Entry for Encyclopedia of Biometrics
January 30, 2008

TITLE OF ENTRY

Liveness: Fingerprint

BYLINE

Stephanie A. C. Schuckers, Clarkson University

SYNONYMS

Vitality, anti-spoofing

DEFINITION

In biometric systems, 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. While fingerprint systems may have an excellent performance and improve security, previous studies have shown it is not difficult to make molds of latent fingerprints left by legitimate users and to create fake fingers made from Play-Doh, gelatin and silicone materials to fool a variety of fingerprint scanners, termed spoofing. Liveness detection reduces the risk of spoofing by requiring a liveness signature in addition to matched biometric information. Methods can be divided into hardware and software categories. Hardware methods include measurement like pulse oximetry, electrocardiogram, or odor while software based measurements use additional processing of the biometric information itself to isolate liveness signatures like perspiration and deformation. While liveness algorithm makes spoofing more difficult, they need to be considered as components of a biometric system which bring with it performance characteristics, as well factors such as ease of use, collectability, universality, spoof-ability, permanence, and, in some cases, even uniqueness. No system is perfect in its ability to prevent spoof-attacks. However, liveness algorithms can reduce this vulnerability to minimize the risk of spoofing.

MAIN BODY TEXT

Fingerprints are graphical ridge-valley patterns from human fingers. Fingerprint recognition is a widely used and efficient technique for biometric authentication. While fingerprint systems may have excellent performance and improve security, previous studies have shown it is not difficult to make molds of latent fingerprints left by legitimate users and to create fake fingers made from Play-Doh, gelatin and silicone materials to fool a variety of fingerprint scanners (Matsumoto, et al, 2002, Matsumoto et al, 2004, Kang et al, 2003, Schuckers 2002). The most famous of which is the work by Matsumoto and colleagues. In the reports, 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. Casts were made of gelatin material and termed 'gummy fingers'. Verification rates of gummy fingers ranged from 68%-100%. For method of creating a cast from residual fingerprints, all fingerprint systems were able to enroll the spoof finger and verify more than 67% of the attempts. Similar results have been seen on subsequent studies with various materials including silicon, clay, and Play-Doh (Matsumoto, et al, Kang, et al, Schuckers, 2002), and one study which looked at cadaver fingers (Schuckers, 2002). Currently, International Biometric Group with sponsorship from Financial Services Technology Consortium (FSTC) is hosting an effort to conduct spoof trials with vendor volunteers called SPOOF 2007.

It should be noted that vulnerability to spoofing is not assessed as part of the false accept ratio, a typical assessment measure of biometric devices. A false accept is when a submitted sample is incorrectly matched to a template enrolled by another user. 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.

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. Overview of liveness approaches are described in (Schuckers, 2002, Valencia, 2002, Schuckers et al 2004, Coli et al 2007). Performance of fingerprint liveness to separate live and spoof fingers is measured by live false reject rate and spoof false accept rate. Equal error rate between the two measures and receiver operating characteristic curves can also be used as described in Biometric Security Overview. Marcialis, et. al., provides a table which compares datasets used for testing and performance of liveness approaches.

Methods to measure liveness fall into several categories. In (Coli et al 2007), a taxonomy is presented whereby methods are divided into software and hardware-based. We suggests a similar division, but also consider an additional category where liveness is inherent to the biometric, i.e. it must be present in order to capture the biometric (Schuckers, 2002). In the first category, liveness is captured through additional hardware integrated with the fingerprint sensor. The first category in software-based involves further processing the biometric signature to obtain liveness information. For example, this may mean extracting perspiration information from fingerprint image. The second software based approach is where liveness is an inherent part of the biometric, in other words, the biometric cannot be captured unless the subject is alive. An example for this category is the electrocardiogram which has been suggested as a biometric (Biel, et al, 2001) and where liveness is inherent to collection of this biometric. Liveness in most cases is not inherent to be able to measure a fingerprint biometric. Most systems which consider liveness in fingerprint do so through additional software or hardware processing. Electrocardiogram might be considered a special case as it has been suggested as an additional measurement to fingerprint recognition so it can be considered as hardware liveness approach and it may be potentially inherent to the biometric if the electrocardiogram is used as a biometric.

