2011 International Conference on Information and Network Technology
IPCSIT vol.4 (2011) © (2011) IACSIT Press, Singapore

Secure Learning Algorithm for Multimodal Biometric Systems against Spoof Attacks

Zahid Akhtar [1, +] and Nasir Alfarid [2]

[1] Dept. of Electrical and Electronic Engineering, University of Cagliari, Italy
[2] Cognizant Technology Solutions, India

Abstract. Spoof attack is one of the major challenge that can decline the security and reliability of the biometric systems. Multimodal biometric systems are commonly believed to be more resilient against spoof attacks than systems using single biometric trait. However, a recent study has questioned, contrary to a common claim, that multimodal systems can be cracked by spoofing *only one* trait and pointed out the need of developing new algorithms to enhance robustness of the multimodal systems against spoof attacks. In this paper, we propose a new learning algorithm that can improve the security of multimodal systems against spoof attacks. Our algorithm uses simulated spoof attacks to learn the impostor distribution with different practical spoofing scenarios. Empirical results, using *NIST-BSSR1* benchmark data set, show that the proposed algorithm increases the security and robustness of the systems significantly against spoof attacks.

Keywords: Biometrics, Multimodal biometric system, Score fusion rules, Spoof attacks.

1. Introduction

Biometrics is a method to uniquely recognize a person using the physical or behavioral attributes. The biometric trait used in the authentication process should be hard to circumvent [1]. Unfortunately, recent studies have shown that biometric traits can be stolen and replicated to attack the biometric systems [2-6]. This attack is know as ”spoof attack” which is carried out by presenting fake biometric trait to the sensor of the biometric systems. The spoof attacks does not require any knowledge about system’s internal operation mechanism leading to increased number of potential attackers. A traditional counteraction against spoof attacks is ”liveness” detection (vitality testing) method which confirms that the presented biometric trait to the system is from a live person and is not an artificial one. However, no method has fully been matured yet.

Multimodal biometric systems, which integrate two or more biometrics to achieve better recognition and security results than unimodal (one single) biometric systems, are also taken into consideration as a defense mechanism against spoof attacks. To date, a large amount of work has been carried out to provide empirical evidence of improvement in recognition rate but there is no experimental evidence to support security enhancement. It is claimed that multimodal systems are more robust against spoof attacks, since it is more difficult to evade several systems than to evade just *one* [1]. This claim was established under the hypothesis that to evade a multimodal system the attacker needs to evade *all* fused individual systems *simultaneously*.

However, a recent work [7] empirically showed that a multimodal biometric system made up of a face and a fingerprint matchers can be evaded by spoofing *only one* matcher. However, the experiment in [7] was carried out under the unrealistic assumption that spoofed and genuine traits are identical which produces same output matching scores, which is not true in real world [3] [8]. If the results in [7] is to be hold then multimodal systems are impediment for an attacker rather than real defense mechanism. Hence, it is crucial to develop new fusion rules and learning algorithms to improve robustness of the multimodal systems against

[+] Corresponding author. Tel.: + 393294913022 ; fax: + 390706755782.
E-mail address: z.momin@diee.unica.it

spoof attacks. In [7] two possible fusion rules were proposed that take spoof attacks into account . However, the proposed rules are trained under the unpractical hypothesis that spoofed biometric traits are indistinguishable to genuine traits which yield identical matching scores. Moreover, the parameters, the internal security of each individual biometric system, and the attempt of spoof attack succeeds, on which they depend are difficult to tune in practice. The open issue is to design new fusion rules and algorithms with practical hypothesis about spoof attacks, plus less and easy to implement parameters to yield better results.

In this paper, we propose a secure learning algorithm to enhance the robustness of multimodal biometric systems against spoof attacks. Our algorithm is based on adding simulated spoof attacks in to the impostor distribution. We model spoof attack scores as function of the genuine and impostor scores. Our algorithm trains learning based fusion rules, using single parameter ”percentage of impostor attempt spoof attacks”, for all possible spoofing scenarios such that when: i) only one trait has been spoofed; ii) only subset of traits has been spoofed; iii) all traits have been spoofed. To evaluate the improvement in robustness of the system against spoof attacks, we compare the probability of an impostor being authenticated as genuine user when trained by traditional and our proposed secure learning algorithms.

