Evaluation of serial and parallel multibiometric systems under spoofing attacks

Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, Fabio Roli
Department of Electrical and Electronic Engineering - University of Cagliari
Piazza d'Armi, 09123 Cagliari, Italy
{z.momin,fumera,marcialis,roli}@diee.unica.it

Abstract

Recent works have investigated the robustness to spoofing attacks of multi-modal biometric systems in parallel fusion mode. Contrary to a common belief, it has been shown that they can be cracked by spoofing only one biometric trait. Robustness evaluation of multi-modal systems in serial fusion mode has not yet been investigated, instead. Thus, the aim of this paper is to comparatively evaluate the robustness of multi-modal systems, in serial and parallel fusion modes, under spoofing attacks. In particular, we empirically investigate the vulnerability of serial and parallel fusion of face and fingerprint biometrics to real spoofing attacks. Our results show that multi-modal systems in both fusion modes are vulnerable to attacks against a single biometric trait. On the other hand, they show that the serial fusion mode can attain a favorable trade-off between performance, verification time, and robustness against spoofing attacks.

1. Introduction

Spoofing attacks are one of the main threats to the security of biometric systems. They are carried out by submitting a counterfeited biometric (i.e., a replica of the client's biometric) to the sensor. For instance, a gummy finger can be used to fool a fingerprint recognition system [4]. Spoofing attacks have a great practical relevance because they do not require advanced technical skills and, therefore, the potential number of attackers is very large. It has been shown throughout the history of automated personal recognition that spoofing attacks can be carried out against many types of biometrics, like face and iris (e.g., some recent works are [4, 9, 8]). To deal with spoofing attacks, several "liveness" detection methods have been proposed [8]. However, liveness detection has a major disadvantage when coupled with a biometric system: it typically increases the percentage of genuine users being rejected as impostor (i.e., the false reject rate, FRR).

Besides ad hoc countermeasures, it is commonly believed that multi-modal biometric systems are intrinsically more robust against spoofing attacks [15]. This belief is based on the intuitive hypothesis that the attacker has to spoof *all* fused biometrics *simultaneously* to crack them. However, conversely to the above belief, some recent works have shown experimentally that multi-modal systems in *parallel fusion mode* can be evaded by spoofing *only one* of the fused biometrics [13, 12, 10, 3, 5, 7].

Vulnerability of multi-modal systems in *serial fusion mode* to spoofing attacks has not been investigated so far, instead. Despite the fact that multi-modal systems in serial fusion mode exhibit some potential advantages with respect to the parallel multi-modal systems, such as [11, 2]: (i) the majority of genuine users are authenticated by using only one biometric trait, that is, the first one in the processing chain (this can be particularly true if some partitioning of users is possible [6]); (ii) all available biometrics are necessary only for a few selected users. This overcomes the drawback of multi-modal systems in parallel fusion mode, where all biometrics for all users are required to perform authentication, and thus the corresponding verification time depends on the slowest system. It is thus interesting to investigate the robustness of serial fusion of multi-modal systems against spoofing attacks, and thoroughly compare it with the robustness of parallel multi-modal systems. This can also help to devise novel methods to design systems robust to spoofing attacks.

Based on the above motivations, in this paper we made a first step toward the above goal, by empirically analyzing the robustness of serial fusion of bi-modal systems made up of a face and a fingerprint matcher, against several real spoofing attacks, and compare it to the robustness of the corresponding parallel systems. To this aim, we collected four data sets with real spoofing attacks. Two data sets contain fake fingerprints fabricated with silicon and latex, which are representative of the state-of-the-art, and were also used in the Second Fingerprint Liveness Detection Competition [16]. Two other data sets contain spoofed faces. One of them was obtained by putting in front of the camera the photo of each user displayed on a laptop screen. The

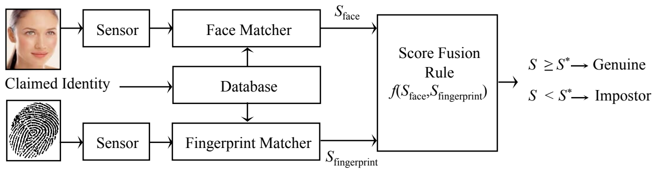

Figure 1. Outline of the considered multi-modal biometric system in parallel fusion mode.

other one is public data set recently used in the Competition on Countermeasures to 2D Facial Spoofing Attacks [8]. We also carried out our experiments on parallel multi-modal systems using well known score fusion rules: product, weighted product, and likelihood ratio rule (LLR), in order to compare their robustness with one of the corresponding systems in serial fusion mode.

