Global Information Assurance Certification Paper

BIOMETRICS: BEYOND THE GUMMY FINGER

Kenneth Kiesel

GIAC Security Essentials Certification
(GSEC)

Practical Version 1.4b

July 30, 2004

SUMMARY

Security professionals must not simply implement technology designed to fortify security but also investigate vendor claims and keep abreast of discovered vulnerabilities within such designs. Naiveness of such vulnerabilities often result in a less secure environment enabling others to circumvent defenses and penetrate systems. Biometrics is just one in a number of technologies designed to increase the security level and information assurance posture (Defense in Depth) of a physical and/or logical access system.

This paper examines the methodology of traditional fingerprint authentication, briefly discusses artificial vulnerabilities, then proceeds to depict and explain anti-spoofing developments. Specifically, research concentrated on enhancements of liveness testing to traditional authentication and innovative technological advances of finger authentication beyond use of fingerprints.

TRADITIONAL FINGERPRINTS

To date fingerprint-based identification is the most widely implemented biometric technique for fielded applications. Fingerprints are known to be unique and immutable for each individual. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The authentication of a fingerprint can be determined by the minutiae as well as Correlation-based recognition.

Minutia

Every person has minute raised ridges of skin on the inside surfaces of their hands and fingers and on the bottom surfaces of their feet and toes, known as 'friction ridge skin'. Friction ridges do not run evenly and unbroken across our fingers, hands, toes and feet. Rather, they display a number of characteristics known as minutiae. The principle categories of minutiae (Figure 1) are as follows:[1]

- ridge ending - a ridge that ends abruptly;
- bifurcation - a single ridge that divides into two ridges;
- lake or enclosure - a single ridge that bifurcates and reunites shortly afterwards to continue as a single ridge;
- short ridge, island or independent ridge - a ridge that commences, travels a short distance and then ends;
- dot - an independent ridge with approximately equal length and width;
- spur - a bifurcation with a short ridge branching off a longer ridge; and
- crossover or bridge - a short ridge that runs between two parallel ridges.

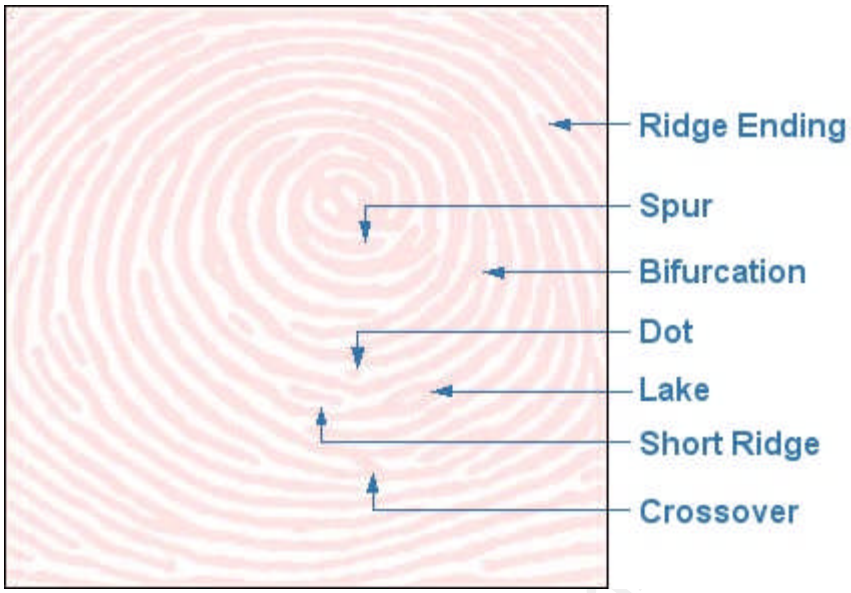

Figure 1 Minutiae Categories

Minutiae-based techniques identify a subset of minutiae points, map their relative placement on the finger, and store an image or template of results for future authentication.

Pattern-based

Pattern recognition, take into account the global pattern of ridges and furrows. Pattern types fall into one of three categories whorls, arches and loops shown in Figure 2. Pattern techniques require the precise location of a registration point, most notably the core of the print, and are affected by image translation and rotation.

