Pattern Recognition Letters 33 (2012) 1148–1156

Contents lists available at SciVerse ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Combining perspiration- and morphology-based static features for fingerprint liveness detection

Emanuela Marasco [a,b,*], Carlo Sansone [a]

[a] Dipartimento di Informatica e Sistemistica, University of Naples Federico II, via Claudio 21, 80125 Naples, Italy
[b] Lane Department of Computer Science and Electrical Engineering, West Virginia University, P.O. Box 6109, Morgantown, WV, USA

ARTICLE INFO

Article history:
Received 2 November 2010
Available online 30 January 2012
Communicated by M.S. Nixon

Keywords:
Biometrics
Spoofing
Liveness detection
Fingerprint scanners

ABSTRACT

It has been showed that, by employing fake fingers, the existing fingerprint recognition systems may be easily deceived. So, there is an urgent need for improving their security. Software-based liveness detection algorithms typically exploit morphological and perspiration-based characteristics separately to measure the vitality. Both such features provide discriminant information about live and fake fingers, then, it is reasonable to investigate also their joint contribution.

In this paper, we combine a set of the most robust morphological and perspiration-based measures. The effectiveness of the proposed approach has been assessed through a comparison with several state-of-the-art techniques for liveness detection. Experiments have been carried out, for the first time, by adopting standard databases. They have been taken from the Liveness Detection Competition 2009 whose data have been acquired by using three different optical sensors. Further, we have analyzed how the performance of our algorithm changes when the material employed for the spoof attack is not available during the training of the system.

1. Introduction

In many applications, a high level of security has been provided by different biometric devices. In particular, fingerprint scanners are the most widely adopted for personal identification. However, the security of a fingerprint-based identification system is compromised in presence of fake biometric data. In fact, it is possible to deceive automatic fingerprint identification systems by presenting a well-duplicated synthetic finger. Artificial fingerprints carrying the identity of enrolled users and created to attempt to gain unauthorized access are referred as *spoof* (Nixon et al., 2007). This kind of attack at the sensor level can occur when people wish to disguise their own identity or when a person wants to gain privileges of an authorized person. To minimize sensor vulnerability, different approaches have been proposed. As an efficient means to circumvent attacks that use spoof fingers, *liveness detection* has been suggested.

In the context of fingerprint recognition, *liveness detection* means the capability of the system to detect if the biometric sample presented is really from a live finger tip or not. Liveness methods may belong to two main categories. The first one exploits characteristics as the temperature of the finger, the electrical conductivity of the skin and the pulse oximetry. They can be detected by using additional hardware in conjunction with the biometric sensor. This makes the device costly. The second category performs an extra process on the biometric sample in order to detect the vitality information directly from the fingerprint images. In this paper, we focus on this second category of approaches, known as *software-based* (Schuckers et al., 2006). The existing software-based solutions may include *dynamic* or *static* methods (Jin et al., 2007). Static characteristics (as temperature,conductivity) and dynamic behaviors (skin deformation, perspiration) of live finger tips have been extensively studied in fingerprint liveness detection research. In particular, morphology- and perspiration-based characteristics have been typically exploited separately. Since both features provide discriminant information about live and fake fingers, it is reasonable to investigate also their joint contribution.

In this paper, we propose a novel fingerprint liveness detection method which provides fingerprint vitality using static measures extracted from only one image and based on a combination of skin perspiration and morphologic properties (Schuckers et al., 2006). Moreover, we propose a feature selection process that should be able to choose the best feature set for each fingerprint sensor. This also allowed us to reduce the time needed for extracting features from images. The performance of the proposed method has been compared with several other state-of-the-art algorithms. Such a comparison has been made, for the first time, by adopting standard databases taken from the Liveness Detection Competition 2009 (LivDet09) in which *Biometrika*, *CrossMatch* and *Identix* sensors

* Corresponding author at: Dipartimento di Informatica e Sistemistica, University of Naples Federico II, via Claudio 21, 80125 Naples, Italy.

E-mail addresses: emanuela.marasco@unina.it (E. Marasco), carlosan@unina.it (C. Sansone).

0167-8655/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.patrec.2012.01.009

were used (Marcialis et al., 2009). Further, we presented a novel study focused on how the performance of the liveness detection algorithms changes when fake fingers are produced by employing materials that are different with respect to those adopted for training. Also in this case our algorithm demonstrated better performance with respect to the other algorithms under comparison.

The paper is organized as follows. An overview of the existing methodologies for fingerprint liveness detection is presented in Section 2. In particular, three static methods based on morphologic characteristics are described. Our approach and the combined features are presented in Section 3. Some comparative results against the three previous described methods are reported in Section 4, by considering first the assumption that all the materials employed for realizing the spoof attacks are available for the training of the system, then the case when the material is new. Finally, our conclusions are drawn in Section 5.

2. Related works

Previous works have shown that it is possible to spoof a variety of fingerprint technologies through relatively simple techniques. For example, in 2002, Matsumoto et al. (2002) conducted experimental *spoofing* research by creating gummy fingers to attack fingerprint verification systems. They have reported a vulnerability evaluation of 68%–100% for cooperative users and 67% for not-cooperative users (when data were extracted from latent fingerprints).

In general, attackers use molds of fingers made with materials as *Silicone*, *Play-Doh*, *Clay* and *Gelatin* (gummy finger). Fig. 1 shows a fingerprint image obtained by using a mold made of silicone. In this section, we describe the two main software-based approaches that have been proposed so far in the literature.