Our results show that the robustness of multimodal biometric systems, with eight different score fusion rules, increases remarkably when trained by our proposed algorithm as compared to traditional algorithm.

2. A Secure Learning Algorithm against Spoof Attacks

In a multimodal biometric system, information fusion can be carried at various levels: feature extraction level, matching score level and decision level. Fusion at the matching score level is generally preferred due to ease in accessing and combining of matching scores. Several score fusion rules for multimodal system have been proposed in the literature [10-13], but most of them concentrate on performance improvement and do not consider security aspects specially robustness against spoof attacks. In traditional fusion rules and training algorithms, the impostor distribution is approximated without taking into consideration the hypothesis that some impostor may have spoofed a biometric trait. Since, they are trained only using ”non-spoofed” impostor samples, therefore tend to be vulnerable to spoof attacks [7].

Hence, our objective is to develop a robust and easy to implement algorithm against spoof attacks without affecting the overall performance of the multimodal systems. We propose a approach to design robust multimodal system, based on adding simulated spoof attacks to the training set. The underlying rationale is that the traditional learning algorithm does not consider that, in practice, an impostor may have spoofed one or more biometric modalities, and hence approximated impostor distribution my not be the true representative. A straightforward way to solve this problem is constructing real spoof attack samples and training the system on these samples to update the security level against spoof attacks. However, fabricating fake (spoofed) biometric trait is a difficult and labor-intensive task [3]. The alternative solution we propose is to simulate spoof attacks at the matching score level, by appropriately modeling it from the available genuine and impostor training samples. It is worth noting that our proposed approach is similar to noise injection methods used in neural network classifiers to improve it’s generalization capability [14]. The main difference between our proposed algorithm and this methods is that our algorithm is aimed at improving robustness and security of the multimodal systems against spoof attacks. Also, similar strategy, by considering worst-case and only one trait has been spoofed, is presented in [16].

On the basis of reported empirical evidences about spoofed biometric trait distribution in [3-6], we made a heuristic assumption that the spoofed trait’s score is simply an average of genuine and impostor scores, which generally are only available data to the system designer. Our method is depart from the worst-case scenario carried out in [7], where the spoofed trait matching score follows the genuine matching score distribution, which is not true in real world [3] [8].

In the following, we denote the matching score as random variable S and denote G and I such that the input biometric trait are of genuine and impostor users while F is a spoofed biometric trait. Based on the above discussion, we propose the following Algorithm 1 secure learning algorithm to approximate the impostor distribution with spoof attack samples. The algorithm creates a training multimodal data set to train the system against each possible spoof attack scenario. There are $2^N - 1$ possible scenarios to spoof the

multimodal system made up of N number of matchers. For instance, there are three spoofing scenarios for a multimodal biometric system made up of a face and a fingerprint matchers; when i) only the face has been spoofed; ii) only the fingerprint has been spoofed; iii) both, the face and fingerprint, have been spoofed.

The number of spoofed samples to be added in to the training set are controlled by a single parameter (α) i.e. the number of impostors attempt spoof attack (for instance, 1% of the total impostors). We consider that equal number of impostors attempt spoof attacks for each spoofing scenarios.

This algorithm follows standard learning algorithm. In standard learning algorithm, the system is trained on "non-spoofed" impostor data, while in the proposed algorithm simulated spoof attack samples are incorporated in to the training data allowing training the system against all possible spoofing scenarios.

Different values of α in Algorithm 1 will allow to set the robustness of the system against spoof attacks as per the requirements. The robustness against spoof attacks of the system is likely to increase, when trained by the secure learning algorithm as compared to the traditional learning algorithm. Hence, the above procedure can be used to design robust multimodal systems. The main feature of our proposed algorithm is to make the system adversary-aware, and prevent the spoof attacks by adding them to the training set.

Algorithm 1: Secure Learning Algorithm for Multimodal Biometric Systems against Spoof Attacks

Inputs:

- A training set $\begin{pmatrix} S_{Gtr} \\ S_{Itr} \end{pmatrix}$ and a testing set $\begin{pmatrix} S_{Gts} \\ S_{Its} \end{pmatrix}$ made up of $n \times N$ matching score matrices coming from genuine and impostor users;
- α : Number of impostors attempt spoof attacks (percentage of impostors attempt spoof attacks).
- A score fusion rule

Output: The system's performance under spoof attacks, when trained by traditional and our proposed secure learning algorithms.