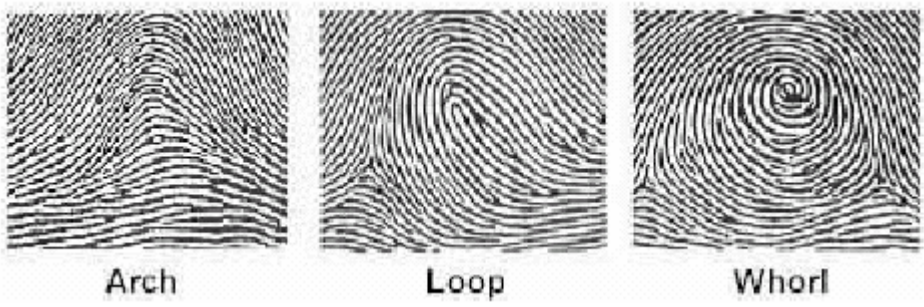

Figure 2 Pattern types

TRADITIONAL SCANNERS

Fingerprint images must first be captured and stored or converted into a template for utilization in any authentication system. Traditional fingerprint scanners fall into one of two general classifications – optical or capacitive.

Optical

All optical scanners whether using a glass prism, sheet prism, or fiber optic provide an optical path to a charge-coupled device (CCD). (Glass prism as illustrated in figure 3) The CCD is designed in an array with each cell generating electrical signals in response to strength of light received. Each cell records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example). Typically, an analog-to-digital converter in the scanner system processes the analog electrical signal to generate a digital representation of this image.

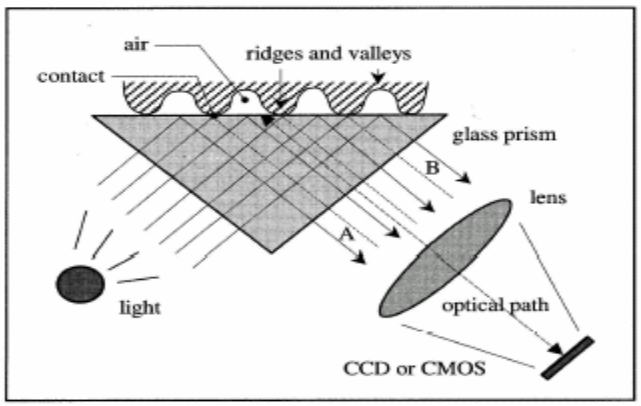

Figure 3 Optical Scanning

The scanning process starts when you place your finger on a glass plate, and a CCD camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system actually generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges)[2]

Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in more or less light, and then tries the scan again.

Capacitive

Capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

The diagram below shows a simple capacitive sensor. The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger. [2]

The two conductor plates form a basic capacitor, an electrical component that can store up charge. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air (figure 4). Just as the intensity of light varied between a ridge and valley the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley. This difference in capacitance results in a different voltage outputs for ridges and valleys.

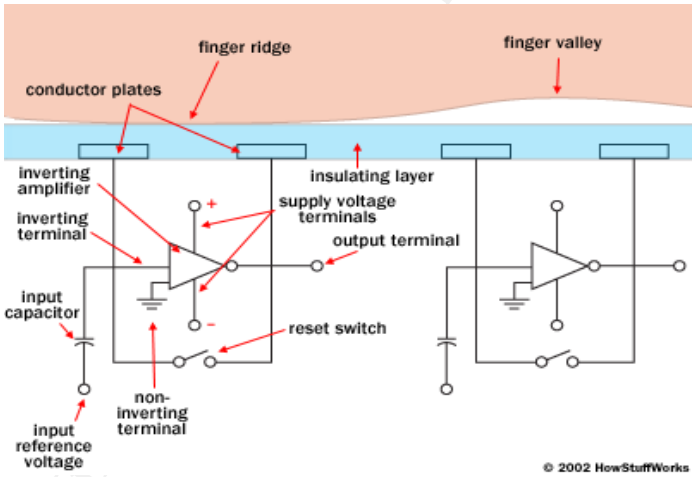

Figure 4 Capacitive Scanning

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, similar to the image captured by an optical scanner.

SPOOFING

Spoofing is a method hackers utilize to gain access to unauthorized data or a system by posing as an authorized host or user. Biometric spoofing is performed by capturing an individual's biometric characteristic used for authentication and once obtained, utilizing it to claim the identity of such

individual. The unauthorized hacker now simply presents the captured biometric and is granted access based upon the authorized user's privileges.

