Schuckers SAC, *Spoofing and Anti-Spoofing Measures,* Information Security Technical Report, Vol. 7, No. 4, pages 56 – 62, 2002.

Spoofing and Anti-Spoofing Measures

Stephanie A. C. Schuckers, Ph.D.
Clarkson University and West Virginia University

Article for Elsevier Information Security Report on Biometrics

December 10, 2002

Contact Information:
Clarkson University
Dept. of Electrical and Computer Engineering
Box 5720
Potsdam, NY 13699

315-268-6536 (phone)
315-268-7600 (fax)

sschucke@clarkson.edu

Spoofing and Anti-Spoofing Measures

Stephanie A. C. Schuckers, Ph.D.
Clarkson University and West Virginia University

Introduction

Biometric devices have been suggested for use in applications from access to personal computers, automated teller machines, credit card transactions, electronic transactions to access control for airports, nuclear facilities, and border control. Given this diverse array of potential applications, biometric devices have the potential to provide additional security over traditional security means such as passwords, keys, signatures, picture identification, etc. While biometrics may improve security, biometric systems also have vulnerabilities. System vulnerabilities include attacks at the biometric sensor level, replay attacks on the data communication stream, and attacks on the database, among others [1]. This chapter will focus on the vulnerability of attacks at the sensor level, including the spoof attack or use of an artificial biometric sample to gain unauthorized access. Several recent highly publicized articles which reported on the spoofing vulnerabilities will be described, in addition to spoofing research performed in my laboratory at West Virginia University. Finally, anti-spoofing measures which can be implemented to minimize the risk of an attack will be summarized.

Spoofing Background

Attacks at a biometric sensor level can be divided into several scenarios [2]. Attacks can include forcibly compelling a registered user to verify/identify, presenting a registered deceased person or dismembered body part, using a genetic clone, and introduction of fake biometric samples or spoofing. Several of these scenarios are described below and potential solutions apply to most. Attacks using force and genetic clones are the exception. For attacks using force, this risk exists with currently used security measures. Things used to minimize risk include cameras, "panic" buttons, alarms, etc. In the case of genetic clones, in most cases, biometric samples still differ between individuals, even identical twins. However, the algorithm may not be robust enough to distinguish these differences. DNA is an exception, where clones would be identical; however, DNA has not been developed at this point for use in a verification/identification scenario.

Before spoofing is described in more detail, it may be helpful to discuss how the false accept ratio, a typical assessment measure of biometric devices, is related to spoofing. A false accept is when a submitted sample is incorrectly matched to an template enrolled by another user [3]. This only refers to a zero effort attempt, i.e., an unauthorized user making an attempt with their own biometric to gain access to a system. If the false accept ratio is kept low, then the probability of specific user *with criminal intent* matching another template is very low. The false accept ratio does not give information on the vulnerability of a system to spoof attacks.

Two recent highly publicized drew attention to the spoofing vulnerabilities of biometric devices [2, 4]. Other articles addressing spoofing include [5, 6]. The first is a group from Yokohama National University in Japan. Matsumoto and colleagues developed a method to spoof fingerprint devices [2]. In this method, two different techniques were

used to create a mold. The first directly used a subject's finger to create the mold in free molding plastic. The second involved making a mold from a latent fingerprint image. The latent fingerprint was enhanced with cyanoacrylate adhesive, a digital camera was used to photograph the latent fingerprint, and software enhanced and flipped the image. The image then was printed onto a transparency sheet with an inkjet printer creating a mask. The mask was used to form the cast with photosensitive-coated PCB. Finally, artificial fingers were created from the casts using gelatin, commonly used for confectionary. The author terms these artificial fingers as "gummy fingers".

Gummy fingers from five individuals were made using the direct method and one subject using the latent method. Eleven common biometric fingerprint devices were tested which included both optical and capacitive technologies. When security levels were available, devices were set to the highest security level. Multiple tests were performed and included:

-enrolling a live finger and verifying with a live finger
-enrolling a live finger and verifying with a gummy finger
-enrolling a gummy finger and verifying with a live finger
-enrolling a gummy finger and verifying with a gummy finger

Each subject was verified 100 times and the average results were presented. Example images from the study are shown in Figure 1.

