Published in IET Biometrics
Received on 28th March 2013
Revised on 21st October 2013
Accepted on 28th November 2013
doi: 10.1049/iet-bmt.2013.0020

ISSN 2047-4938

Presentation attack detection methods for fingerprint recognition systems: a survey

Ctirad Sousedik, Christoph Busch

Norwegian Information Security Laboratory (NISlab), Gjøvik University College, Teknologiveien 22, 2815 Gjøvik, Norway
E-mail: ctirad.sousedik@hig.no

Abstract: Nowadays, fingerprint biometrics is widely used in various applications, varying from forensic investigations and migration control to access control as regards security sensitive environments. Any biometric system is potentially vulnerable against a fake biometric characteristic, and spoofing of fingerprint systems is one of the most widely researched areas. The state-of-the-art sensors can often be spoofed by an accurate imitation of the ridge/valley structure of a fingerprint. An individual may also try to avoid identification by altering his own fingerprint pattern. This study is a survey of presentation attack detection methods for fingerprints, both in terms of liveness detection and alteration detection.

1 Introduction

For over a century now, fingerprints have been widely used as a biometric characteristic by forensic sciences. Nowadays, large national and international databases contain millions of records, at the disposal of forensic investigations and migration control. Fingerprints are also being used for access control concerning security sensitive environments such as access to protected facilities or sensitive data. Recently, fingerprint recognition systems have been deployed as access control to rather common facilities like recreation areas, fitness-centres and so on. Fingerprint capture devices are widely available on the market, which provides for a variety of applications.

The fingerprint is a well-known biometric characteristic, which is valued for its uniqueness even in cases of identical twins [1]. No other biometric characteristic has probably been so well tested in real-world situations for such a long time. Today's state-of-the-art automatic fingerprint recognition algorithms perform with high recognition accuracy on databases containing hundreds of millions of records.

Nevertheless, the state-of-the-art fingerprint sensors can be a significant security problem. Even though the current comparison algorithms are very mature in terms of searching records for an appropriate match, the entire system can be spoofed by an accurate imitation of the ridge/valley structure of the fingertip, which could have for instance been generated with low cost resources from the signal that has been derived from a latent fingerprint [2–9].

Numerous approaches to solve the problem of liveness detection for fingerprint sensors have been published. The hardware-based solutions suggest a new sensing technology, which would be difficult to deceive because of the nature of the fingerprint capture process. The software-based methods on the other hand try to use data that can be obtained from the currently existing sensors, and add a software liveness detection module. Although the software methods do have limited possibilities because of the fixed hardware, they also have the advantage of lower costs that are limited to the deployment costs of a software update.

Another possible way of deceiving the fingerprint sensor is the fingerprint alterations. The impostor alters or damages his fingerprint pattern in order to avoid automatic identification based on his enrolled fingerprints. The fingerprint alteration detection along with liveness detection belong to the group of presentation attack detection (PAD) methods (Fig. 3).

This paper is organised as follows: Section 2 summarises the various existing fingerprint sensing technologies. Section 3 discusses the known methods for deceiving fingerprint sensors. Section 4 analyses and discusses the concepts and the ideas of the existing fingerprint liveness detection approaches, whereas Section 5 reviews the performance of the methods mentioned. Section 6 draws conclusions and suggests future research.

2 Fingerprint sensing technologies

Numerous principles have been utilised in order to develop a sensor capable of capturing the ridge/valley structure of a fingerprint. The fingerprint sensing technologies can be divided into two groups as illustrated by Fig. 1.

The technologies that belong to the optical sensor group generally utilise a system of light sources, lens, prisms or optical fibres along with a photosensitive surface to capture the fingerprint pattern. The solid state sensors are usually developed as a single chip solution, where the sensing mechanism is integrated on the silicon chip. Typically, solid state sensors can be produced in smaller sizes than optical sensors, yielding the possibility of integration into portable

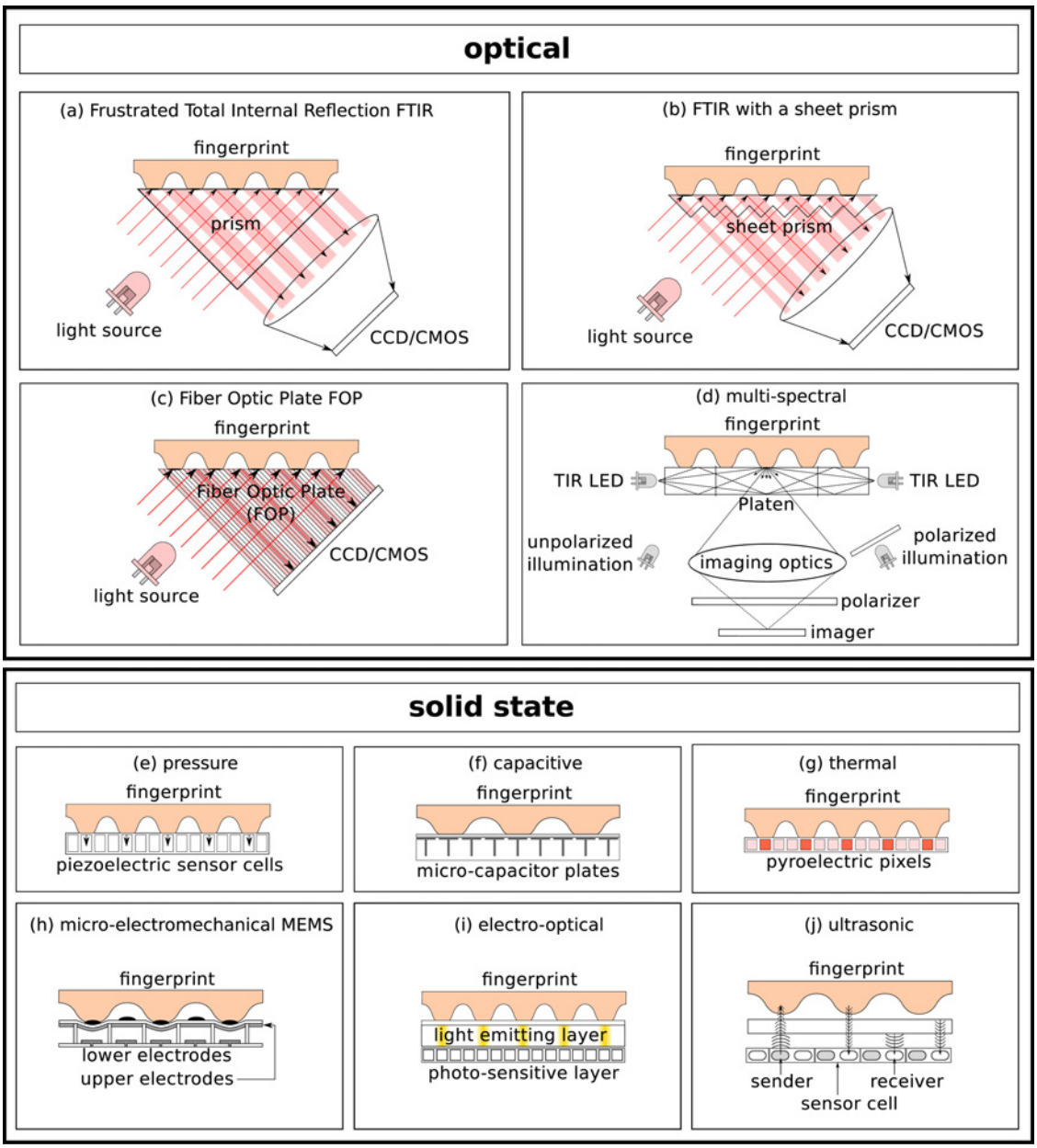

Fig. 1 *Fingerprint sensing technologies [10–12]*

Optical:
a Frustrated Total Internal Reflection (FTIR)
b FTIR with a sheet prism
c Fibre optic plate (FOP)
d Multi-spectral

Solid state:
e Pressure
f Capacitive
g Thermal
h Micro-electromechanical
i Electro-optical
j Ultrasonic

devices. Alternatively, the fingerprint sensing technologies can be classified into 'swipe', 'touch' and 'touchless' categories. The swipe sensors require the biometric capture subjects to swipe their finger over the sensor surface. The fingerprint is captured from the time-series acquired. Although this approach can lead to higher failure-to-acquire (FTA) rates, it allows the sensor area to be of much smaller size than that of the touch sensors, which can reduce the production costs. The touch sensors provide a sensor surface large enough to capture the fingerprint by using a single static scan. The touchless sensors do not require the capture subject to press his finger against a flat surface. The fingerprint is scanned in its original condition. These sensors do not suffer from the problems of touch-based sensors, such as skin deformation, latent fingerprints on the surface or hygienic issues [13].

One of the first fingerprint sensing technologies has been the Frustrated Total Internal Reflection (FTIR). The technology utilises a prism, a LED light source and a CCD/CMOS camera as illustrated by Fig. 1*a*. The finger is put onto the prism surface and another side of the prism is illuminated by the LED light source. The fingerprint ridges that are in contact with the prism surface absorb the light, whereas the surface under the valleys reflects the light towards the CCD/CMOS camera. This way of the fingerprint surface analysis makes it difficult to deceive the

doi: 10.1049/iet-bmt.2013.0020

sensor with a fake two-dimensional (2D) representation of the fingerprint such as a photo [10, 14].

The FTIR technology suffers from disadvantages of larger size, particularly because of the presence of the prism. To solve this problem, the sheet prism FTIR technology replaces the single large prism with a large number of small adjacent prisms as illustrated by Fig. 1*b*. This approach reduces the size of the sensors, however, it also somewhat reduces the final image quality [10, 14].

Another way of dealing with the size constraints caused by the presence of the prism is the fibre optic plate (FOP) method. In this case, the single large prism from the classical FTIR design is replaced with a grid of optical fibres as shown by Fig. 1*c*. The fingerprint ridges are in contact with the optical fibres, and scatter the light emitted by a LED light source. The optical fibres under the valleys reflect the light to a CCD/CMOS photosensitive surface [10, 14].

A relatively new approach to fingerprint sensing is the multi-spectral technology (Fig. 1*d*). This technology enables the capturing of multiple images of the fingertip under various illumination conditions, as regards the wavelength, the orientation and the polarisation of the light emitted. The captured images depict the fingertip at various depths and with variations depending on the different absorption of the individual wavelengths in the fingertip [12]. The aggregative analysis of these images improves the FTA rates of the sensor in difficult conditions (dirty fingers, damaged surface fingerprint etc.).

In contrast to the optical technologies, the solid state fingerprint sensors (Fig. 1) can typically be integrated in a single chip, thus decreasing the resulting size and the costs.

