits (i.e. signature, voice) these type of approaches are known as mimicry. In These types of attacks, imposter needs no knowledge about the biometric system. Therefore spoofing attack becomes the most common threat to the biometric system.

2.1 Simulation of Possibilities of Spoof Attack

In the presence of a spoof attack, a forger tries to simulate a copy of genuine trait and apply it to the sensor of the system. It is obvious that the more this imitative copy becomes similar to the original one, the more the matcher produces similarity score closer to the genuine score. It seems that for a trait, the scatter plot of its imposter scores shifts toward the scatter plot of its genuine scores. So, in this simulation step, we gradually transfer the scatter plot of imposter scores toward the scatter plot of genuine scores in ten steps. We introduce this ability of simulation as possibility of spoofing. At first for each matcher, differences between genuine and imposter scores are divided into 10 equal slices. Then they are added to each standard imposter scores in ten steps to show various possibilities of spoof attack (Hariri & Shokouhi, 2011).

$$S_{Spoof} = S_{imposter} + k(S_{genuine} - S_{imposter}) \quad k \in [0.1, 0.2, \dots, 1]$$

Equation 1. Various possibilities of simulation of spoof scores for each matcher.

"k" parameter denotes the intensity of spoofing, as coefficient of possibility, which indicates the accuracy of simulation. We use it in the percentage form, so 10%, 20%... are used instead of 0.1, 0.2, ... , k=0% denotes nonspoofed state. For under spoofing matchers, primary imposter scores in standard state are randomly replaced by simulated spoofed scores with various possibilities.

Figure 2 presents samples of this simulation process, where scatter plot variations of imposter scores for C face and RI fingerprint matchers occur against various possibilities of spoofing. These possibilities indicate the intensities of spoof attack to a biometric trait which vary from 0%, without attack, to 100%, complete simulation of authorized traits. In the worst spoof state (step 10), the scatter plot of spoofed scores overwhelms the scatter plot of genuine scores.

3. Methods of Experiment

An Attempt to spoof a biometric authentication system degrades its vulnerability and increases its identification error rates. Variations of authentication error rates point out the growth of penetration rate for the under attack system. This section is allocated to the methodology of our experiment in this paper. In the first part, we mention the utilized database of matching scores and present the process of scores preparation for combination. The combination rules and comparison criterion are explained here as well.

3.1 Matching Scores Database

Experiments have been done based on multimodal public database released by National Institute of Standard and Technology (NIST), which is named Biometric Scores Set - Release 1 (BSSR1) (National Institute of Standards and Technology). This database contains true similarity scores of face and fingerprints which belong to one person. This dataset is suited to the study of score-level fusion-based multimodal, multi-algorithmic and multi-sample biometrics (He *et al.*, 2010; Nandakumar, Chen, Dass, & Jain, 2008). Two commercial face matchers, labeled with C and G, have generated similarity scores based on a frontal face comparison and a public fingerprint matcher has generated one left and one right index matching score, denoted by LI and RI respectively.

This information is taken from a set of 517 people. For each individual, one genuine score and 516 imposter scores are available. Therefore the database contains four subsets of genuine and four subsets of imposter scores. Henceforward we address these matchers by their labels for brevity.

Range of similarity scores completely varies for various matchers. For example for C face matcher it is [0 1] but for RI fingerprint matcher it is [0 260]. For applying similar effect of different matchers and modalities in combination, their matching scores must be first transformed to a same domain. This process is named normalization. Many of normalization methods are very sensitive to outlier scores, so they are not robust. For homogeneity of scores in fusion process, we normalize all scores by using one of the robust normalization methods. It is the hyperbolic tangent normalization procedure, based on Hampel estimator (Hampel, Ronchetti, Rousseeuw, & Stahel, 2005).

$$s'_f = \frac{1}{2} \left\{ \tanh \left(m \left(\frac{s_f - \text{mean}(Ess_f)}{\text{std}(Ess_f)} \right) \right) + 1 \right\}$$

Equation 2. Hyperbolic tangent normalization procedure based on Hampel estimator.