2.1. Dynamic approaches

Dynamic features derive from the analysis of multiple frames of the same finger. A typical *dynamic* property of a live finger is the perspiration phenomenon that starts from the pores and evolves in time across the ridges, see Fig. 2. This distinctive spatial moisture pattern can be detected by observing multiple fingerprint images acquired at two appropriate different times. An interesting method based on perspiration changes in live fingers was presented in (Abhyankar and Schuckers, 2009). In this method, the changing perspiration pattern is isolated through a wavelet analysis of the entire fingerprint image. For an image processing algorithm, to quantify the sweating pattern is challenging. Since this pattern is a physiological phenomenon, it is variable across subjects. Further, 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., 2003). Its effectiveness requires an efficient extraction of the evolving pattern from images.

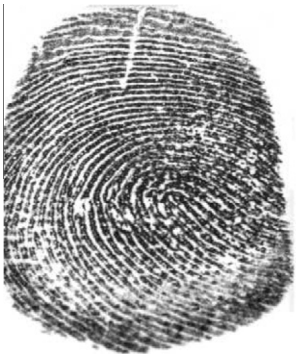

Fig. 1. An example of fingerprint obtained by using a mold made of silicone.

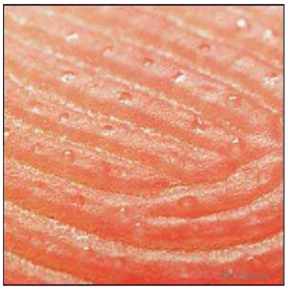

Fig. 2. The image shows a macro photography of a live fingerprint.

2.2. Static approaches

Static features can be extracted from a single fingerprint impression or as a difference between different impressions. Generally, static measurements may be altered by factors such as the pressure of the finger on the scanner surface. According to the taxonomy proposed in (Coli et al., 2008), features extracted by different impressions can be skin deformation-based or morphology-based, while features extracted by a single impression can be perspiration-based or morphology-based. Morphology-based features give a general description of the fingerprint pattern using its geometrical properties. Those based on the perspiration phenomenon quantify perspiration patterns along ridges in live subjects. Elastic deformations due to the contact, the pressure and the rotation of the fingertip on the plane surface of the sensor, are more evident in fake fingerprints made using artificial materials than in live fingerprints. Deformation-based methods detect liveness by comparing these distortions through static features (Chen et al., 2005). The elastic behavior of live and fake fingers has been analyzed by extracting a specific set of *minutiae points*, see Fig. 3. The second type of static features using multiple impressions relies on a morphologic investigation which exploits the thickness of the ridges that is modified after producing the fingerprint replica.

Methods which exploit intrinsic properties of a single impression study the skin perspiration phenomenon. The vitality indica-

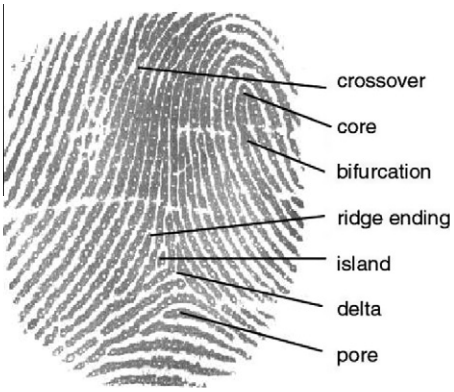

Fig. 3. The image shows the discontinuities that interrupt the flow of ridges which are the basis for most fingerprint authentication methods. Minutiae are the points at which a ridge stops, and bifurcations are the points at which one ridge divides into two. Many types of minutiae exist, including dots (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).

tion can be found by using Wavelet Transform and Fast Fourier Transform (Coli et al., 2007). Wavelet analysis is able to capture the non-regular shape typical of the ridges in an image acquired from a live finger. Images taken from artificial fingers show a more regular shape. Fourier Transform is employed to study the regular periodicity of pores on the ridges in live fingerprints. Such a regularity is not present in signals corresponding to spoof fingerprints. Liveness detection methods which search for morphological characteristics of fingerprint images, are significantly more efficient when based on the surface coarseness. A novel morphologic static feature based on the Fourier Transform has been exploited in (Coli et al., 2007), where the modulus of the Fourier Transform of a given fingerprint image is computed. The approach is based on the observation that some high frequency characteristics, such as the ridge line discontinuity, are less defined in fake fingerprint images; then, the difference between live and fake fingerprints can be measured in terms of *high frequency energy* which quantifies the amount of residual spectrum on the high frequencies. This approach, however, has been tested only on one database; further, the comparison with respect to methods existing in the scientific literature seems only in a preliminary state. Finally, a promising texture-based method was proposed in (Nikam and Agarwal, 2008). In this approach textural details captured by using local binary pattern histograms and ridge frequency and orientation information captured by using wavelet energy features were combined.

Below, we describe three static *morphology-based* methods which exploit a single fingerprint image for vitality information extraction and which have been used for a comparison with our approach in Section 4. Each of them exploits a subset of the features we used in our algorithm. Note that also (Coli et al., 2008) reports experiments on state-of-the-art features. In their study, however, both dynamic and static features were employed, while in the current approach we employ only static features; further we evaluate the related discriminant power on standard databases.

Moon et al. (2005) proposed a method based on analyzing the surface coarseness in high resolution (1000 dpi) fingertip images. It has been observed that the surface of a fake finger is much coarser than that one of the human skin. The coarseness feature is measured by computing the standard deviation of the residual noise of the fingerprint image. The alternation of the ridges and valleys, known as ridge/valley pattern, makes the fingertip surfaces intrinsically coarse at a certain scale. This effect of the ridge/valley pattern which may contribute to the surface coarseness was minimized by investigating the input image using a wavelet decomposition at different scales. In particular, the image is enhanced through a histogram equalization and converted into a mono-dimensional signal representing the gray level profile of the ridges. The residual noise was calculated as difference between the two fingerprint images before and after de-noising. The standard deviation of the residual noise gives the information about the pixel value fluctuation which is generally stronger in the noise residue of a coarser surface texture, see Fig. 4 and Fig. 5. To make a decision Moon used a threshold equal to 25; in general, however, the optimal threshold value depends on the database adopted for carry out experiments. We empirically found that it may significantly vary with the material employed to realize spoof samples and the resolution factor. This algorithm is fast and convenient but it works well only in presence of an high resolution sensor (1000 dpi, while the common commercial sensors present a resolution of about 500 dpi) (Coli et al., 2007).