The pressure-based fingerprint sensors are based on the piezoelectric effect. Piezoelectric materials produce small amounts of voltage when pressure is applied. The sensing technology makes use of a grid of piezoelectric cells that yield different amount of voltage depending on whether or not they are in contact with the ridges on the fingertip surface. From the differences, the fingerprint pattern can be captured (Fig. 1*e*) [10].

The capacitive fingerprint sensing technology utilises a grid of microcapacitor plates. The finger that is put onto the sensor acts as a second plate for each of the microcapacitors. The ridges that are in closer contact with the surface yield different resulting capacitances than the valleys. By using these differences, the fingerprint pattern is captured (Fig. 1*f*) [10, 14].

The thermal technology utilises a 2D array of thermo-sensitive cells made of pyroelectric materials. When the finger is put onto the sensor, the fingerprint pattern is captured as it depends on the temperature differences between the ridges and the air in the valleys (Fig. 1*g*) [10, 14].

Another approach that has been based on the pressure differences between the ridges and the valleys of a fingerprint is the micro-electromechanical technology. The sensor consists of a 2D sensor cell array as illustrated by Fig. 1*h*. If the fingerprint ridge is put on a sensor cell, the upper electrode is pushed down causing a capacitance change in the cell capacitor. The differences between the capacitances of the cell capacitors under the ridges and the valleys are used to obtain the fingerprint pattern (Fig. 1*h*) [11].

The electro-optical technology makes use of a photosensitive layer and a light emitting layer as shown by Fig. 1*i*. The light emitting layer emits light based on the electric potential on its surface. Since the fingerprint ridges touch the surface and the valleys do not, the electric potential varies across the surface, generating a fingerprint representation that is captured by the photosensitive layer [14].

In the ultrasonic fingerprint sensing technology, the differences of the acoustic impedance between the ridge skin and the air in the valleys are utilised in order to capture a fingerprint pattern. The acoustic signal is transmitted towards the fingertip surface, and the reflected echo is captured to reproduce the ridge/valley structure. This acoustic technology is also capable of analysing the sub-surface layers of the skin, enabling lower FTA rates (Fig. 1*j*) [10].

The radio frequency technology analyses the changes of the electromagnetic field of the radio frequencies because of the presence of the fingertip. Every cell of the detector grid acts like a microantenna and detects variations because of the presence of the fingerprint pattern. The technology can also analyse the sub-surface information in the fingertip, yielding better functionality in difficult conditions [10].

A summary of the design properties of the above discussed fingerprint sensing technologies is provided by Table 1.

3 Fingerprint sensor spoofing methods

In general, the fingerprint spoofing methods can be divided into two classes. If the actual finger of the genuine enrolled individual is available during the fake [In the International Standardisation project ISO/IEC 30107, instead of the term

Table 1 Fingerprint sensing technologies [10, 12]

Type		Sensing method	Properties
optical	miniaturisation limitations	FTIR	larger size because of the prism and the optics
		FTIR with a sheet prism	more compact, reduced prism size
		FOP	compact design, the prism and the optics are replaced by optical fibres
		multi-spectral	multi-spectral scanning, better functionality in difficult conditions
		electro-optical	measurement of difference in the electric potential caused by the fingerprint pattern
solid state	single-chip design	radio frequency	measures changes in the electromagnetic field in the fingertip, better functionality in difficult conditions
		capacitive	capacitance measurement, susceptible to electrostatic discharge
		ultrasonic	measures the acoustic impedance of the ridges and the air in the valleys
		pressure	measurement of the pressure caused by the ridges using the piezoelectric effect
		micro-electromechanical	measurement of the pressure caused by the ridges by the capacitance change in the cell capacitors
		thermal	measures the temperature of the ridges and the valleys air, environment-dependent

fake, the term artefact is defined as follows: artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns.] fabrication process, the fabrication methods are called 'cooperative' [5, 15, 16] or 'direct casts' [3, 4, 17]. On the other hand, if the original finger is not directly available, the methods are called 'non-cooperative' [5, 15, 16] or 'indirect casts' [3, 4, 17]. It is worth noting that these terms can be somewhat misleading because the methods either do or do not require the original finger to be present during the fake finger fabrication process. It is not important in what manner the original finger was available – it could be possible to obtain physical control of the original finger by means of violence, drugs, blackmailing and so on. Fig. 2 summarises various fingerprint faking approaches.

The 'direct casting' methods make use of the availability of the original finger to create a fake fingerprint. The fake fingerprint is created by means of a mould made of materials like thermoplastic [3, 4], silicone [3, 4], plasticine [9], candle wax [9] and so on. The mould material needs to be sufficiently soft so that the original finger can be pressed against it to create a negative of the original fingerprint. The finger needs to be pressed against the mould in a very careful fashion so that all the fingerprint details are being preserved and lifted back; and the mould needs to be able to harden, providing the negative for the fake fingerprint fabrication. Afterwards, the actual fake finger is created by using the mould. Various materials like latex [3, 4], silicone [5–7, 9], gelatin [6, 8] and so on can be used, but it is necessary to take the mould material into consideration as well. The mould and the fake fingerprint material must not join together during the fake fingerprint hardening process, neither must they chemically react so that the quality of the resulting finger would be impaired. It must also be possible to remove the hardened fake fingerprint from the mould without having bits of the mould stuck in the resulting 3D fingerprint pattern [9].

The 'indirect casting' methods take advantage of other ways of obtaining the fingerprint pattern indirectly. Latent fingerprints left by the genuine enrolled individual on various surfaces can be exploited. Initially, it is necessary to visualise the latent fingerprint, since it is not directly visible in most cases. Various methods to perform this visualisation step are known from forensics. One of the methods is application of very fine-grained powders on the latent fingerprint. The powder sticks to the latent fingerprint and the rest of the powder that did not get stuck can be gently removed. In such a way, the latent fingerprint becomes clearly visible and can even be lifted off the surface by using a special tape that glues the visualised fingerprint on its surface. The visualised latent fingerprint is then digitised by means of photographing or scanning and digitally enhanced in order to compensate for the loss of quality that is present because of the usage of latent fingerprints. The digitised fingerprint is also converted to a black and white mask that is used in further steps. Afterwards, the mask is printed on a thin transparent film. It is possible to use this film directly as a mould because the toner deposit creates elevations on the surface of the film [3, 4, 9]. Alternatively, the mould can be created by using printed circuit board (PCB) technology. The film with the fingerprint on-print is put on the PCB and illuminated with UV light. The parts of the PCB exposed to the UV light can be then etched away in order to create a mould with the fingerprint pattern [5, 7–9]. Finally, the fake fingerprint is created by using the film or the etched PCB as a mould. Various materials can be used, such as latex [3, 4], silicone [5, 7, 9] gelatin [8, 9], plasticine [9], wood cement [9], glue [3, 4] and so on. The material is put in the mould and after hardening the fake fingerprint is removed from it and is ready to use.

In addition to the above mentioned group of methods, the mould for the fake fingerprint of the fake fingerprint itself can be produced by any other means that can provide for sufficient detail (ordered rubber stamp, 3D printers etc.). The range of possible fake fabrication materials is rather large and difficult to predict, which poses a great challenge for finding an effective countermeasure.

