A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems

Emanuela Marasco, West Virginia University
Arun Ross, Michigan State University

Several issues related to the vulnerability of fingerprint recognition systems to attacks have been highlighted in the biometrics literature. One such vulnerability involves the use of artificial fingers, where materials such as play-doh, silicone, and gelatin are inscribed with fingerprint ridges. Researchers have demonstrated that some commercial fingerprint recognition systems can be deceived when these artificial fingers are placed on the sensor, i.e., the system successfully processes the ensuing fingerprint images thereby allowing an adversary to spoof the fingerprints of another individual. However, at the same time, several countermeasures that discriminate between live fingerprints and spoof artifacts have been proposed. While some of these anti-spoofing schemes are hardware-based, several software-based approaches have been proposed as well. In this paper, we review the literature and present the state-of-the-art in fingerprint anti-spoofing.

Categories and Subject Descriptors: C.2.2 [**Pattern Recognition**]: Applications

General Terms: Design, Algorithms, Performance

Additional Key Words and Phrases: Biometrics, Fingerprints, Anti-Spoofing, Person Verification, Liveness Detection

ACM Reference Format:
Emanuela Marasco, Arun Ross, 2014. A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems *ACM Comput. Surv.* 47, 2, Article A (September 2014), 36 pages.
DOI: http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics such as fingerprints, face, iris, gait and voice [Jain et al. 2011]. The use of fingerprints as a biometric attribute has been extensively discussed in the scientific literature, and a variety of techniques have been developed for performing fingerprint recognition. Fingerprint recognition systems have been incorporated into a number of forensic, civilian and commercial applications [Maltoni et al. 2003].

Given its widespread usage, researchers have analyzed the vulnerability of these systems to different types of adversary attacks [Ratha et al. 2001], including fingerprint obfuscation and impersonation. Fingerprint obfuscation [Feng et al. 2009; Yoon et al. 2010] refers to the deliberate alteration of the fingerprint pattern (e.g., cutting or burning the fingertips) by an individual who wants to avoid being recognized by the system. For example, a person in a watch-list may attempt to modify their fingerprint pattern to prevent being matched against their entry in the watch-list. Mutilated fingerprints have been encountered in both law enforcement and large-scale national

Author's addresses: E. Marasco, Lane Department of Computer Science and Electrical Engineering, Morgantown WV 26506 (USA); A. Ross, Department of Computer Science and Engineering, East Lansing MI 48824 (USA).

DOI: http://dx.doi.org/10.1145/0000000.0000000

identification or border control systems [Feng et al. 2009]. In December 2009, it was determined that a Chinese woman who had been previously deported from Japan had re-entered the country after surgically swapping her right hand fingerprints with those of her left hand[1]; consequently, the fingerprint recognition system deployed at the Japanese immigration checkpoint had failed to match her fingerprints against those in the deportee-database. Fingerprints can also be obliterated by burning, cutting, abrading or by simply removing a portion of the skin from the fingertip; additionally, they can be imitated, by removing a portion of the skin from the fingertip, then filling the removed part with skin from other parts of the body [Yoon et al. 2012].

"What about Impersonation?" is also a common question people ask about fingerprint recognition systems [Miller 1994]. Well-duplicated artificial fingerprints, referred to as spoof artifacts, can be presented to a fingerprint sensor in order to deceive the recognition system [Schuckers 2002]. This corresponds to a sensor-level attack where an adversary intends to gain unauthorized access to a system by using the biometric traits of someone who is legitimately enrolled in the system [Nixon et al. 2007] [Holland-Minkley 2006]. Furthermore, an attacker may create a new "identity" using an artificial biometric trait that can be enrolled in the system and then shared between different people [Kluz 2005; Valencia and Horn 2003]. Several spoofing techniques have been reported, including the use of artificial fingerprints made of gelatin, moldable plastic, play-doh and silicon, produced by using a mold obtained from a live finger or from a latent fingerprint [Abhyankar and Schuckers 2009] [Stén et al. 2003b]. Since fingerprint systems that control access to devices where confidential information is kept are expected to be highly reliable (e.g., laptops, tablets, smartphones, etc.), spoof attacks represent an important concern. In March 2013, a Brazilian doctor was accused of using spoof fingers to "check-in" co-workers who were not present at the work place[2]. In September 2013, only a few days after the iPhone5S equipped with the Touch ID fingerprint sensor was released, a German group announced that the sensor could be fooled by using a sheet of latex or wood glue hosting the fingerprint ridges of a person[3]. In order to minimize this vulnerability, different *spoof detection* methods have been suggested. Spoof detection refers to the capability of the system to determine whether the object being placed on the sensor corresponds to a live finger or not [Sepasian et al. 2010].

The importance of spoof detection has been further highlighted by the TABULA RASA (Trusted Biometrics under Spoof Attacks) project[4] funded by the European Commission (7th Framework Program) which is playing a significant role in increasing the robustness of biometric systems to spoof attacks by developing effective countermeasures. Further, the Biometrics Vulnerability Assessment Expert Group (BVAEG)[5] was formed by the Biometrics Institute to raise awareness about the vulnerability of biometric systems to various types of attacks and to encourage vendors to develop efficient solutions for detecting and deflecting these attacks. Its overall mission is to reduce vulnerabilities in biometrics including those due to spoof attacks.

1.1. Fingerprint features

A fingerprint refers to a flowing pattern on the fingertip of an individual consisting of ridges and valleys (see Fig. 1) [Maltoni et al. 2003]. Fingerprints can be represented

[1]http://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505
[2]http://nexidbiometrics.com/brazilian-doctor-arrested-for-using-fake-fingerprints/
[3]http://secureidnews.com/news-item/apples-touch-id-spoofed/
[4]http://pralab.diee.unica.it/it/TabulaRasaEuroproject
[5]http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group-bvaeg.html

by using global information (e.g., finger ridges) or local information (characteristics derived from the ridges). Ridge details are generally described in hierarchical order at three different levels. At global level (Level 1), macro details such as the pattern type of ridges and valleys can be detected. Ridges exhibit one or more regions where they assume a distinctive shape which can be classified as loop, delta or whorl (see Fig. 2). At local level (Level 2), the details consist of different anomalies like ridge ending and ridge bifurcation, referred to as minutiae points or Galton characteristics (see Fig. 3). Each minutia included in a fingerprint image is represented by its location (x,y) and the ridge direction at that location (θ). At a very fine level (Level 3), details such as sweat pores and incipient ridges can be detected in the fingerprint pattern (see Fig. 4) acquired by high resolution scanners (1000 dpi) [Maltoni et al. 2003]. Based on their position on the ridges, pores can be considered open or closed. A closed pore is entirely enclosed by a ridge while an open pore intersects the valley [Jain et al. 2007].

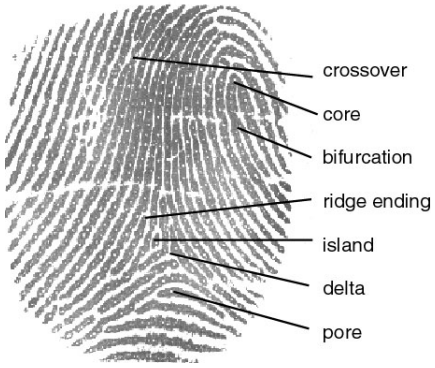


Fig. 1. The image shows the discontinuities that interrupt the flow of ridges which are the basis for most fingerprint authentication methods. Ridge endings are the points at which a ridge stops, and bifurcations are the points at which a ridge divides into two. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other). Image taken from http://cnx.org/content/m12574/latest/ [Harrison et al. 2004], with permission of OpenStax CNX.

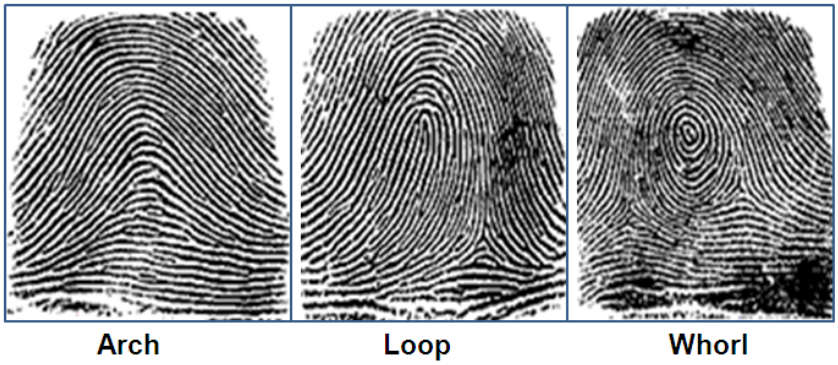


Fig. 2. Level 1 fingerprint details. Level 1 (pattern) refers to macro detail such as ridge flow and pattern type. Image taken from http://cnx.org/content/m12574/latest/ [Harrison et al. 2004], with permission of OpenStax CNX.

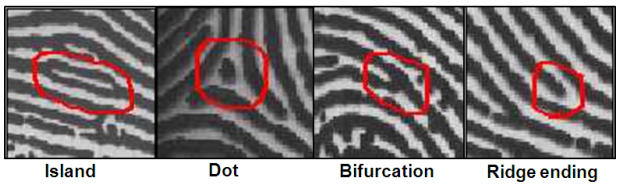


Fig. 3. Level 2 fingerprint details. Level 2 (points) refers to the Galton characteristics, or minutiae points, such as bifurcations and endings. Image taken from http://cnx.org/content/m12574/latest/ [Harrison et al. 2004], with permission of OpenStax CNX.

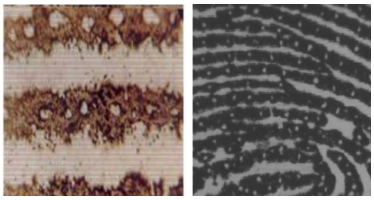


Fig. 4. Level 3 fingerprint details. The image on the left shows a photo-graphical example of pores. The image on the right is output from a high resolution sensor (1000 dpi) that captures the location of pores in detail. Both images are from [H. Choi and Kim 2007], with permission of Waset Team International Science Council. ©Waset

1.2. Fingerprint Sensing

Fingerprints can be acquired by using different technologies [Maltoni et al. 2003]. In optical sensors, the finger is placed on a transparent prism and the image is obtained through a camera. In total internal reflection (TIR) sensors, ridges and valleys are imaged in contrast: ridges are in contact with a glass platen and when the surface is illuminated through one side of the prism, the light entering the prism is reflected at the valleys and absorbed at the ridges. In general, sensors based on this technology are vulnerable to spoof artifacts developed using materials having a light reflectivity similar to that of the skin. Moreover, optical devices produced by different manufacturers usually present physical differences between units (i.e., lenses). Subsequently, fake fingerprint detection rates can vary across units. In particular, devices which use micro-prisms embedded in a thin plastic are robust to spoof attacks [Willis and Lee 1998].

In capacitive devices, the finger is modeled as the upper electrode of a capacitor, while a metal plate is modeled as the lower electrode. Given the difference in terms of capacitive values between skin-sensor and air-sensor contact, the variation in capacitance between valleys and ridges can be measured when the finger is placed on the sensor. Capacitive sensors are vulnerable to soft artificial fingerprints commonly made of gelatin.

In thermal sensors, the finger is placed on pyro-electric material which converts variations in temperature into voltage. The contact of the ridges with the sensing material causes a change in temperature, while the temperature remains constant under the valleys that are not in direct contact with the material. The signal (image) disappears once a thermal equilibrium is reached between the finger and the chip [Han et al. 1999; Han et al. 2005].

In ultrasound sensors, the difference in terms of acoustic impedance between the skin of the ridges and the air in the valleys is exploited. Acoustic waves are transmitted towards the fingertip surface and the reflected signal is captured by a receiver. This category of sensors is more vulnerable to artificial fingerprints when materials possessing the same echoing properties of fingers are used to circumvent the scanner.

2. FINGERPRINT SYSTEM SECURITY

Between acquiring biometric data and delivering a result, there are various points where attacks may occur and compromise the overall security of a biometric system. Several weak links and vulnerabilities are identified by Ratha *et al.* in [Ratha et al. 2001] (see Fig. 5):

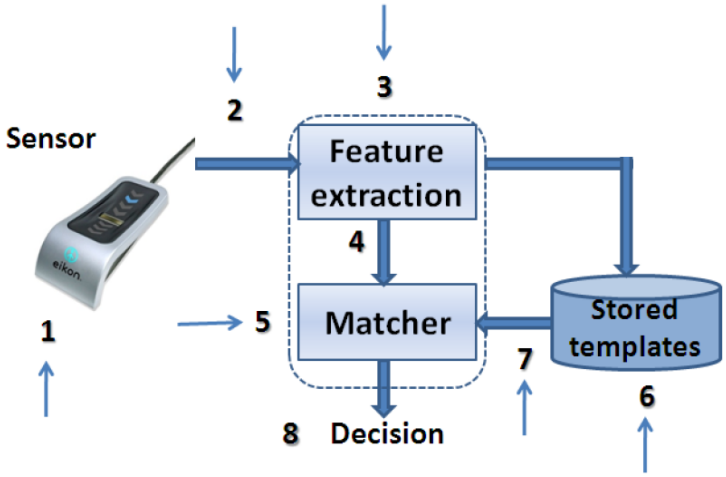


Fig. 5. Vulnerable points of attacks in a biometric system.

(1) Presentation Attack. A reproduction of the biometric modality is presented as input to the sensor [Uludag and Jain 2004].
(2) Biometric Signal Replication. The sensor is bypassed and biometric data previously stored or intercepted is resubmitted (e.g., copy of a fingerprint image).
(3) Feature Modification. The feature extractor is substituted with a trojan horse in which features are preselected by the attacker.
(4) Replacing Features. The set of features extracted from the input biometric trait is replaced with a fraudulent set of features.
(5) Overriding the Matcher. The matcher is corrupted and forced to output match scores preselected by the attacker.
(6) Replacing Templates. One or more templates are modified by an attacker such that an authorized identity is associated with a fraudulent template.
(7) Modifying Data through the Channel. The templates transmitted through the channel are intercepted and corrupted.
(8) Altering the Decision. The final match result is overridden by an attacker.

This paper focuses on presentation attacks which do not require specific knowledge about the system operation [Galbally et al. 2007].