Our experimental results provide a clear evidence that multi-modal biometric system in both (serial and parallel) modes can be cracked by real spoofing attacks, even when *only one* of the fused traits is spoofed. However, our results also show that serial fusion mode can be more robust against spoofing attacks than parallel fusion mode.

The paper is organized as follows. Sect. 2 provides a concise description of multi-modal biometric systems in serial and parallel fusion mode, with reference to the ones considered in this paper, and summarizes state-of-the-art on their robustness against spoofing attacks. Sect. 3 describes the data sets, the adopted fusion rules and the experimental protocol. Experimental results are reported in Sect. 4. Preliminary conclusions are finally drawn in Sect. 5.

2. Background

In this section we first give a short illustration of multi-modal biometric systems, and then summarize previous works on their robustness against spoofing attacks.

2.1. Multi-modal biometric systems

2.1.1 Parellel fusion mode

Fig. 1 depicts the outline of multi-modal biometric system in parallel fusion mode, with reference to the one considered in this study, namely a standard bi-modal verification system based on a face and a fingerprint matcher. In multi-modal systems, information fusion can be carried out at sensor, feature extraction, matching score or decision level. Due to ease in accessing and combining of matching scores, fusion at matching score level is the most commonly adopted approach in the literature, and is also adopted in this study, as in [13, 12, 10, 3, 5, 7].

In a *verification* setting, each user presents his face and fingerprint to the respective sensors, and claims his identity. Each matcher then separately compares the presented trait with the corresponding template of the claimed identity, and produces a face and a fingerprint matching score, S_{face} and $S_{\text{fingerprint}}$, respectively. Finally, these matching scores are fused through a fusion rule $f(S_{\text{face}}, S_{\text{fingerprint}})$. If the fused score S is equal or greater than a predefined threshold S^*, then user is accepted as genuine, otherwise it is rejected as an impostor.

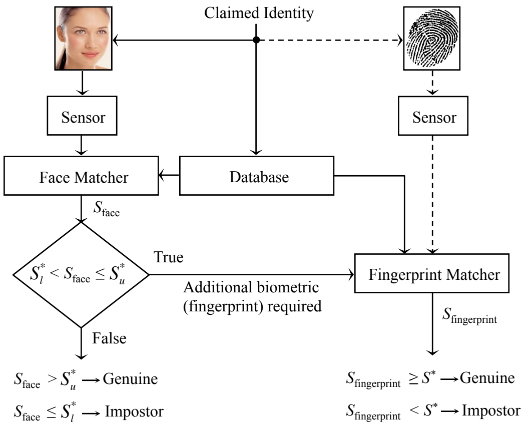
Claimed Identity
Sensor
Sensor
Face Matcher
Database
S_{face}
$S_l^* < S_{\text{face}} \leq S_u^*$
True
Additional biometric (fingerprint) required
Fingerprint Matcher
$S_{\text{fingerprint}}$
False
$S_{\text{face}} > S_u^* \rightarrow$ Genuine
$S_{\text{face}} \leq S_l^* \rightarrow$ Impostor
$S_{\text{fingerprint}} \geq S^* \rightarrow$ Genuine
$S_{\text{fingerprint}} < S^* \rightarrow$ Impostor

Figure 2. Outline of the considered multi-modal biometric system in serial fusion mode.

2.1.2 Serial fusion mode

We adopted the serial fusion framework based on a triple threshold approach proposed in [11], as outlined in Fig. 2. The user first only provides his face to the system, which is processed and matched against the respective template. If the face matching score S_{face} is greater than a predefined upper threshold S_u^*, the user is accepted as a genuine, else if $S_{\text{face}} \leq S_l^*$, the user is rejected as an impostor. If S_{face} falls in the interval $(S_l^*, S_u^*]$ ("uncertainty region", see Fig. 3), then the user has to present fingerprint as well to the system to be finally authenticated.[1] The motivation behind the use of face biometric at the first stage in the processing chain is thoroughly explained in Section 4.