For the direct method of creating the cast, all fingerprint systems were able to enroll the gummy finger. Verification rates of gummy fingers in all four scenarios ranged from 68%-100%. For method of creating a cast from residual fingerprints, all fingerprint systems were able to enroll the gummy finger and verify more than 67% of the attempts.

Secondly, Lisa Thalheim and Jan Krissler for c't magazine, while in a less rigorous fashion, demonstrated the vulnerability of a variety of biometric technologies [4]. For fingerprint devices, they tested six capacitive, two optical, and one thermal scanners. For several capacitive based devices, they were able to verify (1) by simply breathing on the fingerprint scanner to reactivate the latent fingerprint, (2) by using a bag of water on top of the latent fingerprint, and (3) by dusting the latent fingerprint using graphite powder, stretching adhesive film over it and applying pressure. One optical scanner was able to be spoofed using (3) above with the addition of a halogen light for intense backlighting. Both the optical and thermal devices were spoofed using wax casts and silicon molds.

One facial recognition system was tested for spoofing vulnerabilities [4]. First, the facial recognition stored its reference image in a readily accessible file. The testers displayed this image on a laptop computer and used it to verify in the system. Second, they surreptitiously took three pictures of an authorized user and were able to successfully verify by displaying the images on a laptop computer. Finally, when a liveness algorithm was activated in the facial recognition software, a short video clip was successful in defeating the system.

The third biometric technology type tested was iris recognition [4]. In order to spoof this system, a high quality print of an iris was able to spoof the system, but required that a hole be punched over the pupil and a real pupil be presented behind the fake biometric.

Recent Spoofing Research

The Biomedical Signal Analysis Laboratory at West Virginia University has been developing spoofing techniques in order to test a new liveness algorithm [7]. Our spoofing technique involves a mold made from dental impression material (combination of type 0 and 3) and casts made from Play-Doh and clay. Example images are shown in Figure 2. These materials are most effective since they are moisture based and most fingerprint technologies are able to image them. We enrolled eleven live subjects, formed molds from the eleven subjects, created six casts from each subject, and attempted to verify for each cast. Various fingerprint scanners, including capacitive DC, capacitive AC, optical and opto-electronic technologies, were tested. All security levels were tested. Results shown here are for the highest security level (Figure 3). For certain fingerprint scanners, most subjects' casts were able to spoof the system. For all technologies, at least 3 of 11 subject's casts were of sufficient quality to spoof fingerprint devices at least once.

It should be noted that one device was chosen from each technology type. Even though the specific device manufacturer's name is withheld, these results are tests of the entire system from scanner to image processing to pattern recognition algorithms. Conclusions regarding one technology over another should not be made, but rather, these tests are a demonstration that spoofing is possible with a variety of fingerprint devices.

In addition, we also tested cadaver fingers in an attempt to address the possibility that dismembered fingers could be used to spoof fingerprint devices. In this method, fourteen cadaver fingers were enrolled and, if able to enroll, verified six times each. Images are shown in Figure 2 and results are shown in Figure 4. For one device, six cadaver fingers were not able to enroll. Cadaver fingers were able to be verified from 40-94% of the time.

Impact on Biometric Devices

Numerous popular media articles have come out attacking biometric devices based on these published reports. While some have gone so far as to say that these studies have completely discredited the industry and that biometric devices are not useful as security measures, these statements are extreme. While someone could steal and make a copy of my office key to gain unauthorized entry, this does not discredit the use of keys. If anything, studies demonstrating spoofing vulnerability does bring attention to several important issues when considering the use of biometric devices.