An interesting texture-based approach using a single fingerprint image was proposed by Nikam and Agarwal (2009). They analyzed liveness of a fingerprint image by using the gray level associated to the fingerprint pixels. The gray level distribution in a fingerprint image changes when the physical structure changes. This information is quantified by using several texture features. Real and fake fingerprint images present different textural properties useful for vitality detection. 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 characteristics of artificial material surface, such as gelatin or silicone, spoof fingers show high uniformity of gray levels along ridges. The gray level distribution of the single pixels is modeled as first order statistics, while the joint gray level function between pair of pixels is modeled as second order statistics. The authors proposed Gabor filter-based features, since fingerprints exhibit oriented texture-like pattern and Gabor filters can optimally capture local frequency and orientation information. The basic steps of the adopted procedure are listed as follows:

- *Step1*: Fingerprint image is filtered using a bank of 4 Gabor filters oriented in 4 directions 0°, 45°, 90° and 135°.
- *Step2*: A gray level co-occurrence matrix method is applied to filtered images to extract textural details.
- *Step3*: Dimensionality of the features is reduced by Principal Component Analysis (PCA).

Features are used to train three different classifiers: a Neural Network (NN), a Support Vector Machine (SVM) and OneR. A Multilayer Perceptron (MLP) is used as NN and a Radial basis function (RBF) is used as the SVM kernel, with parameters C and γ as 1 and 2.3, respectively. The three classifiers are then fused using the "Max Rule". This approach presents good performance when the *core point* (see Fig. 3) is accurately located. However, existing core detection algorithms do not work well in the presence of poor quality images or with very dry or wet fingerprints, resulting in a *noisy* core.

An approach based on multiresolution texture analysis and the inter-ridge frequencies analysis of fingerprint images has been proposed by 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. First order statistics model the gray level distribution of the single pixels by using histograms, while second order statistics refer to the joint gray level function between pair of pixels. 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 fingerprint local-ridge frequency analysis. Error rates were computed after processing the statistics and the local ridges frequencies features by using Fuzzy-C-means classifier. This algorithm does not depend on the perspiration phenomenon and it is able to overcome the dependence on more than one fingerprint image. However, it presents limitations in real scenarios, since the computation of the local-ridge frequencies may be affected by cold weather and different skin conditions, including dirty fingers and wet fingers.

3. The proposed approach

Among the software-based approaches proposed in the scientific literature, methods which rely only on one impression result in a faster authentication. However, none of the static approaches developed so far seems to be able to separate fake and live fingerprints with acceptable error rates. They usually exploit a limited set of features which can perform differently as the resolution of the images under consideration, as well as the material used for spoofing, varies. Further, in general each individual static feature we previously described is able to capture the vitality by exploiting a different aspects of the fingerprint. Then, the proposed investigation focuses on combining features taken from different

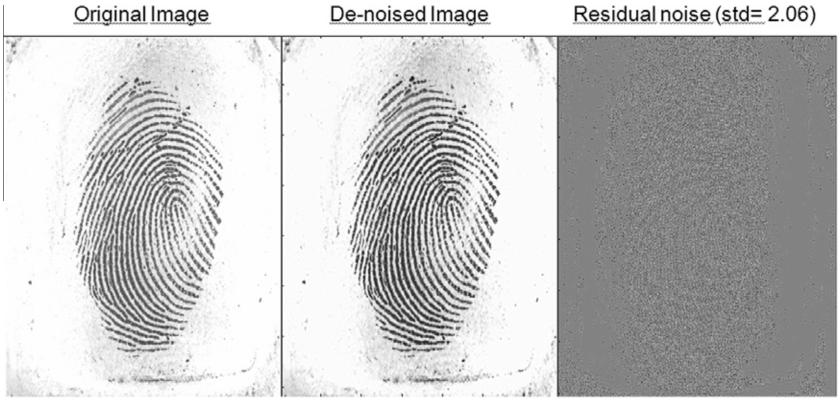

Fig. 4. Wavelet-based de-noising of a human fingerprint (image taken from Identix database) and the corresponding residual noise.

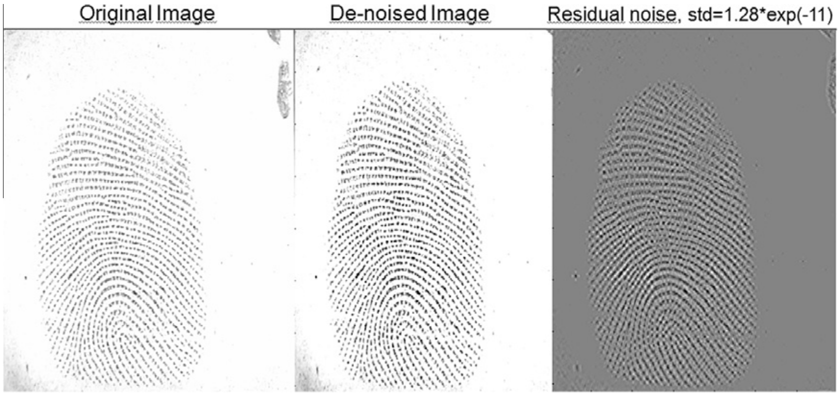

Fig. 5. Wavelet-based de-noising of a fake fingerprint made of silicone (image taken the from Identix database) and the corresponding residual noise.

approaches, in particular, from the morphology- and the perspiration-based ones. Morphology-based approaches, in fact, try to model the difference between live and fake images, while perspiration-based approaches try to infer dynamic information from a single static impression. A combination of perspiration- and morphology-based features is then expected to achieve better performance than any of the individual measures improving the vitality detection accuracy. Moreover, in order to cope with different image resolution factors, we propose a feature selection process that should be able to choose the best feature set for each fingerprint sensor. This also allowed us to reduce the time needed for extracting features from images.