To sum up, let $P(S|\text{Genuine})$ and $P(S|\text{Impostor})$ represent the conditional probability density functions of the fused similarity score S ranging in $[0, 1]$, for genuine and impostor users, respectively. Then for a particular threshold (S^*), the performance of a parallel multi-modal system, in terms of FAR (False Acceptance Rate) and FRR (False Rejection Rate), can be estimated as:

$$\text{FAR}(S^*) = \int_{S^*}^{1} P(S|\text{Impostor})\text{d}s, \qquad (1)$$

$$\text{FRR}(S^*) = \int_{0}^{S^*} P(S|\text{Genuine})\text{d}s. \qquad (2)$$

[1] This scheme can be extended to more than two biometrics as studied in [14], where the effect of estimation erros has also been discussed.

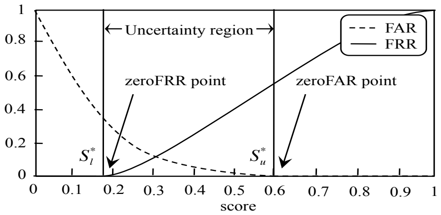

Figure 3. FAR and FRR as a function of the score value. The decision is taken by the fingerprint matcher, in the uncertainty region. Note that S_l^* and S_u^* are the two possible lower and upper acceptance thresholds, respectively, for the face matcher.

The overall performance of a serial system can be estimated as follows:

$$\text{FAR}(S^*) = \text{zeroFRR}_{\text{face}} \int_{S^*}^{1} P(S_{\text{fingerprint}}|\text{Impostor})\mathrm{d}s, \tag{3}$$

$$\text{FRR}(S^*) = \text{zeroFAR}_{\text{face}} \int_{0}^{S^*} P(S_{\text{fingerprint}}|\text{Genuine})\mathrm{d}s, \tag{4}$$

where $\text{zeroFRR}_{\text{face}} = \text{FAR}_{\text{face}}(S_l^* : \text{FRR}_{\text{face}}(S_l^*) = 0), \text{zeroFAR}_{\text{face}} = \text{FRR}_{\text{face}}(S_u^* : \text{FAR}_{\text{face}}(S_u^*) = 0)$ (see [11] for further details). Eqs. 1-4 allow one to compute the DET curves of the systems.

2.2. Vulnerability of multi-modal biometric systems to spoofing attacks

With the rapid growth in use of biometric systems, issues about their robustness and security against external attacks are also raising. Several researchers are investigating the vulnerabilities of biometric systems, the potential attacks and the related countermeasures. Eight possible different stages where security of biometric systems can be compromised have been identified in the literature. Among the others, submitting an artificial biometric replica of a genuine user, known as "spoofing attack", has been under investigation since the early 1900s [4]. Some works have also shown that iris and face verification systems may be fooled by using suitable contact lenses [9], and simple photographs [8] of a genuine user. Although several fake detection algorithms have been proposed to avoid spoofing attacks [1], state-of-the-art is not mature yet. The most general effect of liveness detection systems is the increase in FRR, because several "live" traits are misclassified as "fake". Therefore, the overall acceptability and performance of biometric verification systems decreases when they are embedded with liveness detection algorithms.

As mentioned in the introduction, multi-modal systems are commonly believed to be intrinsically more robust against spoofing attacks, under intuitive hypothesis that an attacker needs to spoof *all* fused biometric traits *simultaneously* in order to crack them. However, some recent works [13, 12, 10, 3, 5, 7] have questioned the validity of this belief, and have empirically shown that spoofing *only one* trait is sufficient to evade a parallel multi-modal system. Reported results with widely used fusion rules showed that the FAR under spoofing attacks can increase dramatically, even when only one trait is spoofed. Notably, most of the results in [13, 12, 10] were obtained under the pessimistic assumption that the attacker is able to fabricate a perfect replica of the genuine biometric trait, which was simulated by assuming that the distribution of matching scores of fake traits is identical to the one of genuine users. However, experiments carried out using real spoof attacks against fingerprints in [12], showed that the resulting score distribution was considerably different from the genuine one. Similar results were reported in [3, 5, 7], on real spoofing attacks against fingerprints and faces. This means that the above pessimistic condition is not always representative of real spoofing attacks.