2.1. Artificial Fingerprints

Artificial fingerprints are usually made of materials which can be scanned by existing commercial fingerprint scanners. Items like play-doh and clay are good materials for spoofing due to their moisture-based texture [Toth 2005; Galbally et al. 2007]; however, this may not be true across different types of scanners employing different principles for sensing the fingerprint. An attacker who wishes to manufacture an artificial fingerprint must have a representation of the original fingerprint [Franco and Maltoni 2008]. The duplication of a fingerprint can be a cooperative process, where the real owner participates in the creation of the artificial fingerprint, or a non-cooperative process (see Fig. 6 and 7). In a realistic scenario, it is highly unlikely that a person will agree to produce a mold of his finger; in this case duplication can be done using latent fingerprints. Matsumoto *et al.* in [Matsumoto et al. 2002] described how to make molds from live fingers and the corresponding artificial clones based on these molds. They evaluate 11 different fingerprint sensors, both capacitive and optical, in the presence of gelatin-based artificial fingerprints. Reported results showed a high spoof acceptance rate (which is undesirable from the system's perspective). Although high resolution scanners (1000 dpi) have become commercially available [Imamverdiev et al. 2009], most Automated Fingerprint Identification Systems (AFIS) employ only Level 1 and Level 2 features [Brislawn et al. 1996; Garris and McCabe 2000; Jain et al. 1997]. This means spoofing methods have to primarily reproduce only first and second level information [Jain et al. 2007]. Techniques employed for spoofing are categorized in Fig. 9 and described below [Geller et al. 1999; Geller et al. 2001; Wiehe et al. 2004; Fladsrud and Sollie 2004].

Fig. 6. Making an artificial fingerprint directly from a live finger: plastic is used to obtain the mold and gelatin to obtain the cast. Image taken from [http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf], with permission of Dr. T. Matsumoto.

2.1.1. Cooperative Duplication

— *Direct mold*. The spoof is created from a live finger mold. The finger of the subject is pressed on the surface of a dental impression material or plaster; the negative impression of the fingerprint is fixed on it and a mold is obtained. The mold is then filled with a moisture-based material (e.g., gelatin or liquid silicon) and the spoof is produced [6].

[6]http://www.journalofaestheticsandprotest.org/4/fingerprint/fingerprint.pdf

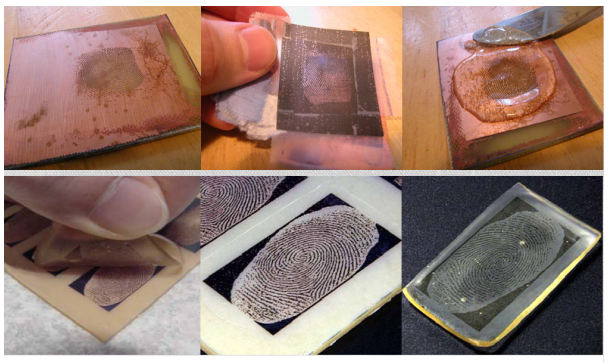


Fig. 7. Making an artificial fingerprint from residual fingerprint using Printed Circuit Board (PCB). Image taken from [Matsumoto et al. 2002; Stén et al. 2003a], with permission of Dr. T. Matsumoto.

Fig. 8. A dead human finger. The sample is taken from the dataset collected at Clarkson University [http://middleware.internet2.edu/idtrust/2011/slides/04-biometrics-schuckers.ppt], with permission of Dr. S. Schuckers.

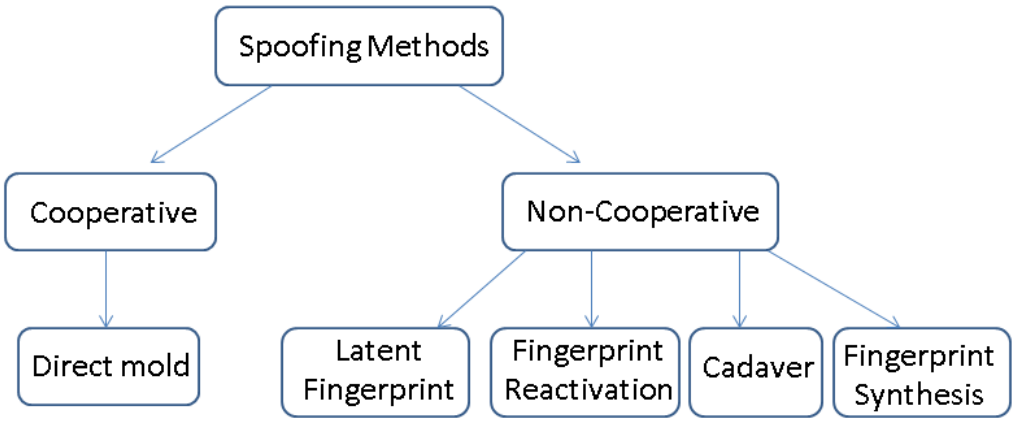


Fig. 9. A taxonomy of existing methods employed for creating artificial fingerprints.

2.1.2. Non-Cooperative Duplication

— *Latent fingerprints*. There are several methods for revealing latent fingerprints. Here we briefly describe only three methods in the context of spoofing [Bowden-Peters et al. 2012]. The first method is based on latent fingerprint lifted with pow-

der. The fingerprint left on a surface is placed on a transparency and it is visualized by powdering with a brush. The powder is removed from the background using scotch tape. This lifted print is placed on the sensor. The second method is based on a photolithographic PCB (Printed Circuit Board) mold. The fingerprint is placed on a transparency and enhanced by brushing with a black powder. Then it is photographed by using a digital camera and printed on a transparency to create a mask for etching the PCB. The mask is placed on the circuit and exposed to UV light. The plaster cast of the fingerprint is filled with liquid silicon rubber to create a waferthin gummy and it is attached to a live finger before being placed on a sensor. The third method is based on a recent advancement that shows the unique ability to lift latent fingerprints from various surfaces and visualize them under daylight within 30 seconds. Such an ultrafast recognition is based on an electrospun nanofiber mat [Yang et al. 2011].

— *Fingerprint reactivation*. Simple techniques such as breathing on the sensor, placing a water filled plastic bag or brushing graphite powder on the sensor have been used to reactivate latent fingerprints deposited on a sensor.
— *Cadaver*. This refers to the usage of a dead finger (Fig. 8).
— *Fingerprint synthesis*. A fingerprint image is reconstructed from a fingerprint template (e.g., minutiae points) of a user enrolled in the system [Franco and Maltoni 2008]. Reversibility of minutiae templates has been demonstrated in several works [Ross et al. 2007; Maltoni et al. 2003; Hill 2001; Galbally et al. 2008; Franco and Maltoni 2008]. Once a digital image of the fingerprint is derived from the minutiae template, it can then be transferred to a spoof artifact.

Additionally, there are methods for depositing viscous materials, including the oily substance known as sebum found in human fingerprints. The deposition method has been tested using an artificial sebum material which is a soft wax-like mixture having a solid state at room temperature [Staymates et al. 2013]. An array is created to print a square containing ten rows and ten columns of single dots of sebum as can be seen in Fig. 10.

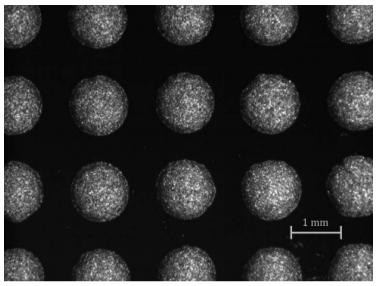


Fig. 10. Micrograph of sebum dots on painted metal surface [Staymates et al. 2013], reproduced by permission of The Royal Society of Chemistry

When the owner cooperates, the spoof fingerprint is of usually better quality compared to the case with no cooperation. However, the quality of the reproduced fingerprint image may be affected by the confluence of different factors such as the initial pressure of the finger on the cast and the contact of the stamp on the sensor acquisition surface, which may alter the fingerprint shape [Coli et al. 2007b]. Furthermore, rates of successful spoof attacks are influenced by the nature of both the mold and the spoof [Espinoza and Champod 2011a]. First, the mold material impacts the quality of the spoof; some molds are more amenable for reproducing the fingerprint pattern than

others. The efficiency of a mold depends also on how many times it has been used: increased usage will lead to deterioration resulting in poor quality artificial fingerprints. For example, repeated use of gelatin fingers will result in a rapid degradation of the quality of the prints provided [Elliott et al. 2007]. Additionally, the quality of the spoof varies based on their thickness, drying time spent and potential defects due to the creation process. Poor quality spoofs can be obtained when reproducing the fingerprint pattern pertaining to subjects with thin ridges.

The submission of a "good" spoof increases the probability of being accepted as a live sample. Performance can be affected by factors related to the right amount of moisture and the humidity conditions of the acquisition environment. The nature of human interaction impacts spoof acceptance rate as well [Yamada et al. 2000]. Practical techniques for defeating biometric devices were discussed in [Lane and Lordan 2009]. After testing 15 different materials for molding, they reported that clay, plasticine and blutac are the best materials to create an accurate mold since they are easy to use and fast to create. In particular, clay performs excellently well when reproducing details of the fingerprint at all the three levels: ridge, minutiae and pores. They also tested eight materials for casting and reported that PVA glue is both easier to use and faster to obtain. The best combinations of materials found are clay or blutac with gelatine or latex. Spoof acceptance rate also depends on the deployed sensing technology. Both capacitive and optical devices are more vulnerable to the aforementioned spoofing techniques compared to thermal sensors. Moreover, silicone fingerprints are usually rejected by capacitive sensors but they pose a threat to optical sensors, while the behavior of these two sensors is opposite in the case of gelatin fingerprints [Sepasian et al. 2010]. A risk analysis is reported in Table I.

3. ANTI-SPOOFING METHODS FOR FINGERPRINTS

Liveness detection techniques represent a common countermeasure to address the issue of spoofing and they can be *hardware-based* or *software-based* (see Fig. 11).

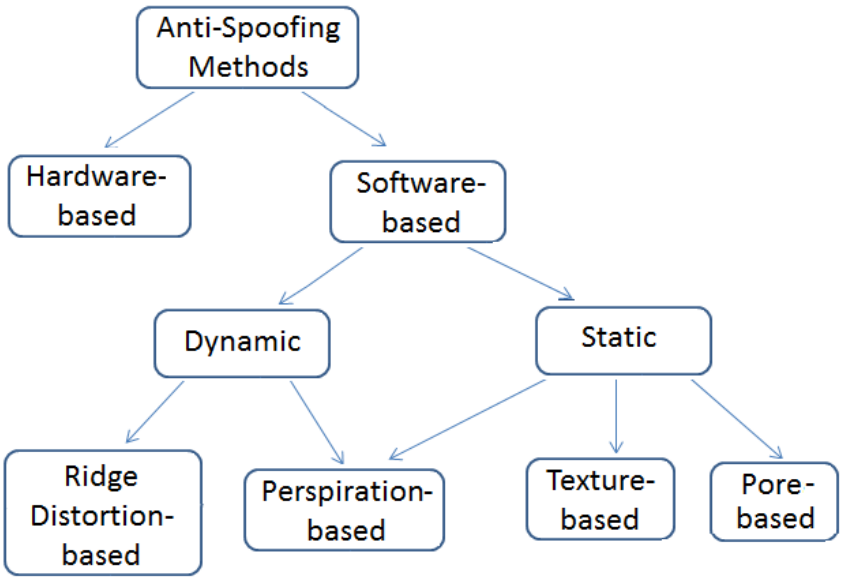


Fig. 11. A taxonomy of the existing anti-spoofing approaches.

Table I. Spoofing methods and materials used for duplicating fingerprints

Method	Reference	Cast material	Mold type	Sensor tested	SFAR
cooperative	[Matsumoto et al. 2002] *et al.*	gelatin	moldable plastic	optical capacitive	68% - 100%
non-cooperative	[Matsumoto et al. 2002] *et al.*	gelatin	PCB	optical capacitive	67%
cooperative	[van der Putte and Keuning 2001]	silicone rubber	plaster	optical capacitive	83%[7]
non-cooperative	[van der Putte and Keuning 2001]	silicone waterproof cement	PCB	optical capacitive	83%
non-cooperative	[Matsumoto 2002] [Endo et al. 2003]	conductive silicon	plastic	optical capacitive	81.82%[8]
non-cooperative non-cooperative non-cooperative	[Thalheim et al. 2002] [Thalheim et al. 2002] [Thalheim et al. 2002]	breathing on the sensor water-filled plastic bag powder adhesive	-	capacitive	-
non-cooperative	[Thalheim et al. 2002]	powder adhesive	-	optical	-
cooperative	[Barral and Tria 2009]	glycerin gelatin	wax silicone	optical capacitive	ease to succeed
cooperative	[Barral and Tria 2009]	glycerin gelatin	wax silicone	thermal swipe	few successes out of 10 trials
cooperative	[Schuckers 2002]	play-doh	dental impression	capacitive DC opto-electric optical capacitive AC	12% 27% 58% 70%
cooperative	[Schuckers 2002]	cadaver		capacitive DC opto-electric optical	90% 41% 85%
cooperative	[Sandstrom 2004]	gelatin	silicone	optical capacitive capacitive-swipe	66%[9] 70% 0%
cooperative	[Espinoza et al. 2011]	silicone thermoplastic	Siligum[10]	optical[11]	distribution of scores[12]
non-cooperative	[Espinoza et al. 2011]	white glue latex	Siligum	optical	distribution of scores[13]
cooperative	[Elliott et al. 2007]	gelatin	silicone	optical	90.7%
cooperative	[Blommé 2003]	gelatin	silicone paste	capacitive optical	55.4% 33.4%

Hardware-based solutions exploit characteristics of vitality such as temperature of the finger, electrical conductivity of the skin, pulse oximetry, skin resistance [Nixon et al. 2004] [Reddy et al. 2008; 2007]. These methods require additional hardware in conjunction with the biometric sensor and this makes the device expensive. To make matters worse, an improper integration of the additional hardware can result in a vulnerable scenario where a spoof artifact is placed on the fingerprint sensor and a live finger is placed on the added hardware [Al-Ajlan 2013; Singh and Singh 2013; Coli et al. 2007b]. In the *challenge/response* liveness detection technique, an electro-tactile pattern is observed as response to electric pulses transmitted into the fingertip during authentication [Sousedik and Busch 2014; Yau et al. 2008; Memon et al. 2012]. In the *odor-based* spoof detection, an acquisition system made of an array of chemical sensors designed to detect characteristic pattern of an odor is employed; experiments showed that when the odor sensors are exposed to skin or gelatin the voltage decreases, while it increases when sensors are exposed to silicon or latex [Baldisserra et al. 2005]. Some research investigated the application of optical coherence tomography (OCT) to detect

