International Journal of Information Processing, 8(3), 42-50, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Serial and Parallel Biometric Fusions under Spoofing Attacks

Zahid Akhtar[a]

[a]Dept. of Mathematics and Computer Science, University of Udine, Udine 33100, Italy,
Contact: zahid.akhtar@uniud.it

In this paper, we investigate the robustness of multimodal biometric systems against spoofing attacks. A few recent works have questioned, contrary to a common claim, that a multimodal system in parallel fusion mode can be cracked even if a single biometric trait is spoofed. Robustness of multimodal biometric systems in serial fusion mode against spoofing attacks has so far not been investigated. We compare the performance of the multimodal systems with each mode under different spoofing attack scenarios. We carry out the assessment, first under worst-case scenario, state-of-the-art method, that the attacker is able to fabricate an exact replica of the genuine biometric trait and then validate our findings using *realistic* spoofing attacks obtained by fabricating fake biometric traits, namely non-worst case scenarios. We empirically found that multimodal biometric systems in both fusion modes are not intrinsically robust against spoofing attacks as believed so far. In particular, multimodal systems in serial fusion mode can be even less robust than systems in parallel mode, when only the best individual matcher is spoofed. Nonetheless, systems in serial fusion mode can be more robust than systems in parallel mode, when all matchers are spoofed.

Keywords : Biometrics, Biometric Fusion, Multimodal Systems, Robustness Evaluation, Spoofing Attacks.

1. INTRODUCTION

Biometrics is a scientific method to identify a person based on their physiological or behavioral traits such as face, fingerprint and so on. Due to increased security demands, individuals, governments and industries have greatly accepted and deployed biometrics as an authentic technique. Each biometric trait is supposed to pose attributes like uniqueness, universality, acceptability and hard to forge [1]. Unfortunately, recent researches have shown that an attacker can steal, copy, capture and reproduce the biometric traits to attack the biometric systems [2–4]. This kind of attack, faking biometric trait input to the system is known as *spoofing attack*. Spoofing attack is related to the sensor, and is also called as "direct attack".

With the great usage of biometric based security systems, their issues about resilience and security against attacks are also raising. Several researchers are studying the vulnerabilities of biometric systems, the potential attack mechanisms with their counteractions. As pointed out in [5], a generic biometric system has eight vulnerable points that can be exploited by an attacker to get unauthorized access to a system. Among the others, spoofing attack is a growing concern. Spoofing attack does not require developed technical skill and information about the system's internal operational mechanism, leading to increased number of potential attackers. For instance, 60% fake fingerprints reproduced using gum were accepted as legitimate user by the system in [2]. One possible counteraction suggested in literature is "liveness" detection (vitality testing) [4], but no method is fully matured yet.

Besides "liveness" detection, multimodal biometric systems have been proposed to enhance the recognition accuracy as well as security against attacks as compared to the unimodal (one single) biometric systems that made them up. Extensive empirical evidences have shown that they are effective to accuracy improvement. It is also claimed that multimodal systems are more robust against spoofing attacks,

Table 3
FAR (%) of the Face-Fingerprint system in parallel fusion mode, with the Sum, Weighted Sum rules (top), and Face-Fingerprint and Fingerprint-Face Systems in serial fusion mode (bottom), when either the fingerprint, the face or both, the fingerprint and face are spoofed, at three operating points.

Operating Point	Face-Fingerprint system in parallel fusion mode					
	Sum			W. Sum		
	Fing. Sp.	Face Sp.	Both Sp.	Fing. Sp.	Face Sp.	Both Sp.
0% FAR	41.39	1.69	53.60	39.87	1.00	48.11
0.01% FAR	52.14	3.09	63.67	50.75	2.30	57.89
0.1% FAR	63.91	5.05	76.50	59.84	3.66	63.93

Operating Point	Face-Fingerprint system in serial fusion mode			Fingerprint-Face system in serial fusion mode		
	1st Stage	2nd Stage	Both Stages	1st Stage	2nd Stages	Both Stages
	Face Sp.	Fing. Sp.	Both Sp.	Fing. Sp.	Face Sp.	Both Sp.
0% FAR	7.40	45.59	41.69	44.60	7.88	6.27
0.01% FAR	16.30	61.05	56.41	59.70	18.30	15.70
0.1% FAR	26.30	68.99	66.89	67.50	28.54	24.33

matchers are spoofed.

In the future, we will further analyze the robustness of the systems by constructing proper large data set containing real spoof attacks, and also evaluate the robustness of the system in serial fusion mode with parallel fusion mode at it's last stage in the processing chain.