Laboratory testing has shown artificial fingers that are easily made of cheap and readily available gelatin, were accepted by extremely high rates by fingerprint devices with optical or capacitive sensors. Highly publicized articles drew attention to the spoofing vulnerabilities of biometric devices. Most notably, Matsumoto and colleagues, from Yokohama National University in Japan, developed a method to spoof fingerprint devices making a mold from plastic, originating from both a live finger and a latent fingerprint. Artificial fingers were then created from the casts using gelatin, commonly used for confectionary, where the resultant casts were termed "gummy fingers" [2][3].
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 through simple techniques for fingerprint spoofing such as (1) by breathing on the fingerprint scanner to reactivate the latent fingerprint, (2) by using a bag of water on top of the latent fingerprint, (3) by dusting the latent fingerprint using graphite powder, stretching adhesive film over it and applying pressure, and (4) by using wax casts and silicon molds. [3][4]
Most recently, Marie Sanstom conducted similar experiments this year (2004) for her Master's thesis, dispelling vendor's claims of anti-spoofing enhancements of optical and capacitive scanners. Nine different systems were tested at the CeBIT trade show in Germany and all were deceived[5]

ANTI-SPOOFING RESEARCH & DEVELOPMENT

Security is based upon the founding principles of availability, integrity, and confidentiality. Anti-spoofing techniques are designed to enhance confidentiality by deterring hackers from gaining unauthorized access. An important aspect of anti-spoofing is to ensure that increased security does not occur at the cost of availability. Implementation must not come at a cost that makes availability (access to data) untimely.

A goal of biometric anti-spoofing is to increase security for devices by validating a claimed identity and that a captured biometric used enrollment and authentication is from a living human.

Existing anti-spoofing techniques for fingerprint devices use:
– Medical-type measurements – pulse
– Change based measurements– temperature, perspiration
Or
– Single skin attributes – color, skin thickness, conductivity

While existing techniques increase the security of a biometric, each is either costly, time consuming, or fairly easy to defeat

Disclosure of the ease to spoof fingerprints led to technological research and developments to implement anti-spoofing measures and derive alternate biometric characteristics from fingers.

Multiple Fingers

The ability to spoof a system can be significantly decreased by incorporating the use of multiple fingers required for enrollment and authentication. Systems can be designed and implemented to operate under one of the following three methods:

- query/response (randomization) - after all fingers are enrolled, application randomly selects finger(s) required to present for authentication.
- combination – multiple fingers are enrolled in a user defined sequence this same sequential presentation is then required for authentication.
- complete - all fingers enrolled are required for authentication.

Liveness Detection

Definition of liveness testing

Liveness detection, i.e. determining whether an introduced biometric is coming from a live source or not, has been suggested as a means to circumvent attacks that use spoof fingers. 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.[6] Ideally, systems should measure for liveness simultaneously with the capture and authentication of the biometric data.

Perspiration

Although not used in traditional minutia or pattern recognition systems, sweat glands and pores reside in the human fingertip that produce perspiration. Skin pores, like fingerprints, never spontaneously change or disappear but remain in their relative constant positions moistening the fingers with sweat.

Doctor Stephanie A. C. Schuckers and a small group from the Biomedical Signal Analysis Laboratory (BioSAL) have developed a method for liveness detection with fingerprint scanners. They have developed an algorithm for the detection of a perspiration pattern over the fingertip skin. This algorithm quantifies the sweating pattern and makes a final decision about the liveness of the fingerprint presented.

Due to the high dielectric constant of sweat, capacitive scanners are well suited for fingerprint authentication systems with perspiration detection. Fingertip perspiration results in a moistened fingertip being presented for authentication. The sweat on the skin surface increases the capacitance between the finger and scanner resulting in an enhanced darker image capture.

The key to this technology is based upon the physiological fact that perspiration starts from the pores and transverses along the ridges into the valleys. This perspiration creates time sensitive images that display the darkening ridges as the area is moistened with sweat. The capture of this process produces core perspiration information and patterns.

The designed algorithm utilizes both static, perspiration beginning at the pores, and dynamic, image darkness transition over a five second period, approaches to authenticate and liveness validation. Two images are captured within this five-second period and provide the data required for the algorithm to determine the perspiration pattern.

System anti-spoofing is based upon the difficulty in recreating the perspiration pattern resulting from the static approach. This algorithm prevents an attacker from simply presenting an artificial or cadaver finger moistened with a solution equivalent to sweat and being authenticated.