To sum up, results in [13, 12, 10, 3, 5, 7] have shown that the robustness of multi-modal systems to spoofing attacks should not be taken for granted, and needs to be carefully investigated. So far, the vulnerability of *serial* multi-modal systems to real spoofing attacks has not been evaluated, despite they have some potential advantages over *parallel* ones. Hence, in this work we empirically investigate the robustness of serial systems, and compare it with the one of parallel systems, under various real spoofing scenarios.

3. Experimental setup

3.1. Data sets

Fingerprint spoofing. *LivDet2011.* This data set consists of 80 users; here, by "user" we mean a distinct finger, even if it belongs to the same individual. Each "live" finger and its corresponding fake replica were acquired in two different sessions, separated by about two weeks. All ten fingers of each indiviual were considered. Fake fingerprints were fabricated by consensual method described in [16]. The mold was produced using plasticine-like materials, while the spoofs were created with latex and silicon, which are commonly adopted materials. The fingerprint images were acquired using the well-known Biometrika FX2000 optical sensors. This data set is publicly available and was also used for assessing the performance of fingerprint liveness detection systems at the Second International Competition on Fingerprint Liveness Detection (LivDet11) [16].

Face spoofing. We used two data sets called Photo Attack and Print Attack, which was lately released publicly.

Photo Attack. This data set, collected by the authors, consists of "live" and "fake" face images acquired in two sessions, with a time interval of about two weeks between them, under different lighting conditions and facial expres-

Data set	Number of clients	Number of live per client	Number of spoofs per client
LivDet2011-Latex	80	5	3
LivDet2011-Silicon	80	5	3
Photo Attack	40	60	60
Print Attack	50	16	12

Table 1. Size and characteristics of the fingerprint and face data sets used in the experiments.

sions. The spoofed faces were fabricated using the "photo attack" method as in [8]. In this method photo of the targeted user is displayed on a laptop screen, which is then captured through the camera. To this aim, we used the testing live face images of the users, thus simulating a scenario in which the attacker can obtain photos of the targeted user under a setting similar to the one of the verification phase.

Print Attack. After the "Competition on countermeasures to 2D facial spoofing attacks", held in conjunction with the International Joint Conference on Biometrics in 2011, the Print Attack data set was made publicly available [8]. The data set is composed of 200 video clips of printed-photo attack attempts to 50 users, under different lighting conditions, and of 200 real-access attempts from the same user. We extracted the "live" and spoofed face images from the corresponding videos. In particular, for each user, we extracted 12 "live" face images and 16 spoofed face images from each video clip.

The size and the characteristics of the above data sets are summarized in Table 1.

3.2. Fusion rules

To evaluate serial and parallel multi-modal systems under spoofing attacks, we adopted one fixed rule (Product) and two trained ones (Weighted product and Likelihood ratio) in parallel fusion mode.

Product. The fused score is obtained as: $S = S_{\text{face}} \times S_{\text{fingerprint}}$.

Weighted product. $S = S_{\text{face}}^{w} \times S_{\text{fingerprint}}^{1-w}$.
The weight w was computed by maximizing the system performance on a given operational point, namely, by minimizing FRR on training data, for a given value of FAR.

Likelihood ratio (LLR). It is based on setting a threshold on the ratio:

$$\frac{p(S_{\text{face}}|\mathrm{G}) \cdot p(S_{\text{fingerprint}}|\mathrm{G})}{p(S_{\text{face}}|\mathrm{I}) \cdot p(S_{\text{fingerprint}}|\mathrm{I})} \ ,$$

where the distributions $p(\cdot|\mathrm{G})$ and $p(\cdot|\mathrm{I})$ were approximated by fitting training data with a Gamma distribution, which provided a good approximation of our data.