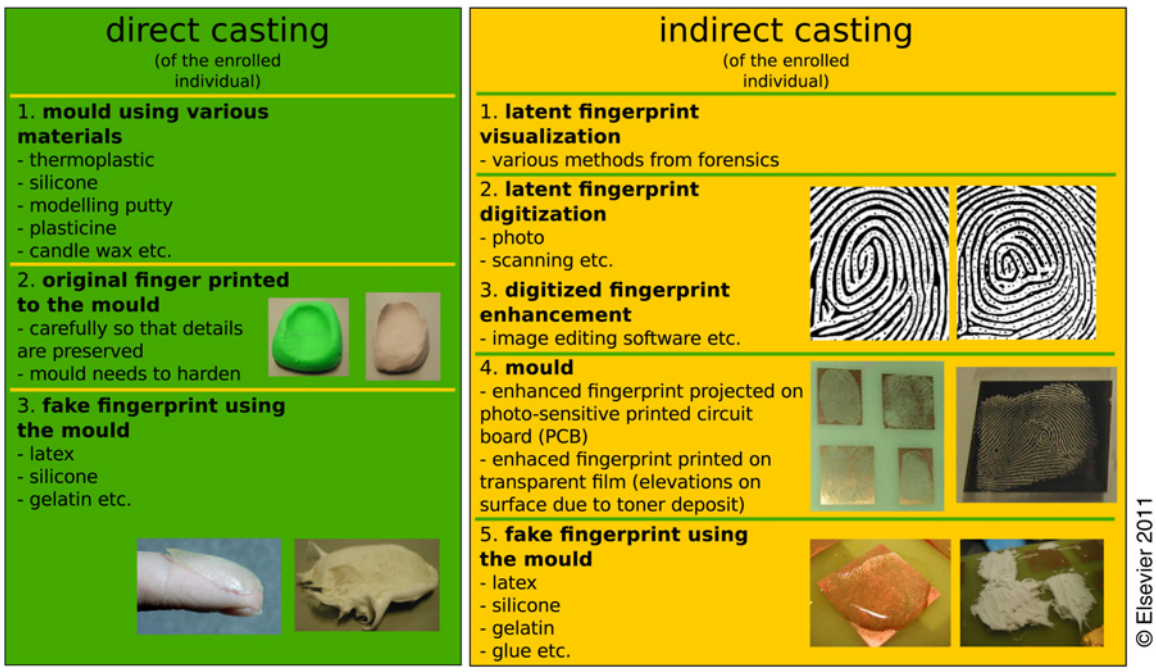

Fig. 2 *Fingerprint sensor spoofing methods [3–9]*

IET Biom., 2014, Vol. 3, Iss. 4, pp. 219–233
doi: 10.1049/iet-bmt.2013.0020

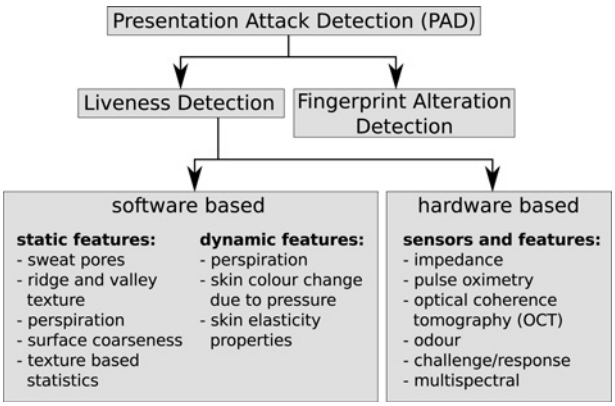

Fig. 3 *PAD methods*

4 PAD for fingerprint sensors

To satisfy the security requirements for a biometric fingerprint recognition system, it should not be possible to deceive a fingerprint sensor. The sensor should reject any fake fingers created from any material as well as a dead cut-off finger. In addition to the usage of fake or cut-off fingers, the impostors can change their fingerprint patterns so that they would be able to escape their identification in terms of the fingerprint identification pipeline. Ideally, the sensor should be equipped with a PAD capability in order to correctly handle the above mentioned impostor scenarios. As illustrated by Fig. 3, the PAD methods for the fingerprints include liveness detection and fingerprint alteration detection. The term PAD is defined by the standardisation project, ISO/IEC 30107 [18], and, in addition to the detection of fake or altered biometric characteristics, it includes also the detection of coercion, non-conformity and obscuration. The liveness detection methods can be further divided into hardware and software-based groups [19]. The hardware-based methods try to add liveness detection to the existing fingerprint sensor designs by addition of new hardware components, or even try to create a new sensing technology that would be difficult to deceive because of the scientific principles used in the fingerprint acquisition process. The software-based methods, on the other hand, process the image signal provided by the existing fingerprint sensors, and add the liveness detection capability by augmenting the software architecture with a dedicated attack detection algorithm that is capable of distinguishing the patterns between genuine living fingers and fake or even cut-off fingers. Thus, the software-based methods enable limited costs but at the same time they imply less universal applicability. The main challenge of a liveness detection method is to cope with widely varying properties of a living finger. Owing to the large variations of the properties of the living fingers, it is typically possible to create a fake representation with the correct attributes, as long as the number of the properties verified is rather small. It is difficult to predict and consider all the possible fake fingerprint fabrication methods and artefact materials and thus many of the fake detection approaches can be circumvented, as soon as the right novel artefact material and fabrication method have been identified.

4.1 Fingerprint alteration detection

One of the groups of techniques used by the impostors to spoof the fingerprint biometric sensors are fingerprint alterations (see Fig. 3). The impostor attempts to change his own fingerprint pattern by various means, such as cutting the finger, application of acids or even fingerprint transplantations. The main goal of the impostor is to destroy or alter his fingerprints to such an extent that the automated system is unable to find a match in the identification process. In such a case, he might avoid the consequences of being on the blacklist (e.g. because of recorded criminal activities etc.). Fingerprint alteration detection along with liveness detection belong to the group PAD methods as illustrated by Fig. 3.

Feng *et al.* [20] have proposed a method to detect altered fingerprints by analysis of the orientation field determined by the fingerprint ridge structure. Fingerprint alterations introduce discontinuities in the orientation field that would not be possible in a genuine unaltered finger. The authors have extracted features based on these discontinuities and classified the fingerprints by using support vector machines (SVMs). The authors report 92% of correctly identified altered fingerprints in a dataset of synthetic fingerprints generated by using 976 genuine fingerprints. Yoon *et al.* [21] have developed an approach based on the anomalies in the orientation fields and the minutiae distributions of the altered fingerprints. The method has been tested on a large-scale database of 4433 altered fingerprints from 270 subjects, providing for 70.2% correctly identified altered fingerprints at a false positive rate of 2.1%. Tiribuzi *et al.* [22] have combined the minutiae density maps and the orientation entropies of the ridge-flow in order to identify the altered fingerprints. The authors have reported a 90.4% classification accuracy on a dataset of 1000 genuine and synthetic altered fingerprints. Yoon *et al.* [23] also examined the possibility of comparing the altered fingerprints with their original unaltered versions. The authors conclude that for some altered fingerprints this should be possible, even in cases when the severity of the alteration seems to be large. Petrovici and Lazar [24] suggested that the altered fingerprints could be detected by the analysis of the singularities in the fingerprint orientation field. Petrovici [25] has also proposed a method for the synthetic generation of the altered fingerprints from their genuine counterparts.

So far, most of the researchers have developed and tested their alteration detection methods on synthetic data. The quality of the synthesis method varies, which yields for varying difficulty of the subsequent classification task. A public dataset of altered fingerprints would be necessary for a fair benchmark of these approaches.

4.2 Software-based liveness detection

The software-based methods of liveness detection try to make use of the existing hardware designs, and add the liveness detection capability by updating the software part of the fingerprint sensor design. The software-based methods have the potential to differentiate a captured genuine living finger from the signal stemming from a fake finger when the captured sample was generated at a high resolution. Some categorisation of the methods has been proposed in the literature [14, 19]. The methods can be divided into two categories based on whether they work with a single static 2D scan, or need multiple 2D scans at different time points during the acquisition process that support the observation of the dynamic properties.

4.2.1 Static methods: The static software-based liveness detection methods make use of a single 2D scan available

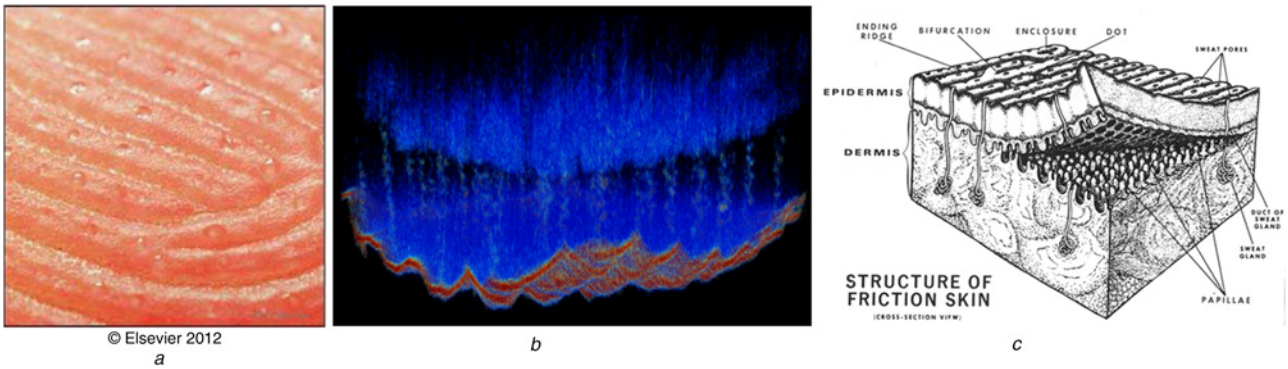

Fig. 4 *Sweat pores and sweat glands: tiny structures, present in the fingerprint ridges, responsible for the sweat fluid production*

a Sweat pores [26]
b OCT scan of the sweat glands [27]
c Fingertip skin structure (courtesy of the FBI)

from the classical 2D sensors. The methods analyse various differences between scans of genuine and fake fingers that are caused by differences in elastic properties, inaccurate reproduction of the genuine fingers, absence of skin perspiration and so on.

Sweat pores: One of the ideas applied is the detection and the analysis of the sweat pores. The sweat pores are very small circular structures present in the fingerprint ridges of the living fingers that are the endings of internal skin structures called sweat glands (Fig. 4).

The sweat glands are responsible for production of sweating fluid. The liveness detection methods based on the analysis of the sweat pores usually expect that such small structures would be very difficult to reproduce with sufficient quality when the fake finger is produced. Espinoza and Champod [17] claim that even though it is possible to replicate the sweat pores by using the fake fingerprint fabrication methods, the quantities of the pores differ in the fingerprints generated by the real living fingers compared with the fingerprints generated by the fake fingers and the difference can be used as a measure of the liveness detection. Manivanan *et al.* [28] suggest a method for static detection of the active sweat pores in the fingerprint scans that have been captured by sensors of higher resolutions than typically available (>800 dpi). They suggest the integration of this method into the fingerprint sensors in order to perform liveness detection. Choi *et al.* [29] suggested a method that analyses the sweat pores and uses a statistic based on their distances from one another (individual pore spacing) as one of the features to distinguish between genuine and fake fingers. The method has been presented on a dataset of 500 dpi images.

Ridge and valley texture: Another possibility is to analyse the highly detailed textures of the fingerprint scans and look for differences because of inaccurate reproduction of the original finger or differences in the elastic properties of the genuine and the fake fingers. Tan and Schuckers [30] use an approach based on the extraction of the signal in the valleys of the scanned fingerprint. The valleys are thinned to obtain a skeleton that determines the valley signal and the signal is then analysed in a multi-resolution fashion by using wavelets in order to perform liveness detection. The Tan and Schuckers [30] fingerprints are compared with the fingerprints obtained from genuine living fingers. Jin *et al.* [31] suggest that the middle ridge and the middle valley signals are interesting features that can be used to distinguish between living and fake fingers. They skeletonise the fingerprint and its inverted version in order to obtain the skeletons of the ridge and the valley structures. Afterwards, they analyse the 1D signals extracted from underneath the skeletons – the middle ridge signal and the middle valley signals. They claim that because of problems with achieving a high-quality replication of the sweat pores in the fake fingerprints, a middle ridge signal generated from a fake fingerprint scan is generally less periodic than a middle ridge signal generated by a genuine living finger. They also observed that living fingers usually yield scans with less noisy middle valley signals than the fake fingers. In addition, their method uses the overall clarity of the ridge/valley structure examined in the spectral domain as one of the classification features. Marasco and Sansone [32] also analyse the ridge signal determined by the ridge skeleton as one of the features for their liveness detection method.

Perspiration: When a living finger is put on the surface of a fingerprint sensor, the sweat fluids start to spread along the ridge/valley structure and the changes are observable in a matter of seconds. Even though this phenomenon of perspiration can be used in the dynamic methods by observing changes in the scan over time, there are also suggestions that this phenomenon is important even in the case of a single 2D scan of a fingerprint. Jin *et al.* [31] observed that even in a single 2D scan, the pores obtained by using a living finger look different than the pores obtained by using a fake finger because of the perspiration phenomenon. The perspiration phenomenon is utilised by Tan and Schuckers in [33]. The authors obtain a skeleton of the ridge structure and afterwards extract the ridge signal determined by this skeleton. The signal is later analysed by using wavelets and classified in order to distinguish between the fake and the living fingers. In their other paper, Tan and Schuckers [34] also analyse the middle ridge signal obtained from the centres of the ridges by means of the ridge structure skeleton. Owing to the perspiration phenomenon, the middle ridge signal obtained from a living finger is of a periodic nature determined by the periodic occurrence of the active sweat pores. Owing to the absence of the sweating process, the middle ridge signals obtained from the fake and the cut-off fingers do not exhibit this significantly periodic nature. In addition to the middle ridge signal analysis, the method analyses the middle valley signal that has also been observed to differ between the living and the fake fingerprint scans. Marasco and Sansone [26] propose an approach that combines the multiple static features based both on perspiration and the differences between the morphologies of the living and the fake

IET Biom., 2014, Vol. 3, Iss. 4, pp. 219–233
doi: 10.1049/iet-bmt.2013.0020

fingers. They extract the features based on the multiple first-order image statistics, the spacing between the sweat pores, the grey-level intensity ratios and the noise residue that is acquired by subtraction of the original and the denoised fingerprint scan. In addition to the ridge signal analysis discussed above, Marasco and Sansone [32] use several first-order statistics as the features for the classification process. They also use the multiple features based on the pixel grey-level intensities. Their approach is based on the assumption that the living fingers have less uniform grey-levels along the ridges compared with the fake fingers and also the contrast between the ridges and the valleys is higher in case of genuine living fingers. They also calculate the ratios between the brighter and the darker pixels of the acquired fingerprint scan and analyse the noise residue obtained by application of the wavelet-based approach.