Table II. Dynamic software-based anti-spoofing approaches. The performance metrics used are False Live Rejection (FLR), False Spoof Acceptance (FSA), and Equal Error Rate (EER)

Dynamic Algorithm	Category/ Technique	Database	Sensor	Error Rates
[Abhyankar 2004]	Perspiration/ Wavelet	WVU04	Capacitive Optical Electro-optical	FLR=0%; FSA=0% (Th=40.74) FLR=0%; FSA=0% (Th=44.55) FLR=0%; FSA=0% (Th=31.60)
[Antonelli et al. 2006]	Distortion/ Optical Flow	BSL	Optical	EER=11.24%
[Jia and Cai 2007]	Distortion; Perspiration/ Statistics	Tsinghua	Capacitive	EER=4.78%
[Zhang et al. 2007]	Distortion/ Thin-Plate Spline	CAS	Optical	EER=4.5%
[Abhyankar and Schuckers 2010]	Perspiration/ Wavelet	Clarkson10 -#1	Optical	EER=6.7%

Table III. Hybrid (dynamic and static) software-based anti-spoofing approaches for fingerprints. The performance metrics used are False Live Rejection (FLR), False Spoof Acceptance (FSA) and Equal Error Rate (EER)

Hybrid Algorithm	Category/ Technique	Database	Sensor	Error rates
[Derakhshani et al. 2001] [Derakhshani et al. 2003a]	Perspiration/ Statistics; Fourier	WVU01	Capacitive	EER=11.11%[a]
[Parthasaradhi et al. 2004]	Perspiration/ Statistics; Fourier	WVU04	Optical Capacitive	FLR=0%; FSA=0%-18.2%
[Parthasaradhi et al. 2005]	Perspiration/ Statistics; Fourier	WVU05	Capacitive Optical Electro-optical	FLR=6.77%-20%; FSA=5%-20% FLR=0%-26.9%; FSA=4.6%-14.3% FLR=6.9%-38.5%; FSA=0%-19%
[Tan and Schuckers 2005]	Perspiration; Statistics	Clarkson05	Optical Capacitive Electro-optical	FLR=0%; FSA=8.3% FLR=6.7%; FSA=0% FLR=7.7%; FSA=5.3%

[a] Evaluation performed across diverse populations.

artificial materials commonly used for spoofing optical fingerprint scanners [Cheng and Larin 2006; Chang et al. 2008; Bossen et al. 2010; Dubey et al. 2007; Nasiri-Avanaki et al. 2011]. OCT allows to image some of the subsurface characteristics of the skin and extract the internal features of multilayered tissues; this method can penetrate the surface to a maximum depth of 3 mm. Sub-surface information about the finger can also be collected with a multi-spectral imager operating in conjunction with the sensor; properties such as spectral qualities of live skin, chromatic texture of skin and blanching on contact have been exploited [Nixon and Rowe 2005].

In this paper, we focus on the second category of anti-spoofing approaches where the digital image acquired by the sensor is further processed in order to distinguish a live from a spoof [Schuckers et al. 2006]. Software-based solutions may exploit *dynamic* behaviors of live fingertips (e.g., ridge distortion, perspiration) or *static* characteristics (e.g., textural characteristics, ridge frequencies, elastic properties of the skin) [Jin et al. 2007]. A sample of software-based approaches to fingerprint liveness detection is reported in Tables II, III and IV.

3.1. Dynamic Features

Dynamic features are derived by processing multiple frames of the same fingerprint. In general, two successive images captured over a time interval of 2 or 5 seconds are analyzed (see Fig. 12).

Table IV. Static software-based anti-spoofing approaches. The performance metrics used are False Live Rejection (FLR), False Spoof Acceptance (FSA), Equal Error Rate (EER) and Total Error Rate (TER)

Static Algorithm	Category/ Technique	Database	Sensor	Error Rates
[Moon et al. 2005]	Texture/ Wavelet	Hong Kong	Optical[a]	FLR=0%; FSA=0% (Th=25)
[Schuckers and Tan 2006]	Perspiration/ Wavelet	Clarkson06; MSU	Optical Capacitive	FLR=8%-20%; FSA=8%-20% FLR=0%-10%; FSA=0%-10%
[Abhyankar and Schuckers 2006]	Texture/ Statistics	Clarkson06	Optical Capacitive Electro-optical	EER=2.7% EER=3.5% EER=7.7%
[Choi et al. 2007]	Pores; Texture/ Wavelet	Yonsei	Optical	TER=14.89%
[Coli et al. 2007a]	Texture/ Fourier	Cagliari	Optical	FLR=0.4%; FSA=0%
[Jin et al. 2007]	Texture/ Fourier	INHA07	Optical	FLR=23%; FSA=12%
[Nikam and Agarwal 2008b]	Texture/ LBP; Wavelet	MNNIT	Optical	TER=3%-6%
[Nikam and Agarwal 2008a] [Nikam 2009]	Texture/ Curvelet	MNNIT	Optical	TER=1.82%-5.65%
[Nikam and Agarwal 2009a]	Texture/ Co-occurrence	MNNIT	Optical	TER=1.82%-5.65%
[DeCann et al. 2009]	Perspiration/ Statistics	Clarkson09 -#1	Optical	TER=4.5%
[Abhyankar and Schuckers 2009]	Perspiration/ Wavelet	Clarkson09 -#2	Optical	EER=13.85%
[Galbally et al. 2009]	Quality/ Gabor Filters	ATVS	Optical	TER=7%
[Nikam and Agarwal 2009c]	Texture/ Ridgelet	MNNIT	Optical	TER=4.94%-7.53%
[Lee et al. 2009]	Texture/ Fourier	KPU	Optical	TER=11.4%
[Nikam and Agarwal 2009b]	Texture/ Curvelet	MNNIT	Optical	TER=1.78%-5.65%
[Yau et al. 2009]	Color change/ Distance		Optical	FLR=0%; FSA=20%
[Marasco and Sansone 2010]	Texture; Perspiration/ Fourier; Wavelet	LivDet09	Optical	FLR=12.6%; FSA=12.3%
[Tan and Schuckers 2010]	Perspiration/ Fourier; Wavelet	Clarkson10 -#2	Optical	TER=0.9%
[Jin et al. 2011]	Quality Butterworth	INHA11	Optical	TER=6.5%
[Memon et al. 2011]	Pores/ Number of Pores	Lausanne11	Optical	FLR=8.3%; FSA=21.2%
[Galbally et al. 2012]	Quality/ Gabor Filters; Direction Field; Intensity; Fourier	ATVS	Optical	TER=10%
[Marasco and Sansone 2012]	Texture; Perspiration/ Fourier; Wavelet	LivDet09	Optical	FLR=12.6%; FSA=12.3%[b]
[Ghiani et al. 2012a]	Texture/ LPQ	LivDet11	Optical	EER=12.3%
[Gragnaniello et al. 2013]	Texture/ Weber Descriptor	LivDet09; LivDet11	Optical	FLR=0.20%; FSA=0.41% FLR=4.9%; FSA=2.41%
[Ghiani et al. 2013]	Texture/ BSIF	LivDet11	Optical	TER=7.22%

[a] High resolution (1000 dpi)
[b] Results on LivDet09 and LivDet11 are average error rates on the different sensor datasets; the minimum is reported.

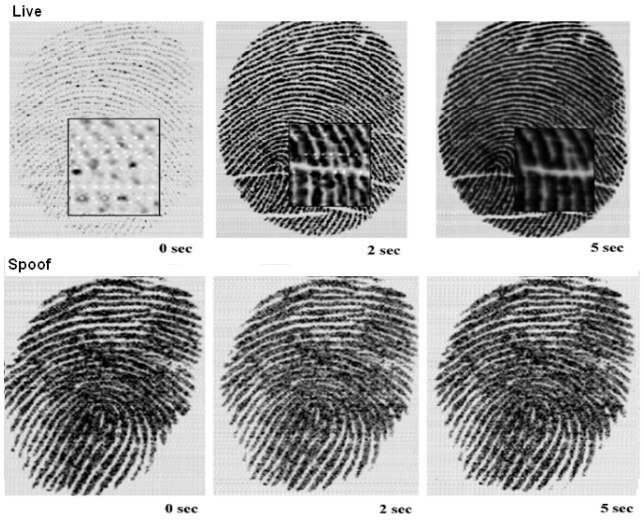


Fig. 12. The image shows multiple frames of both live and spoof fingerprints [Parthasaradhi et al. 2005] ©IEEE.

3.1.1. Perspiration-based. Perspiration is a phenomenon typical of live fingers. The sweat starts from pores and diffuses in time along ridges making regions between pores darker in the image (see Fig. 13). The spatial moisture pattern can be captured by observing multiple fingerprint images acquired over a short span of time.

Fig. 13. The image shows a macro photography of a live fingerprint [http://www.flickr.com/photos/72100379@N05/6544784445], with permission of B. Hoffman.

Several methods based on perspiration changes have been proposed [Schuckers et al. 2004]. Live fingerprints exhibit non-uniformity of gray level along ridges due to perspiration which propagates along sweat pores; this is accentuated when viewed over time. Spoof fingerprints show high uniformity even over time. Since perspiration is a physiological phenomenon, it is variable across subjects. Additionally, it presents a certain sensitivity to the environment, the pressure of the finger, the time interval and the initial moisture content of the skin [Derakhshani et al. 2003b]. Its effectiveness requires an efficient extraction of the evolving pattern from images. Dynamically, perspiration can be quantified by temporal changes in the ridge signal. The change in gray-level between the first and last images in a sequence can be measured by considering the local maxima and minima of the ridge signal. The swing in live fingerprints is generally higher than that in spoof artifact and it is smaller in the last image compared to the first since moisture creates peaks in the fingerprint ridge signal. The temporal pattern of moisture is measured by computing features such as the percentage change in the

standard deviations of the first and last fingerprint signals, the total fluctuation ratio (see Eqn. (1)) and the min/max growth (see Eqn. (2)) [Derakhshani et al. 2003a]. Moreover, the simple mean of the signal difference (last - first) has been efficiently exploited since its value is less for a finger with no life.

$$\Delta = \frac{\sum_{i=1}^{m} C_{1i} - C_{1i-1}}{\sum_{i=1}^{m} C_{2i} - C_{2i-1}} \tag{1}$$

where m refers to the length of the ridge signal and C_{1i} and C_{2i} to the i^{th} pixel gray-level value in the first and second capture, respectively.

$$\Delta = \frac{\sum_{i=1}^{m} (C_{2i}^{min} - C_{1i}^{min})}{\sum_{i=1}^{m} (C_{2i}^{max} - C_{1i}^{max})} \tag{2}$$

where C_{1i}^{min}, C_{2i}^{min}, C_{1i}^{max} and C_{2i}^{max} are the minima and maxima of the first and last images, respectively. Parthasaradhi et al. [Parthasaradhi et al. 2005] introduced two additional dynamic features, viz., the dry and wet saturation percentage changes which measure how fast the dry saturation disappears and how fast the moist saturation appears, respectively. These measures account for the time taken for the propagation of moisture from pores. They speculated that the use of these measures will lead to a more robust technique across diverse populations.

Abhyankar and Schuckers proposed an interesting method where the changing perspiration pattern is isolated through a wavelet analysis of the entire fingerprint image [Abhyankar and Schuckers 2009]. Firstly, both images acquired by the biometric scanner (2 seconds apart) are enhanced by using median filtering and histogram equalization. Then, wavelet analysis is performed by computing wavelet packets to focus on high frequency components that capture the circular transitions from dark to white around pores, and multi-resolution analysis (MRA) to focus on low frequency components that capture the periodicity of pore locations. For each sub-band, changing wavelet coefficients from the first to the second image are considered and the vitality measure is computed based on the total energy associated with them. Coefficients that do not change by more than 40% are not considered.

3.1.2. Ridge Distortion-based. A study of skin distortion was performed by Antonelli *et al.* in [Antonelli et al. 2006]. When pressing and moving a real finger on a scanner surface, the distortion produced is much more significant than that produced by a spoof. Skin distortion is analyzed by processing a sequence of frames acquired at a high frame rate while the user rotates his finger on the sensor surface whilst applying some pressure. The finger is assumed to be non-distorted at the beginning of the sequence. Movements of single blocks are detected and modeled using optical flow. The resulting Distortion Code sequences are compared [Cappelli et al. 2001].

Jia *et al.* analyzed the human skin elasticity by using a sequence of fingerprint images to capture the finger deformation process [Jia and Cai 2007]. Live fingerprints are discriminated from spoofs based on the observation that, for live fingers, an increase of pressure causes an increase of both fingerprint area (see Eqn. (3)) and signal intensity (see Eqn. (4)). A positive value of the correlation coefficient of these features has been shown be a good indicator of fingerprint liveness.

$$S_i = N_i \times W \times W \tag{3}$$

where S_i is the fingerprint area of the i^{th} frame and N_i is the number of blocks whose variance is greater than a certain threshold. The variance is computed for each block of size $W \times W (= 16 \times 16)$.

$$Int_i = \frac{\sum_{I(x,y)\geq\epsilon} I(x,y)}{S_i} \tag{4}$$

where Int_i is the intensity signal of the i^{th} frame, $I(x,y)$ is the intensity of the fingerprint area S_i, and ϵ is the threshold used to separate pixels corresponding to the fingerprint from those in the background.

Zhang *et al.* modeled the distortion of live and spoof fingerprints using a Thin-plate Spline (TPS) [Zhang et al. 2007]. The elasticity of the human skin impacts how live fingers distort. Spoof materials are typically much more rigid compared to the human skin. Subsequently, under the same distortion condition caused by the same directional pressure, their deformation is lower. The global distortion is represented by the minutiae displacement, and parameters of the TPS model are computed using a series of paired minutiae obtained before and after distortion. The discrimination is made based on the bending energy vector of the TPS model. The performance of this approach relies on the precision of minutiae extraction and pairing.

3.2. Static Features

Static features can be extracted from a single fingerprint impression and, compared to other approaches based on a single impression, are cheaper and faster. Static features may concern textural characteristics, skin elasticity, perspiration-based features or a combination of these.

