TESTING BIOMETRIC SYSTEMS AGAINST SPOOFING ATTACKS

Yadigar Imamverdiyev[1], Lala Karimova[2], Vugar Musayev[3], James Wayman[4]

[1-3]Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az; lala@itsc.ab.az; vuqarmusa@gmail.com
[4] San Jose State University, San Jose, USA, *James.Wayman@sjsu.edu*

The deliberate attempt to defeat the function of a biometric system is referred to as "spoofing". "Biometrics" is defined as "automated recognition of individuals based on their behavioural and biological characteristics"[1], so the function of a biometric system is to recognize individuals. Biometric systems can be of two types: those designed to confer benefits or services only on those recognized (such as access to secure spaces or bank accounts), and those designed to confer benefits or services only on those not recognized (such as for prevention of issuance of multiple identity documents to the same individual, or the denial of border crossing benefit to those on "watchlists"). Consequently, spoofing can take either of two forms: the deliberate attempt to be recognized by an individual who is not known to the biometric system; and the deliberate attempt to not be recognized by an individual who is known.

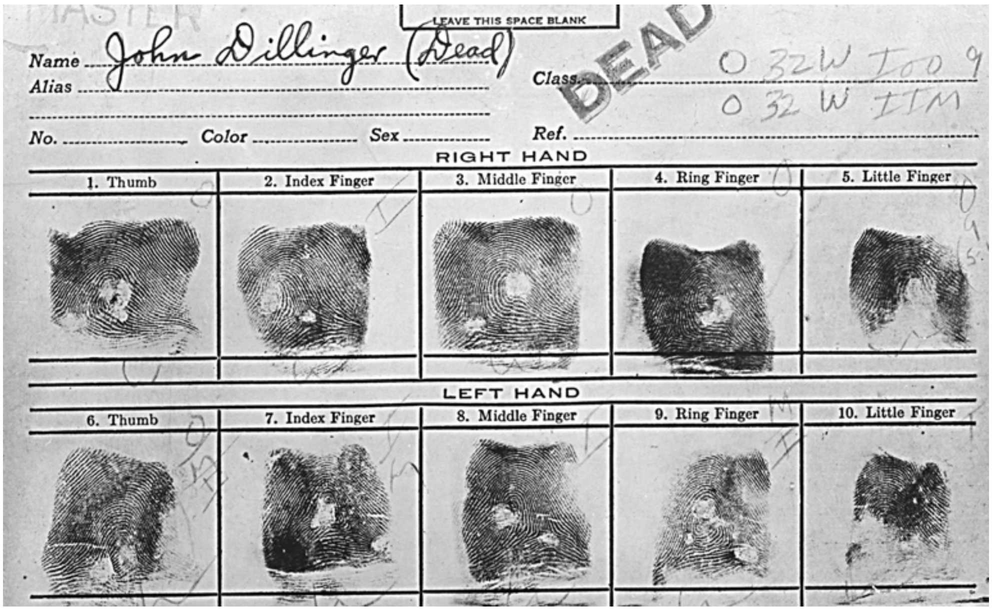
Most of the literature on biometric spoofing has considered only the first form. Attackers have traditionally been referred to as "impostors", commonly defined as "a person who assumes a false identity in order to deceive or defraud" [2]. This definition seems to apply better to attackers attempting to be recognized when they should not be, than it does to attackers seeking not to be recognized when they should be. Some have suggested that "impostor" should be used for attackers attempting to be recognized as someone else and "identity concealer" used for attackers attempting not to be recognized at all. For lack of better terminology, we will adopt those terms here.

Today the recognition of an individual based on physiological and behavioral characteristics is applied as a primary means of authentication in many areas. Most countries are in the process of adding biometric characteristics to government issued identification documents, particularly passports, and it is expected that biometric technologies will be applied even more widely in the future. We can anticipate that attacks on these systems will follow their proliferation. Therefore, in addition to improving new technologies in biometric identification, developing new methods for securing them against "spoofing" of either type is equally important.

Identity Concealers

Although the automated recognition of individuals dates only to the 1960s, human recognition based on biological measurements dates to the 1880s [3]. These early applications were generally of a forensic nature, so attackers sought to avoid recognition. John Dillinger, a famous US bank robber in the 1930s, underwent plastic surgery to repair a scar on his face and used acid to intentionally damage his fingerprints, with the hope that police would not be able to recognize him. Figure 1 shows his damaged fingerprints. After his death, an internal memo within the Bureau of Investigation (soon thereafter renamed the "Federal Bureau of Investigation) stated that "…the changes made on these impressions were not of such a character that identification could have been defeated since each and every impression reveals sufficient characteristics to establish an identification through the conduct of necessary 'reference' searches" [4], but we don't know if the damage would have been extensive enough to fool an modern automatic fingerprint recognition system (AFIS).