Surface coarseness: Moon *et al.* [35] suggested an approach based on another difference between the fingerprint scans obtained from the living fingers in comparison to the fake fingerprint scans. They claim that the large molecules of the materials used to produce the fake fingerprints tend to agglomerate causing the surface of the resulting fake to be somewhat coarser compared with the original living finger. They apply the wavelet-based denoising procedure on the fingerprint scan, and calculate the noise residue by subtracting the original and the denoised image from each other. The properties of this noise residue are analysed for liveness detection purposes. A similar approach was taken by Pereira *et al.* [36]. The authors tried to apply the surface coarseness analysis for the classical fingerprint scanner resolution of 500 dpi.

General texture analysis and feature fusion: Nikam and Agarwal have published several methods based on the statistical analysis of the fingerprint scans. They have experimented with features based on a combination of the grey-level co-occurrence matrices (GLCMs) and the wavelet transform [37], the Ridgelet transform [38, 39], the Gabor filters [40] and the Curvelet transform [41]. In addition, they tried to obtain the features by application of the local binary patterns along with the wavelet transform [42]. By using the above mentioned approaches, they obtained a large number of features that could be used to distinguish between the live and the fake fingers. They reduce the number of features by means of the principal component analysis or the sequential forward floating selection (SFFS) and classify the fingerprint scans into live and fake by using a hybrid classifier based on neural networks, SVMs or the AdaBoost technique. Pereira *et al.* [43] have combined a number of features that have been suggested by the previous research. They use individual pore spacing, residual noise, multiple features based on the first-order image statistics, features based on the ratios between the darker and the brighter pixels and features based on the strength and the clarity of the ridge structure. The initial variety of features is reduced by application of the SFFS technique and the classification is performed using a MLP neural network and a SVM. Coli *et al.* [44] also analyse the fingerprints in the spectral domain. They report that the energies of the high frequency bands are useful in distinguishing between the fake and the genuine living fingers, because the fake fingers do not preserve the high frequency details of the living fingers. Galbally *et al.* [45] proposed a detection method based on the analysis of the multiple quality oriented features in the fingerprint scans. They extract the features based on the continuity and the smoothness of the ridge flow in the good quality fingerprints along with the features describing the overall and the local clarity of the ridge structure. The classification is performed by using the linear discriminant analysis method.

4.2.2 Dynamic methods: Another group of software-based liveness detection methods try to distinguish between the living and the fake fingers by analysing the time series of the fingerprint images acquired during the scanning phase, rather than analysing a single 2D scan only. These methods can make use of any of the above discussed static features, but they also utilise the differences between the frames in the time series.

Skin distortion: Antonelli *et al.* [47] have proposed a dynamic liveness detection approach based on the skin distortion. During the fingerprint acquisition, the biometric capture subject is required to slightly rotate the finger in the counterclockwise direction. A series of images are obtained during the rotation process. Optical flows are calculated in the acquired sequence and distortion maps are obtained. They compare the distortion codes acquired in the enrolment phase with the distortion codes obtained in the identification phase in order to identify whether a finger of the enrolled individual was used. Jia *et al.* [46] use an approach that does not require any special behaviour from the capture subject. A series of images is acquired when the subject puts his finger onto the sensor as illustrated by Fig. 5. The authors extract the features based on the area of the fingerprint that is in contact with the sensor. The features describe how the scan of the contact area changes in size and brightness when the finger is being put on the sensor. They use a classifier based on the Fisher linear discriminant analysis. Zhang *et al.* [48] have published a dynamic software liveness detection method based on fingerprint deformation analysis by using the thin-plate spline (TPS) model. The method requires the capture subject to put the finger on the sensor surface, and then apply some pressure in four different directions. The method uses a minutiae-based algorithm to detect the corresponding minutiae between the distorted fingerprint images and the undistorted fingerprint. Distortions of the minutiae positions are used to calculate the TPS models of the distortions and the bending energy vectors are extracted. The bending energy vectors are compared with the

Fig. 5 *Time-series of the fingerprint scans [46]*

pre-trained fuzzy set of the bending energies in order to distinguish the genuine living fingers from the fake ones.

Perspiration: A relatively widely researched approach to the dynamic software-based liveness detection is the analysis of the perspiration phenomenon that was already mentioned above for the static approaches. When a living finger is put on the surface of a fingerprint sensor, the fingerprint scan slightly changes in time because of the moisture produced by the sweat glands. This moisture pattern is analysed across the scans obtained in multiple time points in order to verify that a genuine living finger is put on the sensor. This phenomenon is a possible means of separation, because the fake and even the cut-off fingers do not produce similar patterns when scanned by the sensor. One of the early research papers on the perspiration phenomenon for liveness detection was conducted by Derakhshani *et al.* [49] with emphasis on the capacitive fingerprint sensors. They capture two fingerprint images at time points 0 and 5 s and compare the middle ridge signals extracted from them. They observed that the middle ridge signal of the first scan is of a much more wavy nature because of the spreading of the moisture. They extract the features based on these differences along with a feature that describes the amount of energy of the expected frequency of pore occurrence. Finally, they use a classifier based on a back-propagation neural network in order to distinguish between the genuine living fingers and the cut-off and the fake ones. The method is further improved by Parthasaradhi *et al.* [50] by addition of features that deal with the situation when a fingerprint signal goes out of the dynamic range of the sensor because of extreme dryness/moisture. They tested the method with the electro-optical and the optical sensing technologies in addition to the capacitive sensing technology only. They have performed further experiments with the classifiers based on neural networks, discriminant analysis and OneR method.

Abhyankar and Schuckers [51] have also utilised the wavelet analysis for perspiration-based liveness detection. They capture two consecutive images at 0, 2 s and analyse the differences between them (Fig. 6). They decompose the low-frequency content of the image by using the multi-resolution analysis and the high-frequency content by using the wavelet packet analysis. From all the resulting subbands, they filter out the low-energy coefficients to keep only the most significant information. Afterwards, they compute the difference between the transformation of the first fingerprint image and the transformation of the last fingerprint image in order to obtain a representation of the changes because of the perspiration phenomenon. From this representation of the difference between the two images, only significant coefficients representing larger changes are kept. The classification is performed based on the total energy of the remaining coefficients. Jia and Cai [52] have combined the features based on skin elasticity with the features determined by the perspiration phenomenon. The method operates with a series of multiple fingerprint images taken in a time period of a few seconds. They extract one feature analysing the energies of the spatial frequencies of the pore occurrences in the middle ridge signal in a way similar to [49]. The second static feature is based on the grey-level distributions. The first two dynamic features are based on the change of the fingerprint area in contact with the sensor surface during the time sequence, and the third dynamic feature is based on the comparison of the 'bumpiness' between the middle ridge signal of the two consecutive fingerprint scans as in [49]. Decann *et al.* [53] have published a fingerprint liveness detection algorithm that utilises an adaptation of the standard computer vision region labelling technique. In the first step, they obtain the skeletons of the fingerprint ridge structure and the fingerprint valley structure. Afterwards, the difference image between the scans that have been acquired at subsequent points in time, is computed. By using the mask, the region labelling algorithm is run starting from the points along the fingerprint skeletons. The result of this step is a set of small regions along the ridges and the valleys in the difference image as based on the image intensities. The region labelling approach can be applied also to a single binarised fingerprint image rather than a difference image. The extracted features used for classification are based on the numbers of such small regions, their size distribution and so on. Nikam and Agarwal [54] have published a method of distinguishing between the live and the fake fingers as based on the wavelet analysis of the middle ridge signal. They compute the middle ridge signals of the two consecutive fingerprint images as determined by the skeleton of the ridge structure, and then apply the wavelet analysis on the two obtained signals. Various classification features are extracted as based on the differences between the coefficients in the obtained subbands. Marcialis *et al.* [55] have proposed a method based on detection of the sweat pores in two consecutive fingerprint scans captured at 0 and 5 s. They extract a skeleton of the ridge structure and along this skeleton they search for the sweat pores by using the template comparison method. The pore extraction is done both for the first and the second fingerprint scan. The classification features are based on the differences of the pore quantities between the two scans and on the distances of the pores from each other. Standard fingerprint quality measures are also added to the classification feature set. Memon *et al.* [56] suggest a method for detection of the active sweat pores in the high-resolution fingerprint sensors (>800 dpi). They filter the fingerprint image by using a high-pass filter to obtain high frequency information associated with the small patterns expressed by the active sweat pores. The resulting image is then correlated with a correlation filter that represents a usual response of an active sweat pore. The obtained local maxima that are higher than a given threshold are considered to represent the active sweat pores. Abhyankar and Schuckers [57] have proposed a liveness detection method based on analysis of the signal changes between the so called singular points that can be detected in a fingerprint scan. The singular points are points in a fingerprint scan that have specific properties in the spatial domain and in different scales when analysed by the wavelet analysis. The singular points are

Fig. 6 *Fingerprint images acquired*
a Immediately
b After 2 s [51]

IET Biom., 2014, Vol. 3, Iss. 4, pp. 219–233
doi: 10.1049/iet-bmt.2013.0020

detected in two consecutive fingerprint scans taken at 0 and 2 s. Afterwards, the singular points are linked across the two images. The linking is mapped into the time domain by using B-spline interpolation and further analysed by using the empirical mode decomposition method. The classification is based on the energies of the decomposed signals.

4.3 Hardware-based liveness detection

Various ideas have been behind the introduction of an improved fingerprint sensing technology or an update to the existing hardware designs in order to make the sensors difficult to deceive.

Challenge/response: Yau *et al.* [58] have proposed a challenge/response-based liveness detection method for the fingerprint sensing technologies. The sensor is equipped with an electrode array that is capable of generating electric pulses that are transferred into the fingertip of the biometric capture subject. Depending on which electrodes are activated, the array can make the subject feel an impression of a tactile pattern underneath his finger. To successfully accept the finger, the capture subject must verify the pattern by choice of an offered visual pattern on a screen. The idea is that by using fake fingers the electro-tactile pattern will not be perceivable making the authentication impossible.