s_f and s'_f denote primary and normalized matching scores of f matcher, f denotes the type of matchers. The 'm' parameter influences the spread of normalized genuine scores, and its value is related to the standard deviation of scores distribution of each modality. Mean Ess_f and $\text{std}(Ess_f)$ denote the mean and standard deviation of Ess_f (Estimated score of each matcher), Ess_f denotes the Hampel estimate of distribution of original genuine scores. For more information see (He *et al.*, 2010; A.K. Jain, Nandakumar, & Ross, 2005)

3.2 Combination rules and Comparison criterion

Matching score level fusion methods are more applicable than other fusion approaches due to the ease in access to matching scores. Also the obtainable information in score level is more than decision level (He *et al.*, 2010). Context of verification has two main classes as output results: class of "Genuine user" for accepted clients and class of "Imposters" for rejected clients. Figure 3 shows individual similarity scores obtained from different

matchers. They are combined to produce a single score which is then compared with a threshold to make the final decision.

S_1 and S_2 are matching scores of biometric traits and S denotes the combined score. If S becomes more than the threshold, the client will be accepted as a genuine and if not, it will be rejected as an imposter user.

In this paper we investigate the bimodal multi biometric systems in which only one of their matchers, face or fingerprint matcher has been spoofed. We apply five fixed fusion rules for combination of various matching scores in the score level of authentication system. These fusion rules are as follows:

$$S_{sum} = \sum_{i=1}^R S'_i$$

Equation 3. Sum combination rule for adding matching scores.

$$S_{prod} = \prod_{i=1}^R S'_i$$

Equation 4. Product combination rule for multiplying matching scores.

$$S_{max} = \max_{i=1}^R S'_i = \max(S'_1, S'_2, \dots, S'_R)$$

Equation 5. Max combination rule for finding maximum score between matching scores.

$$S_{min} = \min_{i=1}^R S'_i = \min(S'_1, S'_2, \dots, S'_R)$$

Equation 6. Min combination rule for finding minimum score between matching scores.

$$S_{Bayes} = \frac{S'_1 * S'_2}{(1 - S'_1)(1 - S'_2) + S'_1 S'_2}$$

Equation 7. Bayes combination rule for fusion scores with Bayes rule (Suen & Lam, 2000).

Where S'_1 and S'_2, \dots, S'_R denote the normalized scores of individual matchers (standard or spoofed), $R=2$ in bimodal system and $S_{sum}, S_{product}, S_{min}, S_{max}$ and S_{Bayes} denote combined scores of Sum, Product min, max (Kittler, Hatef, Duin, & Matas, 1998) and Bayes fusion rules.

We simulate four multimodal systems by using four sets of matching scores of mentioned database. Two modalities include face and fingerprints are applied to each multimodal system. Our Experimental systems contain combinations of: G Face and LI fingerprint, G Face and RI fingerprint, C face and LI fingerprint and C face and RI fingerprint matchers. For brevity we denote these systems by corresponding symbols like (G-RI) or (C-LI).

Receiver Operating Characteristic (ROC) curve is generally used for performance evaluation of authentication systems. For comparing the robustness of multimodal systems with FAR error rate at each work point, we prefer to directly referring to the ROC curves. Deviation rates of authentication errors are used as comparative criterion between standard and under spoofing systems. Variations are compared in 3 operating test points including 0%, 1% and 10% FAR error rates. These operating points include all operation regions of authentication systems. Decision thresholds are calculated on the entire primary scores for finding desirable operating points. FRR is calculated by scatter plot of genuine scores. As the scatter of genuine scores is the same in both standard and spoofed system, according to Figure 2, then FRR amount for both systems is the same. Therefore, deviation rates of FAR are used as comparison criterion between standard and under spoofing authentication systems. All experiments are repeated with various sequences of matching scores and the average of all results is reported independently from the sequence of scores in database.

4. Experimental Results

At first, we examine the performance of all matchers in the database. The obtained results help us to explain the observations in combined systems which contain the mentioned matchers against spoofing. Figure 4 shows the ROC curves for all experimental matchers, which means the same FAR have different GAR. We address a matcher with more GAR in desired operating point (Golfaelli, Maio, & Malton) as the "accurate matcher" and a matcher with lower GAR at the same point as less accurate or "weak matcher".