3.2.1. Texture-based. Spoof and live fingerprint images exhibit different textural properties such as morphology, smoothness and orientation. Thus, texture can be exploited for spoof detection.

Texture coarseness. Residual noise of the fingerprint image indicates the difference between an original and de-noised image, in which the noise components are due to the coarseness of the fake finger surface [Abhyankar and Schuckers 2006]. Materials used to make fake fingers such as silicon or gelatin consist of organic molecules which tend to agglomerate and, thus, the surface of a live finger is generally smoother than an artificial one [Moon et al. 2005]. The standard deviation of the residual noise is a good indicator of texture coarseness since the pixel value fluctuation in the noise residue of a coarser surface texture is generally stronger. The surface coarseness is treated as a kind of Gaussian white noise added to the image. The amount of residual noise is computed by using a wavelet-based filter which allows for analyzing the image at different scales. This helps reduce the coarseness inherent in the ridge/valley pattern that does not represent the information of interest. In particular, the image is de-noised with a Symlet by applying a soft-threshold for wavelet shrinkage. Spoof detection methods based on texture coarseness work well on high resolution (1000 dpi) fingerprint images; but common commercial sensors present a resolution of about 500 dpi [Coli et al. 2007b].

First order statistics. The likelihood of observing a certain gray value at a randomly-chosen location in the image can be computed from the histogram of pixel intensities related to the image. Let $H(n)$ indicate the normalized histogram value and let N be the number of bins. The set of first order statistical properties is defined by the following equations [Abhyankar and Schuckers 2006]:

— Mean:

$$\mu = \frac{1}{N}\sum_{n=0}^{N-1} H(n) \tag{5}$$

— Energy:

$$e = \sum_{n=0}^{N-1} H(n)^2 \tag{6}$$

— Entropy:

$$s = -\sum_{n=0}^{N-1} H(n) log H(n) \tag{7}$$

— Median:

$$M = \arg\min_{a} \sum_{n} H(n)|n-a| \tag{8}$$

— Variance:

$$\sigma^2 = \sum_{n=0}^{N} (n-\mu)^2 H(n) \tag{9}$$

— Skewness:

$$\gamma_1 = \frac{1}{\sigma^3} \sum_{n=0}^{N-1} (n-\mu)^3 H(n) \tag{10}$$

— Kurtosis:

$$\gamma_2 = \frac{1}{\sigma^4} \sum_{n=0}^{N-1} (n-\mu)^4 H(n) \tag{11}$$

— Coefficient of variation:

$$cv = \frac{\sigma}{\mu} \tag{12}$$

Second Order Statistics. The joint gray level function between pairs of pixels in a single fingerprint image is a texture-based approach used by Nikam *et al.* [Nikam and Agarwal 2009b]. Due to the presence of sweat pores and the perspiration phenomenon, authentic fingerprints exhibit non-uniformity of gray levels along ridges, while due to the surface characteristics of the fabrication material used, such as gelatin or silicon, spoof fingers show high uniformity of gray levels along ridges. The gray level distribution of the pixels is modeled using first order statistics, while the joint gray level function between pair of pixels is modeled using second order statistics. The authors proposed the use Gabor filter-based features, since fingerprints exhibit oriented texture-like pattern and Gabor filters can optimally capture both local frequency and orientation information.

Local-Ridge Frequency Analysis. A promising approach based on multi-resolution texture analysis and the inter-ridge frequency analysis was proposed by Abhyankar and Schuckers [Abhyankar and Schuckers 2006]. They used different texture features to quantify how the gray level distribution in a fingerprint image changes when the physical structure changes. Two secondary features were used, Cluster Shade and Cluster Prominence, based on the co-occurrence matrix. These features derived from a multi-resolution texture analysis were combined with features derived from a ridge-frequency analysis, and a Fuzzy-C-means classifier was used to distinguish between live prints and spoofs. This method does not depend on the perspiration phenomenon and is able to overcome dependence on more than one fingerprint image. However, it

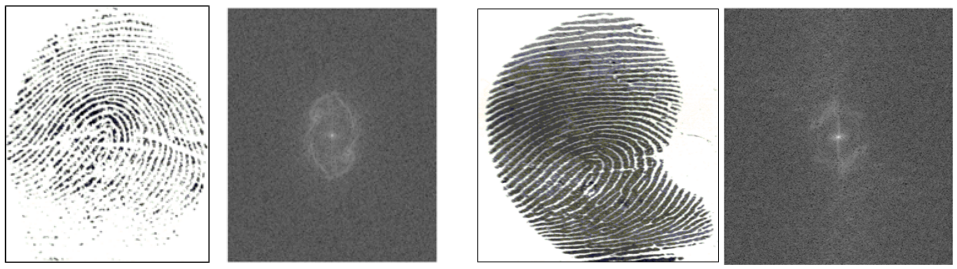
presents limitations in realistic scenarios, since the computation of the local-ridge frequencies may be affected by cold weather and different skin conditions, including dirt and moisture.

Local Phase Quantization (LPQ) Analysis. Earlier works focused on simply analyzing the spectrum of a fingerprint image. Given that the fingerprint can present different orientations, a rotation invariant Local Phase Quantization (LPQ) technique can point out the differences in the spectrum between live fingerprints and spoof artifacts. A novel set of features for detecting liveness based on the LPQ of the fingerprint image were defined by Ghiani *et al.* [Ghiani et al. 2012b] [Ojansivu et al. 2008] [Ojansivu and Heikkilä 2008] [Martins et al. 2012]. The approach measures the difference between live and spoof fingerprints in terms of high frequency information loss. One important property of the LPQ is its robustness to the blurring effect. Thus, such a technique is believed to be particularly effective when dealing with images acquired from artificial fingerprints.

Power Spectrum Analysis. The fabrication process alters frequency details between ridges and valleys. For spoofs, most of the energy in the Fourier domain is present in the center of the image which corresponds to low frequency data in the image domain [Coli et al. 2007a]. Fig. 14 illustrates the power spectrum of both live and spoof (gelatin) fingerprint images. A fingerprint image produces a ring pattern around the center in the power Fourier spectrum due to the ridge-valley texture [Jin et al. 2007]. In live fingerprints, micro-characteristics such as those due to ridge line discontinuity or transverse cuts on ridge lines increase their thickness. Thus, in the Fourier domain live fingerprint images typically exhibit more high frequency characteristics than spoofs. The strength of the power spectrum amplitude reflects the strength of the ridge-valley texture. The amount of residual spectrum on the high frequencies is computed as indicated in Eqn. (13).

$$e = \int \int_S |F(u,v)|^2 dudv \tag{13}$$

where F(u,v) is the Fourier Transform of the input fingerprint image and S the integration region which is given in terms of a circular region centered around the zero frequency. Spoof and live images are then separated using statistics computed on the values of the radius of the region [Marcialis et al. 2012a].



(a) (b)

Fig. 14. (a) Live fingerprint image and corresponding power spectrum; (b) spoof (gelatin) fingerprint image and corresponding power spectrum. Both images are taken from the CrossMatch database of LivDet09 [Marcialis et al. 2009], with permission of G. Marcialis.

Local Binary Pattern (LBP). LBP characterizes the spatial variation of local image texture and has been used for spoof detection. The texture is defined as the joint dis-

tribution of gray values in a circularly symmetric neighbor set of P image pixels on a circle of radius R (see Eqn. (14)).

$$T = t(g_c, g_0, ..., g_{P-1}) \tag{14}$$

where g_c is the gray value of the center pixel of the local neighborhood and $g_0, ..., g_{P-1}$ are the gray values of P equally spaced pixels on the considered circular symmetric neighbor set. First, the gray value of the center pixel of the circularly symmetric neighbor set is subtracted from the gray values of the circularly symmetric neighborhood [Nikam and Agarwal 2008b] [Martins et al. 2012]. Then, features are extracted from the histograms of LBP images computed as indicated in Eqn. (15) [Ojala et al. 2002; Mäenpää 2003].

$$LBP = \sum_{p=0,...,P-1} s(g_p - gc)2^p \tag{15}$$

where $s(x) = 1$ if $x \geq 0$, else $s(x) = 0$.

Weber Local Descriptor (WLD). This descriptor consists of two components: the differential excitation and the orientation [Chen et al. 2010; Chen et al. 2008]. It is based on the Weber's law and it states that the human perception of a pattern does not depend only on the change of a stimulus such as lighting, but also on the original intensity of the stimulus. The just-noticeable-difference, δI, between two stimuli is proportional to the initial stimulus intensity, I. Changes of a pixel are expressed as differences between its neighbors and the pixel. The differential excitation $\epsilon(x)$ of a current pixel x is computed as indicated in Eqn. (16), where x is the target pixel in a 3×3 patch. The orientation corresponds to the gradient orientation.

$$\epsilon(x) = \arctan \sum_{i=0}^{7} \frac{x_i - x}{x} \tag{16}$$

Combining WLD with LPQ resulted in a better spoof detection performance compared to using only WLD [Gragnaniello et al. 2013].

Binarized Statistical Image Features (BSIF). Local image patches are linearly projected into a subspace whose basis vectors are obtained from images by using Independent Component Analysis (ICA); coordinates of each pixel are thresholded and a binary code is computed. Such a value represents the local descriptor of the image intensity pattern in the neighborhood of the considered pixel [Kannala and Rahtu 2012]. Let X be an image patch of $l \times l$ pixels and W_i a linear filter of the same size. The filter response is obtained as:

$$s_i = \sum_{u,v} W_i(u, v)X(u, v) \tag{17}$$

The binarized feature b_i is obtained by setting $b_i = 1$ if $s_i > 0$, and 0 otherwise. The set of filters is learned from a training set of natural image patches via ICA by maximizing the statistical independence of the filter responses [Hyvärinen et al. 2009]. The fingerprint representation is, therefore, obtained by learning, instead of manually tuning, based on statistical properties of the input signal; this procedure provides flexibility to the designed descriptor [Ghiani et al. 2013].

3.2.2. Perspiration-based. Individual Pore Spacing. The presence of active perspiration around pores can be captured by studying the regular periodicity of pores on the ridges. The occurrence of pores causes a certain gray-level variability in the fingerprint image.

The gray-level variations correspond to variations in moisture due to the pores and the presence of perspiration. Such a variability in gray level can be analyzed in the Fourier domain after mapping the two-dimensional fingerprint image into a one-dimensional signal representing the gray level values along the ridge and referred to as *ridge signal* [Derakhshani et al. 2003b]. Spatial frequencies of pores can be analyzed through Fourier Transform [Derakhshani et al. 2003a]. First, the image is processed to remove noise and it is converted into a binary image. Then, a thinning routine is applied to determine the fingerprint ridge paths. Finally, the FFT of the main ridge is computed. The swing of the signal decreases in time as the moisture spreads; the general oscillation is higher for live fingerprint signals where the maxima are almost constant but the minima increase, due to the spread of moisture in time. Fourier coefficients of interest are from 11 to 33, since these values correspond to spatial frequencies (0.4 - 1.2 mm) of pores. The formula for this static measure, *SM*, is defined as follows:

$$SM = \sum_{k=11}^{33} f(k)^2 \tag{18}$$

where $f(k)$ is expressed by the following:

$$f(k) = \frac{\sum_{i=1}^{n} |\sum_{p=1}^{256} S_{0i}^{a}(p) e^{-j2\pi(k-1)(p-1)/256}|}{n} \tag{19}$$

$$S_{0i}^{a} = S_{0i} - mean(S_{0i}) \tag{20}$$

where n is the total number of individual ridges and S_{0i} is the i^{th} ridge.

Intensity-based features. In [Tan and Schuckers 2005], an intensity-based approach was proposed. The number of pixels at each gray level is analyzed using image histograms. The following features are then used: *i) Gray Level 1 Ratio*, corresponding to the ratio between the number of pixels having a gray level belonging to the range (150, 253) and the number of pixels having a gray level belonging to the range (1, 149); *ii) Gray Level 2 Ratio*, corresponding to the ratio between the number of pixels having a gray level belonging to the range (246, 256) and the number of pixels having a gray level belonging to the range (1, 245). Moreover, the uniformity of gray levels along ridge lines and the valley/ridge contrast have been observed to have high discriminative power. In particular, as shown in Fig. 15, real fingerprints exhibit non-uniformity of gray levels and high ridge/valley contrast values. It has also been observed that the general variation in gray-level values of spoof fingerprints is less than those in live images (although this can change based on the fabrication material used). This information can be captured by computing the gray-level matrix gradient of the image.

3.2.3. Quality-based. In anti-spoofing algorithms, fingerprint quality measures such as strength, continuity and clarity of ridges have been considered. The ridge strength can be computed in two ways: *i)* using the energy concentration along the dominant direction of the ridges which can be obtained as a ratio between the two eigenvalues of the covariance matrix and the gradient vector, and *ii)* using the energy concentration in the power spectrum since in high quality images energy is concentrated in a few bands while in low quality images the energy is spread across bands. Ridge continuity is captured by measuring the continuity of the orientation field; high quality images typically have a smooth flow of ridges in a local constant direction [Galbally et al. 2012]. The ridge clarity is obtained by measuring the mean and the standard deviation of the foreground image. Furthermore, a local clarity score is computed based on the overlap area between the gray level distributions of ridges and valley which has to be very small for high clarity ridges/valleys. Quality measures that have been effectively

Fig. 15. Grey-level uniformity analysis in real and spoof fingerprint images. Images taken from the LivDet 2009 database, with permission of G. Marcialis.

used for spoof detection are spectral band energy, middle ridge line and middle valley line [Jin et al. 2011]. Due to the difficulty of copying pores along the ridges during the spoof creation process, the middle ridge line signals of spoof have fewer periodic peaks compared to live fingerprints. Additionally, due to low elasticity and valley depths, the gray-scale values of spoofs are generally lower compared to live fingerprints.

3.2.4. Pore-based. Manivanan *et al.* proposed a method to detect pores by applying two filtering techniques: high-pass filters and correlation filters [Manivanan et al. 2010a; 2010b]. A high-pass filter was used to extract active sweat pores, and a correlation filter was used for locating the position of pores: see Fig. 16. Marcialis *et al.* analyzed pore distribution and number of pores in three regions around the fingerprint core [Marcialis et al. 2010] [Tidu 2010]. Memon *et al.* extended Manivanan's study by attempting to determine the optimum threshold value to detect the correlation peaks corresponding to active pores [Memon et al. 2011; Memon 2012]. Espinoza *et al.* proposed a spoof detection method based on comparing pore quantity between spoof and live fingerprint images [Espinoza and Champod 2011b].