Odour: Baldisserra *et al.* [59] have suggested the usage of an electronic noise to distinguish between the live and the fake fingers. The living fingers are expected to express different odour than the fake fingers, rendering the odour analysis a suitable means of separation. The authors have experimented with electronic noses in order to distinguish between the genuine fingers and the fake fingers made of latex, gelatin and silicone.

Pulse oximetry: Another idea about how to perform the liveness detection by using special hardware is to use the pulse oximetry approach. For the living fingers, blood circulates through the tissues. The oxygenated haemoglobin in the blood carries oxygen to the cells, and becomes deoxygenated afterwards. New oxygenated haemoglobin is periodically brought to the tissues with every heartbeat. The research has shown that oxygenated haemoglobin strongly absorbs light of wavelengths of about 940 nm, whereas the deoxygenated haemoglobin has the strongest light absorption of about 660 nm [60]. Pulse oximetry is based on an analysis of the periodic changes in the absorption of light of the two wavelengths that take place in the tissue because of blood circulation as illustrated by Fig. 7. The principle of absorption of the two wavelengths by haemoglobin is also utilised in biometric vein imaging.

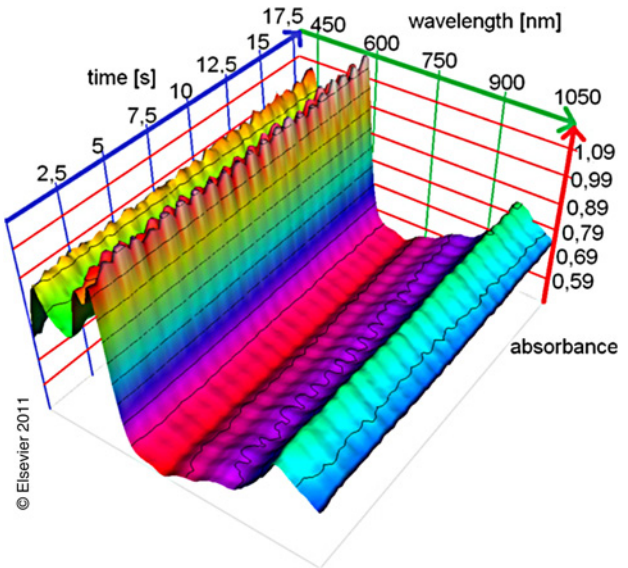

Fig. 7 *Changes of the light absorption because of blood circulation [61]*

Reddy *et al.* [60] have proposed a pulse oximetry-based method of the fingerprint liveness detection. In their design, the finger is illuminated by two LEDs of wavelengths of 660 and 940 nm, respectively. The light is captured by a single sensor. To distinguish between the responses as determined by the two light sources, the activity of the LEDs is modulated in time. Periodical changes in the absorption of light from the two sources are analysed in order to identify whether a genuine living finger is being scanned. Hengfoss *et al.* [61] have analysed the absorption of light of various wavelengths in the living and the fake/cadaver fingers by using a spectrometer. They have also analysed the periodic changes of the light absorption in time, because of the blood circulation. They have observed that the fake/cadaver fingers do not express this periodic pattern.

Multi-spectral properties: Analysis of the fingertips under the multi-spectral circumstances is another way of dealing with the problem of fingerprint liveness detection. The genuine living finger is made of tissues that generally do not have the same properties as the fake/cut-off fingers when illuminated by various wavelengths of light. Analysis of the fingerprint scans obtained by using multiple wavelengths of light is a possible classification approach. The multi-spectral design described by Rowe *et al.* [12] is utilised in the LUMIDIGM technology [62]. The sensor acquires multiple images of the fingertip under various illumination conditions, as regards the wavelength, the orientation and the polarisation of the light emitted. The captured images depict the fingertip at various depths and with variations depending on the different absorption of the individual wavelengths in the fingertip [12]. The liveness detection is performed by the analysis of these scans. Another possibility is to illuminate the finger by a multi-spectral light source, and analyse the whole transmission/reflectance signature in the range of the spectrum. Hengfoss *et al.* [61] have published an extensive analysis of the multi-spectral signatures of the living against the fake/cadaver fingers. They emphasise another interesting phenomenon that is a possible means of classification. When a living finger is put on the surface of the sensor and some pressure is applied, the blood is pressed away from the tissues. This process is observable on the change of the multi-spectral signature in time. The authors report that this phenomenon appears only for the genuine living fingers and not for the fake or cadaver ones. The multi-spectral signature also changes in time because of blood circulation in the tissues. These two dynamic features are possible means of separation along with the static features extracted from a single multi-spectral signature. Chang *et al.* [63] acquire multiple fingerprint images by using the light of the wavelengths in 400–850 nm. Edge detection is performed on each of these images. The energies of the fingerprint scans obtained by using various wavelengths and the edges detected in the images are used as the features for classification.

Heartbeat movements: Some research has been conducted on the detection of the fine movements of the living fingers because of heartbeat. These approaches utilise the fact that

the heartbeat causes periodic slight volumetric changes of the tissues [64]. Drahansky *et al.* [64] suggest the usage of a high-resolution camera to detect the distances between the specific points on the fingerprint as they change in time, and use the resulting signal as a liveness detection measure. As another possibility of making use of the same principle of periodic volumetric changes, they propose distance measurements by using a laser.

Electrical properties: Another idea is to use the difference in the electrical properties of the living skin compared with the fake materials. Martinsen *et al.* [65] have used an electrode array to measure the impedance of the fingerprint tissue. The system performs liveness detection by means of multiple measurements by using different electrodes on the array. In addition, the frequency properties of the signal to which the tissue is exposed vary during the measurement process. The authors claim that the electrodes that are farther apart from each other on the array cause the internal tissues to have larger influence on the resulting impedance. In this way, by comparison of the results from different electrodes with different distances from each other, they can indicate the presence of a living fingertip with a multi-layer structure of the living skin. Shimamura *et al.* [66] suggested a way of how to integrate a fake fingerprint detection module into a capacitive fingerprint sensor. Their fraud detection method is based on the impedance measurements.

Optical coherence tomography (OCT): Some research has been conducted on the application of the OCT for the fingerprint sensing scenario. The OCT is a medical imaging method widely used for retina scanning. The technology utilises the interference of beams of light of low coherence length in order to measure the reflectance of the scanned material at different positions and depths. In this way, a volumetric scan of the material can be acquired. Owing to the general scattering of the light as it travels deeper into the tissue, this method can penetrate the surface to a maximum depth of about 3 mm. Cheng and Larin [67] have applied the OCT for fingerprint liveness detection by using the autocorrelation analysis. They obtained 2D in-depth scans of a part of the fingertip in the x direction (2.4 mm) and the z direction (2.2 mm). Afterwards, they computed an autocorrelation function in the depth direction. They have demonstrated that the obtained autocorrelation function is very different for the case of the living and the fake fingers. Cheng and Larin [68] were also among the first to obtain the 3D density representations of the real and the fake fingerprints obtained by the OCT technology, and to experiment with these scans. In their paper, they also publish a 3D OCT scan of a fake fingerprint surface on a real living finger. The dimensions of the scanned volume are $1.6 \times 2.4 \times 10$ mm. Peterson and Larin [69] have experimented with various neural network-based approaches in order to perform classification of the fingertip OCT scans into the living and the fake samples. They use the features based on various first-order image statistics and Gabor filter responses. Dimensionality of the vector of the Gabor filter responses is reduced by using the self-organising maps approach. The application of the OCT technology for the fingerprint liveness detection scenario is summarised in [63]. Nasiri-Avanaki *et al.* [70] have also published a paper that demonstrates the usability of OCT scanning for distinguishing between the genuine living fingers and the fake ones. Bossen *et al.* [71] have demonstrated that the inner and the outer fingerprint extracted from an OCT scan can be used for classification by using the standard fingerprint comparison methods. In a paper developed under the supervision of Ralph Breithaupt from the German Federal Office for Information Security (BSI), Menrath [72] proposes methods for the detection of sweat glands, as well as an approach for extraction of the outer and the inner fingerprint from an OCT scan. Sousedik *et al.* [27] have proposed an automatic method for detection of the layered structure in an OCT fingerprint scan and experimented with the classification of the scans into fake and genuine ones.

5 Liveness detection performance

A benchmark of the previously mentioned methods is difficult. Although the metrics needed for such a benchmark are now introduced by the international standardisation project ISO/IEC 30107 [18], there is not yet a ground truth database. Most of the authors have produced their own databases of the fake and the living fingers as a part of their research work. The databases vary in the size of the sets, in the methods used to create the fake fingers, and in the usage of the cadaver fingers. Some authors evaluate their methods by using fake fingers created by using the 'direct casting' methods, some add also fakes produced by means of the 'indirect casting' methods. The usage of the materials for fabrication of the fake fingerprints and mould materials also vary between the authors and the publications. Since the quality of a fake fingerprint strongly influences the performance of a liveness detection method, it is challenging to conduct a fair assessment based on the results obtained on such widely varying data. The sensor that has been used for data acquisition is another variable in the evaluation datasets. Only some of the software-based methods have been tested with multiple sensor technologies. Different detection rates on different sensing technologies suggest that the sensor technology that has been used for data acquisition is of significant importance. It is difficult to say whether the features would perform well on another sensing technology.

In addition, the static and the dynamic software approaches require different inputs – the static approaches make use of a single fingerprint scan, whereas the dynamic approaches need a time series of images. Various static software-based methods have different requirements on the image resolution, and can relate to a specific sensor technology that produces the patterns detected by the method. The dynamic approaches have to deal with different resolution requirements, and also with varying requirements on the time-sequence analysed. Although some methods make use of two consecutive images (obtained at various intervals), the other methods use a series of multiple images obtained at a given frame rate.

These varying requirements on the input fingerprint data analysed make the development of a standard evaluation database rather difficult, even for the software-based approaches. The development of a database that would be applicable to testing of the hardware-based approaches would be even more difficult.

Nevertheless, there have been attempts to create such standardised dataset for evaluation of the software-based liveness detection approaches. In 2009, Marcialis *et al.* [73] organised the first international fingerprint liveness detection competition, LivDet 2009. The competition makes it possible for researchers and companies to submit their algorithms for evaluation on a large-scale standardised dataset of the fingerprints obtained both from the living and the fake fingers. The dataset consists of a large number of

IET Biom., 2014, Vol. 3, Iss. 4, pp. 219–233
doi: 10.1049/iet-bmt.2013.0020

scans from three different optical fingerprint scanners. A subset of 25% of the data was made available as a training set before final submission and evaluation by using the remaining 75% of the data. Detailed information about the datasets used in LivDet 2009 is listed in Table 2. The single-scan nature of the dataset used in LivDet 2009 makes the competition relevant only for the static software-based liveness detection approaches.