3.1. The considered morphology-based features

- *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 *Silicone* or *Gelatin* consist of organic molecules which tend to agglomerate, thus the surface of a live finger is generally smoother than an artificial one (Moon et al., 2005). In the present work, the coarseness of the image can be measured by computing the standard deviation of the residual noise of an image, where the amount of residual noise was computed by using a wavelet-based approach. According to the approach proposed by Moon et al. (2005), we have treated the surface coarseness as a kind of Gaussian white noise added to the image. Firstly, the image was de-noised with a *Symlet* by applying a *soft-threshold* for wavelet shrinkage. The noise residue was achieved by calculating the difference between the two finger tip images before and after de-noising. The *Noise Residue Standard Deviation* is a good indicator of texture coarseness since the pixel value fluctuation in the noise residue of a coarser surface texture is generally stronger.
- *First order statistics*: measure the likelihood of observing a gray value at a randomly-chosen location in the image. The gray level associated to each pixel is exploited to determine a vitality degree of the fingerprint image. They can be computed from the histogram of pixel intensities in the image. The goal is to quantify the variations of the gray level distribution when the physical structure changes. The distinction between a fake and a live finger is based on the difference of these statistics. If $H(n)$ indicates the normalized histogram and N the number of bin, the set of first order statistical properties used in this work are as follows (Abhyankar and Schuckers, 2006):
  - Energy:
  $$e = \sum_{n=0}^{N-1} H(n)^2 \tag{1}$$
  - Entropy:
  $$s = -\sum_{n=0}^{N-1} H(n) log H(n) \tag{2}$$
  - Median:
  $$M = \arg\min_{a} \sum_{n} H(n)|n - a| \tag{3}$$

– Variance:

$$\sigma^2 = \sum_{n=0}^{N}(n-\mu)^2 H(n) \tag{4}$$

– Skewness:

$$\gamma_1 = \frac{1}{\sigma^3}\sum_{n=0}^{N-1}(n-\mu)^3 H(n) \tag{5}$$

– Kurtosis:

$$\gamma_2 = \frac{1}{\sigma^4}\sum_{n=0}^{N-1}(n-\mu)^4 H(n) \tag{6}$$

– Coefficient of variation:

$$cv = \frac{\sigma}{\mu} \tag{7}$$

3.2. The considered perspiration-based features

- *Individual pore spacing*. Extensive research has shown that pore patterns are unique to each individual (Abhyankar and Schuckers, 2006). A photo-micrograph of pores is shown in Fig. 6. For the purpose of the proposed approach, we focus on analyzing the occurrence of pores that causes a gray value variability in the fingerprint image. This tendency can be studied by using the Fast Fourier Transform (FFT), then the fingerprint image has to be transformed into a *ridge signal*, representing the gray-level value along the ridge. The discrimination between a live finger and a fake one is performed in the space of the total energy of the *ridge signal*. In this method, according to the algorithm proposed in (Derakhshani et al., 2003), the 2-dimensional fingerprint image was mapped to 1-dimensional signal which represents the gray-level values along the ridges. This technique enables quantification of the perspiration phenomenon in a given image. The gray-level variations in the signal correspond to variations in moisture due to the pores and the presence of perspiration. By transforming the signal in the Fourier domain lets to measure this static variability in gray-level along the ridges. In particular, the focus is on frequencies corresponding to the spacial frequencies of the pores. Firstly, by using a median filter the image was processed to remove noise and device effects. Such as de-noised image was converted into a binary one. Second, a thinning routine was applied on the binary image and the fingerprint ridge paths, composed by only one pixel, were determined. Connections were removed to have only individual curves. Finally, the FFT was computed and the total energy associated to the spatial frequencies of the pores were obtained as static feature. The coefficients of interest are from 11 to 33, since these values correspond to the spacial frequencies (0.4–1.2 mm) of pores. The formula for this static measure *SM* is given from the following:

$$SM = \sum_{k=11}^{33} f(k)^2 \tag{8}$$

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

$$f(k) = \frac{\sum_{i=1}^{n}\left|\sum_{p=1}^{256} S_{0i}^{a}(p)e^{-j2\pi(k-1)(p-1)/256}\right|}{n} \tag{9}$$

$$S_{0i}^{a} = S_{0i} - mean(S_{0i}) \tag{10}$$

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

- *Intensity-based*. From the intensity distribution perspective, among the 256 different possible intensities, the spoof and cadaver fingerprints images are distributed in the dark (<150) (Tan and Schuckers, 2005). The current study uses image histograms showing the number of pixels at each different intensity values found in the image and it focuses on the gray level values along the ridge, represented by the *ridge signal*. We have computed two particular features: (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, we have analyzed the uniformity of gray levels along ridge lines and the contrast between valleys and ridges. As Fig. 7 shows, real fingerprints exhibit non-uniformity of gray levels and high ridge/valley contrast values. Then, the general variation in gray-level values of in a spoof fingerprint is less than a live one. To capture this information we have computed as additional feature the *Gradient* of the gray-level matrix of the image.