First, it is surprising that everyone is so astonished that biometric devices can be spoofed. No security system is completely spoof-proof. No matter what barriers are put in place, those that are motivated will find a way to get around those barriers. That said, unrealistic claims of system performance lead to unrealistic expectations as to what the device can do.

This leads to the second point. A potential user must consider the application and the security level needed. Is the biometric device being used to make it easier to access your home computer (instead of having to remember a pin)? In this case, the fact the system is vulnerable to spoofing may not matter, since ease of access is the goal. If higher security is needed for other applications, there are several measures that can be taken to make spoofing more difficult. First, the biometric can be combined with a password or smart card. While individually each security measure has vulnerabilities, in combination, these security measures can make it that much more difficult for an unauthorized person to gain access. Other measures to increase difficulty of spoofing include (1) supervising the verification/identification process, (2) enrolling several biometric samples (i.e. several fingers) and asking the user to present a specific sample, (3) multi-modal biometrics, and (4) liveness detection. These are described in detail in the next section.

The third issue is more directed at the industry than potential users. Exposure of spoofing vulnerabilities allow the industry to make improvements to their devices, including developing liveness algorithms and other anti-spoofing techniques described below. Potential users can demand that the industry address these issues.

The International Biometric Group has posted an excellent white paper which covers these and other issues related to spoofing and liveness detection [8].

Anti-Spoofing Measures

As discussed above, there are several types of anti-spoofing techniques that could be used that would make it more difficult to spoof a system. Using passwords or smart cards, enrolling several samples, and supervising the verification process are self-explanatory. Another method for anti-spoofing is the use of multi-modal biometric systems. Multi-modal biometrics is the combination of several biometric types into one biometric system, for example, combining fingerprint recognition with facial recognition. Much research is being performed in this area to determine the best way to combine information from several biometric systems, whether it is at the feature extraction level or at decision level. From an anti-spoofing point of view, multi-modal biometrics is more difficult to spoof since it would require, for example, both a spoof fingerprint and a high-quality facial image or video.

Lastly, one anti-spoofing measure is something called liveness detection. Even though biometric devices use physiologic information for identification/verification purposes, these measurements rarely indicate liveness. The goal of liveness testing is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. Liveness detection is based on recognition of physiological information as signs of life (1) from liveness information inherent to the biometric, (2) from additional processing of information already captured by biometric reader, and (3) from acquisition of life signs by using additional hardware. In addition, liveness detection can also include something called the challenge/response. In this case, the user will see, hear or feel something and do something in response.

Several types of biometric systems contain liveness information inherently, for example, facial thermograms (IRID, Inc,), near-IR measurement of hand vein patterns (Nextern and Neusciences), ear canal shape and acoustic properties, gait [9], body odor, keystroke patterns [10], and electrocardiogram [11]. While these require a live person in order to measure the biometric, the biometric technologies are not as mature as other biometrics modalities like fingerprint and iris recognition.

Several liveness detection algorithms have been suggested which use additional processing of information already collected from the biometric system. First, the Biomedical Signal Analysis Laboratory at West Virginia University is developing a liveness detection algorithm which is based on the detection of perspiration in a time progression of fingerprint images. Initial research has shown the ability to separate live and spoof/cadaver fingers using image processing and pattern recognition in an initial dataset of 54 subjects with a capacitance based scanner [7]. An additional 90 subjects are currently being tested with a variety of fingerprint technologies (optical, capacitive AC, capacitive DC, optoelectronic). This method considers the grey levels along the ridges where differences in moisture correspond to differences in grey levels. The differences in moisture include peaks at the perspiration pores and valleys in between the pores. These differences decrease over time as perspiration traverses the ridges. More testing is needed to determine if the perspiration characteristics are generalizable over a large range of people. Obviously those with low moisture may not be able to use a fingerprint scanner, in general, and therefore liveness is not the main issue. In addition, since a specific change in moisture is needed, highly perspiration-saturated fingers may not exhibit liveness. However, current testing has shown that simply wiping the finger is sufficient. More environmental testing is needed.