Four different algorithm solutions were evaluated by LivDet 2009. The best performing algorithm was submitted by Dermalog Identification Systems GmbH. The second was an academic solution from Galbally *et al.* [45]; and the two last algorithms were from two anonymous sources. In this paper, the results are presented in terms of the ISO/IEC 30107 metrics, namely false non-live detection rate (FNLDR) and false live detection rate (FLDR). The FNLDR metric represents the proportion of the live presentation characteristics incorrectly classified as being non-live, whereas the FLDR metric represents the proportion of the non-live presentation characteristics incorrectly classified as being live. The paper published by LivDet 2009 [73] mentioned an unusually high FNLDR of the evaluated algorithms on the set of the genuine living fingers from the Biometrika sensor (Table 3). The lower number of distinct live subjects in the training set for the Biometrika dataset, was mentioned as a possible explanation (Table 4). Table 4 also demonstrates the large effect of the sensor on the classification accuracy. Even though all the sensors were optical, large differences in liveness detection performance of the same methods were recorded.

Another run of the liveness detection competition was organised by Yambay *et al.* [15] in 2011. This time, the competition consisted of two parts – algorithms and systems. Similar to LivDet 2009, the algorithm part allowed the academics and the companies to submit their static liveness detection solution for the fingerprints. The new system part of the competition provided a framework for evaluation of the hardware-based solutions. The competitors could submit their hardware solution to the competition, and the performance of the system was evaluated by using a unified protocol that allowed for a fair benchmark of the systems' performance.

The software-based part of the competition was evaluated by using a large-scale dataset obtained by using four different fingerprint sensing devices – Biometrika, Digital Persona, Italdata and Morpho (formerly Sagem). A more detailed description of the datasets is given in Table 5.

Four thousand fingerprint images per fingerprint device were acquired (2000 spoof samples and 2000 live samples). The fake fingerprints used for collections for the dataset were made of gelatin, latex, PlayDoh, silicone and wood glue for the Digital Persona sensor and the Morpho sensor. The fake fingerprints used with the Biometrika and the ItalData sensors were made of gelatine, latex, ecoflex (platinum-catalysed silicone), silicone and wood glue. Details about the numbers of samples obtained by using genuine living fingers per sensing device are given in Table 6.

Table 4 Number of unique subjects in LivDet 2009 (Indentix and Crossmatch samples acquired in multiple sessions, Biometrika samples acquired in a single session) [73]

Scanners	No. of training subjects	No. of testing subjects	Aver images/ subject
Identix	35	125	18.75
Crossmatch	63	191	15.75
Biometrika	13	37	40.0

Table 5 Datasets used in LivDet 2011 [15]

Dataset	Sensor	Sensor model	Resolution, dpi	Image size
#1	Biometrika	FX2000	500	315 × 372
#2	Digital persona	4000B	500	355 × 391
#3	ItalData	ET10	500	640 × 480
#4	Morpho	MSO300	500	352 × 384

Table 6 Datasets used in LivDet 2011 [15]

Dataset	Sensor	Live training samples	Live testing samples	No. of fingers
#1	Biometrika	1000	1000	200
#2	Digital persona	1000	1000	200
#3	ItalData	1000	1000	200
#4	Morpho	1000	1000	112

Table 2 Datasets used in LivDet 2009 [73]

Dataset	Scanners	Model no.	Resolution, dpi	Image size	Live samples	Fake samples
dataset 1	Crossmatch	Verifier 300 LC	500	480 × 640	2000	2000
dataset 2	Identix	DFR2100	686	720 × 720	1500	1500
dataset 3	Biometrika	FX2000	569	312 × 372	2000	2000

Table 3 Classification results of the algorithms submitted to LivDet 2009 [73] reported with the FNLDR and the FLDR

Submitted	Identix		Crossmatch		Biometrika		Average	
Algorithms	FNLDR, %	FLDR, %	FNLDR, %	FLDR, %	FNLDR, %	FLDR, %	FNLDR, %	FLDR, %
dermalog	2.7	2.8	7.4	11.4	74.1	1.9	20.1	5.4
ATVS	9.8	3.1	8.8	20.8	71.7	3.1	30.1	9.0
anonymous	15.2	11.5	27.1	18.9	56.0	17.6	32.8	16.0
anonymous2	9.8	11.3	14.4	15.9	15.6	20.7	13.2	16.0

Three software-based liveness detection solutions were submitted to the algorithm part of the LivDet 2011 competition. The solutions were provided by the Chinese Academy of Sciences, the Institute of Automation (CASIA); Federico II University (Federico); and Dermalog Identification Systems GmbH (Dermalog). Detailed information about the performance of these algorithms on the large-scale datasets collected for LivDet 2011 is listed in Table 7. The results again demonstrate a strong variation in the classification accuracy depending on the sensor that was used for data acquisition. The benchmarks from LivDet 2009 and 2011 do not demonstrate the improvement of the liveness detection capabilities. The results suggest that the quality of the fake finger and its fabrication technique have a very significant influence on the performance of the methods, rendering the methods vulnerable to novel fake fabrication techniques and approaches.

The performance evaluation of the liveness detection capabilities of the fingerprint recognition systems submitted to LivDet 2011 is shown by Table 8. The FLDR known represents the false live detection rate for the fake fingerprints produced by using the recipes published in the competition description. The FLDR unknown represents the false live detection rate for the fake fingerprints produced by using the recipes that were not published in the competition description. The error rates in Table 8 suggest that the performance of the methods is strongly affected by the particular fake fingers used for the spoofing attempt. The fake finger fabrication techniques that were unknown prior to the development of the methods or variations of the known techniques could pose a significant security risk.

Ghiani *et al.* [74] have used the large-scale database produced in the scope of the LivDet 2011 competition to evaluate the performance of several existing liveness detection algorithms on a single dataset. They have benchmarked the performance of the methods based on the local binary patterns, the detection of the pores [55], the power spectrum [44], the wavelet energy signature [42], the wavelet analysis of the ridge signal [33], the valley noise analysis [30], the curvelet energies [41] and the GLCMs [41]. The benchmark results for the analysed methods are shown by Tables 9 and 10.

Marcialis *et al.* [75] have performed additional testing of the above mentioned liveness detection approaches with various regions of interest and under various data acquisition conditions. Coli *et al.* [76] have experimented with various liveness detection features and evaluated their classification performance.

For the cases when the self-declared performance scores could be interpreted in terms of the ISO/IEC 30107 FNLDR and FLDR metrics, the self-declared scores of the above discussed methods are included in Table 11.

A relatively large performance gap can be observed if the performance scores reported by the authors are compared

Table 8 Classification results of the systems submitted to LivDet 2011 [15] reported with the FNLDR and the FLDR

Submitted systems	FLDR, %	FNLDR, %	FLDR known, %	FLDR unknown, %
Dermalog	0.8	42.5	0.4	1.3
Greenbit	39.5	38.8	19.1	70

Table 9 FLDR of the methods as evaluated by Ghiani *et al.* [74]

	Biometrika, %	Italdata, %	Digital persona, %	Morpho, %
LBP	16.40	15.10	8.70	4.34
pores detection [55]	27.80	22.00	30.50	49.90
power spectrum [44]	23.90	29.40	23.50	21.81
wavelet energy [42]	73.00	51.80	15.10	16.22
ridges wavelet [33]	47.10	63.10	37.00	18.15
valleys wavelet [30]	48.60	39.10	12.40	55.12
curvelet energy [41]	55.10	40.70	27.40	39.58
curvelet GLCM [41]	16.40	25.20	22.00	25.00

Table 10 FNLDR of the methods as evaluated by Ghiani *et al.* [74]

	Biometrika, %	Italdata, %	Digital persona, %	Morpho, %
LBP	5.90	22.00	12.60	12.70
pores detection [55]	26.90	35.30	41.70	30.40
power spectrum [44]	37.40	56.20	30.80	41.20
wavelet energy [42]	27.40	41.80	13.00	27.90
ridges wavelet [33]	30.50	50.80	18.10	22.90
valleys wavelet [30]	9.40	8.20	13.70	9.00
curvelet energy [41]	35.30	55.10	16.40	17.50
curvelet GLCM [41]	29.40	36.30	14.70	31.10

Table 7 Classification results of the algorithms submitted to LivDet 2011 [15] reported with the FNLDR and the FLDR

	FNLDR			FLDR		
	Dermalog, %	Federico, %	CASIA, %	Dermalog, %	Federico, %	CASIA, %
Biometrika	11	38	29.7	29	42	38.1
ItalData	15.10	39.90	50.6	28.50	40.10	2.8
Morpho	15.10	13.80	22.1	12.50	13.10	23.6
Digital persona	66	6.20	16.1	6.20	11.60	34.7
average	35.30	26.60	29.625	17.60	24.50	24.8

doi: 10.1049/iet-bmt.2013.0020

Table 11 Scores obtained from the results as declared by the authors reported as the FNLDR and the FLDR

Method		FNLDR, %	FLDR, %
Nikam and Agarwal [41]		1.62	2.08
Nikam and Agarwal [37]		2.16	2.5
Nikam and Agarwal [40]		2.16	2.5
Espinoza and Champod [17]		8.3	21.2
Galbally *et al.* [45]	Biometrika	1.54	2.12
	CrossMatch	11.94	10.3
	Identix	7.07	6.4
Pereira *et al.* [43]	DB 1	7.35	2.42
	DB 2	13.68	4.52
Marasco and Sansone [32]	Biometrika	12.2	13.0
	CrossMatch	17.4	12.9
	Identix	8.3	11.0
Nikam and Agarwal [39]		1.62	3.33
Nikam and Agarwal [42]		1.62	3.33
Tan and Schuckers [30]	Precise	0	1.6
	Secugen	0	9
	Ethentica	0	7.4
	Biometrika	9.1	0
Marasco and Sansone [26]	Biometrika	12.2	13.0
	CrossMatch	17.4	12.9
	Identix	8.3	11.0
Decann *et al.* [53]		1.2	1.2
Tan and Schuckers [34]		0.9	0.9
Nikam and Agarwal [54]		2.08	0.9
Jia and Cai [52]		4.49	4.49
Antonelli *et al.* [47]		11.24	11.24
Zhang *et al.* [48]		4.5	4.5
Jia *et al.* [46]		4.78	4.78

with the results that were reported by the independent evaluations conducted by Ghiani *et al.* [74], LivDet 2009 [73] and LivDet 2011 [15]. The most recent results of LivDet 2013 [77] confirm that the liveness detection methods are vulnerable against the high-quality fake fingerprints that were created by using the 'direct casting' fake fabrication methods.

Both the authors and the independent evaluators report on the liveness detection performance concerning all the fake fabrication techniques, materials and individual fake fingerprints. The authors do not specify whether some individual fake fingerprints produced by specific techniques are generally more successful than others. Since the attacker typically needs only a single fake fingerprint to be able to deceive a specific liveness detection method successfully, such information is of crucial importance. The performance of the methods has been evaluated in terms of the resistance against well-known, low-cost fake fingerprint fabrication techniques, rather than against a targeted effort to spoof a specific fingerprint recognition system.