The BioSAL group is aggressively analyzing their algorithm, striving to reduce the current five-second acquisition time. The addition of this perspiration-based liveness detection algorithm to any fingerprint scanning system has the potential to dramatically reduce the susceptibility of fingerprint scanners to spoof attacks.

Ultra-sound

Ultra-sound technology has been incorporated into a number of diagnostic systems utilized in the medical profession. Optel claims to have enhanced this technology in an Ultrasonic fingerprint scanner that is “impossibile” to fake.

Optel’s claims are based upon the fundamentals that acoustic waves are mechanical in nature and their properties are affected by the mechanical properties of materials. The unique composition of live tissue and the inherent difficultly to reproduce this mechanical effect enable a fingerprint image reconstruction by emitting acoustic waves and measuring the surface scattering and characteristics received waves. Any acoustic waves received that are inconsistent with those of live tissue are discarded.

It should be noted that the optical and electrical features of finger are not very special and can be copied with other materials. In contrast, the mechanical

parameters are not easy to copy, if at all, and the associated behaviors of this structure are probably impossible to accurately reproduce. [7]

Optel's new approach can additionally check for pulse as a second indication of liveness. This is accomplished by measuring changes in time caused by blood flow during the scan.

Spectroscopy

Spectroscopy is the science that describes how light is affected by a substance with which it interacts. Light comprises different wavelengths (colors) each producing unique characteristics of a substance. A sampling of these characteristics produce a spectrum that identifies a particular substance.

Skin is comprised of many different layers. When broadband light is used to illuminate the skin, a portion of the light is diffusely reflected and shows the effect of a number of physiological characteristics of the skin and underlying tissue that it passed through including:[8]

Thickness of skin layers
Morphology of skin interfaces
Scattering properties due to collagen density and orientation
Gender- and age-related compositional differences of skin
Optical path length differences

The chemical and structural composition of skin tissue and its optical response produce a unique spectrum. Of great importance to biometrics is the inference that each person's spectrum is unique and identifiable. Of greater importance to security, specifically anti-spoofing, is the premise that the compositional effect is extremely characteristic of "living" human tissue.

Lumidigm Incorporated has developed a deep tissue biometric technology (LumiGuard™) based on spectroscopy of visible and infrared light and the unique characteristics of human skin tissue. Lumidigm's anti-spoofing sensor, Lumisure, is designed around two key parameters, wavelength and configuration. Different wavelengths at the light source produce specific absorbance and scattering information while the configuration of source detectors provide path length and layer information. The scanner's algorithm processes this data and processes liveness and authentication simultaneous.

The claimed ability of LumiGuard™ to provide both biometric securities along with liveness detection are properties required to enhance authentication and to protect against spoofing. As implied in Figure 5, this technology is not restricted to fingers but can be utilized on the palm or any other designated skin tissue area.

Figure 5 Science behind Lumiguard

Lumidigm tested materials commonly employed to spoof fingerprint devices. The spectrum of fingers manufactured from materials such as wood, foam, silicone, and gelatin were all easily discernable from human tissue. Test where even conducted to display the ability to detect rapid changes in biochemistry, temperature and distribution of fluids that result form amputated tissue.

Blood Vessel

Bionics Corporation designed an authentication system based upon the recognition of blood vessel-patterns within the fingertip. As with all biometric technologies the postulation is that no two vessel-patterns are the same. This uniqueness is claimed to hold true even for identical twins.

The technology is similar to an optical fingerprint scanner using infrared light to permeate into the finger and a high quality CCD camera to capture the blood vessel pattern. Unlike fingerprints, the vessel pattern does not generate any latent images that can be utilized for spoofing.

Nailbed

Research has shown that the epidermal tissue beneath the fingernail forms in a very unique parallel structure. This network of parallel tissue is referenced as the nailbed. Rotating one's fingernail under a light reveals parallel lines spaced at intervals. The human nailbed is a unique longitudinal, tongue-in-groove spatial arrangement of papillary papillae and skin folds arranged in parallel rows. During normal growth, the fingernail travels over the nailbed in a tongue-and-groove fashion, as shown in Figures 6 and 7.[9]

