Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection

Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia

Biometrics Recognition Group - ATVS, Escuela Politecnica Superior
Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente, 11
Campus de Cantoblanco - 28049 Madrid, Spain

{javier.galbally, julian.fierrez, javier.ortega}@uam.es

Abstract. A review of the state-of-the-art in direct and indirect attacks to fingerprint and iris automatic recognition security systems is presented. A summary of the novel liveness detection methods, which take advantage of different physiological properties to distinguish between real and fake biometric traits, is also reported.

1 Introduction

Biometric systems can offer several advantages over classical security methods based on something you know (PIN, Password, etc.) or something you have (key, card, ID, etc.) [1, 2]. Traditional authentication systems are not prepared to discriminate between impostors who have illegally acquired the privileges to access a system and the genuine user. Furthermore, in biometric systems there is no need for the user to remember difficult PIN codes that could be easily forgotten or to carry a key that could be lost or stolen.

However, in spite of these advantages, biometric systems have some drawbacks [3], including: *i*) the lack of secrecy (e.g. everybody knows our face or could get our fingerprints), and *ii*) the fact that a biometric trait cannot be replaced (if we forget a password we can easily generate a new one, but no new fingerprint can be generated if an impostor "steals" it). Furthermore, biometric systems are vulnerable to external attacks which could decrease their level of security.

In [4] Ratha identified and classified eight different points of attack on biometric recognition systems, which are depicted in Fig. 1. These vulnerability points can broadly be divided into two main groups:

Direct attacks. In [4] the possibility to generate synthetic biometric samples (for instance, speech, fingerprints or face images) in order to fraudulently access a system was discussed and defined as the first vulnerability point in a biometric security system. These attacks at the sensor level are referred to as direct attacks. It is worth noting that in this type of attacks no specific knowledge about the system operation is needed (matching algorithm used, feature extraction, feature vector format, etc). Furthermore, the attack is carried out in the analog domain, outside the digital limits of the system, so the digital protection mechanisms (digital signature, watermarking...) can not be used.

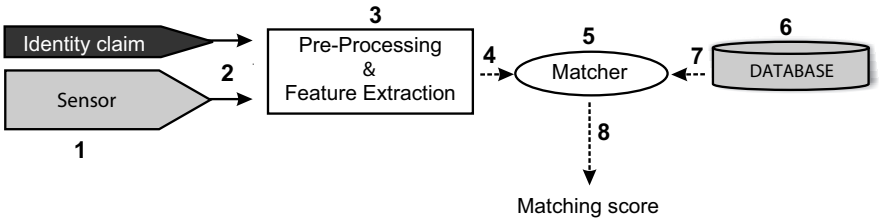

Fig. 1. Architecture of an automated biometric verification system. Possible attack points are numbered from 1 to 8.

Indirect attacks. This group includes all the remaining seven points of attack identified in [4]. Attacks 3 and 5 might be carried out using a Trojan Horse that bypasses the feature extractor, and the matcher respectively. In attack 6 the system database is manipulated (a template is changed, added or deleted) in order to gain access to the application. The remaining points of attack (2, 4, 7 and 8) are thought to exploit possible weak points in the communication channels of the system, extracting, adding or changing information from them. In opposition to direct attacks, in this case the intruder needs to have some information about the inner working of the recognition system and, in most cases, physical access to some of the application components (feature extractor, matcher, database...) is required.

In the present paper we summarize the most relevant attacks carried out on biometric recognition systems based on fingerprints and iris, with special emphasis on the fingerprint trait, where big research efforts on its vulnerability have been made. Some of the recently developed liveness detection techniques, which act as countermeasures against direct attacks, are also introduced.

This paper is structured as follows. Attacks on fingerprint and iris verification systems are reported in Sect. 2. A summary of direct attacks in the fingerprint trait can be found in Sect. 2.1, while indirect attacks to fingerprint recognition systems and direct attacks to iris-based security systems are detailed in Sect. 2.2 and Sect. 2.3 respectively. In Sect. 3.1 and Sect. 3.2 the liveness detection methods used in fingerprint- and iris-based applications are presented. Finally some general conclusions are drawn in Sect. 4.

2 Attacks on Fingerprint and Iris Verification Systems

2.1 Direct attacks on fingerprint-based recognition systems

Fingerprint verification systems are currently the most widely spread in the biometric market commanding more than half of the industry [5], thanks to their high acceptability among users, their use in the forensic environment, and the fact that they can be easily embedded in many electronic devices such as PDA's, mobile phones, keyboards, etc. This has given rise to a big interest in

the scientific community to study the robustness of this type of systems to direct attacks.