3.3. Feature selection and classification

The time to perform the recognition process is a fundamental parameter which affects the performance of the proposed system. A feature selection phase reduces the number of features to be extracted and subsequently the time needed for feature extraction. We have selected the subset of features with highest discriminant power on the training set by using a *Sequential Forward Selection* technique. The feature selection was performed for each sensor.

Different classifiers have been trained, such as a Support Vector Machine, a Decision Tree, a Multilayer Perceptron and a Bayesian classifier. For each sensor, we have chosen the classifier with the highest accuracy on the training set.

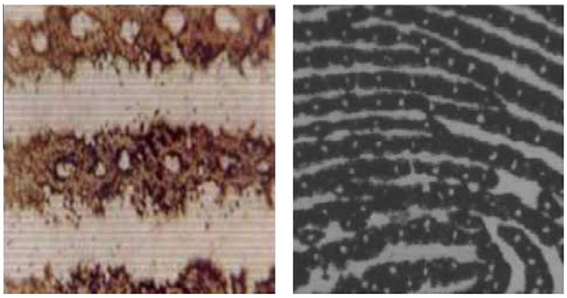

Fig. 6. The image on the left shows a photo-graphical example of pores. The image on the right is output from a high resolution sensor (1000 dpi) that captures the location of pores in detail. Both are taken from Choi et al. (2007).

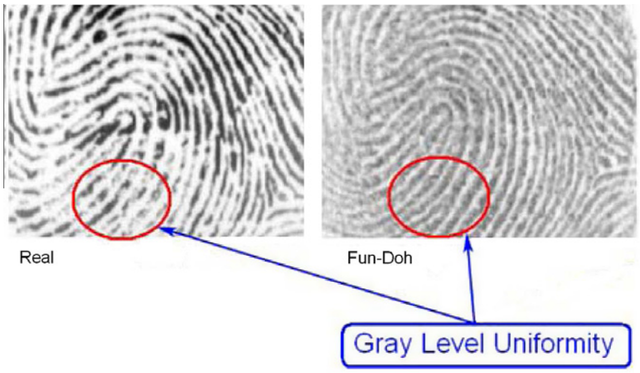

Fig. 7. Gray level uniformity analysis in fingerprint images: high level value for a real fingerprint and low for a spoof. The image was taken from Nikam and Agarwal (2009).

Table 1
Datasets for training.

Database	Subjects	Live images	Fake images	Frames
Biometrika	13	520	520	0 and 5 s
Identix	35	375	375	0 and 2 s
CrossMatch	63	500	500	0 and 2 s

Table 2
Datasets for testing.

Database	Subjects	Live images	Fake images	Frames
Biometrika	37	1440	1440	0 and 5 s
Identix	125	1125	1125	0 and 2 s
CrossMatch	191	1500	1500	0 and 2 s

Table 3
Fingerprint sensors used for LivDet 2009.

Sensors	Model no.	Resolution (dpi)	Image size
Biometrika	FX2000	569	(312 × 372)
Identix	DFR2100	686	(720 × 720)
CrossMatch	Verifier 300 LC	500	(480 × 640)

Table 4
Time required for extracting the proposed set of features on a *Core Duo T8100 2,1 Ghz Intel* Processor.

Feature	Average extraction time (s)
Energy	0.15
Entropy	0.02
Mean	0.02
Variance	0.02
Skewness	0.06
Kurtosis	0.06
Coefficient of variation	0.02
Residual noise std	0.59
Indiv pore spacing	1.00
Gray level 1	0.02
Gray level 2	0.02
Gradient	0.06

4. Experimental results

4.1. Datasets

Our experimental phase was carried out by using three databases taken from the Fingerprint Liveness Detection Competition 2009 (LivDet09) and composed by live and spoof fingerprint images. Each database refers to a different sensor (*Biometrika,CrossMatch* e *Identix*) and each one of them is composed by two subsets, one for training and the other one for testing the algorithm (Marcialis et al., 2009). The considered sensors are optical and the employed fingerprint sensing mechanism acquires the image by placing the finger on a transparent prism and then using a camera. In total internal reflection (TIR) sensors, ridges and valleys are imaged in contrast: ridges are in contact with a glass platen, the surface is illuminated trough one side on a prism and then reflected. Sensors based on this technology are vulnerable to spoof attacks in which the artificial fingerprints are made of materials having a light reflectivity similar to that one of the skin.

Biometrika training dataset is made up by 520 silicone images and 520 live images (13 subjects × 20 acquisitions × 2 frames), with 2 time-series (0 s and 5 s). The corresponding test set is made up by 1440 silicone images and 1440 live images (37 subjects × 20 acquisitions × 2 frames), with 2 time-series (0 s and 5 s). *CrossMatch* training dataset is made up by 500 live images and 500 fake images produced by using silicone, gelatin and *Play-Doh*, with 2 time-series (0 s and 2 s). The corresponding test set is made up by 1500 live images and 1500 fake images produced by using *Silicone*, *Gelatin* and *Play-Doh*, with 2 time-series (0 s and 2 s). *Identix* training dataset is made up by 375 live images and 375 spoof images produced by using *Silicone*, *Gelatin* and *Play-Doh*, with 2 time-series (0 s and 2 s). The corresponding test set is made up by 1125 live images and 1125 spoof images produced by using *Silicone*, *Gelatin* and *Play-Doh*, with 2 time-series (0 s and 2 s). The details regarding the data collection are reported in Tables 1 and 2, while those related to characteristics of the sensors are reported in Table 3.

Table 5
Selected features for each database.