For facial recognition, Identix uses a liveness algorithm which quantifies head movements and/or detects 3D facial image. For iris recognition, detection of eye and pupil movement could be used for liveness detection.

It has also been suggested that additional hardware could be combined with a biometric devices to determine liveness. While these may be an effective means to determine liveness, a potential drawback is that it is not directly measured by the biometric sensor. Therefore, a fake biometric could potentially be presented in combination with a live person and have successful liveness detection. Suggestions for liveness detection in this category for the fingerprint include: temperature sensing [12], detection of pulsation on fingertip [12], pulse oximetry [12, 13], electrocardiogram [12], dielectric response [14], and impedance [14]. Each of these measures has disadvantages. Temperature sensing can be easily faked. Detection of pulsation, pulse oximetry, and electrocardiogram can be performed even if a fake fingerprint is presented, for example, with the use of a translucent fake finger which covers only the fingerprint. Furthermore, while patents have been filed, none of these systems are commercially available except dielectric response and impedance from Guardware Systems [14]. Additional discussion of these types of liveness tests are given in [6]. For voice and facial recognition, it has been suggested to match the lip movement to the voice/face [15], currently available from BioID, Inc.

Lastly, challenge response can be used as an anti-spoofing measure. In this case examples include tactile response to heat or shock, change in expression (smile, frown) (Identix), and repetition of a randomly generated set of phrases (VeriVoice). Involuntary challenge response is also possible including reflex to shock, pupil changes to level of light, and response of muscles to electrical stimulation. Obviously, methods which involve shocking are probably not conducive to user comfort. Furthermore, challenge response may only indicate the presence of a person, not necessarily the authorized person. The biometric information should be combined carefully with the liveness information such they are inseparable.

Many of the liveness methods listed here are not commercially available. While many liveness detection methods have been suggested and some have been implemented, no independent testing has been performed which reports on the effectiveness of these methods for performing liveness detection. Liveness detection is a stage in the verification/identification process. Therefore, it must be treated as part of the biometric system, in that it has an impact on the false reject ratio, false accept ratio, failure to enroll and other statistics. In addition, other characteristics for evaluating biometrics systems such as ease of use, universality, and user acceptance need to be considered before implementing a liveness algorithm. Lastly, liveness algorithms are not spoof-proof and therefore will also have varying degrees of spoofing vulnerability.

An excellent overview of liveness tests is given in [16].

Summary

In summary, although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks. Anti-spoofing methods include addition of supervision, password, smart card, enrollment of several biometric samples, multi-modal biometrics, and liveness testing. Applications must be carefully considered before selecting security measures which will achieve the objectives. While liveness algorithms are available, more testing is needed to assess their effectiveness and impact on the overall biometric system. Lastly, no matter what security measures are in place, no system is spoof-proof. Anti-spoofing measures simply make it more difficult to attack the system.

Acknowledgements
Part of this work was funded by the Center for Identification Technology Research (CITeR), an NSF Industry/University Cooperative Research Center. Special thanks to my colleagues, Lawrence Hornak, Tim Norman, and graduate research assistants, Reza Derakhshani, Sujan Parthnasardi.

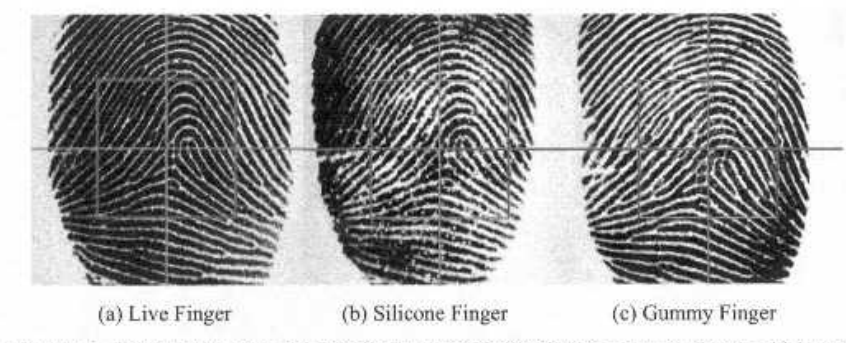

Figure 1. Images from spoofing tests performed in Matsumoto's laboratory [2].