All combination experiments have been repeated for all mentioned combination rules. Conclusions are based on obtained results from all possible combination experiments on the mentioned multi modal database. To present

the results we show the performance and vulnerability curves for face C in combination with fingerprint LI because their performance curves intersect in the middle of the operation region and in lower FAR amounts, RI Fingerprint matcher behaves as an accurate matcher while in higher FAR, C Face matcher is accurate matcher.

In Figure 5 the performance curves of combined (C-LI) system with various combination rules are shown. We see in all bimodal face and fingerprint combination systems that the sum rule has better performance, more GAR at the same FAR, and Min rule has the lower ROC performance curve in standard, without attack, state.

Figure 6 and Figure 7 show deviation curves of combination of C face and LI fingerprint matchers against various possibilities of spoofing respectively. In both of these figures, vulnerabilities of fixed combination rules are shown when face or fingerprint is spoofed.

At first we can see in a combination system that when face or fingerprint matcher is spoofed, except for min combination rule in spoofing face state and product rule in 0% FAR work point, FAR deviation in all work point of system increases so much. Therefore spoofing all modalities of a bimodal system is not necessary to crack it. FAR deviations of combined system especially in large amounts of FAR work points increases so much against growth of intensity of spoofing. For example in Figure 6 for combined system with sum rule, deviation of 0%FAR work point increases to 31% in k=100% possibility of spoofing but deviation of 1%FAR increases to 80% and for 10% FAR it increases to 95% in k=100% complete intensity of spoofing.

Figure 6 shows (C-LI) combined system, which applies min combination rule, behaves completely robust against various possibilities of C face matcher spoofing in every work points; but in contrast, max combination rule shows more vulnerability than other fixed rules in this state. For more examination we can divide the experimental fixed rules into two subsets:

- (1) Arithmetic fixed combination rules, the computing operators which work on matching scores like sum, product and Bayes combination rule.
- (2) Fuzzy fixed combination rules which use fuzzy operators like min and max for combining matching scores.

In other point of view when C face matcher is spoofed, the combined system with applying sum rule has the most FAR error deviation but with applying product rule it has the least FAR deviation among the arithmetic fixed rules.

Figure 7 shows that in (C-LI) combination system when LI fingerprint is spoofed, the max combination rule has the least FAR deviation among other rules in all work points against various possibilities of spoofing fingerprint matcher. In this state the min rule has more vulnerability than other practical fixed rules. With arithmetic combination rule in Figure 7 in contrast to Figure 6, the sum rule has the least and the product rule has the most FAR deviation amounts.

Spoofed states of face or fingerprint matchers show that when the face matcher is spoofed, the vulnerability arrangement of practical fixed rules completely differs from the state in which fingerprint matcher is spoofed.

5. Conclusion

The robustness of combined systems is related to: 1- The performance of matchers which are combined. 2- The combination rule, 3- The combined matcher which is exposed to spoofing and 4- The intensity of spoofing (spoofing possibilities).

In face and fingerprint bimodal systems when the face is exposed to spoof attacks, the min rule is the most robust fixed combination rule for all application regions of the system. However, performance of min combination rule is the lowest in standard state. In contrast, when fingerprint matcher is spoofed, the max combination rule shows the least vulnerability among other fixed rules although the min rule shows the most vulnerability in this state.

With increasing the possibility of spoofing, the vulnerability of combined systems increases. But 0% FAR work point, the most secure application region, shows more robustness than other work points in other application regions against spoofing. An authentication system in very secure application region shows more robustness than other applicable regions especially when the spoofing intensity is less than 50%.

In bimodal combination systems, we see when one of their matchers is spoofed the vulnerability of combined system increases so much, as spoofing another trait is not necessary to crack the combined system.

In designing process of a combined authentication system, paying attention to the security of combined system against spoofing attacks is an urgent need.