Initialization: A null $\alpha \times N$ matrix named S_{Ftr}

1. Compute the spoofed trait's matching score for each matcher using randomly selected genuine and impostor scores with replacement, as follows:
   for i = 1 to N **do** **for** j = 1 to α **do**
   $S_F(j, i) \leftarrow [S_G(j, i) + S_I(j, i)] / 2$
   end for **end for**
2. Update the S_{Ftr} matrix using S_F such that $\alpha/(2^N - 1)$ number of impostors attempt spoof attacks in each possible scenario for spoofing the system.
3. Update the S_{Ftr} matrix for non-spoofed matcher in each spoofing scenario with randomly selected corresponding matcher's impostor scores.
4. Determine the training impostor set for secure learning such that $S_{Fstr} = \begin{pmatrix} S_{Itr} \\ S_{Ftr} \end{pmatrix}$
5. Update training set as: $\begin{pmatrix} S_{Gtr} \\ S_{Fstr} \end{pmatrix}$
6. Set the parameters of fusion rule on original training set (traditional learning) and on training set obtained in step 5 (secure learning), according to given performance requirement of the system.
7. Compute spoof attack matching score S_{Fts} according to steps 1-4 and label them as "impostor".
8. Evaluate the performance of system on $\begin{pmatrix} S_{Gts} \\ S_{Fts} \end{pmatrix}$ using score fusion rule parameters computed in step 6 for traditional learning and secure learning algorithm, respectively.

---

3. Experimental Setup

The performance of proposed algorithm was evaluated using NIST biometric score set Release 1 (BSSR1) benchmark date set [15]. It is made up of similarity scores obtained from two different face matchers (denoted as C and G) and from one fingerprint matcher using left and right index (denoted as RI and LI), on a set of 517 people. For each individual, one genuine score and 516 impostor scores are available for each matcher and each modality. All the scores were normalized using the hyperbolic tangent method [1].

Using the four sets of scores of the NIST data set, we fabricated four different multimodal biometric systems by pairing in all possible ways the face score set with the fingerprint score set. The resulting systems are therefore Face G - Fingerprint LI (denoting the multimodal system made up by the face matcher G and the fingerprint matcher using the left index), Face G - Fingerprint RI, Face C - Fingerprint LI, and Face C - Fingerprint RI. In order to evaluate the performance of the systems under the optimal configuration, the decision thresholds and the parameters of fusion rules were evaluated on the whole original data sets (without spoof attacks) for traditional learning algorithm, while for secure learning algorithm on the whole new data set (with spoof attacks) obtained by Algorithm 1. We trained the system for secure learning algorithm with α (percentage of impostor attempt spoof attacks) value of 4%. The performance of the systems under spoof attacks was evaluated, by replacing each impostor score with spoofed trait matching

scores obtained using step 1 of Algorithm 1, for three spoof attack scenarios when i) only the face has been spoofed; ii) only the fingerprint has been spoofed; iii) both, the face and fingerprint, have been spoofed.

The false acceptance rate (FAR) is the percentage of impostor being accepted as genuine users, and to provide high security the biometric systems operates at a low FAR operating point. To investigate issues 1, 2 and 3 of section 2, we evaluated the increase of FAR due to spoof attacks at 0%, 0.01% and 0.1% FAR operating points, resulting the lowest threshold values that produce FAR on training data set equal to operational points, respectively.

3.1. Score Fusion Rules

We evaluated our proposed algorithm on eight trained score fusion rules. Let s_1, s_2 and s be the scores of face, fingerprint matchers and the fused score, respectively.

1) **Weighted Sum:** The weights (w) for the weighted sum rule can be computed using linear discriminant analysis (LDA)[9]. The aim of using LDA based fusion rule is to obtain fused scores with minimum within-class and maximum between-class variations. The fused scores are computed as: $s = \sum_{i=1}^{N} w_i s_i$

2) **Exponential Sum:** The fused score for N matchers is obtained as follows [11]: $s = \sum_{i=1}^{N} w_i \exp(s_i)$

3) **Tan-hyperbolic Sum:** The fused score is computed as follows [11]: $s = \sum_{i=1}^{N} w_i \tanh(s_i)$

The weights were for exponential sum and tan-hyperbolic sum were computed as in weighted sum rule.