Hardware

The first method uses extra hardware to acquire life signs. Previously developed approaches measure fingertip temperature, pulse, pulse oximetry, blood pressure, electric resistance, odor, multi-spectral information, or electrocardiogram (Osten et al, 1998, Lapsley, et al, 1998, Kallo, et al, 2001, Biel, et al, 2001, Baldisserra, et al, 2006, Nixon, et al, 2005). These methods require dedicated hardware integrated with the fingerprint system. Electrocardiogram is the electrical measurement of the heart collected through electrodes on two skin contact points on the body which need to be on opposite sides of the heart (e.g. two hands, hand and foot). Pulse oximetry is the measurement of the oxygen content of the blood through the comparison of the absorption of two wavelengths of light by the blood. This measurement requires a LED and photodetector on opposite sides of the finger and typically needs to be shielded from ambient light. This absorption also varies has the heart beats and can be a measure of pulse, and therefore may require a few seconds to compute in order to record one or two complete heart beat cycles. A critical component to hardware-based approaches is how the additional hardware is integrated with the fingerprint sensor. It should be integrated in such a way that it cannot be spoofed with any live finger in combination with a spoof.

The following paragraph describes two fingerprint sensors, multispectral and ultrasound, which naturally capture liveness information. They are placed here in the hardware category, because these approaches, while commercially viable, require purchase of a specific scanner and are not applicable to standard fingerprint readers. One commercially available fingerprint sensor (Lumidigm, USA) uses a multispectral sensor, from which multiple wavelengths of light and different polarizations allow new data to be captured which is unavailable from a conventional optical fingerprint reader. Based on the multiple spectral images, they have developed a spoof detection method (Nixon, et al, 2005). Similarly, ultrasound measurements have been suggested as a way to measure fingerprint images (Optel, Poland). While fingerprint measured by ultrasound might be able to image a spoof or cadaver fingerprint itself, using additional information from the ultrasound measurement, would likely be capable of separating live from spoof images. Both approaches most likely need additional processing from the fingerprint image itself to determine liveness.

Software

The second method uses the information already present in the fingerprint image to detect life signs, for example, skin deformation, pores, power spectrum or perspiration pattern.

Skin deformation and elasticity Skin deformation technique uses the information regarding how the fingertip's skin deforms when pressed against the scanner surface (Chen, et al, 2005, Antonelli et al, 2006, Jia et al 2007, Zhang, et al, 2007). The studies show that when a real finger moves on a scanner surface, it produces a significant amount of non-linear distortion. However, fake fingers are more rigid than skin and the deformation is lower even if they are made of highly elastic materials. One approach quantifies this considering multiple frames of clockwise motion of the finger (Antonelli et al 2006). The performance of this method is an equal error rate of 11.24% using 45 live subjects and 40 fake fingers. A study by (Zhang et al, 2007) uses a thin-plate spline distortion model over multiple frames while the finger is moved and resulted 4.5% EER in a dataset of 120 fake fingerprints from silicon from 20 individuals. Another method considers the deformation in a single image compared to a template (Chen et al, 2005). This study achieved 82% for a small dataset.

Perspiration pattern Previously, our laboratory has demonstrated that perspiration can be used as a measure of liveness detection for fingerprint biometric systems. Unlike spoof and cadaver fingers, live fingers demonstrate a distinctive spatial moisture pattern when in physical contact with the capturing surface of the fingerprint scanner. The pattern in fingerprint images begins as 'patchy' areas of moisture around the pores spreading across the ridges over time. Image/signal processing and pattern recognition algorithms have been developed to quantify this phenomenon using wavelet and statistical approaches (Derakshani et al, 2003, Schuckers, et al, 2004, Parthasardhi et al, 2005, Tan, et al, 2005). These approaches require two time-series images, which might be not convenient for the users. Other methods to quantify this phenomenon have been developed for a single image(Tan et al, 2006). Performance has achieved approximately 10% live/spoof EER for earlier papers on a dataset of 80 spoof, 25 cadaver and 58 live images to perfect separation in later papers on this small dataset (Schuckers, et al 2004).

Characteristics of spoof and live images A natural extension to the specific categories above is to begin to assess the characteristics that define live and spoof fingers which cover a broad range (Jia et al, 2007, Uchida 2004, Moon et al, 2005, Coli, et al 2007, Jin et al, 2007, Tan, et al, 2008).