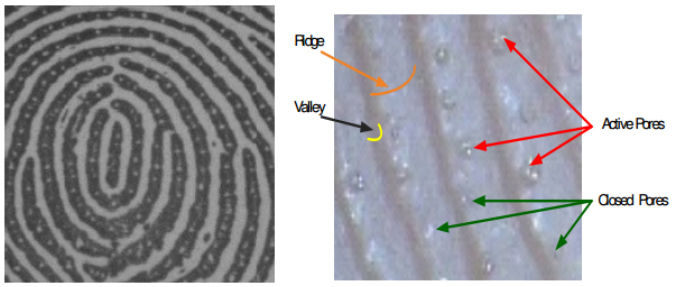


Fig. 16. A 150x150 segment of a high resolution (1000 dpi) fingerprint image showing ridges, valleys, active and closed pores. Image taken from [Memon 2012] ©Memon, with permission of Dr. S. Memon.

4. DATABASES

Development and evaluation of robust liveness detection (or spoof detection) algorithms require the assembling of databases of sufficient size (many subjects, different samples per subject, etc.) corresponding to different fabrication materials and fingerprint sensing technologies. In this section, we review several databases that have been

used in the literature. In particular, we describe the publicly available dataset provided by the Fingerprint Liveness Detection Competition[14]: LivDet 2009 [Marcialis et al. 2009], LivDet 2011 [Yambay et al. 2012], LivDet 2013 [Ghiani et al. 2013]; and, a dataset assembled at the Biometric Recognition Group ATVS[15] [Galbally et al. 2011]. Details are provided in Table V and examples of images are shown in Figs. 17, 18 and 19.

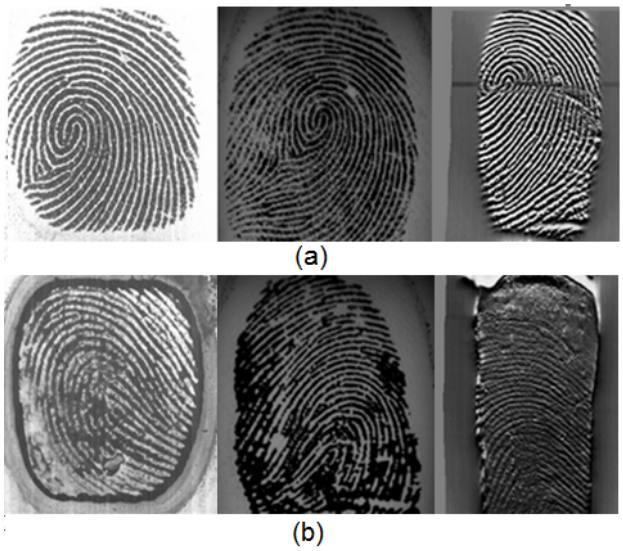


Fig. 17. Examples of live (a) and silicone spoof (b) fingerprint images from the dataset assembled by ATVS, reprinted from ATVS database with permission [Galbally et al. 2012].

According to the protocol established for the competitions, liveness detection algorithms are first trained on a dataset consisting of live and spoof samples where the spoof fingerprints are realized with different fabrication materials using both cooperative and non-cooperative methods. The testing is carried out on a different dataset having the same number of samples as the training set [Ghiani et al. 2013]. In Table VI, we report the lowest total error rates achieved by the algorithms submitted to the fingerprint liveness detection competitions for each available database.

4.0.5. Assessment and Performance Metrics. Metrics for assessing liveness detection performance are different than those used for assessing matching performance [Adler and Schuckers 2009; Shin et al. 2009; Schuckers et al. 2002]. In the Liveness Detection Competitions [Marcialis et al. 2009; Yambay et al. 2012; Ghiani et al. 2013], performance was computed as follows:

$$e = \frac{Ferrlive + Ferrfake}{2} \tag{21}$$

where *Ferrlive* is the rate of misclassified live fingerprints and *Ferrfake* the rate of misclassified fake fingerprints. In some literature, the terms False Live Rejection Rate (FLRR) and False Spoof Acceptance Rate (FSAR) have been used as well: FLRR denotes the percentage of live fingerprint samples that are misclassified as spoofs while

[14]http://prag.diee.unica.it/
[15]http://atvs.iiuam.es/

Table V. Public datasets that are available for evaluating fingerprint liveness detection (or spoof detection) algorithms

Dataset	Sensor	Technology	Model	Resolution	Live	Spoof	Subjects
WVU01	Veridicom	Capacitive	SFPS 100	500 dpi	36	36[a]	33
WVU04	Precise	Capacitive	SC 100	500 dpi	30	30	33
	Ethentica	Electro-optical	USB2500	500 dpi	30	30	total
	Secugen	Optical	FDU01	500 dpi	30	30	
WVU05	Precise	Capacitive	SC 100	500 dpi	31	30	33
	Ethentica	Electro-optical	USB2500	500 dpi	30	30	total
	Secugen	Optical	HFDU01A	500 dpi	31	30	
Hong Kong	Fuji	Optical	S2 (DSLR)	1000 dpi	100	100	23
MSU	Identix	Optical	DFR 200	380 dpi	330	330	33
Clarkson05	Precise	Capacitive	SC 100	500 dpi	30	30[b]	33
	Ethentica	Electro-optical	USB2500	500 dpi	30	30	total
	Secugen	Optical	HFDU01A	500 dpi	31	30	
Clarkson06	Precise	Capacitive	SC 100	500 dpi	58	80	33
	Ethentica	Electro-optical	USB2500	500 dpi	55	80	total
	Secugen	Optical	HFDU01A	500 dpi	58	80	
BSL[c]	Biometrika	Optical	Fx2000	569 dpi	900	400	45
Tsinghua	Veridicom	Capacitive	Fps200	500 dpi	300	470	15
Yonsei	NITGEN	Optical	-	500 dpi	1100	1100	110
INHA07	-	Optical	-	500 dpi	1350	4050	30
Cagliari	Biometrika	Optical	Fx2000	500 dpi	720	720	36
CAS	CrossMatch	Optical	V300	500 dpi	120	120	20
MNNIT	Secugen	Optical	HFDU01	500 dpi	185	240	-
Clarkson09 -#1	Identix	Optical	DFR2100	500 dpi	1526	1588	150
Clarkson09 -#2	Precise	Capacitive	PS 100	500 dpi	58	93	33
	Ethentica	Electro-optical	USB2500	500 dpi	55	82	total
	Secugen	Optical	FDU01	500 dpi	58	90	
KPU		Optical			750	3000	15
Clarkson10 -#1	Precise	Capacitive	PS 100	500 dpi	58	50	33
	Ethentica	Electro-optical	USB2500	500 dpi	55	50	total
	Secugen	Optical	FDU01	500 dpi	58	52	
Clarkson10 -#2	Identix	Optical	DFR2100	686 dpi	644	570	81
ATVS	Biometrika	Optical	Fx2000	569 dpi	272	272	17
	Precise	Capacitive	SC 100	500 dpi	272	272	17
	Yubee	Sweeping	Fingerchip	500 dpi	272	272	17
LivDet09	CrossMatch	Optical	300CL	500 dpi	2000	2000	254
	Biometrika	Optical	Fx2000	569 dpi	2000	2000	50
	Identix	Optical	DFR2100	686 dpi	1500	1500	160
LivDet11	Biometrika	Optical	Fx2000	500 dpi	2000	2000	50
	Sagem	Optical	MSO300	500 dpi	2000	2000	56
	Digital Persona	Optical	400B	500 dpi	2000	2000	100
	Italdata	Optical	ET10	500 dpi	2000	2000	50
INHA11	-	Optical	-	500 dpi	690	1380	46
Lausanne	CrossMatch	Optical	LScan 1000T	1000 dpi		156	13
LivDet13	Biometrika	Optical	Fx2000	569 dpi	2000	2000	75
	CrossMatch	Optical	LScan Guardian	500 dpi	2500	2500	235
	Swipe	-	-	96 dpi	2500	2500	250
	Italdata	Optical	ET10	500 dpi	2000	2000	75

[a]Additionally, WVU01 is made up of 36 cadaver fingers; WVU04 and WVU05 of 8, 12 and 14 cadaver fingers, respectively, for the three sensors used for capture.
[b]Additionally, Clarkson05 is made up of 14 cadaver fingers; Clarkson06 and Clarkson10 of 33, 22 and 25 and 33, 22 and 28 cadaver fingers, respectively, for the three sensors used for capture.
[c]Biometric System Laboratory, University of Bologna

Fig. 18. Examples of live (a) and spoof (b) fingerprint images from the dataset assembled by the organizers of the LivDet competition. Spoof are realized using latex, gelatin and ecoflex, respectively. With permission of G. Marcialis.

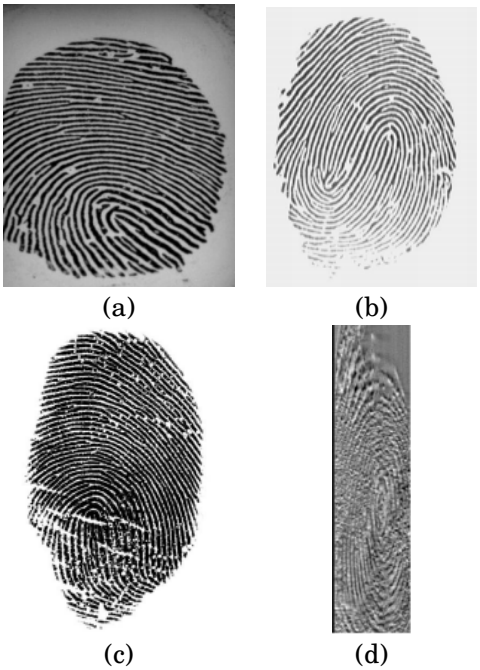


Fig. 19. Fingerprint images taken from the LivDet13 dataset: (a) and (b) spoof samples realized using a non-cooperative method; (c) and (d) spoof samples realized using a cooperative method.

FSAR denotes the percentage of spoof samples that are misclassified as live. Since the spoof detection problem is typical posed as a two-class pattern recognition problem, it

Table VI. Lowest total error rates achieved by the algorithms submitted to three LivDet competitions

LivDet 2009				
Error Rates	**Identix**	**CrossMatch**	**Biometrika**	-
FerrLive	2.7%	7.4%	15.6%	
FerrFake	2.8%	11.4%	1.9%	
LivDet 2011				
Error Rates	**Biometrika**	**ItalData**	**Sagem**	**Identix**
FerrLive	29.2%	28.5%	13.1%	11.6%
FerrFake	10.9%	15.1%	13.8%	6.2
LivDet 2013				
Error Rates	**Biometrika**	**ItalData**	**CrossMatch**	**Swipe**
FerrLive	0.1%	0.2%	0%	3.2%
FerrFake	1.1%	0%	31.3%	11.5%

is possible to generate a Receiver Operating Characteristic (ROC) curve based on the trade-off between the Type I and Type II errors.

Recently, a dedicated set of performance metrics quantifying the ability of a biometric system to correctly detect spoof attacks were discussed by NIST [Johnson et al. 2012; NIST 2012]. Current criteria used for assessing performance of biometric systems do not include well-defined metrics for evaluating anti-spoofing methods [Simoens et al. 2012]. Therefore, technical efforts for the definition of evaluation criteria, metrics and testing methodologies are needed. They should be also contextualized in a standardized reference architecture. The stability of the performance and the degree to which the performance curve varies with respect to influential factors or the range of the algorithm parameters, need to be analyzed as well.

4.0.6. Scientific Reproducibility and Certification. Numerical reproducibility of published results and a standard framework for comparing different anti-spoofing methods are necessary to promote scientific rigor in this field. The current academic and industrial research in anti-spoofing places emphasis on publications and project results, and little on development of community-established standards and replication of experiments and studies (although this is now slowly changing due to the efforts of the TABULA RASA project and BVAEG). Additionally, product certification is required in sensitive applications where a failure could have serious consequences such as a border control system or access to a nuclear facility. Protection Profile (PP) by the Federal Office for Information Security (BSI) in Germany defines a set of requirements for computer and communication security [BSI 2010; Roberts 2007]. It includes the evaluation of Fingerprint Spoof Detection Protection Profile. In particular, an assessment referred to as Vulnerability Assessment was designed to determine whether potential vulnerabilities that have been identified will allow unauthorized access to data and functionality that interfere with authorized capabilities of other users. In July 2013, Morpho (Safran) announced that it was the first company to achieve Common Criteria certification by the BSI for fingerprint spoof detection in a biometric device - the MorphoSmart Optic 301 fingerprint reader.

5. INCORPORATING ANTI-SPOOFING MEASURES INTO A FINGERPRINT MATCHER

Very often it is necessary to integrate an anti-spoofing scheme with the fingerprint matcher in a very explicit manner. In this regard, it may be necessary to fuse the liveness values output by the liveness detector with the match scores output by the matcher. [Marasco et al. 2012] proposed four different architectures to perform this fusion. In three of these methods - two sequential and one based on a conventional classifier - no assumptions were made about the interaction between liveness values and match scores. In the fourth method, a Bayesian Belief Network (BBN) is employed

to explicitly model the influence of liveness values on match scores. Beyond determining whether the two samples being compared belong to the same identity, the overall system determines if the gallery and probe images are both live.

In their work, they view the fingerprint matcher and the liveness detector as "classifiers". The inputs to the matcher are two fingerprint samples (e.g., gallery and probe images). The output is a match score that indicates the similarity between the two samples. A threshold is applied to this match score in order to determine if the samples correspond to the same identity ("Genuine (G)") or different identities ("Impostor (I)"). Thus, the verification stage has two output classes: G and I. The input to the liveness detector is a fingerprint sample (e.g., gallery or probe image). The output is a liveness value indicating the degree of liveness of the sample. A threshold is applied to this liveness value in order to determine if the sample is "Live (L)" or "Spoof (S)". Since there are two fingerprint samples, the liveness detector has four output classes: LL, LS, SL, SS (see Table A).