4) **Perceptron:** The perceptron-based fusion rule for N matchers can be implemented as follows [10]: $s = 1 \Big/ 1 + \exp\left[-(w_0 + \sum_{i=1}^{N} w_i s_i)\right]$. The weights were computed by a gradient descent algorithm.

5) **Weighted Product:** The rule is also known as logarithm opinion pool, is computed as follows [11]: $s = \prod_{i=1}^{N} s_i^{w_i}$. The weights $w_i \in [0,1]$ has been computed by maximizing the system performance on the chosen operational points. This rule accounts the varying discrimination ability and reliability of each matcher.

6) **Exponential Product:** The fused score of the set of N matchers using exponential product rule is obtained as follows [12]: $s = \prod_{i=1}^{N} w_i \exp(s_i)$. The weights were calculated as in weighted product rule.

7) **Tan-hyperbolic Product:** The fused score of the set of N matchers using tan-hyperbolic product rule is obtained as follows [13]: $s = \prod_{i=1}^{N} w_i \tanh(s_i)$. The weights were calculated as in weighted product rule.

8) **Likelihood Ratio Rule (LLR):** This rule computes the fused score as follows: $s = \prod_{i=1}^{N} p(s_i \mid G_i) \Big/ \prod_{i=1}^{N} p(s_i \mid I_i)$

where $p(\cdot|G)$ and $p(\cdot|I)$ are the matching score's probability density function (PDF) of genuine and impostor users, respectively. We used Gaussian to model the genuine and impostor score distributions.

4. Experimental Results

We report the results obtained on Face C-Fingerprint RI and Face G - Fingerprint LI multimodal systems in tables I and II, respectively, using weighted sum and LLR score fusion rules, when trained by traditional and our proposed secure learning algorithms. The results obtained with other fusion rules and systems were qualitatively very similar, and are not reported due to the lack of space.

Operating Point	Traditional learning			Secure learning			Traditional learning			Secure learning		
	Weighted Sum			Weighted Sum			LLR			LRR		
	Fing. Sp.	Face Sp.	Both Sp.	Fing. Sp.	Face Sp.	Both Sp.	Fing. Sp.	Face Sp.	Both Sp.	Fing. Sp.	Face Sp.	Both Sp.
0%FAR	52.80	0.89	53.06	1.18	0.49	0.88	58.52	40.50	68.14	1.03	0.97	2.43
0.1%FAR	76.95	1.83	83.04	1.93	0.83	1.07	82.93	68.82	85.81	2.44	1.09	9.94
1%FAR	83.11	2.23	89.04	2.03	0.99	2.97	89.84	83.11	93.62	3.01	1.45	11.38

Table I: FAR(%) of the Face C-Fingerprint RI system, with the weighted sum and LLR rules, when either the fingerprint, the face or both the fingerprint and face are spoofed, at three operating points.

Operating Point	Traditional learning			Secure learning			Traditional learning			Secure learning		
	Weighted Sum			Weighted Sum			LLR			LRR		
	Fing.	Face	Both	Fing.	Face	Both	Fing.	Face	Both	Fing.	Face	Both

	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.	Sp.
0%FAR	36.81	0.63	39.57	1.05	0.47	0.40	48.20	31.10	56.25	1.03	0.81	2.25
0.1%FAR	66.92	1.10	72.00	1.26	0.79	1.00	71.65	43.00	86.04	1.90	1.03	6.04
1%FAR	79.24	2.20	83.98	1.84	0.84	2.01	87.50	55.81	91.51	2.04	1.11	8.96

Table II: FAR(%) of the Face G-Fingerprint LI system, with the weighted sum and LLR rules, when either the fingerprint, the face or both the fingerprint and face are spoofed, at three operating points.

The following observations can be made on tables I and II.

1) Spoofing only one biometric trait can be sufficient to evade a multimodal system. For instance, from table I for LLR rule when trained by traditional learning algorithm, it can be seen that at 1% FAR operating point the FAR under attack attained values up to 89.84%, when *only one* trait was spoofed. The results on four different data sets and eight score fusion rules with non-worst case attacks are further support to the results in [7] where using two data sets and two fusion rules with worst-case attacks were presented.