These include image power spectrum which reveals stamp fabrication process (Coli, et al 2007), noise residue in the valleys due to spoof material (Moon et al, 2005, Tan, et al, 2008), and combinations of multiple factors, for example, fusion of perspiration and deformation features in (Jia, et al, 2007).

Image power spectrum has been considered as an effective feature for vitality detection (Coli, et al 2007, Jin, et al 2007). The difference between live and spoof images is mainly due to the stamp fabrication process which causes an alteration of frequency details between ridge and valleys. The Fourier transform feature can quantify the difference in terms of high frequency information loss for fake fingers. This approach is tested for a single scanner and silicone spoof material with average spoof/live EER of 2.4% on a dataset of 720 fake and 720 live images from 36 individuals (Coli, et al 2007) and for gelatin and silicon with average of 23% EER for a dataset of 900 fake and 450 live images from 30 individuals (Jin, et al 2007).

In other study by (Jia et al 2007), a sequence of images is used to measure skin elasticity, but some of the measures may be capturing perspiration information as described above. No special motion is required of the finger. They achieve results of 4.78% on a dataset of 470 spoof images from 47 spoof casts and 300 live images from 15 individuals. In a second study, fusion of multiple features, two based on perspiration signal and two based on skin elasticity, was performed in (Jia & Cai, 2007). Result showed 4.49% EER on the same dataset.

Liveness Algorithm Framework

Fingerprint liveness algorithm can fall into types described above (hardware, software, inherent). Other factors which separate liveness algorithms include (1) dynamic/static, (2) user training, and (3) binary/user specific. Table 1 compares five fingerprint liveness algorithms within the context of this framework.

- ***Dynamic or static***: Liveness algorithms may require only one frame or rely on multiple frames to measure the dynamic nature of the system to detect liveness (Coli et al 2007). For example, many of the perspiration proposed approaches require more than one image (Derakhshani, et al, 2003), although recent work has used one image (Tan et al, 2006). Other dynamic approaches are related to deformation (Antonelli et al 2006, Zhang, et al, 2007, Jia et al 2007). Note that pulse oximetry do not require multiple fingerprint image frames, however, they may require more time to record one or more full heart cycles.
- ***User training***: Some liveness algorithms rely on specific user actions to determine liveness. This may include a procedure (deformation changes due to rotating the finger) which require user training (Antonelli et al 2006, Zhang, et al, 2007).
- ***Binary (live/spoof) versus user specific***: Liveness algorithms can be made general across all subjects, that is, the same algorithm is used for all subject to determine liveness producing a binary result: live or non-live. Other approaches can be made subject specific, that is, a liveness algorithm is imbedded as part of the biometric template. For example, work has been shown for storing a perspiration pattern specific to an individual (Abhyankar, et al 2005). While not specifically mentioned for the multi-spectral fingerprint scanner (Lumidigm, USA) it is possible that a medical spectroscopy-based liveness approach could be user specific. Electrocardiogram can also be user-specific, that is, used as a biometric (Biel et al 2001).

Other characteristics for evaluating biometrics systems, such as ease of use, collectability, user acceptance, universality, uniqueness, permanence, and spoof-ability, need to be considered before implementing a liveness algorithm. These were described in the Biometric Security Overview Chapter. Table 2 considers the same liveness algorithms from Table 1 within the context of this framework.