There have been different studies reported in literature regarding the analysis of vulnerabilities of fingerprint-based biometric systems to direct attacks. In [6] the authors classify the different methods to create gummy fingers in two main categories: with and without the cooperation of the legitimate user. In [6] two methods are described (one of each class) and results on six commercial sensors (optical and solid state) are reported. Out of the six sensors tested five of them accepted the imitation as real on the first attempt while the remaining sensor permitted the access to the system on the second attempt.

Matsumoto et al. [7] carried out similar experiments to those reported in [6] this time with fake fingerprints made of gelatin. Again they distinguished between the case in which they had the cooperation of the fingerprint owner and the situation in which the latent fingerprint had to be lifted from a surface. In the case in which the genuine user cooperated to make the gummy fingers, recognition rates between 68 and a 100% were reported for the fake fingerprints in all the 11 systems tested. For the imitations generated without the cooperation of the user the acceptance rate was always above 60%.

More recently, in [8] the authors tested two fingerprint verification systems, one minutiae based and the other one based on the ridge pattern, over a database of over 500 real samples and as many fake images captured with two different sensors (optical and thermal sweeping). The gummy fingers were made out of modeling silicone and three scenarios were considered in the experiments, namely: *i*) enrolment and test with real fingerprints, *ii*) enrolment and test with fake fingerprints, and *iii*) enrolment with real fingerprints and test with the respective imitations. Both systems showed a considerable decrease in their level of performance when being attacked (third scenario considered).

Some other interesting experiments concerning direct attacks on fingerprint-based verification systems can be found in [9] and [10].

2.2 Indirect Attacks on fingerprint-based recognition systems

Although Hill in [11] reported an attack to a biometric system database (vulnerability point 6 in Fig. 1), most of the works regarding indirect attacks use some type of variant of the hill climbing technique [12]. In this preliminar work a basic hill climbing attack is introduced and tested over a simple image recognition system based on filter-based correlation. This attack uses the score given by the matcher to iteratively change a synthetically created template until the score exceeds a fixed decision threshold and the access to the system is granted. Thus, depending on whether we create a synthetic image file or we directly generate the synthetic feature vector, these attacks can belong to type 2 or 4, respectively.

When the hill climbing is directed to the input of the feature extractor (type 2 attack), no information about the template storage format is required. Only the size and file format presented to the feature extractor is needed. Adler proposed in [13] a type 2 attack with a face recognition system. The input image is conveniently modified until a desired matching score is attained. Adler reports

results on three comercial recognition systems and shows that after 4000 iterations a score corresponding to a very high confidence (99.9%) of matching scores is reached for all systems tested.

In [14] Uludag and Jain introduced a hill climbing algorithm to attack a fingerprint verification system which was further studied in [15]. In these attacks a synthetic random minutia template is presented to the input of the matcher (type 4 attack) and, according to the score generated, it is iteratively changed until the system returns a positive verification. The minutiae in the template are modified one at a time and the change is only stored if the score returned by the matcher improves the previous one, otherwise it is discarded. Thus, to carry out this type of attack we need: *i*) the resolution and size of the images captured by the sensor (which is usually a parameter specified by the vendor), *ii*) the template format, and *iii*) access to the matcher input (to present the synthetic templates) and output (to get the necessary feedback from the scores). In this case we know *how* the information is stored, but not *what* the information is.

In [16] Cappelli et al. describe a fast and reliable method to generate realistic synthetic fingerprint images, which is implemented in the software tool SFinGe (Synthetic Fingerprint Generator). With this application, a type 4 attack (to the input of the matcher) using synthetic generated templates could easily be converted to a type 2 attack (to the input of the feature extractor) using the corresponding synthetic fingerprint images. Thus, the attack would be simplified as the intruder would not need to know the storage format used in the system. Furthermore, an algorithm to reconstruct the real fingerprint image from its ISO minutia-based template has been recently proposed in [17]. In this case, if a legitimate user's template is compromised it could be used to carry out a type 2 attack against the system (reconstructing the real fingerprint image), or even a direct attack (building a gummy fingerprint from the image).

2.3 Direct attacks on iris-based recognition systems

Although the iris acquisition process still leaves room for improvement (collecting good quality iris images from medium distances is still an open issue), the iris is one of the most strongly emerging biometric traits in the market, thanks to the high accuracy of the algorithms used in its recognition. Iris-based verification systems have shown a remarkable performance on normal operation conditions, however, several works have pointed out their vulnerabilities to very simple direct attacks carried out with photographs of the user's iris.