References

- Bergamini, C., Oliveira, L. S., Koerich, A. L., & Sabourin, R. (2009). Combining different biometric traits with one-class classification. *Signal Processing*, 89(11), 2117-2127. <http://dx.doi.org/10.1016/j.sigpro.2009.04.043>
- Bubeck, U. M., & Sanchez, D. (2003). *Biometric authentication: Technology and evaluation*. San Diego State Univ., San Diego, CA.
- Dass, S. C., Nandakumar, K., & Jain, A. K. (2005). A principled approach to score level fusion in multimodal biometric systems. In T. Kanade, A. Jain & N. K. Ratha (Eds.), *Audio and Video Based Biometric Person Authentication, Proceedings*, 3546, 1049-1058. Berlin: Springer-Verlag Berlin.
- Fox, N. A., Gross, R., Cohn, J. F., & Reilly, R. B. (2007). Robust biometric person identification using automatic classifier fusion of speech, mouth, and face experts. *IEEE Transactions on Multimedia*, 9(4), 701-714. <http://dx.doi.org/10.1109/tmm.2007.893339>
- Golfarelli, M., Maio, D., & Malton, D. (1997). On the error-reject trade-off in biometric verification systems. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(7), 786-796. <http://dx.doi.org/10.1109/34.598237>
- Hampel, F. R., Ronchetti, E. M., Rousseeuw, P. J., & Stahel, W. A. (2005). *Robust Statistics: The Approach Based on Influence Functions* (Wiley Series in Probability and Statistics). <http://dx.doi.org/10.1002/9781118186435>
- Hariri, M., & Shokouhi, S. B. (2011). Possibility of spoof attack against robustness of multibiometric authentication systems. *Optical Engineering*, 50, 079001. <http://dx.doi.org/10.1117/1.3599874>
- He, M., Horng, S. J., Fan, P., Run, R. S., Chen, R. J., Lai, J. L., . . . Sentosa, K. O. (2010). Performance evaluation of score level fusion in multimodal biometric systems. *Pattern Recognition*, 43(5), 1789-1800. <http://dx.doi.org/10.1016/j.patcog.2009.11.018>
- Hong, L., Jain, A., & Pankanti, S. (1999). Can Multibiometrics Improve Performance? Paper presented at the Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, NJ, USA.
- ISO, & IEC19792. (2009). Information technology -- Security techniques -- Security evaluation of biometrics *ISO/IEC 19792:2009*.
- Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advanced in Signal Processing, Proceeding*, 17. <http://dx.doi.org/10.1155/2008/579416>
- Jain, A. K., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12), 2270-2285. <http://dx.doi.org/10.1016/j.patcog.2005.01.012>
- Kang, B. J., & Park, K. R. (2009). Multimodal biometric authentication based on the fusion of finger vein and finger geometry. *Optical Engineering*, 48, 090501. <http://dx.doi.org/10.1117/1.3212651>
- Kittler, J., Hatef, M., Duin, R. P. W., & Matas, J. (1998). On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3), 226-239. <http://dx.doi.org/10.1109/34.667881>
- Monwar, M., & Gavrilova, M. (2008). A robust authentication system using multiple biometrics. *Computer and Information Science*, 189-201. http://dx.doi.org/10.1007/978-3-540-79187-4_17
- Nandakumar, K., Chen, Y., Dass, S. C., & Jain, A. K. (2008). Likelihood ratio-based biometric score fusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(2), 342-347. <http://dx.doi.org/10.1109/TPAMI.2007.70796>
- National Institute of Standards and Technology. NIST Biometric Scores Set. [Online] Available: <http://www.itl.nist.gov/iad/894.03/biometricscores/index.html>
- Prabhakar, S., & Jain, A. K. (2002). Decision-level fusion in fingerprint verification. *Pattern Recognition*, 35(4), 861-874. [http://dx.doi.org/10.1016/S0031-3203\(01\)00103-0](http://dx.doi.org/10.1016/S0031-3203(01)00103-0)
- Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems journal*, 40(3), 614-634. <http://dx.doi.org/10.1147/sj.403.0614>
- Rodrigues, R. N., Ling, L. L., & Govindaraju, V. (2009). Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages & Computing*, 20(3), 169-179. <http://dx.doi.org/10.1016/j.jvlc.2009.01.010>

Suen, C., & Lam, L. (2000). Multiple classifier combination methodologies for different output levels. Paper presented at the Multiple Classifier Systems, MCS2000, Cagliari, Italy.