- ***Ease of use***: Some liveness approaches may be easier to use. For example, fingerprint deformation approach which requires a specific rotation procedure may be considered more difficult to use (Antonelli et al 2006, Jia, et al, 2007). Lumidigm approach for spectroscopy where liveness is collected as part of the biometric collection itself may be considered easier to use.
- ***Collectibility***: The hardware, equipment setup, and relationship to the user impacts the collectability of the liveness algorithm. For example, approaches which may be more difficult to collect include the electrocardiogram which requires two points of contact on opposite sides of the body or pulse oximetry where the finger must be enclosed to protect from ambient light. In comparison, approaches which use the traditional biometric equipment for measurement of liveness might be considered easier to collect.
- ***User acceptance***: For fingerprint liveness, approaches which may have low user acceptance are ones that are more likely to be linked with medical conditions due to privacy concerns (electrocardiogram, pulse oximetry, multi-spectral).
- ***Universality***: Obviously all authorized users should be live when presenting their biometric; however, the liveness signature may be difficult to measure in some subjects. For example, perspiration in fingerprint images may be difficult to measure in individuals with very dry skin, also a problem with measuring the fingerprint image itself.
- ***Uniqueness***: For liveness approaches which are inherent to the biometric, this factor is critical. However, as mentioned above, electrocardiogram in combination with fingerprint would not need uniqueness as a characteristic, whereas, the electrocardiogram alone may need further research to address uniqueness (Biel, et al 2001).
- ***Permanence***: Permanence typically refers to permanence of the specific biometric pattern over time. Similar to above, this more directly applies to liveness approaches which are inherent to the biometric, where the biometric/liveness signature may vary over time. For example, in the initial work introducing perspiration patterns as a unique liveness pattern, only three months were considered (Abhyankar, et al 2005). It is unknown if these patterns persist beyond that period. Electrocardiogram may also have difficulties with permanence as the electrocardiogram is impacted by health conditions (Biel, et al 2001).
- ***Spoof-ability***: Spoof-ability considers the possibility is that the liveness mechanism that is put in place to protect the system from spoofing can be spoofed. For example, in the case of pulse oximetry, it may be possible to spoof with a clear spoof which allows transmission of the light needed to make the pulse oximetry measurement. This goes beyond the performance of the liveness algorithm described above, because it requires assessment of spoofing approaches that have yet to be replicated in the database used to test the liveness algorithm.

Summary

In summary, liveness systems are being suggested to reduce the vulnerability due to spoofing. Liveness measures have an inherent performance, that is, ability to separate spoof and live attempts. In addition, liveness algorithms have other factors and considerations including ease of use, collectability, user acceptance, universality, uniqueness, permanence, and spoof-ability. One factor which is difficult to measure is spoof-ability, the possibility that the liveness measure can be spoofed. In this chapter, we use the term liveness, fully acknowledging that it is not a perfect system and that it is not possible to recreate all possible spoof attempts for a system. Furthermore, there may be measurements which rule out specific spoofs but cannot be shown to absolutely measure liveness. For example, algorithms may be designed which may readily detect silicon, but not gelatin, spoof images. In summary, it is unlikely that any system will perfectly measure liveness and be spoof-proof. Liveness may be boiled down to an attempt to stay one step ahead of those intending to defeat the system through spoof attacks. Methods such as liveness or anti-spoofing are critical to the security and credibility of biometric systems to protect from security vulnerabilities to the degree needed for a particular application.

RELATED ENTRIES

Security and Liveness
Vulnerabilities
Liveness Iris

REFERENCES

Abhyankar A, Schuckers SAC**,** Characterization, similarity score, and uniqueness of fingerprint perspiration patterns, *Proceedings of Audio- and Video-Based Biometric Person Authentication: 5th International Conference*, *Lecture Notes in Computer Science*, Kanade et al (eds.) Springer Verlag GmbH, 3546: 860-868, 2005

A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis", IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006.

D. Baldisserra, A. Franco, D. Maio and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis", in proceedings International Conference on Biometric Authentication (ICBA06), Hong Kong, January 2006.

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.

Y. Chen, A. Jain, and S. Dass, Fingerprint Deformation for Spoof Detection, Proc. Of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 2005

P. Coli, G. L. Marcialis, F. Roli, *Power spectrum-based fingerprint vitality detection* , IEEE Workshop on Automatic Identification Advanced Technologies AutoID 2007.

P. Coli, G. L. Marcialis, F. Roli, *Vitality Detection from Fingerprint Images: A Critical Survey*, Advances in Biometrics, Volume 4642/2007, pp. 722-731.

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.

Jia Jia, Lianhong Cai, Kaifu Zhang and Dawei Chen, A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis, Advances in Biometrics, Volume 4642/2007, pp. 309-318.

Jia Jia and Lianhong Cai, Fake Finger Detection Based on Time-Series Fingerprint Image Analysis, in Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, Springer, Volume 4681/2007, pp. 1140-1150.

Changlong Jin, Hakil Kim, and Stephen Elliott, Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum, in Information Security and Cryptology - ICISC 2007, Springer, Volume 4817/2007, pp. 168-179.

H. Kang, B. Lee, H. Kim, D. Shin, J. Kim, A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules, KES 2003, pp. 1245-1253, 2003.

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

P. D. Lapsley, J. A. Less, D. F. Pare, Jr., N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow", SmartTouch, LLC, U.S. Patent #5,737,439, April 7, 1998.