Feature		Biometrika	CrossMatch	Identix
Morphology-based	*Energy*		x	x
Morphology-based	*Entropy*	x		x
Morphology-based	*Mean*	x	x	x
Morphology-based	*Variance*		x	x
Morphology-based	*Skewness*		x	x
Morphology-based	*Kurtosis*		x	x
Morphology-based	*Coefficient of variation*	x	x	x
Morphology-based	*Residual noise std*	x	x	x
Perspiration-based	*Pore spacing*	x	x	
Perspiration-based	*Gray level 1*		x	
Perspiration-based	*Gray level 2*	x		x
Perspiration-based	*Gradient*	x	x	x

Table 6
Performance of the proposed algorithm.

	Ferrlive (%)	*Ferrfake* (%)	*e* (%)
Biometrika	12.20	13.00	12.60
CrossMatch	17.40	12.90	15.20
Identix	8.30	11.00	9.70
Average	12.60	12.30	12.47

Table 7
Performance of the best algorithm submitted to the Liveness Detection Competition 2009.

	Ferrlive (%)	*Ferrfake* (%)	*e* (%)
Biometrika	15.60	20.70	18.20
CrossMatch	14.40	15.90	15.20
Identix	9.80	11.30	10.60
Average	13.20	16.10	14.67

4.2. Performance of our method

In this paper, the classification performance was evaluated by adopting the same parameters used during LivDet09, defined below:

- *Ferrlive*: rate of misclassified live fingerprints.
- *Ferrfake*: rate of misclassified fake fingerprints.

The performance indicator is given from the error *e* averaged on the three databases *Biometrika*, *CrossMatch* and *Identix*, where *e* for each database is computed as follows:

$$e = \frac{Ferrlive + Ferrfake}{2} \tag{11}$$

The time required for feature extraction is reported in Table 4 for each feature exploited in our approach. Table 5 reports the features selected for each sensor by using a *Sequential Forward*

Table 8
Performance of the method of Moon on the three databases LivDet09 using Symlet wavelet for de-noising.

	Threshold	*Ferrlive* (%)	*Ferrfake* (%)	*e* (%)
Biometrika	20.60	20.80	25.00	23.00
CrossMatch	3.1^{-11}	27.40	19.60	23.50
Identix	10.50	74.70	1.60	38.20
Avg		40.97	15.40	28.23

Table 9
Performance of the method of Nikam (Max Rule) on the three databases LivDet09.

	Ferrlive (%)	*Ferrfake* (%)	*e* (%)
Biometrika	14.30	42.30	28.30
CrossMatch	19.00	18.40	18.70
Identix	23.70	37.00	30.35
Avg	19.00	32.57	25.78

Table 10
Performance of the method of Abhyankar and Schuckers on the three databases LivDet09.

	Ferrlive (%)	*Ferrfake* (%)	*e* (%)
Biometrika	24.20	39.20	31.70
CrossMatch	39.75	23.30	31.53
Identix	48.40	46.00	47.20
Avg	37.45	36.17	36.81

Table 11
Performance of the proposed approach on CrossMatch and Identix databases.

	CrossMatch			*Identix*		
	Gelatin (%)	*Play-Doh* (%)	*Silicone* (%)	*Gelatin* (%)	*Play-Doh* (%)	*Silicone* (%)
Ferrlive	6.5	5.7	12.6	3.8	19.2	9.7
Ferrfake	25.9	16.7	10.0	42.3	5.5	30.6
e	16.2	11.2	11.3	23.05	12.35	20.15

Selection technique. The individual discriminant power of each feature considered in this work, has shown a certain dependence on the database, while the joint (usage of both perspiration- and morphology-based features) discriminant power has been high on all the three databases. This is confirmed by the fact that in all cases both morphology- and perspiration-based features have been selected. The subset of features selected for all the three sensors was composed by three morphology-based features (mean, standard deviation of the residual noise and the coefficient of variations) and one perspiration-based feature (*gradient*). Table 6 reports the results obtained by employing the proposed method, the achieved average error rate is 12.47%. On *Biometrika* and *Identix* datasets, the highest accuracy was achieved by using a Multilayer Perceptron classifier, while on *CrossMatch* dataset, by using a Decision Tree classifier.

As a first comparison, we report in Table 7 the performance achieved by the algorithm which won of the LivDet09 Competition, referred to as *Anonymous2*. It made an error of 14.67% averaged on the three databases. It can be noted that our approach performed better on the average; moreover, on two datasets we obtaind better results with respect to *Anonymous2*,while the same results on the third one (*CrossMatch*).

4.3. Comparison with existing static methods

Since the characteristics exploited by the algorithm which won the LivDet09 competition are not known, we compared our algorithm to other approaches which exploit only morphology-based or perspiration-based features, in order to have an experimental proof that a combination of them achieves better classification performance. In particular, we considered the three static methods described at the end of Section 2.

To implement the approach proposed by Moon, fingerprint images were firstly enhanced through a histogram equalization pre-processing, then they were de-noising by adopting different kind of filters in order to maximize the performance. A median filter produced residual noise standard deviation values similar to those obtained in the approach proposed by Moon, while wavelet-based filters produced lower values. Table 8 reports the best performance obtained by using a Symlet wavelet for de-noising. According to the procedure proposed in (Moon et al., 2005), the wavelet shrinkage was performed by applying a soft-threshold. On the *CrossMatch* database, composed by a significant percentage of poor quality images, the threshold assumed the lowest value. In our experiments, we also used wavelet packets since they work on high frequencies, and it is known that, fingerprint images present the majority of the components just at high frequencies. This procedure is performed by cutting the frequency domain in the middle at each filtering step, and keeping the high-frequency components only (Walczak et al., 1996). Wavelet packets were able to improve the classification accuracy only when the resolution was high enough, such as on *Identix* database where the error decreased from 38.20% to 35.90%.