3.3. Experimental protocol

We adopted the following experimental protocol:

- Since no multi-modal data sets including spoofing attacks are publicly available, we created four *chimerical* multi-modal data sets, by combining the face and fingerprint images of pairs of clients of the available fingerprint (Latex and Silicon Spoofs) and face (Photo Attack and Print Attack) data sets. Creating chimerical data sets is a common procedure exploited in works on multi-modal systems, when no real data sets are available [15].
- We run the above procedure ten times, obtaining ten different chimerical data sets. For each data set, we used 40% of the users as training set, and the remaining ones as testing set. Reported results are average values over the 10 runs.
- The fake matching scores were computed by comparing each fake image of a given user with the corresponding template image.
- The performance was evaluated by computing Detection Error Trade-off (DET) curves. A DET curve is obtained by plotting the FRR as a function of the FAR, obtained by varying the decision threshold. Note that the FAR under spoofing attacks is defined as the percentage of spoof attempts that got accepted as genuine, which is also referred to as Spoof FAR (SFAR) [10].

  The fingerprint and the face verification systems used for the experiments were implemented using the NIST Bozorth3[2] and the Elastic Bunch Graph Matching (EBGM)[3] matching algorithms, respectively.

  We investigated three attack scenarios: (a) only fingerprints are spoofed; (b) only faces are spoofed; (c) both fingerprints and faces are spoofed (both spoofing).

4. Experimental Results

The results are reported in Figs. 4-5. For sake of space, we report only the results on two out of the four data sets used in the experiments: latex spoofed fingerprints and photo-attack spoofed faces (Figs. 4-5, first and second columns); silicon spoofed fingerprints and print-attack spoofed faces (Figs. 4-5, third and fourth columns). Each column of Figs. 4-5 refer to different fusion rule in parallel system as well as corresponding serial one. Qualitatively similar results were obtained with other two data sets and weighted product rule.

Additionally, the results of Fig. 5 are tabulated in Tables 2-3. We report the performance attained by all fusion

[2] www.nist.gov/itl/iad/ig/nbis.cfm

[3] www.cs.colostate.edu/evalfacerec/algorithms5.php

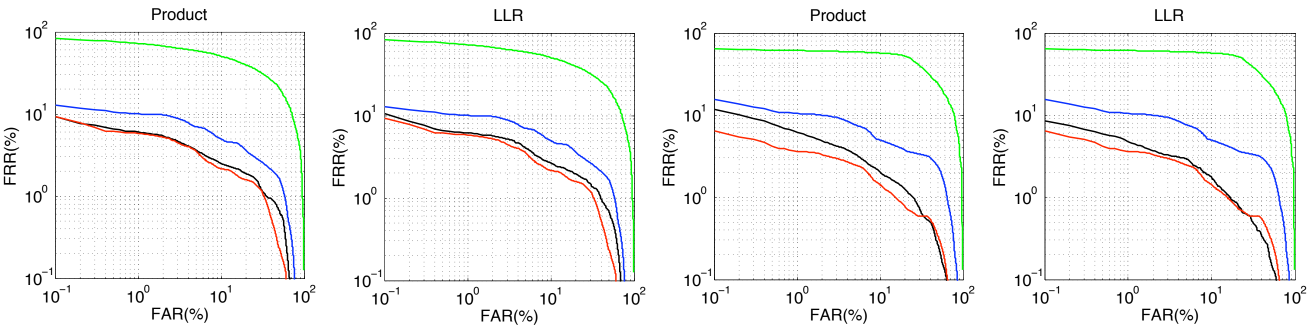

Figure 4. Average DET curves attained under normal operation on the test set using latex spoofed fingerprints and photo attack spoofed faces (first and second columns), and using silicon spoofed fingerprints and print attack spoofed faces (third and fourth columns). Each column refers to a different parallel score fusion rule, indicated in the title of each plot. Each plot contains the DET curves of the systems with no spoofing attack. Green: unimodal face system. Blue: unimodal fingerprint system. Red: serial multi-modal system. Black: parallel multi-modal system.

rules (including the weighted product rule) and serial system, for EER operating point. This allows us to compare more directly performance (in terms of FAR and FRR) and robustness to spoofing attacks (in terms of SFAR), besides making the results better accessible. Furthermore, the tables also give information about the standard deviation of EER and SFAR, which is not provided by the DET curves.

We can first observe in Fig. 4 that, under normal operation (i.e., no spoofing attacks), fusion in both modes improved the performance with respect to the best individual matcher (fingerprint, here). In particular, the performance of the adopted serial fusion scheme is comparable with that of the standard parallel fusion schemes.