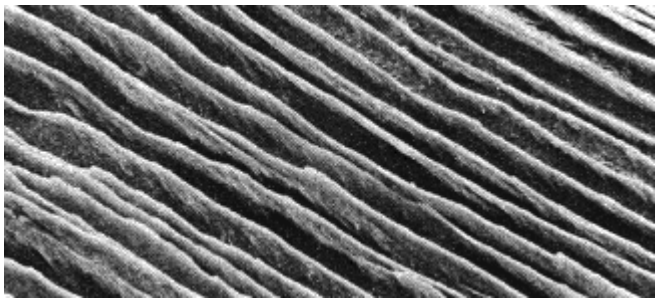

Figure 6

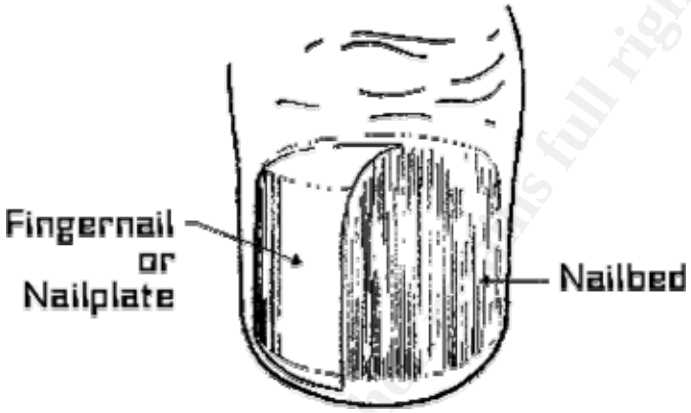

Figure 7

Interferometry is based upon the principle that two waves that coincide with the same phase amplify each other while two waves with opposite phases cancel each other. This interference phenomenon is utilized to measure very small distances and thicknesses.

AIMS Technology, Inc has incorporated the science of interferometry into a finger scanner enabling the use of the nailbed as a biometric authenticator. They capitalize on the effects of back scattered light introduced through the fingernail to determine the polarized phase changes at the interface between the fingernail and the nailbed. Polarized changes of the optical signals are analyzed by a proprietary algorithm that reconstructs the unique nailbed pattern. This pattern is utilized to generate a numerical string equivalent to a barcode, shown in Figure 8. This "barcode" is unique to each individual and becomes the identifier for authorization systems.

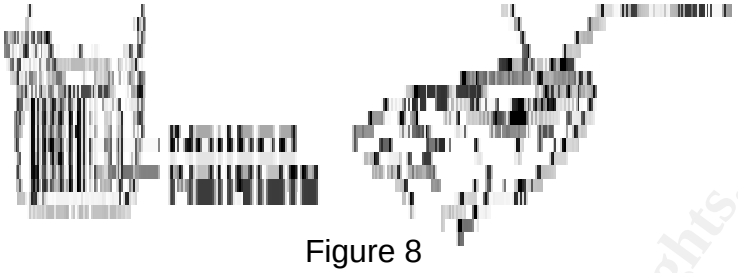

Figure 8

The nailbed is protected and hidden by the fingernail significantly decreasing the capture and utilization of this biometric as a spoofing mechanism. AIMS claims, "it is virtually impossible to obtain a false-positive match, i.e., the finger must be a living organism".

CONCLUSION

After attending the SAN's Security Essentials track, the instructor, Eric Cole, left this forever lasting statement imprinted into my memory: "What can be used for Good, can also be used for Evil". This continual battle is ever present in our world of cybersecuity.

The use of fingerprints and incorporation of fingerprint scanners into authentication systems was designed to strengthen the security of information systems. Ability to capture, replicate, and spoof fingerprint scanners transitioned this security enhancement into a vulnerability.

It is imperative that System integrators and Security professionals maintain visibility with emerging technologies and keep abreast of security vulnerabilities. I have presented a few enhancements and some alternatives to fingerprint authentication technologies. I strongly recommend not relying on vendor claims but seek results from independent test laboratories that validate such claims.

Endnotes

[1] "CrimTrac Fingerprint Analysis – The Basics", Commomwealth of Australia 2001 < http://www.crimtrac.gov.au/fingerprintanalysis.htm> (June 6, 2004)

[2] Harris Tom, "How Fingerprint Scanners Work", <http://travel.howstuffworks.com/fingerprint-scanner.htm/printable> (June 22, 2004)

[3] Schuckers SAC, "Spoofing and Anti-Spoofing Measures", Information Security Technical Report, Vol. 7, No. 4, pages 56 – 62, 2002. Stephanie A. C. Schuckers, Ph.D., Spoofing and Anti-Spoofing Measures
Clarkson University and West Virginia University, Article for Elsevier Information Security Report on Biometrics, December 10, 2002,
<http://www.citer.wvu.edu/members/publications/files/15-SSchuckers-Elsevior02.pdf> (June 24, 2004)