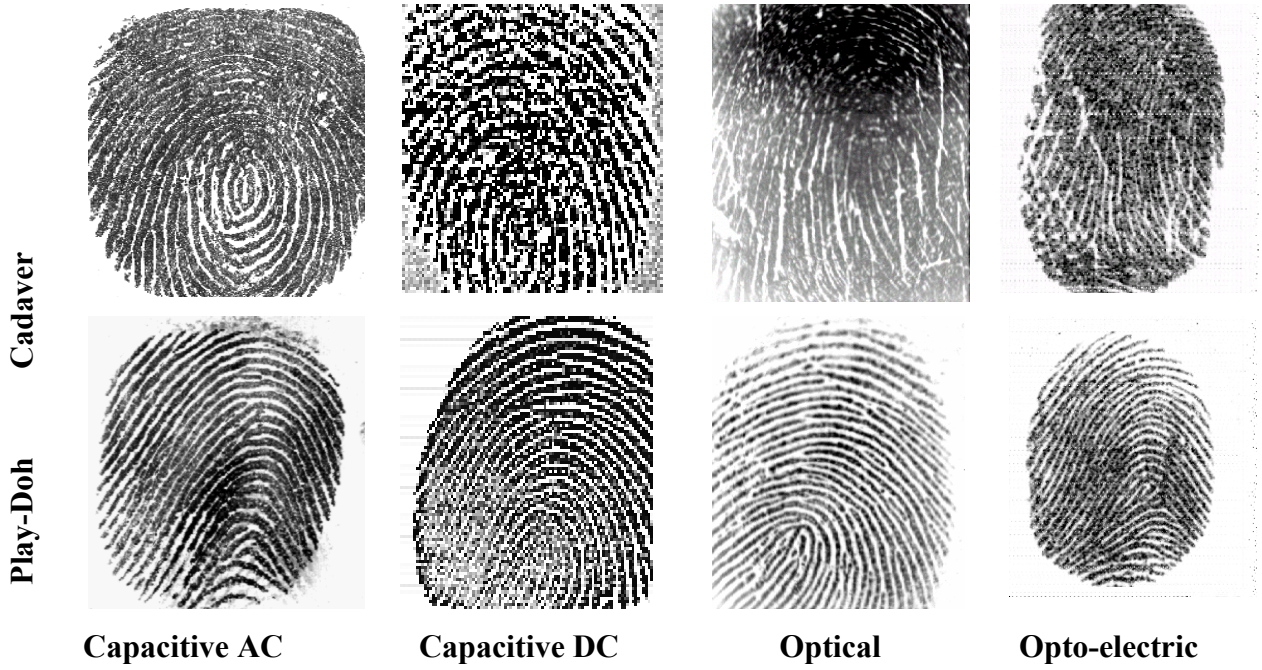

Figure 2. Images of spoof fingerprints made from Play-Doh and of cadaver fingerprints for a variety of fingerprint scanner technologies.

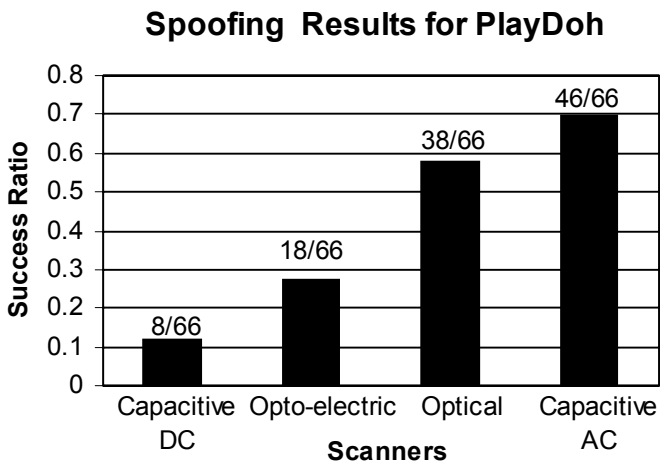

Figure 3. Results of verification of Play-Doh molds made from eleven subjects, each verifying six times. The enrolled image was from the live finger.