Specifically, taking into account the same verification time of face and fingerprint matcher of [11], respectively 0.1 and 3 s, the average genuine users verification time is about 1.7 and 3 s for the "face → fingerprint" (system used in this work) and the "fingerprint → face" serial systems, respectively (we refer reader to [11] for further details). The average verification time of parallel fusion is always equal to that of the slowest biometric (i.e., 3 s), instead. Moreover, we found that under normal operation "face → fingerprint" serial systems performed much better than "fingerprint → face" ones, namely, quoting from [11], "the best serial combination is always made up of the worst matcher followed by the best one". Hence, we adopted "face → fingerprint" system in this work.

From Fig. 5, it is easy to see that the performance of the serial and parallel multi-modal systems under a real spoofing attack against only one trait is significantly worse than under normal operation. However, the performance of the serial systems under spoof attacks is better than the one attained by parallel ones, in all spoofing scenarios. Accordingly, we can say that the serial systems considered in our experiments exhibited a higher robustness to real spoofing attacks, than the corresponding parallel systems.

It is also worth noting that in all the considered systems the increase in FAR when only fingerprints are spoofed is much higher than when only faces are spoofed. Namely, attacking the most accurate biometric is an effective and opportunistic strategy for the attacker. Thereby, our results substantiate an additional befit of using fingerprint matcher at the second stage in a face and fingerprint serial system.

To sum up, our results provide some evidence that multi-modal systems, in both serial and parallel fusion modes, are vulnerable to spoofing attacks. However, the performance of serial systems is much better (although still not suitable for requirements of security applications) than that of parallel ones. Accordingly, serial multi-modal systems can attain a better trade-off between performance, verification time, user acceptability and robustness against spoofing attacks.

Rule/System	No Spoof EER%	Face SFAR%	Fing. SFAR%	Both SFAR%
Product	4.06±1.1	4.84±1.3	62.52±2.4	67.45±1.9
W. Product	4.46±1.2	4.71±2.5	63.22±2.6	65.04±2.4
LLR	4.40±1.1	6.47±1.0	95.20±2.4	97.01±2.6
Serial	4.00±0.8	4.39±0.9	57.29±2.0	62.12±2.1

Table 2. SFAR at EER (no spoof) for the considered fusion rules and serial system on LivDet2011-Latex and Photo Attack.

Rule/System	No Spoof EER%	Face SFAR%	Fing. SFAR%	Both SFAR%
Product	3.87±0.9	6.87±1.2	36.62±2.7	53.88±3.1
W. Product	3.69±1.0	4.28±2.7	42.81±2.1	46.67±1.6
LLR	3.20±1.0	6.60±2.9	70.71±2.2	88.39±3.2
Serial	2.98±1.1	3.74±2.6	32.85±2.0	40.11±2.5

Table 3. SFAR at EER (no spoof) for the considered fusion rules and serial system on LivDet2011-Silicon and Print Attack.