Table A: Notations used when combining match scores with liveness values.
Inputs:
Let m be the match score between the gallery and probe samples as computed by the matcher.
Let l_g be the liveness measure value assigned by the liveness detector to the gallery sample.
Let l_p be the liveness measure value assigned by the liveness detector to the probe sample.
Events:
Let $I = 0\ (1)$ denote a genuine (impostor) user.
Let $S_g = 0\ (1)$ denote the presence of a live (spoof) biometric presentation at enrollment time.
Let $S_p = 0\ (1)$ denote the presence of a live (spoof) biometric presentation at verification time.
Output classes:
Live-Live-Genuine (LLG): the gallery image and the probe are both live and they have the same identity.
Live-Spoof-Genuine (LSG): the gallery image is live, the probe is spoofed but they correspond to the same identity.
Spoof-Live-Genuine (SLG): the gallery image is spoofed, the probe is live but they correspond to the same identity.
Spoof-Spoof-Genuine (SSG): the gallery image and the probe are both spoofed and they are of the same identity.
Live-Live-Impostor (LLI): the gallery image and the probe are both live but they correspond to different identities.
Live-Spoof-Impostor (LSI): the gallery image is live, the probe is spoofed and they correspond to different identities.
Spoof-Live-Impostor (SLI): the gallery image is spoofed, the probe is live and they correspond to different identities.
Spoof-Spoof-Impostor (SSI): the gallery image and the probe are both spoofed and they correspond to different identities.

— In **Method 1**, the matcher is invoked before the liveness detector as seen in Fig. 20. The matcher in the first stage is used to distinguish genuine from impostor based only on match scores. In the liveness detection stage there are two pairs of classifiers: one pair that is invoked if the input samples are deemed to belong to the Genuine (G) class and another that is invoked if they are deemed to belong to the Impostor (I) class. This arrangement may be redundant (i.e., the use of four different liveness detectors may not be necessary).
— In **Method 2**, the liveness detector is invoked before the matcher as seen in Fig. 21. Depending upon the output of the two liveness classifiers in the first stage (LL, LS, SL or SS), one of four matchers in the verification stage is invoked. For example, the

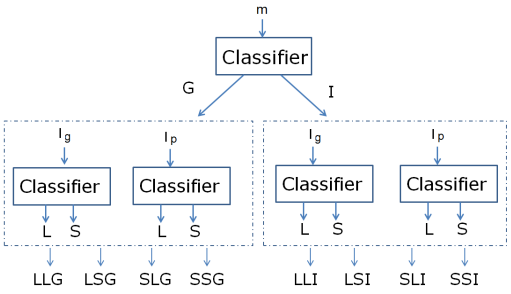


Fig. 20. Architecture of Method 1. Here, the matcher is invoked before the liveness detector. The classifier in the first stage (classifier 1) is used to distinguish genuine from impostor based only on match scores. In the spoof detection stage there are two pairs of classifiers: one pair (classifier 2 and 3) that is invoked if the input samples are deemed by the matcher to belong to the Genuine (G) class and another pair (classifier 4 and 5) that is invoked if they are deemed to belong to the Impostor (I) class. This arrangement may be redundant (i.e., the use of four different liveness classifiers may not be necessary). See Table A for notations.

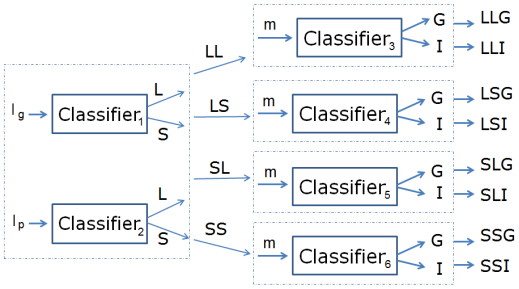


Fig. 21. Architecture of Method 2. Here, the liveness detector is invoked before the matcher. Depending upon the output of classifier 1 and 2 (LL, LS, SL or SS), one of four classifiers in the verification stage is invoked. For example, classifier 3 operates only on input scores between gallery and probe samples that are both classified as Live, while classifier 6 operates only on scores between gallery and probe samples that are both classified as Spoof. See Table A for notations.

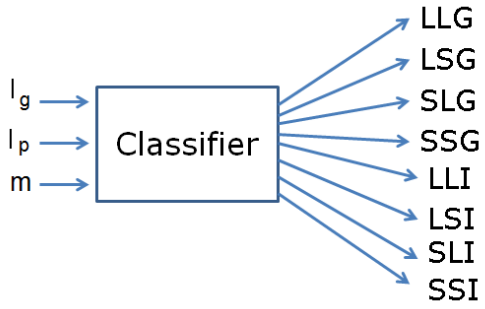


Fig. 22. Architecture of Method 3. Here, the classifier has three inputs: match score, liveness value of gallery sample and liveness value of probe sample. All 3 inputs are used simultaneously in order to determine the output class. See Table A for notation.

first matcher (Classifier 3) operates only on gallery and probe samples that are both classified as Live, while the fourth matcher (Classifier 6) operates only on gallery and probe samples that are both classified as Spoof.

— In **Method 3** (see Fig. 22), the match score and the liveness values are provided as inputs to a single classifier. This classifier has one of eight possible outputs: LLG, LSG, SLG, SSG, LLI, LSI, SLI, SSI. This is an example of a multi label problem. For each class label, the first two letters denote the liveness state of the samples, while the third letter denotes whether the samples correspond to the Genuine or Impostor class (see Table A). In this method, no explicit assumption is made regarding a possible relationship between liveness values and match scores.

— The three methods described above do not explicitly model the relationship between liveness values and match scores. A powerful framework for modeling causal relationships among a set of variables X is offered by graphical models such as Bayesian Belief Networks. A graph is able to capture the way in which the joint distribution over all of the random variables can be decomposed into a product of factors each depending only on a subset of the involved variables. Fig. 23 shows a BBN-based representation, referred to as **Method 4**. The variable I denotes the event related to the presence or absence of a genuine user. It assumes value equal to '0' when the samples belong to the Genuine class and '1' when the samples belong to the Impostor class. The variable m denotes the match score between the two samples (e.g., gallery and probe) whose value is affected by the state of the variable I. For example, a match score between two samples of different individuals (I=1) is likely to be lower than that of samples coming from the same individual (I=0). The variables S_g and S_p represent the events related to the presence of a spoof biometric presentation at enrollment and verification times, respectively. Each assumes the value '1' when the presentation characteristic is a spoof and the value '0' when it is live. The variables l_g and l_p denote the liveness values of the gallery and probe samples, respectively. In this method, it is assumed that the liveness values l_g and l_p influence the corresponding match score, m. The interactions among the involved variables are based on the idea that the events S_g, S_p and I influence a common effect, i.e., the decision made by the biometric system, through variables l_g, l_p and m. This approach has one of eight possible outputs: LLG, LSG, SLG, SSG, LLI, LSI, SLI, SSI (see Table A).

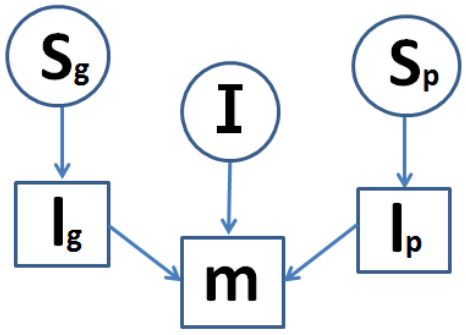


Fig. 23. Architecture of Method 4. The Bayesian Network combines match scores and the corresponding liveness measure values. In this configuration, the liveness measure is assumed to influence match scores.

Rattani and Poh [Rattani and Poh 2013] used fusion schemes based on Gaussian Mixture Model (GMM), Gaussian Copula (GC) and Quadratic Discriminant Analysis (QDA) to combine quality measures with liveness values and match scores. They considered both zero-effort and non-zero effort attacks in their evaluation scheme. [Rattani et al. 2013], incorporated the influence of sensors on the liveness values, quality and match scores using a Bayesian Graphical Model. They demonstrated that incorporating quality (besides liveness values and match scores) into the fusion framework improves overall recognition accuracy; further, the Bayesian model accounted for differences in sensor used during the training and test stages.

6. IMPACT OF SPOOFING ON MULTIMODAL SYSTEMS

Recent investigations demonstrated that, multimodal systems can be deceived when only a subset of the fused modalities is spoofed [Rodrigues et al. 2010] [Rodrigues et al. 2009] [Akhtar et al. 2011a] [Marasco and Sansone 2011b] [Marasco 2010]. Rodrigues *et al.* empirically showed that even if only one modality is spoofed in a bimodal biometric system, the probability of deceiving the multimodal system dramatically increases [Rodrigues et al. 2010]. In particular, they evaluated three different fusion schemes: weighted sum, likelihood ratio and Bayesian likelihood ratio. The vulnerability of multimodal biometric systems to partial spoof attacks was also explored by Johnson *et al.* in [Johnson et al. 2010]. They described a framework for evaluating fusion algorithms by focusing on their security risk when one or a subset of the combined modalities is spoofed. They analyzed the simple sum rule which is the top performer amongst several rule-based strategies. They used a dataset composed of match scores corresponding to three modalities (i.e., face, fingerprint and iris) belonging to 240 subjects. Their study involved a scenario where one of the three modalities is spoofed and a scenario where two of the three modalities are spoofed. The SFAR increased sharply in the second scenario where two modalities were spoofed.

The investigation about how well real spoof attacks can be simulated using match scores has been carried out on different datasets by [Biggio et al. 2012] and [Akhtar et al. 2011b]. They showed that the worst-case scenario - where the genuine match score distribution corresponding to spoof attacks is assumed to be similar to that of live fingerprints - can be too pessimistic. The approach proposed in [Marasco et al. 2011] demonstrated that a more robust fusion can be realized by incorporating a fingerprint liveness detection algorithm in the combination scheme. In general, liveness-based fusion rules make multibiometric systems more robust to spoof attacks [Marfella et al. 2012].

7. CHALLENGES AND OPEN ISSUES

There are several challenges and open issues in the field of anti-spoofing:

— Most spoof (or liveness) detection algorithms proposed in the literature are learning-based, i.e., they learn a decision policy to distinguish real fingerprints from fake ones based on a set of training samples consisting of both live and spoof fingerprints. In most cases, the spoofs encountered in the test set are made from materials previously encountered in the training set. This can optimistically bias the performance of spoof detection algorithms; in fact, it has been demonstrated that the performance of spoof detection algorithms can decrease when the materials used in the training and test sets are different [Marasco and Sansone 2011a]. It is, therefore, necessary to develop generalized countermeasures that are not impacted by the fabrication material used to create the spoofs [Rattani and Ross 2014b; 2014a].
— Learning-based spoof detection schemes are often impacted by the fingerprint sensor used to capture the images (see Fig. 24). Consequently, when a different sensor

is used during testing, it is likely that the spoof detection algorithm will be unsuccessful in detecting spoofs. Additionally, human factors such as placement, pressure and physiology, and environmental conditions such as temperature and humidity can degrade spoof detection performance [Tan et al. 2010; Marcialis et al. 2012b]. Developing interoperable spoof detection algorithms is of paramount importance [Gottschlich et al. 2014].

— It is necessary to design effective methods for integrating spoof detection into a fingerprint verification system. Further, the influence of spoof artifacts on match scores has to be systematically studied. Such a study would assist in the design of effective fusion schemes for consolidating match scores, liveness values and quality measures. Ideally, the system should immediately reject a fingerprint that it is deemed to be a spoof; however, due to the large error rates demonstrated by spoof detection algorithms, summarily rejecting a fingerprint based on liveness values only may result in an increased False Non-Match Rate (FNMR). A robust fusion scheme can judiciously use liveness scores in conjunction with match scores (and quality values) to render a final decision.
— Methods for certifying the level of security of a fingerprint system against spoof attacks has to be developed and rigorously implemented [Sébastien et al.]. However, such a certification scheme is not easy to develop due to the large number of fabrication materials that can be used to generate spoofs; further, it may be difficult to predict the types of spoofs attacks that can be launched in the future. The development of new sensors for fingerprint acquisition can also change the types of materials that are relevant for spoof attacks.
— The advent of mobile biometrics has highlighted the need for designing anti-spoofing methods that can be incorporated in resource-constrained devices such as smartphones. This means, existing countermeasures (both hardware-based and software-based) have to be modified in order to ensure that they can be used in diverse computing platforms.

Fig. 24. Spoof fingerprints obtained using the same material (silicone) but scanned by two different optical devices (CrossMatch and Biometrika respectively) taken from LivDet09, with permission of G. Marcialis.

8. CONCLUSIONS

The art of attacking a biometric system has gained sophistication over the past several years. One such attack involves the use of fake fingers or spoofs in order to defeat the biometric recognition system. The success of spoof attacks has been demonstrated by several researchers. Artificial fingerprints are usually made of materials which can

be scanned by existing commercial fingerprint scanners. Thus, there is a need for developing robust liveness detection or anti-spoofing schemes in order to maintain the integrity of fingerprint recognition systems.

In this paper, we reviewed different types of spoof attacks and discussed the various countermeasures that have been developed in the literature to detect or deflect such attacks. The pros and cons of some of these countermeasures were presented. Databases and performance metrics used to evaluate the efficacy of these countermeasures were also discussed. We then presented methods for combining liveness values with match scores and quality measures. Finally, we discussed some of the open challenges in this field. As fingerprint verification systems become widely used, it is necessary to make them resilient to spoof attacks. The advent of mobile biometrics and remote authentication further reinforces the need to design robust anti-spoofing schemes for fingerprints and other biometric modalities.

ACKNOWLEDGMENTS

The authors are grateful for valuable discussions with researchers from Clarkson University (USA), CSC, NIST, University of Naples Federico II (Italy) and University of Cagliari (Italy). They also acknowledge the support of the Center for Identification Technology Research (CITeR), West Virginia University.

REFERENCES

2010. Fingerprint Spoof Detection Protection Profile FSDPP v1.8. (2010).

A. Abhyankar. 2004. A Wavelet-based Approach to Detecting Liveness in Fingerprint Scanners. *SPIE, Orlando, FL, USA* (2004), 278–286.

A. Abhyankar and S. Schuckers. 2006. Fingerprint Liveness Detection using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques. *IEEE International Conference on Image Processing (ICIP)* (October 2006), 321–324.

A. Abhyankar and S. Schuckers. 2009. Integrating a Wavelet based Perspiration Liveness Check with Fingerprint Recognition. *Pattern Recognition* 42 (2009), 452–464.