John Dillinger was an extreme case of an identity concealer criminally-motivated to make permanent and (probably) painful changes to his biometric characteristics. With the development of AFIS, particularly those for use in social service applications to prevent multiple enrollments by one individual, identity concealers learned to take less permanent and less painful changes to their fingerprints, such as by covering them with bandages or applying "super glue" to the ridges. Identity concealers seeking to avoid recognition by iris systems have used pupil dilation drugs such as tropicamide, while those avoiding face recognition systems have worn hats and sunglasses.



MASTER

LEAVE THIS SPACE BLANK

DEAD

Name John Dillinger (Dead)
Alias
Class. 0 32 W I 00 9
0 32 W IIM
No. Color Sex Ref.

RIGHT HAND

1. Thumb	2. Index Finger	3. Middle Finger	4. Ring Finger	5. Little Finger

LEFT HAND

6. Thumb	7. Index Finger	8. Middle Finger	9. Ring Finger	10. Little Finger

Figure 1: John Dillinger's Damaged Fingerprints (image from the files of Ken Moses)

Impostors

The use of artificial fingerprints by impostors has been known within the forensic community since 1931, with one early paper on impostor fingerprints dating to 1904 [5]. The 1971 James Bond movie, "Diamonds are Forever", shows James using latex fingerprints to impersonate a "Peter Franks". Work on understanding the vulnerabilities of automated recognition technologies to impostor attacks dates to this 1970s time period [6-8]. Over the last decade, there have been many highly publicized government, academic and commercial reports documenting successful laboratory impostor attacks on face, iris and fingerprint systems [9-13].

Defenses Against Spoofing

These different forms of attack, by identity concealers or impostors, require different forms of defense. There are technical approaches to detecting some forms of concealment. Iris recognition algorithms have been developed and implemented to detect excessively dilated pupils [14,15]. The NIST Fingerprint Image Quality algorithm can detect incoherent fingerprint ridge patterns [16]. Failure of the detection/segmentation algorithm in a face recognition system may indicate concealment of the face. But the best approach to detecting identity concealers may be supervision of the biometric sample capture process. This is a reasonable solution because applications denying services based on recognition, such as social service benefit application or border crossing "watchlists", are generally supervised anyway. Detected concealment of biometric characteristics can be used as a basis for service denial. Even if some forms of concealment, such as bandaged fingers, are not necessarily evidence of deception, services can be denied until good biometric samples can be acquired. All of this, however, understates the complexity of the problem of differentiating poor from intentionally concealed biometric characteristics. Careful policies will need to be created with the acknowledgment that some individuals may be wrongly denied services.

The problem of detecting impostors can also be addressed through supervision of the data capture process. However, one of the perceived advantages of using biometrics in systems conferring benefits on those recognized, such as access control, is that supervision is not required. Why place a hand geometry system on a door to a secure space if a door supervisor will be required anyway?

It is sometimes suggested that impostor attacks might be mitigated through "liveness testing" – assuring that the biometric characteristic is presented by a living person [17]. Around 1993, the 3M Corporation began developing a biometric system accepting "fingerprint, palm print, voice print (or) retinal" patterns only from an "individual that is not incapacitated, dismembered, or deceased" by using "pulse rate, electrocardiographic signals, spectral characteristics of human tissue, percentage oxygenation of blood, bloodflow, …. electrical property of skin, blood pressure, differential blood volumes, and combinations thereof" [18]. By 1997, 3M had widely demonstrated a well-designed prototype, known as "Blackstone", but determined that there would be no market for such a system, which was expected to cost around US$20,000. In 2000, van der Putte and Keuning showed that even the best of these "liveness" detection methods can be defeated through the cleaver application of physics [19].

Although "liveness" detection can differentiate between live and dead individuals, it cannot differentiate between impostors and legitimate users of a biometric system. Both are alive. Although the 1971 James Bond example was fictional, it is now be possible to construct a fingerprint pattern as thin as the blood-free epidermis to cover a live finger. The problem of detecting impostors is much more difficult because it requires differentiating an artifact or artificially trained pattern from a naturally occurring biometric characteristic. Impostors who train themselves to produce the signature hand movements of another person will not be detectable by a dynamic signature recognition system, even one capable of determining "liveness". Therefore, there can be no universal solution to the problem of detecting impostors. Differentiation of artifacts or trained behaviors will require solutions targeted at each impostor technique. Indeed, much recent work in impostor detection has been aimed at very particular forms of attack [20-23].

Testing Security

There have been several attempts over the last decade to develop a standardized approach to "vulnerability assessment" – determining the likelihood that a biometric system could be defeated by a "spoofing" attack. One set of attempts by the US, Canadian, German and UK governments was to develop a biometric test methodology within the ISO 15408 framework for evaluating information technology product security known as "Common Criteria". Another approach to "non-Common Criteria" security evaluation was the attempt by the international standards community to develop "A Framework for Security Evaluation and Testing of Biometric Technology" known as ISO/IEC JTC1 SC27 NP 19792. Although there was one Common Criteria evaluation of a biometric device in the 1999-2001 time period (a BioScrypt fingerprint system), neither of these approaches have advanced over the last few years because of the cost and time required to organize and complete such tests. The time scale of a thorough vulnerability assessment can easily be greater than the commercial life of a biometric product.