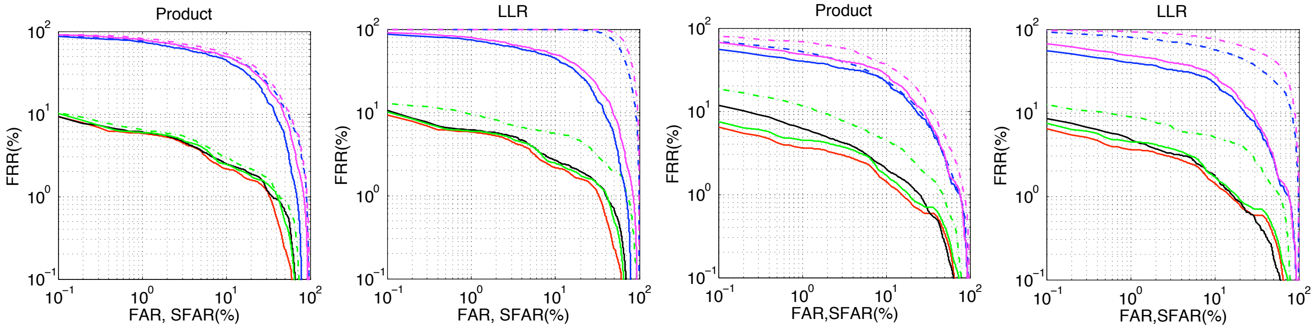

Figure 5. Average DET curves attained on the test set using latex spoofed fingerprints and photo attack spoofed faces (first and second columns), and using silicon spoofed fingerprints and print attack spoofed faces (third and fourth columns). Each column refers to a different parallel score fusion rule, indicated in the title of each plot. Each plot contains the DET curves attained on multi-modal system with no spoofing attack: serial (red curve) and parallel (black curve), and under real spoofing attacks: serial (solid curves) and parallel (dashed curves). blue: fingerprint spoofing only. green: face spoofing only. magenta: both face and fingerprint spoofing.

5. Conclusions

Recent works have analyzed the impact of simulated and real spoofing attacks on parallel multi-modal biometric systems. In this paper, we investigated the robustness of serial multi-modal systems, and compared it with the corresponding parallel systems, using large data sets of real spoofing attacks. Our results confirm that the considered score level fusion rules, that are among the most used ones in the literature, are not intrinsically robust to spoofing attacks, as believed until very recently, since they can be evaded by spoofing only one biometric trait. We also found that spoofing the most accurate biometrics makes more likely to evade a multi-modal system. Nevertheless, we found evidence that serial multi-modal systems are more robust than parallel ones, and can attain a better trade-off between performance, verification time, user acceptability and robustness against spoofing attacks.

Future work will focus on investigating the robustness against spoofing attacks of serial systems consisting of more than two matchers, and of systems that combine both serial and parallel fusion.

Acknowledgment

This work was partly supported by the TABULA RASA project, 7th Framework Research Programme of the European Union (EU), grant agreement number: 257289.

References

[1] J. Daugman. High Confidence Visual Recognition of Persons by a Test of Statistical Independence. *J. IEEE Trans. on Pattern Analysis and Machine Intell.*, 15(11): 1148-1161.1993.

[2] 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). *Patt. Recog. Lett.*, 31(9):884–890, 2010.

[3] Z. Akhtar. Security of Multimodal Biometric Systems against Spoof Attacks. *PhD thesis, University of Cagliari, Italy*, 2012.

[4] B. Geller et al. Chronological Review of Fingerprint Forgery. *J. of Forensic Sciences*, 44(5): 963-968, 1999.

[5] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli. Robustness of multi-modal biometric verification systems under realistic spoofing attacks. *Int. Joi. Conf. Biometrics*, 2011.

[6] A. Ross, A. Rattani and M. Tistarelli. Exploiting the Doddington Zoo Effect in Biometric Fusion. *3rd IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2009.

[7] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli. Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, 1(1):11–24, 2012.

[8] S. Marcel et al. Competition on counter measures to 2-D facial spoofing attacks. *Int'l Joint Conf. on Biometrics (IJCB)*. 2011.

[9] X. He, Y. Lu, and P. Shi. A fake iris detection method based on FFT and quality assessment. *Chinese Conf. on Pattern Recognition*, pp. 316–319, 2008.

[10] P. A. Johnson, B. Tan, and S. Schuckers. Multi-modal fusion vulnerability to non-zero effort (spoof) imposters. *IEEE Workshop on Info. Forensics and Security (WIFS)*, pp. 1–5, 2010.

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

[12] R. N. Rodrigues, N. Kamat, and V. Govindaraju. Evaluation of biometric spoofing in a multi-modal system. *IEEE Int'l Conf. on Biometrics: Theory App. and Sys.*, pp. 1–5, 2010.

[13] R. N. Rodrigues, L. L. Ling, and V. Govindaraju. Robustness of multi-modal biometric fusion methods against spoof attacks. *J. of Visual Lang. and Computing*, 20:169–179, 2009.

[14] G. L. Marcialis, P. Mastinu, and F. Roli. Serial fusion of multi-modal biometric systems. *IEEE BioMS*, pp. 1-7, 2010.

[15] A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*, 2006.

[16] S. Schuckers et al. LivDet2011- fingerprint liveness detection competition 2011. *Int'l Conf. on Biometrics (ICB)*, 2012.