REFERENCES

1. A K Jain, A Ross, S Prabhakar. An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.
2. T Matsumoto, H Matsumoto, K Yamada and S Hoshino. Impact of Artificial "Gummy" Fingers on Fingerprint Systems, *In Optical Security and Counterfeit Deterrence Techniques IV*, 4677:275–289, 2002.
3. X He, Y Lu and P Shi. A Fake Iris Detection Method Based on FFT and Quality Assessment, *In Proceedings of Chinese Conference on Pattern Recognition*, pages 316–319, 2008.
4. Y Kim, J Na, S Yoon and J Yi. Masked Fake Face Detection using Radiance Measurements, *Journal of Opt. Soc. Am.* , 26(4):760–766, 2009.
5. Nalini K Ratha, Jonathan H Connell and Ruud M Bolle. An Analysis of Minutiae Matching Strength, *In Proceedings of Third AVBPA*, pages 223–228, 2001.
6. A Ross, K Nandakumar, A K Jain. *Handbook of Multibiometrics, Springer*, 2006.
7. R N Rodrigues, L L Ling and V Govindaraju. Robustness of Multimodal Biometric Methods against Spoof Attacks, *Journal of Visual Languages and Computing*, 20(3):169–179, 2009.
8. R N Rodrigues, N Kamat and V Govindaraju. Evaluation of Biometric Spoofing in a Multimodal System, *In Proceedins of Fourth IEEE International Conference on Biometrics: Theory Applications and Systems*, pages 1–5, 2010.
9. P A Johnson, B Tan and S Schuckers. Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters, *In Proceedings of IEEE Workshop on Information Forensics and Security*, pages 1–5, 2010.
10. Zahid Akhtar and Nasir Alfarid. Secure Learning Algorithm for Multimodal Biometric Systsems against Spoof Attacks, *In Proceedings of International Conference on Information and Network Technology (ICINT 2011)*, pages 52–57, 2011.

11. Zahid Akhtar, Battista Biggio, Giorgio Fumera and Gian Luca Marcialis. Robustness of Multimodal Biometric Systems under Realistic Spoof Attacks against All Traits, *In Proceedings of IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS 2011)*, pages 5–10, 2011.
12. Battista Biggio, Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis and Fabio Roli. Robustness of Multi-Modal Biometric Verification Systems under Realistic Spoofing Attacks, *In Proceedings of International Joint Conference on Biometrics (IJCB 2011)*, Washington DC, USA, October, 2011.
13. Zahid Akhtar and Sandeep Kale. Performance of Multimodal Biometric Systems Against Spoof Attacks, *In Proceedings of International Conference on Innovative Science and Engineering Technology*, Rajkot, India, April 08-09, 2011.
14. Zahid Akhtar, Sandeep Kale and Nasir Alfarid. Spoof Attacks on Multimodal Biometric Systems, *In Proceedings of International Conference on Information and Network Technology (ICINT 2011)*, pages 46–51, 2011.
15. Zahid Akhtar and Sandeep Kale. Security Analysis of Multimodal Biometric Systems against Spoof Attacks, *In Proceedings of First International Conference on Advances in Computing and Communications (ACC-2011)*, pages 604–611, 2011.
16. K Takabashi, M Mimura, Y Isobe and Y Seto. A Secure and User-Friendly Multi-Modal Biometric System, *In Proceedings of SPIE on Biometric Technology for Human Identification*, 54(4):12–19, 2004.
17. G L Marcialis, F Roli and L Didaci. Personal Identity Verification by Serial Fusion of Fingerprint and Face Matchers, *Pattern Recognition Letters*, 42(11):2807–2817, 2009.
18. L Allano, B Dorizzi, S Garcia-Salicetti. Tuning Cost and Performance in Multimodal Biometric Systems: A Novel and Consistent View of Fusion Strategies based on the Sequential Probability Ratio Test (SPRT), *Pattern Recognition Letters*, 31(9):884–890, 2010.
19. C Y Suen, L Lam. Multiple Classifier Combination Methodologies for Different Output Levels, *In Proceedings of International Workshop on Multiple Classifier Systems (MCS)*, pages 52–66, 2000.
20. Duda R, Hart P and Stork D. *Pattern Classification, John Wiley Inc.*, 2001.
21. Ajay Kumar, Vivek Kanhangad and David Zhang. A New Framework for Adaptive Multimodal Biometrics Management. *IEEE Transactions on Information Forensics and Security*, 5(1):92–102, 2010.
22. NIST: `http://www.itl.nist.gov/iad/894.03/biometricscores/index.html`
23. Libor Spacek. University of Essex Face Database, `http://dces.essex.ac.uk/mv/allfaces/index.html`
24. PolyU HRF Database, `http://www.comp.polyu.edu.hk/~biometrics/HRF/HRF.htm`
25. G Pan, Z Wu and L Sun. Liveness Detection for Face Recognition. *Recent Advances in Face Recognition*, pages 236–252, 2008.
26. David Zhang, Vivek Kanhangad, Nan Luo and Ajay Kumar. Robust Palmprint Verification Using 2D and 3D Features. *Pattern Recognition*, 43(1):358–368, 2010.
27. Kyungnam Kim. Face Recognition using Principal Component Analysis. *Department of Computer Science, University of Maryland*, College Park, USA, 2000.
28. D Maltoni, D Maio, A K Jain and S Prabhakar. *Handbook of Fingerprint Recognition, Springer*, 2003.

Zahid Akhtar is a research scientist in Artificial Vision and Real Time Systems Laboratory at the Dept. of Mathematics and Computer Science, University of Udine (Italy). In 2012, he got his Ph.D degree in Electronic and Computer Engineering at the University of Cagliari (Italy). He thrice received outstanding young researcher fellowships awarded by the Italian Ministry of University and Research. His research is focused on Pattern Recognition and it's applications in Biometrics and Image processing.