T. Matsumoto, Gummy Finger and Paper Iris: An Update, Workshop on Information Security Research, Fukuoka, Japan, Oct. 2004.

T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, Impact of artificial 'gummy' fingers on fingerprint systems, Proceedings of SPIE, vol. 4677, Jan. 2002

Y.S. Moon, J.S. Chen, K.C. Chan, K. So and K.C. Woo, Wavelet based fingerprint liveness detection, Electronic Letters, Vol. 41, Issue: 20, pp. 1112-1113, 2005.

K. A. Nixon, R. K. Rowe, *Spoof detection using multispectral fingerprint imaging without enrollment*, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21, 2005.

D. Osten, H. M. Carim, M. R. Arneson, B. L. Blan, "Biometric, personal authentication system", Minnesota Mining and Manufacturing Company, U.S. Patent #5,719,950, February 17, 1998.

Parthasaradhi S, Derakhshani R, Hornak L, Schuckers SAC, Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335- 343, 2005.

Schuckers SAC, Derakhshani R, Parthasardhi S, Hornak, LA, Liveness Detection in Biometric Devices, in Electrical Engineering Handbook, 3rd edition, CRC Press, Chapter 26, ISBN: 084932274X, 2006.

S. A. C. Schuckers, "Spoofing and anti-spoofing measures," *Information Security Technical Report*, Vol. 7, No. 4, pages 56 – 62, 2002.

S.A.C. Schuckers, Spoofing and anti-spoofing measures, Information Security Technical Report, Vol. 7, No. 4, pages 56 – 62, 2002.

Schuckers SAC, Abhyankar A, A Wavelet Based Approach to Detecting liveness in Fingerprint Scanners, Proceedings of Biometric Authentication Workshop, ECCV, Prague, May, 2004.

B. Tan, S. Schuckers, Liveness detection using an intensity based approach in fingerprint scanner, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 2005.

Tan B, **Schuckers S** A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis, *Journal of Electronic Imaging*, Vol. 17, No. 1, 2008 accepted for publication

B. Tan, S. Schuckers, Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing, IEEE 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006.

Kaoru Uchida, Image-Based Approach to Fingerprint Acceptability Assessment, in Biometric Authentication, Springer, Volume 3072/2004, pp. 294-300.

V. Valencia and C. Horn, "Biometric Liveness Testing," in *Biometrics*, editors: J. D. Woodward, Jr., N. M. Orlans, R. T. Higgins, Ed., McGraw-Hill Osborne Media, New York, 2002.

Yangyang Zhang, Jie Tian, Xinjian Chen, Xin Yang, and Peng Shi, Fake Finger Detection Based on Thin-Plate Spline Distortion Model, Advances in Biometrics, Volume 4642/2007, pp. 742-749.

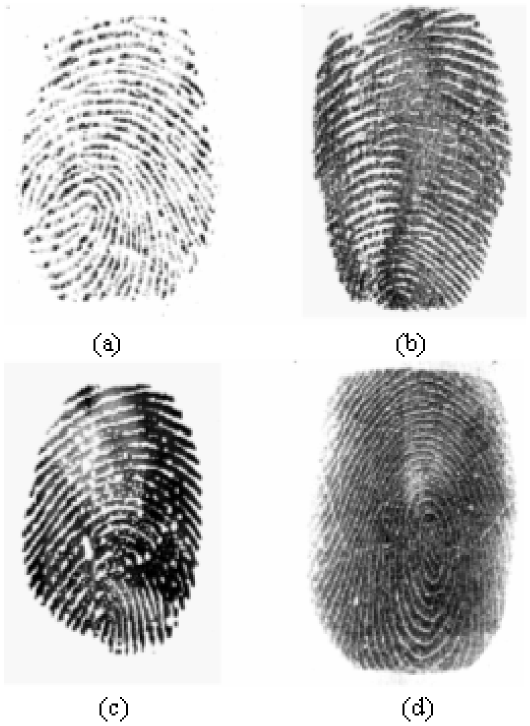

Fig. 1. Example of live and non-live fingerprints captured by Capacitive DC scanner: (a) live finger; (b) spoof finger made from Play-Doh; (c) spoof finger made from gelatin; (d) cadaver finger