Ulery, B., Hicklin, A., Watson, C. I., Fellner, W., & Hallinan, P. (2006). Studies of biometric fusion: US Dept. of Commerce, National Institute of Standards and Technology.

Wang, F. H., & Han, J. Q. (2008). Robust Multimodal Biometric Authentication Integrating Iris, Face and Palmprint. *Information Technology and Control*, 37(4), 326-332.

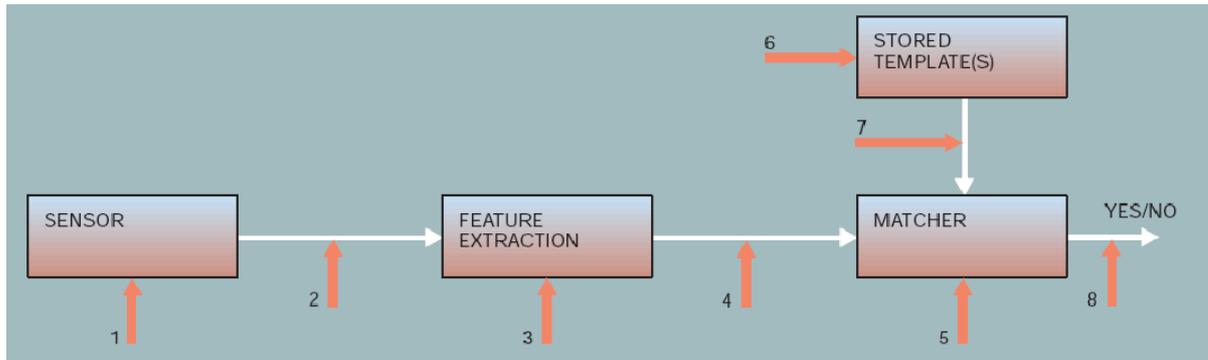
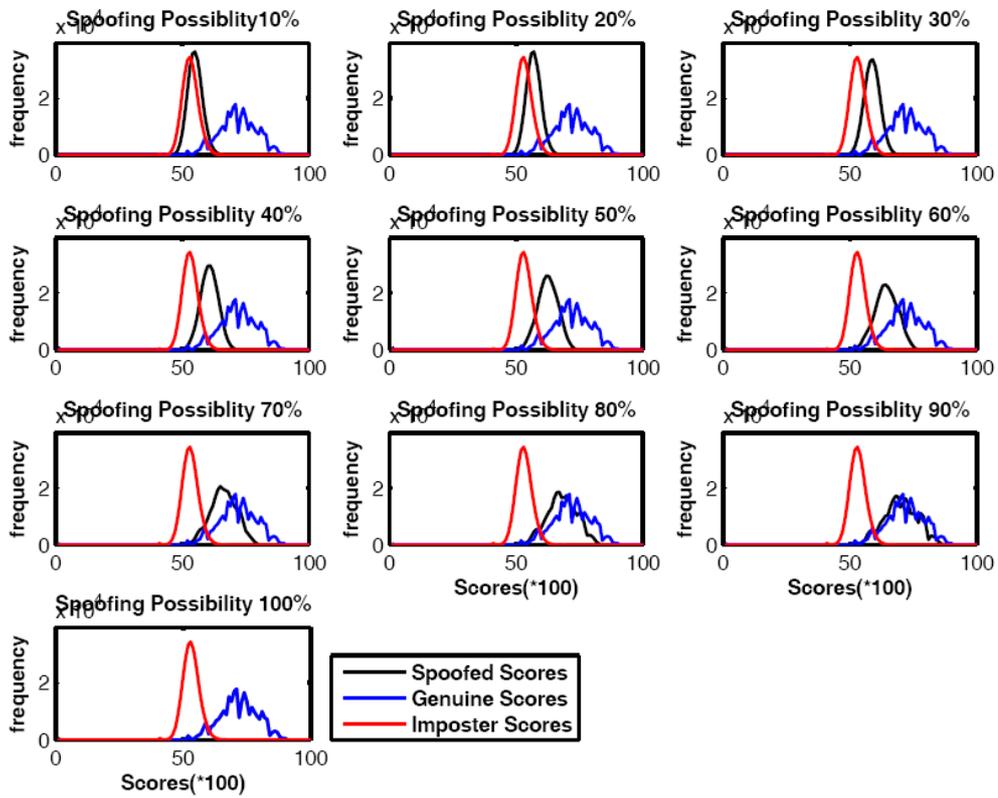
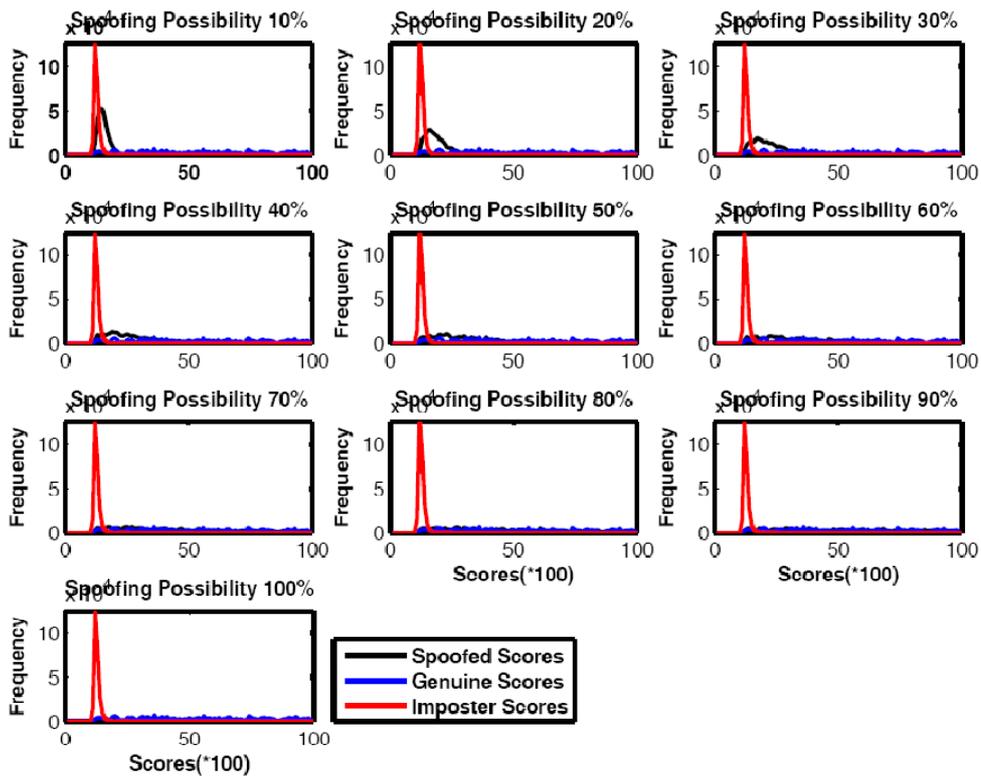