One of the first efforts in the vulnerabilities study of iris verification systems was carried out by Thalheim and Krissler and reported in [9]. In this work an iris image of a legitimate user was printed with a high resolution inkjet printer to fraudulently access the system. The trick was only successful if the pupil in the image was cut off and the eye of the impostor placed behind the paper to give the impression to the system of a real eye. Only one commercial system (the Panasonic's Authenticam BM-ET100) was tested in the experiments showing high vulnerability to this type of attacks. It not only permitted the access with

the fake iris, but also allowed the attacker to log on to the system using the iris picture.

In [18] Matsumoto et al. carried out the first systematic experiment of iris spoofing. Three different iris verification systems were tested, two portable: the IrisPass-h by Oki, and the Authenticam BM-ET100US by Panasonic, and the remaining system being a hard-core device for gate control (IrisPass-WG by Oki). Two different devices were used in the experiments to acquire the images for the fake irises, the camera embedded in the IrisPass-h system and a digital microscope with infrared lighting. As explained in Thalheim's experiments, the images were then printed using a high resolution inkjet printer and the pupil removed from the picture in order to place the impostor's eye behind the fake iris. When using the images taken with the IrisPass camera, all three systems accepted the fake irises as real with a probability of over 50%. In the case of the digital microscope pictures, the attacks success rate was over 15% for the portable systems, and around 5% for the gate control application or bitches.

3 Liveness Detection Methods

3.1 Liveness detection using fingerprints

As a countermeasure against direct attacks, several methods to discriminate between real and fake fingerprints have been proposed over the last few years. One of the first efforts in liveness detection was reported in [19], where the periodicity of sweat and the sweat diffusion pattern were used to detect fake fingerprints applying a ridge signal algorithm. The same technique but using a wavelet-based algorithm was described in [20]. These two works were extended in [21] where a new intensity-based perspiration liveness detection technique is described, reporting detection rates between 90% and 100%.

In [22] Cappelli defined a skin distortion model which is used in [23] to develop a novel liveness detection method based on skin elasticity properties. The user is asked to deliberately rotate his finger when removing it from the sensor surface thus producing considerable skin distortion which is later used as a fingerprint liveness measure. The system was attacked with gummy fingerprints showing a significant improvement over the robustness of the application functioning without the anti spoofing technique (over 95% of the intruders were rejected).

Some research has been carried out to use odor as a liveness detection procedure. In [24] an odor sensor (electronic nose) is used to discriminate the skin odor from that of other materials such as latex, silicone or gelatin. Although the system showed a remarkable performance detecting fake fingerprints made of silicone, it still showed some weakness recognizing imitations made of other materials such as gelatine, as the sensor response was very similar to that caused by human skin.

3.2 Liveness detection using iris

The experiments reported in [9] and [18] have shown the necessity of incorporating liveness detection techniques in the commercial iris verification applications

in order to prevent eventual direct attacks carried out against the system. In the last few years several efforts have been made in this direction, leading to different iris liveness detection methods.

In [25] Daugman proposes some eye features that could be used as countermeasures against direct attacks. Among these characteristics he mentions the spectrographic properties of different parts of the eye (tissue, fat, blood, melanin pigment), the coaxial retinal back reflection (the red eye effect) and the four Purkinje reflections caused by each of the four optical surfaces comprised inside the eye. These reflections can only be observed with very high quality cameras not used in common iris identification systems.

A second group of possible anti spoofing mechanisms highlighted in [25] are those based on behavioural eye features. One of these liveness detection methods is based in the detection of the eye hippus, which is the permanent oscillation that the eye pupil presents even under uniform lighting conditions. Another possibility is to measure the pupil response to a sudden lighting event (switching on of a diode) or to ask the user to do voluntary actions (eye movements, eye blinks). Although all these features could work for liveness detection porpuses, no real implementation is described, nor results reported in [25].

More recently, Pacut and Czajka proposed in [26] a third group of possible anti-spoofing measures different to the spectrographic and behavioral methods suggested by Daugman. This third group of techniques uses the external eye features, such as frequency analysis and 3D detection (passive measurement) or inflicted infrared light reflections from the moist cornea (active measurement), to distinguish between real and fake eyes. In this work, three different liveness detection techniques are described and implemented, and several tests are carried out on a database of over 700 real and printed eye images. Each of the three methods is based on Frequency Spectrum Analysis, Controlled Light Reflection Analysis and Pupil Dynamics Analysis, respectively. Two cameras were used in the experiments (the ET100 and ET300 by Panasonic), and all three techniques showed remarkable performance in the fake eye detection.