2) By comparison of the results obtained by our proposed secure learning algorithm with those obtained with traditional learning algorithm, it is evident that our approach significantly outperforms the traditional algorithm. In other words, the increase of FAR under spoof attacks is very less, in all spoofing scenarios, when trained by proposed secure learning algorithm as compared to when trained by traditional learning algorithm. For example, in table II, for weighted sum rule at 1% operating point the FARs under attack, if only fingerprint is spoofed, are 79.24% and 1.84%, when trained by traditional and proposed secure learning algorithms, respectively.

3) Among all considered fusion rules, LLR rule is least resilient against spoof attacks, though it is referred as the optimal fusion rule.

4) Spoofing the best individual matcher (as the fingerprint one appears for all systems) substantially increases FAR under spoof attacks as compared to spoofing to less accurate matcher. This is an interesting point to be further investigated thoroughly which is subject of our on going work.

5. Conclusion

In this paper, we empirically investigated that multimodal biometric systems are not intrinsically robust against spoof attacks as believed so far. They can be cracked by spoofing *only one* biometric trait, in particular, when trained by traditional learning algorithm. To minimize this vulnerability, we proposed a secure learning algorithm that takes into account all scenarios of spoof attacks a multimodal system can encounter. The experimental results show that our proposed algorithm improves the robustness of the multimodal biometric systems against spoof attacks, significantly.

In the future, we will further examine our algorithm by constructing proper large data sets containing real spoof attacks and modify the algorithm if necessary.

6. References

[1] A. Ross, K. Nandakumar, A.K. Jain. Handbook of Multibiometrics. Springer, 2006.

[2] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino. Impact of Artificial Gummy Fingers on Fingerprint Systems. In: Proc. of SPIE on Optical Security and Counterfeit Deterrence Tech. IV. 2007, vol. 4677, pp. 275-289.

[3] J. Galbally, R. Cappelli, A. Lumini, Guillermo G., D. Maltoni, J. Fierrez, Javier O., D. Maio. An evaluation of direct attacks using fake fingers generated from ISO templates. Patt. Rec. Letters. 2010, 31 (8): pp. 725-732.

[4] S. J. Lee, K. R. Park, J. Kim. Robust Fake Iris Detection Based on Variation of the Reflectance Ratio Between the IRIS and the Sclera. In: Proc. of conference of Biometric Consortium. 2007, pp. 1-6.

[5] Gafurov D., Snekkenes E., P. Bours. Spoof Attacks on Gait Authentication System. IEEE Transactions on Information Forensics and Security. 2007, 2 (3): 491-502.

[6] Hyung-Keun Jee, Sung-Uk Jung, and Jang-Hee Yoo. Liveness Detection for Embedded Face Recognition System. International Journal of Biomedical Sciences. 2006, 1 (4): 235-238.

[7] R.N. Rodrigues, L.L. Ling, V. Govindaraju. Robustness of Multimodal Biometric Methods against Spoof Attacks.

J. of Visual Languages and Computing. 2009, 20 (3): 169-179.

[8] Girija Chetty, W. Michael. Multi-Level Liveness Verification for Face-Voice Biometric Authentication. In: Proc. of Biometrics Symposium. 2006, pp. 1-6.

[9] Duda R., Hart P., Stork D. Pattern Classification. John Wiley Inc., 2001.

[10] A.K. Jain, S. Prabhakar, S. Chen. Combining Multiple Matchers for a High Security Fingerprint Verification System. Pattern Recognition Letters. 1999, 20 (11-13): 1371-1379.

[11] A. Kumar, Vivek K., D. Zhang. A New Framework for Adaptive Multimodal Biometrics Management. IEEE Trans. On Information Forensics and Security. 2010, 5 (1): 92-102.

[12] Kyong I. Chang Kevin W. Bowyer, Patrick J. Flynn, Xin Chen. Multibiometrics Using Facial Appearance, Shape and Temperature. In: Proc. of IEEE Int. Conf. on Automatic Face and Gesture Recognition. 2004, pp. 43-48.

[13] Kar-Ann Toh, Wei-Yun Yau. Combination of Hyperbolic Functions for Multimodal Biometrics Data Fusion. IEEE Trans.on Sys., Man, and Cybernetics. 2004, 34 (2): 1196-1209.

[14] C. M. Bishop. Neural Networks for Pattern Recognition. Oxford: Clarendon Press, 1995.

[15] http://www.itl.nist.gov/iad/894.03/biometricscores/index.html.

[16] B. Biggio. Adversarial Pattern Classification. Ph. D. thesis, DIEE, University of Cagliari, 2010.