Table 9 shows the performance of the method proposed by Nikam which achieved the lowest average error rate, equal to 18.70%, on the *CrossMatch* database where the *Ferrfake* is the lowest too. On *Biometrika* database, the error made on the live fingerprints is the lowest, while regarding the negative class, the training set does not seem to be well represented by the three materials considered to realize the spoof attacks. Table 10 shows the performance of the method proposed by Abhyankar–Schuckers, which achieved the highest error rate, equal to 47.20%, on the *Identix* database having the highest resolution; in this case, *Ferrlive* and *Ferrfake* are both high. On *Biometrika*, the error made on live fingerprints is the lowest also for this approach.

By comparing the results reported in Tables 8–10 with those obtained by our approach (Table 6), it can be noted that we performed better than any of the existing methods on all the three databases. In particular, we showed the lowest average error rate (9.70%) on *Identix* database, while approaches which exploit only one of the two considered categories of features showed the highest error rate on this dataset. The approaches proposed by Moon and Nikam which exploit morphology-based features, in fact, presented an average error rate of 38.20% and 30.35% respectively, while the approach proposed by Abhyankar, which exploits perspiration-based features, had an average error rate of 47.20% (see Table 10). This confirms our claims regards the advantages of using both morphology- and perspiration-based features.

4.4. Analysis of the robustness when the material used for spoofing changes

In our previous experiments, the classifier was trained by using features extracted from fake samples made with all the materials available in each database. In particular, *Gelatin*, *Silicone* and *Play-Doh* are the materials employed in both *Identix* and *CrossMatch* databases. However, a good liveness detection algorithm is expected to be robust when the material used to learn the fake class changes. This aspect is a challenging problem in fingerprint liveness detection, since nowadays materials used for fraudulent spoof attacks are going to become very sophisticated. In this section, we analyze the performance of the existing liveness algorithms in scenarios reproducing the real conditions, where the material used to attack the system is not *a priori* known.

Table 12
Performance of the method proposed by Moon on CrossMatch and Identix databases.

	CrossMatch			*Identix*		
	Gelatin (%)	*Play-Doh* (%)	*Silicone* (%)	*Gelatin* (%)	*Play-Doh* (%)	*Silicone* (%)
Ferrlive	12.30	15.00	35.70	45.20	79.60	40.80
Ferrfake	63.10	61.80	47.30	31.80	4.20	36.80
e	37.70	38.40	41.50	38.50	41.90	38.80

Table 13
Performance of the method proposed by Nikam on CrossMatch and Identix databases.

	CrossMatch			*Identix*		
	Gelatin (%)	*Play-Doh* (%)	*Silicone* (%)	*Gelatin* (%)	*Play-Doh* (%)	*Silicone* (%)
Ferrlive	27.20	43.70	24.20	23.50	29.30	20.00
Ferrfake	22.00	32.90	31.60	16.00	28.80	31.50
e	24.60	38.30	27.90	19.75	29.05	25.75

Table 14
Performance of the method proposed by Abhyankar and Schuckers on CrossMatch and Identix databases.

	CrossMatch			*Identix*		
	Gelatin (%)	*Play-Doh* (%)	*Silicone* (%)	*Gelatin* (%)	*Play-Doh* (%)	*Silicone* (%)
Ferrlive	45.80	29.80	58.60	65.50	61.60	37.90
Ferrfake	12.20	24.40	17.00	2.40	46.40	27.70
e	29.00	27.10	37.80	33.45	54.00	32.80

Table 15
Performance of the analyzed approaches in terms of the average error *e* on the Identix and CrossMatch databases. Last row is reported for the sake of comparison.

Avg *e*	Our method	Moon	Nikam	Abhyankar Schuckers
Gelatin	19.63	38.00	22.18	31.23
Play-Doh	11.78	40.10	33.68	40.55
Silicone	15.73	41.50	26.83	35.30
All materials	12.45	30.85	24.53	39.37

In our experiments, each detection algorithm was trained by using a train set in which the negative class was represented by spoof fingerprints realized with only one of the available materials in the dataset. Table 11 reports the performance of our method. In presence of high resolution images, taken from the *Identix* database, when the training is performed by employing fake fingers made in *Play-Doh* and the testing using *Gelatin* and *Silicone*, the spoofing recognition rate is good. Table 12 shows that the method proposed by Moon wrongly classifies the majority of the fake fingerprints taken from *CrossMatch* database. For a higher resolution factor, such a method presents good robustness in presence of *unknown* materials using for spoofing. Tables 13 and 14 show that the variation in fake materials does not affect the performance of both Nikam and Abhyankar–Schuckers approaches, when the training set is composed only by samples made in *Gelatin*.

As resumed in Table 15, when only one feature is used (i.e. the method by Moon), performance significantly decreases, while algorithms that use more than one feature result more robust to new materials. Once again, our algorithm always overcomes all the existing approaches in all the three considered cases. Note that we could not perform this analysis also for the best algorithm proposed during the LivDet09 because its description is not publicly available.

5. Discussion and conclusions

In this paper, we have proposed a novel approach for liveness detection in fingerprint scanners which combines multiple features derived from a morphological- and a perspiration- based analysis of one fingerprint image. The proposed algorithm has been tested on three different optical sensors.

Our experiments demonstrated that it overcomes the limitations of the existing approaches in real scenarios, where the resolution factor of the fingerprint images is not high enough. Further, since our method does not require additional hardware, the cost of the fingerprint sensor does not increase. The overall system will also be faster, since the required information can be extracted from only one image without scanning twice the user's finger. Our experiments show also that the performance of liveness detection approaches in which only one feature is exploited, decreases in the presence of new materials employed for spoofing. This weakness is reduced when multiple vitality features are extracted. In particular, the combination of morphology- and perspiration-based features showed a high robustness in such a scenario.