4 Conclusions

In order to improve the performance of biometric systems it is of great importance to study its vulnerabilities to external attacks. In the recent years several works have reported experimental results regarding the robustness of automatic recognition systems to direct and indirect attacks. In the present paper a state-of-the-art review of the attacks to fingerprint- and iris-based security systems has been presented. Some of the countermeasures based on physiological properties (i.e. liveness detection methods) proposed in the literature to improve the robustness of the systems, are also summarized.

Acknowledgments. This work has been supported by the TIC2006-13141-C03-03 project of the Spanish Ministry of Science and Technology and the BioSecure NoE. The author J. G. is supported by a FPU fellowship from the Ministerio

de Educacion y Ciencia (Spanish Ministry of Science). J. F. is supported by a Marie Curie Fellowship from the European Commission.

References

1. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. IEEE Trans. on Information Forensics and Security **1**(2) (2006) 125–143
2. Wayman, J., Jain, A., Maltoni, D., Maio, D.: Biometric systems. Technology, design and performance evaluation. Springer (2005)
3. Schneier, B.: The uses and abuses of biometrics. Communications of the ACM **48** (1999) 136
4. Ratha, N., Connell, J., Bolle, R.: An analysis of minutiae matching strength. Proc. AVBPA, International Conference on Audio- and Video-Based Biometric Person Authentication III (2001) 223–228
5. IBG: Biometrics market and industry report 2007-2012. Technical report, IBG (2006)
6. van der Putte, T., Keuning, J.: Biometrical fingerprint recognition don't get your fingers burned. In: IFIP. (2000) 289–303
7. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. In: Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV. Volume 4677. (2002) 275–289
8. Galbally, J., Fierrez, J., Rodriguez-Gonzalez, J.D., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M.: On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In: Proc. of IEEE International Carnahan Conference on Security Technology. Volume 1. (2006) 130–136
9. Thalheim, L., Krissler, J.: Body check: biometric access protection devices and their programs put to the test. c´t magazine (2002)
10. Kang, H., Lee, B., Kim, H., Shin, D., Kim, J.: A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In: KES. LNAI-2774, Springer (2003) 1245–1253
11. Hill, C.J.: Risk of masquerade arising from the storage of Biometrics, B.S. Thesis. Department of Computer Science, Autralian National University (2001)
12. Soutar, C.: http://www.bioscrypt.com/assets/security_soutar.pdf. biometric system security. (2002)
13. Adler, A.: Sample images can be independently restored from face recognition templates. In: Proc. Canadian Conference on Electrical and Computer Engineering (CCECE). Volume 2. (2003) 1163–1166
14. Uludag, U., Jain, A.K.: Attacks on biometric systems: a case study in fingerprints. In: Proc. SPIE. Volume 5306. (2004) 622–633
15. Martinez-Diaz, M., Fierrez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Sigüenza, J.A.: Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In: Proc. IEEE of International Carnahan Conference on Security Technology. (2006) 151–159
16. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer (2003)
17. Cappelli, R., Lumini, A., Maio, D., Maltoni, D.: Can fingerprints be reconstructed from ISO templates? In: Proc. International Conference on Control, Automation, Robotics and Vision. (2006) 191–196

18. Matsumoto, T.: Artificial irises: importance of vulnerability analysis. In: Proc. 2nd Asian Biometrics Workshop. Volume 45. (2004)
19. Derakhshani, R., Schuckers, S.A.C., Hornak, L.A., Gorman, L.O.: Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition **36** (2003) 383–396
20. Schuckers, S.A.C., Abhyankar, A.: A wavelet based approach to detecting liveness in fingerprint scanners. In: Biometric Authentication Workshop (ECCV). (2004)
21. Tan, B., Schuckers, S.: Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. In: Proc. SPIE, Biometric Technology for Human Identification III. (2006)
22. Cappelli, R., Maio, D., Maltoni, D.: Modelling plastic distortion in fingerprint images. In: Proc. International Conference on Advances in Pattern Recognition. (2001)
23. Antonelli, A., Capelli, R., Maio, D., Maltoni, D.: Fake finger detection by skin distortion analysis. IEEE Trans. on Information Forensics and Security **1** (2006) 360–373
24. Baldiserra, D., Franco, A., Maio, D., Maltoni, D.: Fake fingerprint detection by odor analysis. In: Proc. International Conference on Biometrics. LNCS-3832, Springer (2006) 265–272
25. Daugman, J.: Anti spoofing liveness detection. (available on line at http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf)
26. Pacut, A., Czajka, A.: Aliveness detection for iris biometrics. In: Proc. of IEEE International Carnahan Conference on Security Technology. (2006) 122–129