Figure 1. Possible attack points in a biometric system



(a) C face matcher



(b) RI fingerprint matcher

Figure 2. Genuine, imposter and spoofed scores scatter plots with various possibility of spoofing the biometric matchers

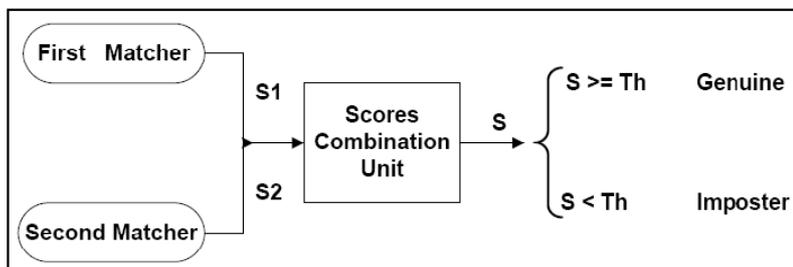


Figure 3. Schematic diagram of score level fusion in combined authentication system

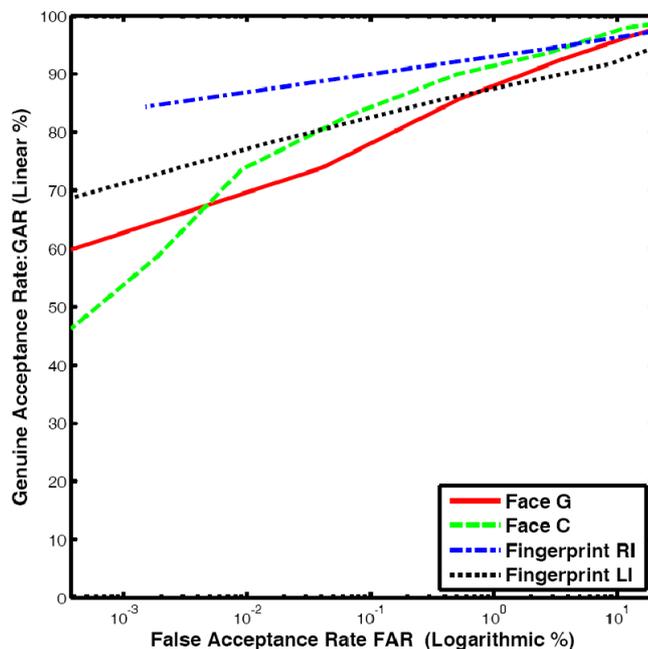


Figure 4. Roc Curves show the performances of various face and fingerprints matchers in a range of desired operating points

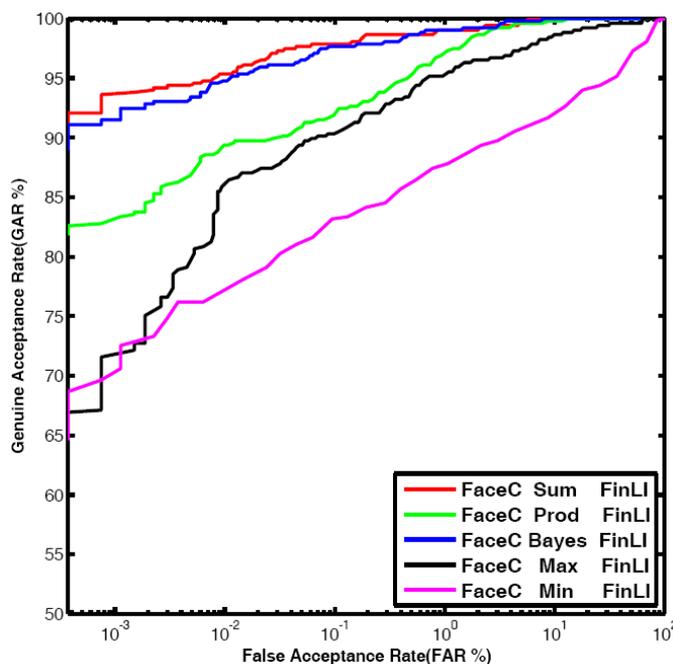


Figure 5. ROC curves for combination of C face and LI fingerprint matchers with 5 fixed combination rules