The performance of the state-of-the-art software fingerprint liveness detection methods suggests that additional hardware is necessary to develop a fingerprint liveness detection solution that would be resistant against targeted attacks. Owing to the large variety of possible artefact material and fabrication techniques, a single aspect dedicated liveness detection sensor can usually be deceived if an appropriate new combination of materials and techniques has been used [78]. To increase the difficulty of producing an artefact, some manufacturers try to include a larger number of supplementary sensors that would capture information on multiple aspects of the scanned characteristic. Even though this greatly increases the difficulty of the artefact fabrication process, the large variety of the properties of the genuine fingers, as well as their artefact counterparts, requires the application of machine learning approaches to process the information from all the sensors and take the final decision whether a genuine characteristic has been presented. Since the performance of the machine learning-based classifiers depends on the training data, the sensor can still be vulnerable if an entirely new material and fabrication technique has been used to produce the artefact characteristic.

A 3D scanning technology, such as OCT, can provide for a large amount of high-resolution data that would capture both the outer and the inner structure of the scanned finger. A reliable method that could verify the genuine structure of the fingertip scan could render the fake fabrication process extremely difficult or even practically impossible. Initial research on the potential of the OCT technology suggests that an OCT scan contains a highly detailed representation of the structure of the scanned fingertip that is sufficient to clearly distinguish between the genuine and the fake fingers [79].

6 Conclusion and future research

Even though the authors often claim very high performance scores allowing for the possibilities of direct practical application of their specific liveness detection method, the results of testing on large-scale datasets in the scope of LivDet 2009 [73], LivDet 2011 [15] and LivDet 2013 [77] suggest that the fingerprint liveness detection cannot be considered a solved problem yet. The results suggest that the performance of the methods strongly depends on the knowledge of the fake fabrication techniques and materials during the development of the method. So far, the methods have been tested rather in terms of the resistance against low-cost, well-known faking techniques than in terms of the resistance against targeted spoofing attacks.

The security of a system is given by the amount of effort needed to circumvent it. So far, most authors have reported the liveness detection performance of their methods as universal rates for all the fakes their method has been tested with. However, the detection performance can vary greatly as it depends on the specific fake type, and the mere quantities do not yield accurate information on the case.

In spite of the research effort so far, the state-of-the-art methods cannot be considered reliable in the environments that require high security levels. A 3D scanning technology, such as the OCT, can provide for highly detailed representations of the structure of a scanned fingertip and thus significantly increase the amount of information available for the liveness detection purposes. A reliable method, which was able to verify the genuine structure of the scan, would render the fake fabrication process extremely difficult. The development of such a method has the potential to provide for a very secure fingerprint recognition solution.

LivDet 2009 [73] and LivDet 2011 [15] provide for publicly available, large-scale standard datasets, which are nevertheless applicable only for the static software-based liveness detection methods. Apart from that, the methods tested on these datasets must be capable of working with the scan resolutions of the samples as those yielded by the sensors of the LivDet projects.

What is more, the methods tested on this dataset must be able to work with the scan resolutions of the samples yielded by the sensors used in the LivDet projects. Further initiative is necessary to create datasets of the high-resolution images obtained in the time series, to provide for a standardised dataset for testing of the dynamic

software-based liveness detection methods. The results are very sensitive to the quality and the fabrication method of the fake fingerprints used to spoof the sensor. Therefore the standard dataset should contain a large number of scans captured by using high-quality fake fingerprints.

The development of a database for the hardware-based liveness detection methods is difficult because of very large variations in the sensing methods. Possibly, a fake fingerprint toolbox could be developed and shared by the research community in order to be able to perform a more reliable benchmarking of the hardware-based methods.

The performance of the liveness detection methods might be improved if some liveness related information were stored in the biometric template itself. In this way, the variations of the finger properties would be reduced and it might also be more difficult to acquire the additional information for the fake fabrication.

The fingerprint alteration detection is in the state of initial research and further initiative is necessary in order to achieve general applicability in practice.

The metrics used by the PAD research community are rather arbitrary and in need of standardisation. Attempts have been made to introduce standards to the field of the PAD in the scope of the international standardisation project, ISO/IEC 30107. The development of a standardised framework for the evaluation of the liveness detection capabilities of the biometric systems constitutes a part of the projects, BEAT – Biometrics Evaluation and Testing [80], and TABULA RASA – Trusted Biometrics under Spoofing Attacks [81].

7 References

1 Han, Y., Ryu, C., Moon, J., Kim, H., Choi, H.: 'A study on evaluating the uniqueness of fingerprints using statistical analysis'. Information Security and Cryptology – ICISC 2004, 2005 (*LNCS*, **3506**), pp. 467–477

2 Zwiesele, A., Munde, A., Busch, C., Daum, H.: 'BioIS study. Comparative study of biometric identification systems'. Proc. 34th Annual Int. Carnahan Conf. on Security Technology, 2000, pp. 60–63

3 Espinoza, M., Champod, C., Margot, P.: 'Vulnerabilities of fingerprint reader to fake fingerprints attacks', *Forensic Sci Int.*, 2011, **204**, (1–3), pp. 41–49

4 Espinoza, M., Champod, C.: 'Risk evaluation for spoofing against a sensor supplied with liveness detection', *Forensic Sci. Int.*, 2011, **204**, (1–3), pp. 162–168

5 Galbally, J., Fierrez, J., Alonso-Fernandez, F., Martinez-Diaz, M.: 'Evaluation of direct attacks to fingerprint verification systems', *Telecommun. Syst.*, 2011, **47**, pp. 243–254

6 Kang, H., Lee, B., Kim, H., Shin, D., Kim, J.: 'A study on performance evaluation of the liveness detection for various fingerprint sensor modules'. Knowledge-Based Intelligent Information and Engineering Systems, 2003 (*LNCS*, **2774**), pp. 1245–1253

7 van der Putte, T., Keuning, J.: 'Biometrical fingerprint recognition: don't get your fingers burned'. Proc. IFIP TC8/WG8.8, 4thWorking Conf. on Smart Card Research and Advanced Applications, 2000, pp. 289–303

8 Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: 'Impact of artificial 'gummy' fingers on fingerprint systems'. Proc. SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002, vol. 4677, pp. 275–289

9 Wiehe, A., Søndrol, T., Olsen, O., Skarderud, F.: 'Attacking fingerprint sensors'. Technical report, NISlab/Gjovik Univ. College, 2004

10 Memon, S., Sepasian, M., Balachandran, W.: 'Review of finger print sensing technologies'. Proc. IEEE Int. Multitopic Conf. (INMIC), 2008, pp. 226–231

11 Sato, N., Machida, K., Morimura, H., *et al.*: 'MEMS fingerprint sensor immune to various finger surface conditions', *IEEE Trans. Electron Devices*, 2003, **50**, (4), pp. 1109–1116

12 Rowe, R.K., Nixon, K.A., Butler, P.W.: 'Multispectral fingerprint image acquisition', in Ratha, N., Govindaraju, V. (Eds.): 'Advances in Biometrics' (Springer, London, 2008), pp. 3–23

13 Lee, C., Lee, S., Kim, J.: 'A study of touchless fingerprint recognition system'. Structural, Syntactic, and Statistical Pattern Recognition, 2006 (*LNCS*, **4109**), pp. 358–365

14 Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: 'Handbook of fingerprint recognition' (Springer London, 2009, 2nd edn.), Ch. 9.5, pp. 386–391

15 Yambay, D., Ghiani, L., Denti, P., Marcialis, G., Roli, F., Schuckers, S.: 'LivDet 2011 – Fingerprint liveness detection competition 2011'. Proc. Fifth IAPR Int. Conf. on Biometrics (ICB), 2012, pp. 208–215

16 Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G., Roli, F.: 'Security evaluation of biometric authentication systems under real spoofing attacks', *IET Biometrics*, 2012, **1**, (1), pp. 11–24

17 Espinoza, M., Champod, C.: 'Using the number of pores on fingerprint images to detect spoofing attacks'. Proc. Int. Conf. on Hand-Based Biometrics (ICHB), 2011, pp. 1–5

18 International Organization for Standardization, ISO/IEC 5th WD 30107: 'Information Technology – Biometrics – Presentation attack detection', 2013

19 Coli, P., Marcialis, G.L., Roli, F.: 'Vitality detection from fingerprint images: a critical survey'. Proc. of the Int. Conf. on Advances in Biometrics (ICB '07), 2007, pp. 722–731

20 Feng, J., Jain, A., Ross, A.: 'Detecting altered fingerprints'. Proc. 20th Int. Conf. on Pattern Recognition (ICPR), 2010, pp. 1622–1625

21 Yoon, S., Feng, J., Jain, A.: 'Altered fingerprints: analysis and detection', *IEEE Trans. Pattern Anal. Mach. Intell.*, 2012, **34**, (3), pp. 451–464

22 Tiribuzi, M., Pastorelli, M., Valigi, P., Ricci, E.: 'A multiple kernel learning framework for detecting altered fingerprints'. Proc. 21st Int. Conf. on Pattern Recognition (ICPR), 2012, pp. 3402–3405

23 Yoon, S., Zhao, Q., Jain, A.: 'On matching altered fingerprints'. Proc. Fifth IAPR Int. Conf. on Biometrics (ICB), 2012, pp. 222–229

24 Petrovici, A., Lazar, C.: 'Identifying fingerprint alteration using the reliability map of the orientation field', *Ann. Univ. Craiova, Series Autom. Comput. Electron. Mechatronics*, 2010, **7**, (34), pp. 45–52

25 Petrovici, A.: 'Simulating alteration on fingerprint images'. Proc. IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2012, pp. 1–5

26 Marasco, E., Sansone, C.: 'Combining perspiration- and morphology-based static features for fingerprint liveness detection', *Pattern Recognit. Lett.*, 2012, **33**, (9), pp. 1148–1156

27 Sousedik, C., Breithaupt, R., Busch, C.: 'Volumetric fingerprint data analysis using optical coherence tomography'. Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG), 2013, pp. 1–6

28 Manivanan, N., Memon, S., Balachandran, W.: 'Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering', *Electron. Lett.*, 2010, **46**, (18), pp. 1268–1269

29 Choi, H., Kang, R., CHoi, K., Kim, J.: 'Aliveness detection of fingerprints using multiple static features'. Proc. World Academy of Science, Engineering and Technology, 2007, vol. 22

30 Tan, B., Schuckers, S.: 'New approach for liveness detection in fingerprint scanners based on valley noise analysis', *J. Electron. Imaging*, 2008, **17**, (1), pp. 011009–011009-9