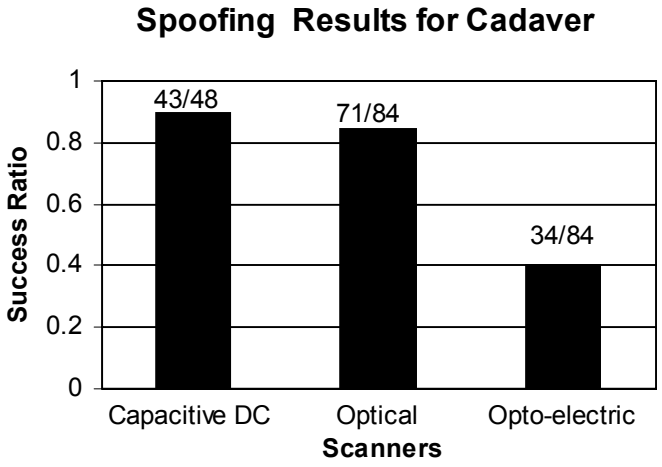

Figure 4. Results of verification of cadaver fingers from 14 subjects, each verifying 6 times. The enrolled image was from the cadaver finger. Six cadaver fingers for one device were unable to enroll.

References

[1] NK Ratha, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems Journal*, v 40, n 3, 2001, p 614-634.

[2] T Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems", *Proceedings of SPIE*, vol. 4677, January, 2002

[3] AJ Mansfield, JL Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices: Version 2.01", National Physical Laboratory Report, CMSC 14/02, United Kingdom, August 2002.

[4] L Thalheim, J Krissler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", *c't magazine*, November 2002.

[5] D Willis, M Lee, "Biometrics Under Our Thumb", *Network Computing*, June 1, 1998.

[6] T van der Putte, J Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, 2000, pp. 289-303.

[7] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners," *Pattern Recognition*, vol. 17, no. 2, 2003.

[8] Liveness Detection in Biometric Systems, *International Biometric Group* white paper, Available at http://www.ibgweb.com/reports/public/reports/liveness.html

[9] PC Cattin, D Zlatnik, R Borer, "Sensor fusion for a biometric system using gait," *IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, Aug 20-22 2001, Baden-Baden, p 233-238.

[10] F Monrose, AD Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, v16, n4, Feb, 2000, p 351-359.

[11] L Biel, O Pettersson, L Philipson, P Wide, "ECG analysis: A new approach in human identification," *IEEE Transactions on Instrumentation and Measurement*, v 50, n 3, June , 2001, p 808-812.

[12] D Osten, HM Carim, MR Arneson, BL Blan, "Biometric, Personal Authentication System", Minnesota Mining and Manufacturing Company, *US Patent #5,719,950,* February 17, 1998.

[13] PD Lapsley, JA Less, DF Pare, Jr., N Hoffman, "Anti-Fraud Biometric Sensor that Accurately Detects Blood Flow", SmartTouch, LLC, *US Patent #5,737,439,* April 7, 1998.

[14] P Kallo, I Kiss, A Podmaniczky, J Talosi, "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus", Dermo Corporation, Ltd. *US Patent #6,175,64,* January 16,2001.

[15] CC Broun, X Zhang, RM Mersereau and MA Clements, "Automatic Speechreading with Application to Speaker Verification," *Proceedings of ICASSP,* May 13-17 2002, Orlando, FL, p I/685-I/688.

[16] V Valencia, C Horn, "Biometric Liveness Testing," *Biometrics*, RSA Press, Ed: John Woodward, to be published.