A. Abhyankar and S. Schuckers. 2010. Modular Decomposition of Fingerprint Time Series Captures for the Liveness Check. *International Journal of Computer and Electrical Engineering* 2, 3 (2010), 1793–8163.

A. Adler and S. Schuckers. 2009. Security and Liveness: Overview. *Encyclopedia of Biometrics* (2009).

Z. Akhtar, B. Biggio, G. Fumera, and G. Marcialis. 2011a. Robustness of Multimodal Biometric Systems under Spoof Attacks. *International Conference on Image Analysis and Processing (ICIAP), Springer* (2011), 159–168.

Z. Akhtar, G. Fumera, G. Marcialis, and F. Roli. 2011b. Robustness Evaluation of Biometric Systems under Spoof Attacks. *Image Analysis and Processing (ICIAP) Springer* (2011), 159–168.

A. Al-Ajlan. 2013. Survey on Fingerprint Liveness Detection. *IEEE International Workshop on Biometrics and Forensics (IWBF)* (2013), 1–5.

A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni. 2006. Fake Finger Detection by Skin Distortion Analysis. *IEEE Transaction on Information Forensics and Security* 1, 3 (2006), 360–373.

D. Baldisserra, A. Franco, D. Maio, and D. Maltoni. 2005. Fake Fingerprint Detection by Odor Analysis. *Advances in Biometrics* (2005), 265–272.

C. Barral and A. Tria. 2009. Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin. 5458 (2009), 57–69.

B Biggio, Z Akhtar, G Fumera, G Marcialis, and F Roli. 2012. Security Evaluation of Biometric Authentication Systems under Real Spoofing Attacks. *IET Biometrics* 1, 1 (2012), 11–24.

J. Blommé. 2003. Evaluation of Biometric Security Systems against Artificial Fingers. *PhD Thesis* (2003).

A. Bossen, R. Lehmann, and C. Meier. 2010. Internal Fingerprint Identification with Optical Coherence Tomography. *Photonics Technology Letters, IEEE* 22, 7 (2010), 507–509.

E. Bowden-Peters, R. Phan, J. Whitley, and D. Parish. 2012. Fooling a Liveness-Detecting Capacitive Fingerprint Scanner. *Cryptography and Security: From Theory to Applications, Springer* (2012), 484–490.

C. Brislawn, J. Bradley, R. Onyshczak, and T. Hopper. 1996. FBI Compression Standard for Digitized Fingerprint Images. *International Symposium on Optical Science, Engineering, and Instrumentation* (1996), 344–355.

R. Cappelli, D. Maio, and D. Maltoni. 2001. Modelling Plastic Distortion in Fingerprint Images. *Advances in Pattern RecognitionICAPR, Springer* (2001), 371–378.

S Chang, Y Cheng, Kirill V Larin, Y Mao, S Sherif, and C Flueraru. 2008. Optical Coherence Tomography used for Security and Fingerprint-sensing Applications. *IET Image Processing* 2, 1 (2008), 48–58.

J. Chen, S. Shan, C. He, G. Zhao, M. Pietikainen, X. Chen, and W. Gao. 2010. WLD: A Robust Local Image Descriptor. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 32, 9 (2010), 1705–1720.

J. Chen, S. Shan, G. Zhao, X. Chen, W. Gao, and M. Pietikainen. 2008. A Robust Descriptor based on Webers Law. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (2008), 1–7.

Y. Cheng and K. Larin. 2006. Artificial Fingerprint Recognition by using Optical Coherence Tomography with Autocorrelation Analysis. *Applied Optics* 45, 36 (2006), 9238–9245.

H. Choi, R. Kang, K. Choi, and J. Kim. 2007. Aliveness detection of fingerprints using multiple static features. *World Academy of Science, Engineering and Technology* 2, 3 (2007).

P. Coli, G. Marcialis, and F. Roli. 2007a. Power Spectrum-based Fingerprint Vitality Detection. *IEEE Int. Work. on Automatic Identification Advanced Technologies (AutoID)* (2007).

P. Coli, G. Marcialis, and F. Roli. 2007b. Vitality Detection from Fingerprint Images: a Critical Survey. *Lecture Notes in Computer Science* 4642 (2007), 722–731.

B. DeCann, B. Tan, and S. Schuckers. 2009. A Novel Region based Liveness Detection Approach for Fingerprint Scanners. *IAPR/IEEE International Conference on Biometrics (ICB), Springer* 5558 (2009), 627636.

R. Derakhshani, S. Schuckers, L. Hornak, and L. OGorman. 2001. Neural Network-Based Approach for Detection of Liveness in Fingerprint Scanners. *International Conference on Artificial Intelligence* (2001), 1099–1105.

R. Derakhshani, S. Schuckers, L. Hornak, and L. OGorman. 2003a. Determination of Vitality from a Non-Invasive Biomedical Measurement for use in Fingerprint Scanner. *Pattern Recognition* 36, 2 (2003), 383–396.

R. Derakhshani, S. Schuckers, L. Hornak, and L. O'Gorman. 2003b. Determination of Vitality from Non-Invasive Biomedical Measurement for use in Fingerprint Scanners. *Pattern Recognition* 36 (2003), 383–396.

S. Dubey, A. Tulsi, S. Chandra, and M. Singh. 2007. Fingerprint Detection using Full-field Swept-source Optical Coherence Tomography. *Applied Physics Letters* 91, 18 (2007), 181106–181106.

S. Elliott, S. Modi, L. Maccarone M. Young, C. Jin, and H. Kim. 2007. Image Quality and Minutiae Count Comparison for Genuine and Artificial Fingerprints. *41st Annual IEEE International Carnahan Conference on Security Technology* (2007), 30–36.

Y. Endo, M. Hirabayashi, and T. Matsumoto. 2003. Can We Make Artificial Fingers That Fool Fingerprint Systems?(Part V). *Joho Shori Gakkai Kenkyu Hokoku* 18 (2003), 251–256.

M. Espinoza and C. Champod. 2011a. Risk Evaluation for Spoofing against a Sensor supplied with Liveness Detection. *Forensic Science International* 204, 1 (2011), 162–168.

M. Espinoza and C. Champod. 2011b. Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks. *IEEE International Conference on Hand-Based Biometrics (ICHB)* (2011), 1–5.

M. Espinoza, C. Champod, and P. Margot. 2011. Vulnerabilities of Fingerprint Reader to Fake Fingerprints Attacks. *Forensic Science International* 204 (January 2011), 41–49.

J. Feng, A. Jain, and A. Ross. 2009. Fingerprint alteration. *MSU Technical Report, MSU-CSE-09-30* (December 2009).

T. Fladsrud and R. Sollie. 2004. Circumvention of Fingerprint Scanners. (December 2004).

A. Franco and D. Maltoni. 2008. Fingerprint Synthesis and Spoof Detection. *Advances in Biometrics* (2008), 385–406.

J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. 2009. Fingerprint Liveness Detection based on Quality Measures. *Biometrics, Identity and Security (BIds)* (2009), 1–8.

J. Galbally, F. Alonso-Fernandez, J. Firrez, and J. Ortega-Garcia. 2012. A High Performance Fingerprint Liveness Detection Method based on Quality Related Features. *Future Generation Comp. Syst.* (2012), 311–321.

J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez. 2008. Fake fingertip generation from a minutiae template. *19th International Conference on Pattern Recognition (ICPR)* (Dec. 2008), 1 –4.

J. Galbally, J. Fierrez, , and J. Ortega-Garcia. 2007. Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection. (June 2007).

J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz. 2011. Evaluation of Direct Attacks to Fingerprint Verification Systems. *Telecommunication Systems* 47, 3-4 (2011), 243–254.

M Garris and R McCabe. 2000. NIST Special Database 27: Fingerprint Minutiae from Latent and Matching Tenprint Images. *http://www.itl.nist.gov/iaui/894.03/databases* (June 2000).

B. Geller, J. Almog, and P. Margot. 2001. Fingerprint Forgery: a Survey. *Journal of Forensic Sciences* 46, 3 (2001), 731.

B. Geller, J. Almog, P. Margot, and E. Springer. 1999. A Chronological Review of Fingerprint Forgery. *Journal of Forensic Sciences* 44 (1999), 963–968.

L. Ghiani, A. Hadid, G. Marcialis, and F. Roli. 2013. Fingerprint Liveness Detection using Binarized Statistical Image Features. *IEEE Biometrics: Theory, Applications, and Systems (BTAS)* (2013).

L. Ghiani, G. Marcialis, and F. Roli. 2012a. Experimental Results on the Feature-level Fusion of Multiple Fingerprint Liveness Detection Algorithms. *ACM Proceedings of the on Multimedia and Security* (2012).

L. Ghiani, G. Marcialis, and F. Roli. 2012b. Fingerprint Liveness Detection by Local Phase Quantization. *21st International Conference on Pattern Recognition (ICPR)* (November 2012), 1–4.

L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. Marcialis, F. Roli, and S. Schuckers. 2013. LivDet Fingerprint Liveness Detection Competition 2013. *IEEE International Conference on Biometrics (ICB)* (2013), 1–6.

C. Gottschlich, E. Marasco, A. Yang, and B. Cukic. 2014. Fingerprint Liveness Detection based on Histograms of Invariant Gradients. *IEEE International Conference on Biometrics (IJCB)* (2014), 1–7.

D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. 2013. Fingerprint Liveness Detection based on Weber Local Image Descriptor. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMs)* (2013), 1–5.

K. Choi H. Choi, R. Kang and J. Kim. 2007. Aliveness Detection of Fingerprint using Multiple Static Features. *World Academy of Science, Engineering and Technology* 28 (2007), 157–162.

J. Han, T. Kadowaki, K. Sato, and M. Shikida. 1999. Thermal Analysis of Fingerprint Sensor Having a Microheater Array. *IEEE Micromechatronics and Human Science (MHS)* (1999), 199–205.

J. Han, Z. Tan, K. Sato, and M. Shikida. 2005. Thermal Characterization of Micro Heater Arrays on a Polyimide Film Substrate for Fingerprint Sensing Applications. *Journal of Micromechanics and Microengineering* 15, 2 (2005), 282.

S. Harrison, J. Beasley, B. Carroll, and R. Baraniuk. 2004. Classification of Images. (December 2004). OpenStax-CNX.

C. Hill. 2001. Risk of Masquerade Arising from the Storage of Biometrics. *Bachelor of Science thesis, The Department of Computer Science, Australian National University* (2001).

A. Holland-Minkley. 2006. Biometric Devices and Fingerprint Spoofing. (January 2006). http://www2.washjeff.edu/users/ahollandminkley/biometric/index.html.

A. Hyvärinen, J. Hurri, and P. Hoyer. 2009. Natural Image Statistics. *Natural Image Statistics: A Probabilistic Approach to Early Computational Vision, Computational Imaging and Vision* 39 (2009).

Y. Imamverdiev, L. Kerimova, and V. Mussaev. 2009. Method of Detection of Real Fingerprints on the Basis of the Radon Transform. *Automatic Control and Computer Sciences* 43, 5 (2009), 270–275.

A. Jain, Y. Chen, and M. Demirkus. 2007. Pores and Ridges: Fingerprint Matching Using Level 3 Features. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 1 (2007), 15–27.

A. Jain, L. Hong, S. Pankanti, and R. Bolle. 1997. An Identity-Authentication System using Fingerprints. *Proc. IEEE* 85, 9 (1997), 1365–1388.

A. Jain, A. Ross, and K. Nandakumar. 2011. *An Introduction to Biometrics*. Springer.

J. Jia and L. Cai. 2007. A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis. *International Conference on Biometrics (ICB)* (2007).

C. Jin, H. Kim, and S. Elliott. 2007. Liveness Detection of Fingerprint based on Band-Selective Fourier Spectrum. *Information Security and Cryptology* 4817 (2007), 168–179.

C. Jin, S. Li, H. Kim, and E. Park. 2011. Fingerprint Liveness Detection based on Multiple Image Quality Features. *Information Security Applications* (2011), 281–291.

P. Johnson, R. Lazarick, E. Marasco, E. Newton, A. Ross, and S. Schuckers. 2012. Biometric Liveness Detection: Framework and Metrics. *NIST International Biometric Performance Testing Conference (IBPC)* (March 2012).

P. Johnson, B. Tan, and S. Schuckers. 2010. Multimodal Fusion Vulnerability to non-zero effort (spoof) imposters. *IEEE International Workshop on Information Forensics and Security (WIFS)* (2010).

J. Kannala and E. Rahtu. 2012. BSIF: Binarized Statistical Image Features. *IEEE 21st International Conference on Pattern Recognition (ICPR)* (2012), 1363–1366.

M. Kluz. 2005. Liveness Testing in Biometric Systems. *Master thesis, Brno, Masaryk University, Faculty of Informatics* (2005), 57.

M. Lane and L. Lordan. 2009. Practical Techniques for Defeating Biometric Devices. *Technical Report* (2009).

H. Lee, H. Maeng, and Y. Bae. 2009. Fake Finger Detection using the Fractional Fourier Transform. *Image and Vision Computing* 27, 3 (2009), 233–244.

T. Mäenpää. 2003. *The Local Binary Pattern Approach to Texture Analysis: Extensions and Applications*. Oulun yliopisto.

D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. 2003. *Handbook of Fingerprint Recognition*. Springer.

N Manivanan, S Memon, and W Balachandran. 2010a. Automatic Detection of Active Sweat Pores of Fingerprint using Highpass and Correlation Filtering. *Electronics Letters* 46, 18 (2010), 1268–1269.

N Manivanan, S Memon, and W Balachandran. 2010b. Security Breaks a Sweat. *Electronics Letters* 46, 18 (2010), 1241–1242.

E. Marasco. 2010. *Secure Multibiometric Systems*. Ph.D. Dissertation. Università degli Studi di Napoli Federico II.

E. Marasco, Y. Ding, and A. Ross. 2012. Combining Match Scores with Liveness Values in a Fingerprint Verification System. *IEEE Biometrics: Theory, Applications and Systems (BTAS)* (2012), 418 –425.

E. Marasco, P. Johnson, C. Sansone, and S. Schuckers. 2011. Increase the Security of Multibiometric Systems by Incorporating a Spoofing Detection Algorithm in the Fusion Mechanism. *The 10th International Workshop on Multiple Classifer Systems (MCS), Springer* (June 2011).

E. Marasco and C. Sansone. 2010. An Anti-spoofing Technique using Multiple Textural Features in Fingerprint Scanners. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMs)* (2010), 8–14.