This notwithstanding, the achieved error rates can be considered still high to think about its use in a possible unimodal real scenario in which very low error rates are required. However, recent studies concerning multimodal scenarios (Rodrigues et al., 2009; Marasco et al., 2011) suggest a possible usage of the proposed algorithm. The idea is to consider a multimodal system in which a spoofing detection algorithm has been integrated and where only one or a subset of the fused modalities has been spoofed; when the modality is detected as *fake*, it is not included in the combination scheme. In this application the proposed algorithm is able to significantly improve the overall multimodal performance (Marasco et al., 2011).

Since we exploited multiple features and adopted a feature selection technique based on the specific sensor, we expect that the proposed approach could be quite robust to a circumvention that arises when the features computed by the algorithm are known. On the other, the tolerance with respect to a possible variation of these features depends on the discriminant power showed by the feature which is under attack. So, as a future research, it would be interesting to carry out experiments where the value of a subset of these features changes, in order to analyze the corresponding impact on the performance of our approach.

Finally, it must be recalled that the three sensors on which we have tested our approach – the ones present in the LivDet09 competition – are optical. Since some of the morphology- and perspiration-based features used in our proposal have been already employed with capacitive or electro-optical sensors (Abhyankar and Schuckers, 2006; Tan and Schuckers, 2005), we expect that our approach could be successfully applied to these other sensor technologies. On the other hand, the applicability to emerging systems in which the finger is optically imaged in 2-D or 3-D will be matter of future research.

Acknowledgments

The authors thank Prof. Stephanie Schuckers of the Department of Electrical and Computer Engineering, Clarkson University, Potsdam (NY) for her useful talks, Prof. Luisa Verdoliva of the Dipartimento di Biomedica, Elettronica e Telecomunicazioni, University of Naples (Italy), for supporting the wavelet analysis techniques and Prof. Davide Maltoni of the Department of Electronics, Informatics and System, University of Bologna (Italy), for his valuable comments about the existing core detection algorithms.

References

Nixon, K., Aimale, V., Rowe, R., 2007. Spoof detection schemes. In: Jain, P.F.A., Ross, A. (Eds.), Handbook of Biometrics. Springer.

Schuckers, S., Derakhshani, R., Parthasaradhi, S., Hornak, L., 2006. Liveness detection in biometric devices. In: Electrical Engineering Handbook, 3rd ed. CRC Press.

Jin, C., Kim, H., Elliott, S., 2007. Liveness detection of fingerprint based on band-selective fourier spectrum. Inform. Sec. Crypt. 4817, 168–179.

Marcialis, G., Lewicke, A., Tan, B., Coli, P., Grimberg, D., Congiu, A., Tidu, A., Roli, F., Schuckers, S., 2009. First international fingerprint liveness detection competition – livdet 2009. Lect. Notes Comput. Sci. 5716, 12–23.

Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S., 2002. Impact of artificial gummy fingers on fingerprint systems. Opt. Sec. Counterfait Deterrence Techniq. IV 4677, 275–289.

Abhyankar, A., Schuckers, S., 2009. Integrating a wavelet based perspiration liveness check with fingerprint recognition. Pattern Recognition 42, 452–464.

Derakhshani, R., Schuckers, S., Hornak, L., O'Gorman, L., 2003. Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition 36, 383–396.

Coli, P., Marcialis, G., Roli, F., 2008. Fingerprint silicon replicas: Static and dynamic features for vitality detection using an optical capture device. Internat. J. Image Graph. (IJIG) 8, 495–512.

Chen, Y., Jain, A., Dass, S., 2005. Fingerprint deformation for spoof detection. In: Biometric Symposium.

Coli, P., Marcialis, G., Roli, F., 2007. Vitality detection from fingerprint images: A critical survey. Lect. Notes Comput. Sci. 4642, 722–731.

Coli, P., Marcialis, G., Roli, F., 2007. Power spectrum-based fingerprint vitality detection. In: IEEE Internat. Workshop on Automatic Identification Advanced Technologies AutoID, pp. 169–173.

Nikam, S., Agarwal, S., 2008. Local binary pattern and wavelet-based spoof fingerprint detection. Internat. J. Biometrics 2.

Moon, Y.S., Chen, J.S., Chan, K.C., So, K., Woo, K.S., 2005. Wavelet based fingerprint liveness detection. Electron. Lett. 41, 1112–1113.

Nikam, S.B., Agarwal, S., 2009. Curvelet-based fingerprint anti-spoofing, signal. Image Video Process. 4, 75–87.

Abhyankar, A., Schuckers, S. 2006. Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In: IEEE Internat. Conf. Image Process, pp. 321–324.

Tan, B., Schuckers, S. 2005. Liveness detection using an intensity based approach in fingerprint scanner. In: Proceedings of Biometrics Symposium (BSYM).

Choi, H., Kang, R., Choi, K., Kim, J., 2007. Aliveness detection of fingerprint using multiple static features. World Acad. Sci. Eng. Tech. 28, 157–162.

Walczak, B., Bogaert, B., Massart, D., 1996. Application of wavelet packet transform in pattern recognition of near-ir data. Anal. Chem. 68, 1742–1747.

Rodrigues, R.N., Ling, L., Govindaraju, V., 2009. Robustness of multimodal biometric fusion methods against spoof attacks. J. Visual Lang. Comput..

Marasco, E., Johnson, P., Sansone, C., Schuckers, S.A.C., 2011. Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism. In: Sansone, C., Kittler, J., Roli, F. (Eds.), MCS, Lecture Notes in Computer Science, vol. 6713. Springer, pp. 309–318.