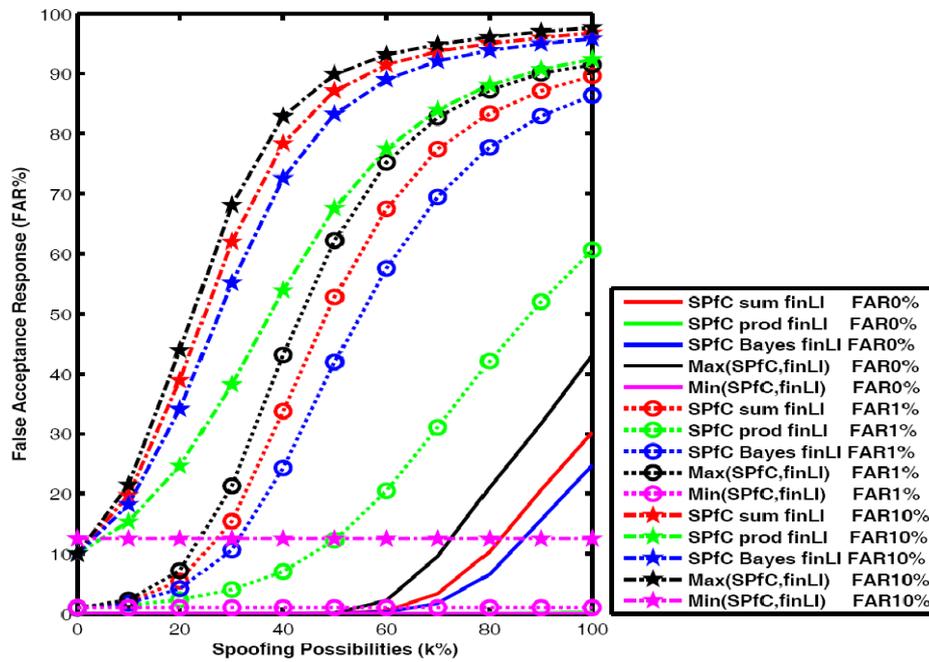


Figure 6. FAR deviation curves for combination of C face and LI fingerprint matchers by 5 fixed combination rules against possibility of spoofing when C face matcher is spoofed in three FAR work points

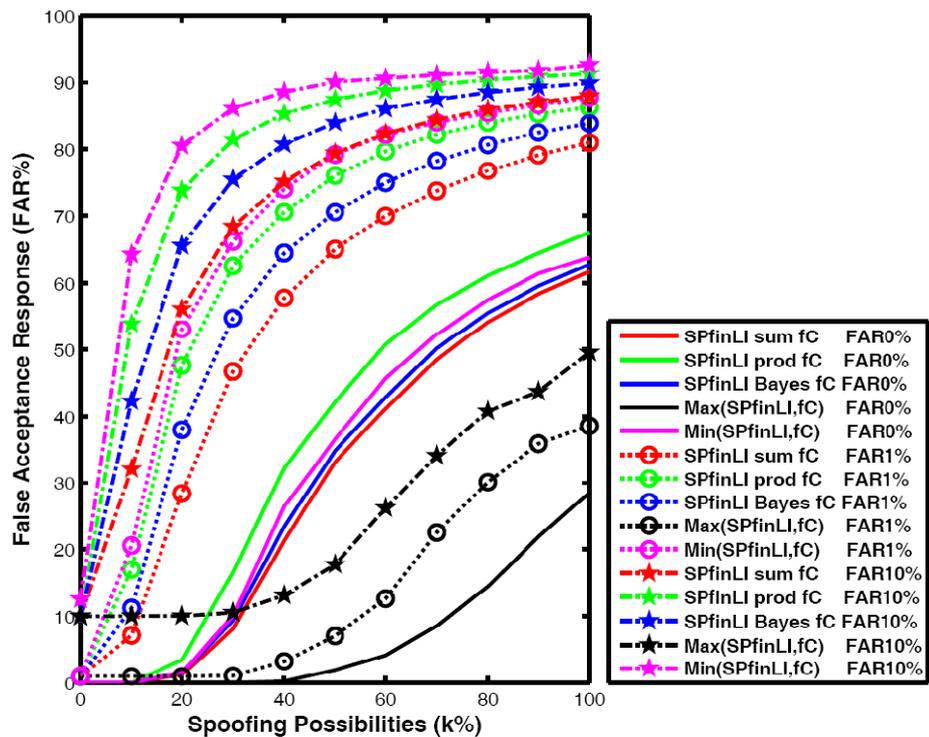


Figure 7. FAR deviation curves for combination of C face and LI fingerprint matchers by 5 fixed combination rules against possibility of spoofing when LI fingerprint matcher is spoofed in three FAR work points