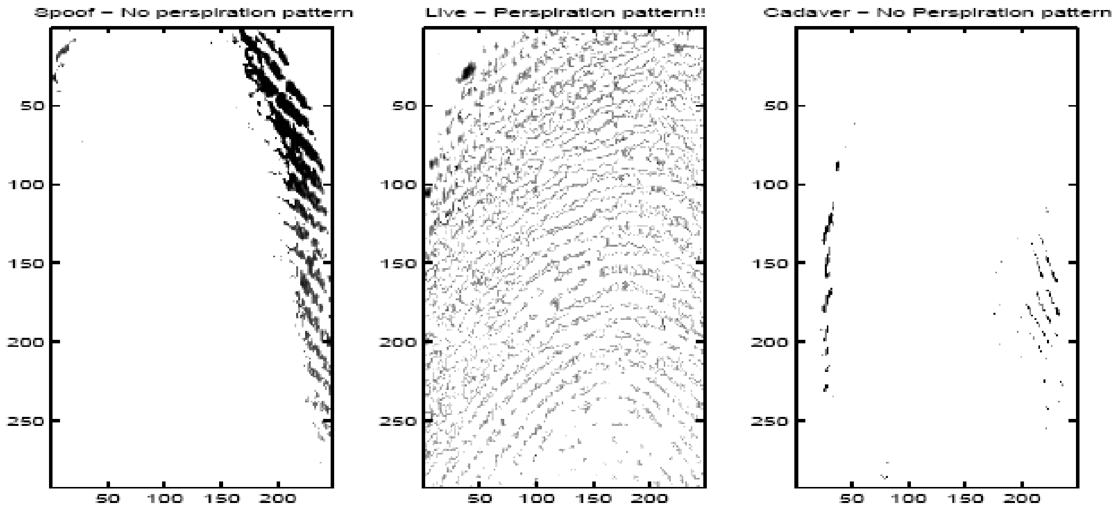

Figure 2. Perspiration patterns. Spoof, live, and cadaver patterns are shown from left to right. The perspiration pattern is the reconstruction of the isolated wavelet coefficients obtained from two fingerprint images in time, by the algorithm described (Schuckers et al, 2004).

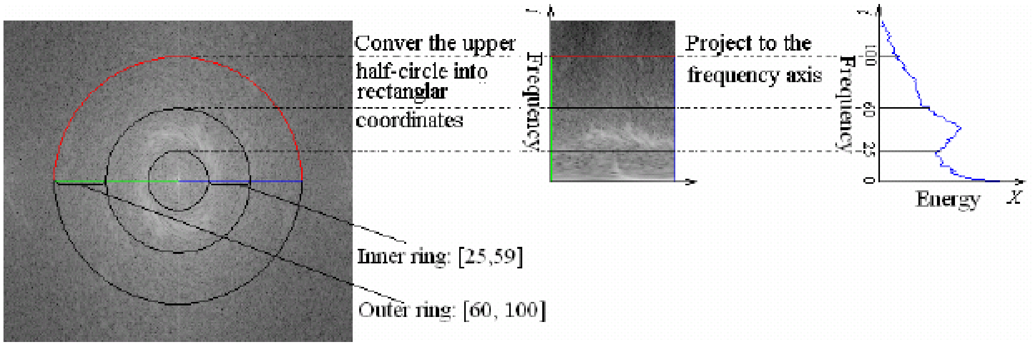

Figure 3. Spectral image of the fingerprint, the ring pattern, and the band-selected frequency analysis from (Jin, et al, 2007).

Table 1. Liveness algorithm types and factors*

	Hardware/ Software	Multiple/ Single	Binary/ User specific	User training
Perspiration	S	M/Si	B/US	None
Pulse oximetry	H	-	B	None
Multi-spectral	H	Si	B/US	None
Deformation	S	M/Si	B	UT or none
ECG	H	-	B/US	UT

*H: Hardware, S: Software, M: Multiple, Si: Single, B: Binary, US: User Specific, UT: User Training, - indicates not applicable

Table 2. Liveness algorithm characteristics*

	Ease of Use	Collectability	User acceptance	Universality	Uniqueness	Permanence	Spoof-ability
Perspiration	H	H	H	M	L	M	M
Pulse oximetry	L	L	L	H	-	-	H
Multi-spectral	H	H	M	H	-	-	L
Deformation	L	L	H	M	-	-	M
ECG	L	L	L	H	L	H	H

*H: High, M: Medium, L: Low, - indicates not applicable