[4] Biomedical Signal Analysis Laboratory, "Spoofing and Liveness Dectection - Brief Background",
<http://biosal - spoofing and liveness detection.htm/> (June 22, 2004)

[5] Sandstrom, Marie, "Liveness Detection in Fingerprint Recognition Systems",, 2004-06-04, <http://www.ep.liu.se/exjobb/isy/2004/3557> (June 25, 2004)

[6] Reza Derakhshani, Sujan Parthnasardi, Lawrence Hornak, Stephanie Schuckers "Perspiration for Detecting Liveness in Fingerprint Scanners—Comparison of Different Classifiers",
<http://biosal - perspiration for detecting liveness in fingerprint scanners.htm/> (June 22, 2004)

[7] Bicz Wieslaw, "The Impossibility of Faking Optel's Ultrasonic Fingerprint Scanners", February 12, 2003
<http://www.optel.pl/article/English/livetest.htm> (June 22, 2004)

[8] Lumidigm Inc, "The Science Behind LumiGuard",
<http://www.lumidigm.com/PDFs/The Science Behind LumiGuard -4.pdf> (June 9, 2004)

[9] AIMS Technology Inc.,"AIMS Biometric Technology",
<http://www.nail-id.com/faqs.html> (June 24, 2004)

References

AIMS Technology Inc.,"AIMS Biometric Technology",
<http://www.nail-id.com/faqs.html> (June 24, 2004)

Bicz Wieslaw, “The Impossibility of Faking Optel’s Ultrasonic Fingerprint Scanners”, February 12, 2003
<http://www.optel.pl/article/English/livetest.htm> (June 22, 2004)

Biomedical Signal Analysis Laboratory, “Spoofing and Liveness Dectection - Brief Background”,
<http://biosal - spoofing and_liveness detection.htm/> (June 22, 2004)

BiometricsInfo.Org, “Liveness Detection in Biometric Systems”
<http://www.biometricsinfo.org/whitepaper1.htm> (June 20, 2004)

Commomwealth of Australia, “CrimTrac Fingerprint Analysis – The Basics”, 2001
< http://www.crimtrac.gov.au/fingerprintanalysis.htm> (June 6, 2004)

Harris Tom, “How Fingerprint Scanners Work”,
<http://travel.howstuffworks.com/fingerprint-scanner.htm/printable>
(June 22, 2004)

Lumidigm Inc, “The Science Behind LumiGuard”,
<http://www.lumidigm.com/PDFs/The Science Behind LumiGuard -4.pdf>
(June 9, 2004)

Reza Derakhshani, Sujan Parthnasardi, Lawrence Hornak, Stephanie Schuckers “Perspiration for Detecting Liveness in Fingerprint Scanners—Comparison of Different Classifiers”,
<http://biosal - perspiration for detecting liveness in fingerprint scanners.htm/> (June 22, 2004)

Sandstrom, Marie, “Liveness Detection in Fingerprint Recognition Systems”, ,
2004-06-04, <http://www.ep.liu.se/exjobb/isy/2004/3557> (June 25, 2004)

Stephanie Schuckers, PhD, Larry Hornak, PhD, Tim Norman, PhD, Reza Derakhshani,Sujan Parthasaradhi, “Issues for Liveness Detection in Biometrics”
<http://www.biometrics.org/html/bc2002_sept_program/2_bc0130_DerakhshabiBrief.pdf> (June 20, 2004)

Schuckers SAC, “Spoofing and Anti-Spoofing Measures”, Information Security Technical Report, Vol. 7, No. 4, pages 56 – 62, 2002. Stephanie A. C. Schuckers, Ph.D., Spoofing and Anti-Spoofing Measures

Clarkson University and West Virginia University, Article for Elsevier Information Security Report on Biometrics, December 10, 2002,
<http://www.citer.wvu.edu/members/publications/files/15-SSchuckers-Elsevior02.pdf> (June 24, 2004)

Thalheim Lisa, Krissler Jan, Ziegler Peter-Michael, "Body Check Biometric Access Protection Devices and their Programs Put to the Test",
< http://www.heise.de/ct/english/02/11/114/> (June 17, 2004

Ton van der Putte, "Spoofing fingerprints as easy as 1,2,3?",
<http://www.keuning.com/biometry/Biometrics_2001.pdf> (June 17, 2004)