31 Jin, C., Li, S., Kim, H., Park, E.: 'Fingerprint liveness detection based on multiple image quality features'. Information Security Applications, 2011 (*LNCS*, **6513**), pp. 281–291

32 Marasco, E., Sansone, C.: 'An anti-spoofing technique using multiple textural features in fingerprint scanners'. Proc. IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010, pp. 8–14

33 Tan, B., Schuckers, S.: 'Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing'. Proc. Computer Vision and Pattern Recognition Workshop (CVPRW '06), 2006, pp. 26

34 Tan, B., Schuckers, S.: 'Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise', *Pattern Recognit.*, 2010, **43**, (8), pp. 2845–2857

35 Moon, Y., Chen, J., Chan, K., So, K., Woo, K.: 'Wavelet based fingerprint liveness detection', *Electron. Lett.*, 2005, **41**, (20), pp. 1112–1113

36 Pereira, L., Pinheiro, H., Cavalcanti, G., Ren, T.I.: 'Spatial surface coarseness analysis: technique for fingerprint spoof detection', *Electron. Lett.*, 2013, **49**, (4), pp. 260–261

37 Nikam, S., Agarwal, S.: 'Wavelet energy signature and GLCM features-based fingerprint anti-spoofing'. Proc. Int. Conf. on Wavelet Analysis and Pattern Recognition (ICWAPR '08), 2008, vol. 2, pp. 717–723

38 Candes, E.J., Donoho, D.L.: 'Ridgelets: a key to higher-dimensional intermittency?', *Philos. Trans. Lond. R. Soc.*, 1999, **357**, pp. 2495–2509

39 Nikam, S.B., Agarwal, S.: 'Ridgelet-based fake fingerprint detection', *Neurocomputing*, 2009, **72**, (10–12), pp. 2491–2506

doi: 10.1049/iet-bmt.2013.0020

40 Nikam, S., Agarwal, S.: 'Gabor filter-based fingerprint anti-spoofing'. Advanced Concepts for Intelligent Vision Systems, 2008 (*LNCS*, **5259**), pp. 1103–1114
41 Nikam, S., Agarwal, S.: 'Fingerprint liveness detection using curvelet energy and co-occurrence signatures'. Proc. Fifth Int. Conf. on Computer Graphics, Imaging and Visualisation (CGIV '08), 2008, pp. 217–222
42 Nikam, S., Agarwal, S.: 'Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems'. Proc. First Int. Conf. on Emerging Trends in Engineering and Technology (ICETET '08), 2008, pp. 675–680
43 Pereira, L., Pinheiro, H., Silva, J., *et al.*: 'A fingerprint spoof detection based on MLP and SVM'. Proc. Int. Joint Conf. on Neural Networks (IJCNN), 2012, pp. 1–7
44 Coli, P., Marcialis, G., Roli, F.: 'Power spectrum-based fingerprint vitality detection'. Proc. IEEE Workshop on Automatic Identification Advanced Technologies, 2007, pp. 169–173
45 Galbally, J., Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J.: 'A high performance fingerprint liveness detection method based on quality related features', *Future Gener. Comput. Syst.*, 2012, **28**, (1), pp. 311–321
46 Jia, J., Cai, L., Zhang, K., Chen, D.: 'A new approach to fake finger detection based on skin elasticity analysis'. Proc. ICB, 2007, pp. 309–318
47 Antonelli, A., Cappelli, R., Maio, D., Maltoni, D.: 'Fake finger detection by skin distortion analysis', *IEEE Trans. Inf. Forensics Sec.*, 2006, **1**, (3), pp. 360–373
48 Zhang, Y., Tian, J., Chen, X., Yang, X., Shi, P.: 'Fake finger detection based on thin-plate spline distortion model'. Advances in Biometrics, 2007 (*LNCS*, **4642**), pp. 742–749
49 Derakhshani, R., Schuckers, S., Hornak, L.A., O'Gorman, L.: 'Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners', *Pattern Recognit.*, 2003, **36**, (2), pp. 383–396
50 Parthasaradhi, S., Derakhshani, R., Hornak, L., Schuckers, S.: 'Time-series detection of perspiration as a liveness test in fingerprint devices', *IEEE Trans. Syst. Man Cybern. C, Appl. Rev.*, 2005, **35**, (3), pp. 335–343
51 Abhyankar, A., Schuckers, S.: 'Integrating a wavelet based perspiration liveness check with fingerprint recognition', *Pattern Recognit.*, 2009, **42**, (3), pp. 452–464
52 Jia, J., Cai, L.: 'Fake finger detection based on time-series fingerprint image analysis'. Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, 2007 (*LNCS*, **4681**), pp. 1140–1150
53 Decann, B., Tan, B., Schuckers, S.: 'A novel region based liveness detection approach for fingerprint scanners'. Proc. Third Int. Conf. on Advances in Biometrics (ICB '09), 2009, pp. 627–636
54 Nikam, S.B., Agarwal, S.: 'Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection', *Int. J. Inf. Comput. Sec.*, 2009, **3**, (1), pp. 1–46
55 Marcialis, G., Roli, F., Tidu, A.: 'Analysis of fingerprint pores for vitality detection'. Proc. 20th Int. Conf. on Pattern Recognition (ICPR), 2010, pp. 1289–1292
56 Memon, S., Manivannan, N., Balachandran, W.: 'Active pore detection for liveness in fingerprint identification system'. Proc. Telecommunications Forum (TELFOR), 2011 19th, 2011, pp. 619–622
57 Abhyankar, A., Schuckers, S.: 'Modular decomposition of fingerprint time series captures for the liveness check', *Int. J. Comput. Electr. Eng.*, 2010, **2**, pp. 426–431
58 Yau, W.Y., Tran, H.L., Teoh, E.K.: 'Fake finger detection using an electrotactile display system'. Proc. Tenth Int. Conf. on Control, Automation, Robotics and Vision (ICARCV 2008), 2008, pp. 962–966
59 Baldisserra, D., Franco, A., Maio, D., Maltoni, D.: 'Fake fingerprint detection by odor analysis'. Advances in Biometrics, 2005 (*LNCS*, **3832**), pp. 265–272
60 Reddy, P., Kumar, A., Rahman, S., Mundra, T.: 'A new antispoofing approach for biometric devices', *IEEE Trans. Biomed. Circuits Syst.*, 2008, **2**, (4), pp. 328–337
61 Hengfoss, C., Kulcke, A., Mull, G., Edler, C., Püschel, K., Jopp, E.: 'Dynamic liveness and forgeries detection of the finger surface on the basis of spectroscopy in the 400–1650 nm region', *Forensic Sci. Int.*, 2011, **212**, (1–3), pp. 61–68
62 LUMIDIGM: 'http://www.lumidigm.com/technology/'
63 Chang, S., Larin, K., Mao, Y., Almuhtadi, W., Flueraru, C.: 'Fingerprint spoof detection by NIR optical analysis', in Yang, J. (Ed.): 'State of the art in Biometrics' (InTech, 2011)
64 Drahansky, M., Notzel, R., Funk, W.: 'Liveness detection based on fine movements of the fingertip surface'. Proc. IEEE Information Assurance Workshop, 2006, pp. 42–47
65 Martinsen, O., Clausen, S., Nysaether, J., Grimnes, S.: 'Utilizing characteristic electrical properties of the epidermal skin layers to detect fake fingers in biometric fingerprint systems – a pilot study', *IEEE Trans. Biomed. Eng.*, 2007, **54**, (5), pp. 891–894
66 Shimamura, T., Morimura, H., Shimoyama, N., *et al.*: 'Impedance-sensing circuit techniques for integration of a fraud detection function into a capacitive fingerprint sensor', *IEEE Sens. J.*, 2012, **12**, (5), pp. 1393–1401
67 Cheng, Y., Larin, K.V.: 'Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis', *Appl. Opt.*, 2006, **45**, (36), pp. 9238–9245
68 Cheng, Y., Larin, K.: 'In vivo two- and three-dimensional imaging of artificial and real fingerprints with optical coherence tomography', *IEEE Photonics Technol. Lett.*, 2007, **19**, (20), pp. 1634–1636
69 Peterson, L.E., Larin, K.V.: 'Image classification of artificial fingerprints using Gabor wavelet filters, self-organising maps and Hermite/Laguerre neural networks', *Int. J. Knowl. Eng. Soft Data Paradigms*, 2009, **1**, (3), pp. 239–256
70 Nasiri-Avanaki, M.R., Meadway, A., Bradu, A., Khoshki, R.M., Hojjatoleslami, A., Podoleanu, A.G.: 'Anti-spoof reliable biometry of fingerprints using en-face optical coherence tomography', *Opt. Photonics J.*, 2011, **1**, (3), pp. 91–96
71 Bossen, A., Lehmann, R., Meier, C.: 'Internal fingerprint identification with optical coherence tomography', *IEEE Photonics Technol. Lett.*, 2010, **22**, (7), pp. 507–509
72 Menrath, M.: 'Fingerprint with OCT'. Master's thesis, Fern-Universität Hagen in Cooperation with Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011
73 Marcialis, G., Lewicke, A., Tan, B., *et al.*: 'First international fingerprint liveness detection competition – LivDet 2009'. Image Analysis and Processing – ICIAP 2009, 2009 (*LNCS*, **5716**), pp. 12–23
74 Ghiani, L., Denti, P., Marcialis, G.: 'Experimental results on fingerprint liveness detection'. Articulated Motion and Deformable Objects, 2012 (*LNCS*, **7378**), pp. 210–218
75 Marcialis, G., Ghiani, L., Vetter, K., Morgeneier, D., Roli, F.: 'Large scale experiments on fingerprint liveness detection'. Structural, Syntactic, and Statistical Pattern Recognition, 2012 (*LNCS*, **7626**), pp. 501–509
76 Coli, P., Marcialis, G.L., Roli, F.: 'Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device', *Int. J. Image Graph.*, 2008, **8**, pp. 495–512
77 Ghiani, L., Yambay, D., Mura, V., *et al.*: 'LivDet 2013 fingerprint liveness detection competition 2013'. Proc. Sixth IAPR Int. Conference on Biometrics (ICB), 2013
78 Sepasian, M., Mares, C., Balachandran, W.: 'Vitality detection in fingerprint identification', *WSEAS Trans. Info. Sci. and App.*, 2010, **7**, (4), pp. 498–507
79 Meissner, S., Breithaupt, R., Koch, E.: 'Fingerprint fake detection by optical coherence tomography'. Proc. SPIE 8571, Optical Coherence Tomography and Coherence Domain Optical Methods in Biomedicine XVII, 2013, vol. 8571
80 Biometrics Evaluation and Testing (BEAT): 'http://www.beat-eu.org/'
81 Trusted Biometrics under Spoofing Attacks (Tabula Rasa): 'http://www.tabularasa-euproject.org/'