E. Marasco and C. Sansone. 2011a. On the Robustness of Fingerprint Liveness Detection Algorithms against New Materials used for Spoofing. *Biosignals 2011 International Conference on Bio-Inspired Systems and Signal Processing* (2011), 1–9.

E. Marasco and C. Sansone. 2011b. On the Security Evaluation of a Multibiometric System based on a Voting Strategy Involving Likelihood Ratio Statistic Tests. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)* (2011), 1–5.

E. Marasco and C. Sansone. 2012. Combining Perspiration- and Morphology-based Static Features for Fingerprint Liveness Detection. *Pattern Recognition Letters* 33 (2012), 1148–1156.

G. Marcialis, L. Ghiani, K. Vetter, D. Morgeneier, and F. Roli. 2012b. Large Scale Experiments on Fingerprint Liveness Detection. *Lecture Notes in Computer Science, Springer Berlin Heidelberg* 7626 (2012), 501–509.

G. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers. 2009. First International Fingerprint Liveness Detection Competition - LivDet 2009. *The 15th International Conference on Image Analysis and Processing (ICIAP)* (September 2009), 12–23.

G. Marcialis, F. Roli, and A. Tidu. 2010. Analysis of Fingerprint Pores for Vitality Detection. *ICPR'10* (2010), 1289–1292.

G. L. Marcialis, P. Coli, and F. Roli. 2012a. Fingerprint Liveness Detection based on Fake Finger Characteristics. *International Journal of Digital Crime and Forensics* (2012).

L. Marfella, E. Marasco, and C. Sansone. 2012. Liveness-based Fusion Approaches in Multibiometrics. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications* (2012), 1–7.

J. Martins, L. Oliveira, and R. Sabourin. 2012. Combining Textural Descriptors for Forest Species Recognition. *38th Annual Conference on IEEE Industrial Electronics Society* (2012), 1483–1488.

T. Matsumoto. 2002. Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis. *Advances in Cryptology ASIACRYPT, Springer* (2002), 574–575.

T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. 2002. Impact of Artificial Gummy Fingers on Fingerprint Systems. *Proc. SPIE* 4677 (2002), 275–289.

S. Memon. 2012. *Novel Active Sweat Pores based Liveness Detection Techniques for Fingerprint Biometrics*. Ph.D. Dissertation. Brunel University School of Engineering and Design.

S Memon, N Manivannan, and W Balachandran. 2011. Active Pore Detection for Liveness in Fingerprint Identification Systems. *Telecommunications Forum (TELFOR), IEEE* (2011), 619–622.

S. Memon, N. Manivannan, A. Noor, W. Balachadran, and N. Boulgouris. 2012. Fingerprint Sensors: Liveness Detection Issue and Hardware based Solutions. *Sensors & Transducers* 136, 1 (2012), 35–49.

B. Miller. 1994. Vital Signs of Identity [biometrics]. *IEEE Spectrum* 31, 2 (1994), 22–30.

Y. Moon, J. Chen, K. Chan, K. So., and K. So. Woo. 2005. Wavelet based Fingerprint Liveness Detection. *Electronic Letters* 41, 20 (2005), 1112–1113.

M. Nasiri-Avanaki, A. Meadway, and A. Bradu. 2011. Anti-Spoof Reliable Biometry of Fingerprints Using En-Face Optical Coherence Tomography. *Optics and Photonics Journal* 1 (2011), 91–96.

S. Nikam. 2009. Wavelet-based Multiresolution Analysis of Ridges for Fingerprint Liveness Detection. *Inderscience Publishers* (2009).

S. Nikam and S. Agarwal. 2008a. Fingerprint Liveness Detection using Curvelet Energy and Co-occurrence Signatures. *IEEE Fifth International Conference on Computer Graphics, Imaging and Visualisation (CGIV)* (2008), 217–222.

S. Nikam and S. Agarwal. 2008b. Local Binary Pattern and Wavelet-based Spoof Fingerprint Detection. *International Journal of Biometrics* 1, 2 (2008), 141–159.

S. Nikam and S. Agarwal. 2009a. Co-occurrence Probabilities and Wavelet-based Spoof Fingerprint Detection. *International Journal of Image and Graphics* 9, 02 (2009), 171–199.

S. Nikam and S. Agarwal. 2009b. Curvelet-based Fingerprint Anti-spoofing. *Signal, Image and Video Processing* 4, 1 (January 2009), 75–87.

S. Nikam and S. Agarwal. 2009c. Ridgelet-based Fake Fingerprint Detection. *Neurocomputing* 72, 10-12 (2009), 2491–2506.

NIST. 2012. Need and Perspectives to Realize Liveness Detection. *IBPC* (March 2012).

K. Nixon, V. Aimale, and R. Rowe. 2007. Spoof Detection Schemes. *Handbook of Biometrics* (2007).

K. Nixon and R. Rowe. 2005. Multispectral Fingerprint Imaging for Spoof Detection. *Defense and Security, International Society for Optics and Photonics* (2005), 214–225.

K. Nixon, R. Rowe, J. Allen, S. Corcoran, L. Fang, D. Gabel, D. Gonzales, R. Harbour, S. Love, and R. McCaskill. 2004. Novel Spectroscopy-based Technology for Biometric and Liveness Verification. *Defense and Security* (2004), 287–295.

T. Ojala, M. Pietikainen, and T. Maenpaa. 2002. Multiresolution Gray-scale and Rotation Invariant Texture Classification with Local Binary Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24, 7 (2002), 971–987.

V. Ojansivu and J. Heikkilä. 2008. Blur Insensitive Texture Classification using Local Phase Quantization. *Image and Signal Processing* (2008), 236–243.

V. Ojansivu, E. Rahtu, and J. Heikkila. 2008. Rotation Invariant Local Phase Quantization for Blur Insensitive Texture Analysis. *IEEE 19th International Conference on Pattern Recognition (ICPR)* (2008), 1–4.

S. Parthasaradhi, R. Derakhshani, L. Hornak, and S. Schuckers. 2004. Improvement of an Algorithm for Recognition of Liveness using Perspiration in Fingerprint Devices. *Defense and Security* (2004), 270–277.

S. Parthasaradhi, R. Derakhshani, L. Hornak, and S. Schuckers. 2005. Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews* 35, 3 (2005), 335–343.

N. Ratha, J. Connell, and R. Bolle. 2001. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM Systems Journal* 40, 3 (2001), 614–634.

A. Rattani and N. Poh. 2013. Biometric System Design Under Zero and Non-Zero Effort Attacks. *IEEE International Conference on Biometrics (ICB)* (2013).

A. Rattani, N. Poh, and A. Ross. 2013. A Bayesian Approach for Modeling Sensor Influence on Quality, Liveness and Match Score Values in Fingerprint Verification. *IEEE International Workshop on Information Forensics and Security (WIFS)* (2013), 37–42.

A. Rattani and A. Ross. 2014a. Automatic Adaptation of Fingerprint Liveness Detector to New Spoof Materials. *IEEE International Conference on Biometrics (IJCB)* (2014), 1–6.

A. Rattani and A. Ross. 2014b. Minimizing the Impact of Spoof Fabrication Material on Fingerprint Liveness Detector. In *Proc. of 21st IEEE International Conference on Image Processing (ICIP)*.

P. Reddy, A. Kumar, S. Rahman, and T. Mundra. 2007. A New Method for Fingerprint Aantispoofing using Pulse Oxiometry. *IEEE Biometrics: Theory, Applications and Systems (BTAS)* (2007), 1–6.

P. Reddy, A. Kumar, S. Rahman, and T. Mundra. 2008. A New Antispoofing Approach for Biometric Devices. *IEEE Transactions on Biomedical Circuits and Systems* 2, 4 (2008), 328–337.

C. Roberts. 2007. Biometric Attack Vectors and Defences. *Computers and Security* 26, 1 (2007), 14–25.

R. Rodrigues, N. Kamat, and V. Govindaraju. 2010. Evaluation of Biometric Spoofing in a Multimodal System. *IEEE Biometrics: Theory, Applications and Systems (BTAS)* (2010).

R. Rodrigues, L. Ling, and V. Govindaraju. 2009. Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks. *Journal of Visual Languages and Computing* (2009).

A. Ross, J. Shah, and A. Jain. 2007. From Template to Image: Reconstructing Fingerprints From Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 4 (2007), 544–560.

M. Sandstrom. 2004. Liveness Detection in Fingerprint Recognition Systems. *PhD Thesis. Linkping* (2004).

S. Schuckers. 2002. Spoofing and Anti-spoofing Measures. *Information Security Technical Report* 7, 4 (2002), 56–62.

S. Schuckers, R. Derakhshani, S. Parthasaradhi, and L. Hornak. 2006. Liveness Detection in Biometric Devices. *Circuits, Signals, and Speech and Image Processing* (2006).

S. Schuckers, L. Hornak, T. Norman, R. Derakhshani, and S. Parthasaradhi. 2002. Issues for Liveness Detection in Biometrics. *IEEE Proceedings of Biometric Consortium Conference, New York* (2002).

S. Schuckers, S. Parthasaradhi, R. Derakshani, and L. Hornak. 2004. Comparison of Classification Methods for Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices. *Biometric Authentication, Springer* (2004), 256–263.

S. Schuckers and B. Tan. 2006. Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing. *Computer Vision and Pattern Recognition Workshop (CVPR)* (2006), 26.

M. Sébastien, M. Nixon, and S. Li. *Handbook of Biometric Anti-Spoofing*. Springer 2014.

M. Sepasian, C. Mares, and W. Balachandran. 2010. Vitality Detection in Fingerprint Identification. *Information Science and Applications* 4 (2010).

Y. Shin, I. Jun, H. Kim, and W. Shin. 2009. Performance Assessment Method for a Forged Fingerprint Detection Algorithm. *Advances in Information Security and Its Application* (2009).

K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. Newton, and B. Preneel. 2012. Criteria Towards Metrics for Benchmarking Template Protection Algorithms. *The 5th IAPR International Conference on Biometrics (ICB)* (2012), 498–505.

Y. Singh and S. Singh. 2013. A Taxonomy of Biometric System Vulnerabilities and Defences. *International Journal of Biometrics* 5, 2 (2013), 137–159.

C. Sousedik and C. Busch. 2014. Presentation Attack Detection Methods for Fingerprint Recognition Systems: a Survey. *IET Biometrics* (2014), 1–15.

J. Staymates, M. Staymates, and G. Gillen. 2013. Evaluation of a Drop-on-Demand Micro-Dispensing System for Development of Artificial Fingerprints. *Anal. Methods, RSC* 5 (2013), 180–186. Issue 1.

A. Stén, A. Kaseva, and T. Virtanen. 2003a. Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner. *4th Australian Information Warfare and IT Security Conference* (2003), 1–8.

A. Stén, A. Kaseva, and T. Virtanen. 2003b. Fooling Fingerprint Scanners-Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner. 2003 (2003), 333–340.

B. Tan, A. Lewicke, D. Yambay, and S. Schuckers. 2010. The Effect of Environmental Conditions and Novel Spoofing Methods on Fingerprint Anti-spoofing Algorithms. *IEEE International Workshop on Information Forensics and Security (WIFS)* (2010), 1–6.

B. Tan and S. Schuckers. 2005. Liveness Detection using an Intensity based Approach in Fingerprint Scanner. In *Proceedings of Biometrics Symposium (BSYM)*.

B. Tan and S. Schuckers. 2010. Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise. *Pattern Recognition* 43, 8 (2010), 2845–2857.

L. Thalheim, J. Krissler, and P. Ziegler. 2002. Body Check: Biometric Access Protection Devices and their Programs put to the Test. *ct magazine* 11 (November 2002).

A. Tidu. 2010. Fingerprint Vitality Assessment by Pores Detection. *M. Sc. Thesis, University of Cagliari* (2010).

B. Toth. 2005. Biometric Liveness Detection. *Information Security Bulletin* 10 (October 2005), 291–297.

U. Uludag and A. Jain. 2004. Attacks on Biometric Systems: a Case Study in Fingerprints. *Proc. SPIE-EI, Security, Seganography and Watermarking of Multimedia Contents VI* (2004).

V. Valencia and C. Horn. 2003. *Biometrics*. Osborne McGraw Hill, New York, Chapter Biometric Liveness Testing, 139–149.

T. van der Putte and J. Keuning. 2001. Biometrical Fingerprint Recognition: Don't Get your Fingers Burned. (2001), 289–303.

A. Wiehe, T. Søndrol, O. Olsen, and F. Skarderud. 2004. Attacking Fingerprint Sensors. *Gjøvik University College* 200 (2004).

D. Willis and M. Lee. 1998. Six Biometric Devices Point the Finger at Security. *Computers and Security, Elsevier* 17, 5 (1998), 410–411.

K. Yamada, H. Matsumoto, and T. Matsumoto. 2000. Can We Make Artificial Fingers That Fool Fingerprint Systems?(Part II). 12 (2000), 109–114.

D. Yambay, L. Ghiani, P. Denti, G. Marcialis, F. Roli, and S. Schuckers. 2012. LivDet 2011 - Fingerprint Liveness Detection Competition 2011. *The 15th International Conference on Image Analysis and Processing (ICIAP)* (April 2012), 208–215.

S. Yang, C. Wang, and S. Chen. 2011. A Release-Induced Response for the Rapid Recognition of Latent Fingerprints and Formation of Inkjet-Printed Patterns. *Angewandte Chemie* 123, 16 (2011), 3790–3793.

W. Yau, H. Tran, and E. Teoh. 2008. Fake Finger Detection using an Electrotactile Display System. *10th International Conference on Control, Automation, Robotics and Vision (ICARCV)* (2008), 962–966.

W. Yau, H. Tran, E. Teoh, and J. Wang. 2009. Fake Finger Detection by Finger Color Change Analysis. *Advances in Biometrics* 4642 (2009), 888896.

S. Yoon, J. Feng, and A. Jain. 2010. Fingerprint Alteration. *The 95th International Educational Conference of the International Association for Identification (IAI), Spokane, WA* (July 2010), 11–17.

S. Yoon, J. Feng, and A. Jain. 2012. Altered Fingerprints: Analysis and Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 34, 3 (2012), 451–464.

Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi. 2007. Fake Finger Detection based on Thin-plate Spline Distortion Model. *International Conference on Biometrics (ICB)* (2007), 742–749.

Received October 2013; revised January 2014; accepted February 2014