Nonetheless, a vulnerability testing methodology should be developed in accordance with the general scheme of testing methodologies, such as the ISO/IEC 19795 series of biometric test standards. The methodology must begin with a listing of possible methods of successful attack, then consider the time/cost/ level of expertise to develop each attack, the time/cost/level of expertise required to implement each, and the probability of success. Once possible attack methodologies against a particular device are known, mitigation efforts can be made against those most likely for success in any planned application. Such information is obviously sensitive, as we would not like to publish or post on-line a recipe book for attackers.

Although it is not possible to make a biometric system which is totally secure against spoofing attacks, anti-spoofing measures and preparation of more and better testing with a practical methodology can reduce their possibility and lead to more secure technologies.

Acknowledgement

The work was supported by research grant Bilateral Grants Program (BGP II) – AZM1-3112-BA-08 from the U.S. Civilian Research & Development Foundation (CRDF), and Azerbaijan National Science Foundation (ANSF), the Azerbaijan National Academy of Sciences (ANAS).

Bibliography

1. ISO/IEC JTC1 SC37 Standing Document 2, version 8, "Harmonized Biometric Vocabulary", August 22, 2007
2. Pearsall, J. (ed), Concise Oxford English Dictionary, Thumb Index Edition, 10th Edition, revised Oxford University Press, 2002
3. Klassy, D., John Dillinger's fingerprints. The California Identification Digest, Volume 7, Issue 6, pp 8-9, 2007
4. Cole, S. Suspect Identities: A history of fingerprinting and criminal identification, Harvard University Press, 2002.
5. Geller, B., Almog, J., Margot, P., and Springer, E, A chronological review of fingerprint forgery. J. Forensic Sci., 44(5), pp. 963-968, 1999.
6. Lummis, R.C. and A. Rosenberg, A. Test of an ASV method with intensively trained mimics. Journ. Acoustic Soc. Am., vol. 51, p.131(A), 1972.
7. Raphael, D., and Young, J. Automated Personal Identification, SRI, Inc, Palo Alto, 1974.
8. National Bureau of Standards, "Guidelines on the evaluation of techniques for automated personal identification", FIPS Publication 48, April, 1977.
9. Willis D., Lee M. Six Biometric Devices Point the Finger at Security. Biometrics under Our Thumb. Network Computing, June, 1998.
10. Matsumoto T., Matsumoto H., Yamada K., Hoshino S. Impact of Artificial Gummy Fingers on Fingerprint Systems. Proceedings of SPIE Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.
11. Thalheim L., Krissler J. Body Check: Biometric Access Protection Devices and their Programs Put to the Test. *c't magazine*, November 2002.
12. Schuckers S.A., Spoofing and Anti-Spoofing Measures,Information Security Technical Report, Vol. 7, No. 4, pp.56 – 62, 2002.
13. Blackburn, D.M., Bone, M., and Philips, P.J. Facial Recognition Vendor Test 2000. DoD Counterdrug Technology Office, February, 2001.
14. Daugman J. How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14(1), pp. 21 – 30, 2004.
15. Daugman J. New Methods in Iris Recognition., IEEE Transactions on Systems, Man, and Cybernetics B, vol. 37(5), pp. 1167 – 1175, 2007.
16. Elham Tabassi, Charles L. Wilson Craig I. Watson Fingerprint Image Quality, NISTIR 7151, National Institute of Standards and Technology, Gaithersburg, MD 2004.
17. V. Valencia and C. Horn, "Biometric liveness testing," in Biometrics, J. D. Woodward Jr., NM Orlans, and RT Higgins, Eds. New York 2003.
18. Osten, D.W., Carim, H.M, Arneson, M.R., and Blan, B.L. Biometric, personal authentication system. Date of issuance: Feb 17, 1998 United States Patent 5719950.
19. Van der Putte, T., and Keuning, J. Biometrical Fingerprint Recognition: Don't get your fingers burned IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289-303, Kluwer Academic Publishers, 2000.
20. Schuckers S.A., Spoofing and Anti-Spoofing Measures,Information Security Technical Report, Vol. 7, No. 4, pp.56 – 62, 2002.
21. Antonelli A., Cappelli R., Maio D., Maltoni D. A new approach to fake finger detection based on skin distortion. In Proceedings of International Conference on Biometrics (ICB), D. Zhang and A. Jain, Eds., vol. LNCS 3832, 2005, pp.221–228.
22. Derakhshani R., Schuckers S. A., Hornak L. A., O'Gorman L. Determination of vitality from a non-invasive biomedical measurement for use in fngerprint scanners. Pattern Recognition, vol. 36, no. 2, pp.383-396, 2005.