International Journal of Electrical, Electronics and Computer Engineering **1**(2): 28-37(2012)

ISSN No. (Online) : 2277-2626

An Anti-Spoofing Technique Using Multiple Textural Features in Fingerprint Scanner

Pravin B Patil and Prof . Shabahat Hasan

Department of Electronics and Communication Engineering,
RKDF Institute, Bhopal, (MP)

(Received 30 Augest, 2012, Accepted 29, September, 2012)

ABSTRACT: Fingerprint verification systems may be circum- vented by fake fingerprints produced using inexpensive materials like gelatin or silicon. An efficient countermeasure against these attacks is given by liveness detection. In the recent literature, different algorithms for detecting signs of vitality have been proposed. The cheapest techniques are software-based and utilize acquired fingerprint images in order to extract static or dynamic characteristics.

In this paper, we propose a novel software-based solution for liveness detection based on static features coming out from the visual texture of the image. The reported results show that the use of our features effectively improves the discriminative power (between live and fake fingerprints) achieved by the algorithms proposed during the Liveness Detection Competition 2009.

I. INTRODUCTION

Biometric systems based on fingerprints are widely adopted for person recognition in many applications requiring a high level of security. However, fingerprint scanners may be easily circumvented by presenting fake fingers, that can be realized by employing some inexpensive materials such as gelatin or silicon [1]. The ability to recognize if a biometric sample is from a live finger or not is becoming a challenging research issue.

To face this problem, two major approaches can be im- plemented [2]. The first one is *hardware-based* and adds to the sensor a device that is able to acquire an explicit vital- ity information like temperature, blood pulsation, electrical conductivity of the skin, etc. This method increases the cost of the overall system since it requires additional hardware. The second one is *software-based* and integrates a liveness detection algorithm into a standard fingerprint sensor. Such solution may use static features, extracted from one or multiple impressions of the same finger or dynamic features, obtained by processing two successive images, captured in a certain time interval [3]. In the first case, textural characteristics, ridge frequencies, elastic properties of the skin, etc. are measured, while in the second case, perspiration signs through the pores are generally extracted after performing a temporal analysis [4].

Last year, some algorithms have been presented during the Liveness Detection Competition [5]. One of them was based on ten features concerning the fingerprint image quality, like strength, clarity and continuity of the ridges, in order to discriminate between live and fake samples. Although this algorithm achieved acceptable perfomances, its usage may be not successfully in many real scenarios where the quality of the images does not present a good level. The countermeasure adopted in the proposed approach is a software-based method that does not add any device to the fingerprint scanner in order to design a non-expensive biometric system. Moreover, the current work utilizes static features, that can be obtained without requiring to the user multiple fingerprints acquired at different times, then the overall recognition process will be faster. In particular, we propose an algorithm for fingerprint liveness detection based on three categories of textural features extracted from a single fingerprint image. The reported results show that the joint use of these three categories of features improves the discriminative capability (between live and fake fingerprints) achieved by the best algorithm proposed during the Liveness Detection Competition 2009.

The paper is organized as follows. In session 2, we describe the sources of information that can be exploited for the fingerprint liveness detection process. Section 3 presents the proposed approach, in

particular the features we used are described. Section 4 reports the experimental procedure and some comparative results against the best algorithm submitted during the Liveness Detection Competition 2009. Section 5 presents our conclusions.

II. RELATED WORKS

Fingerprint *spoofing* refers to a fraudulent access by an unauthorized person into a fingerprint biometric systems by using a fake fingerprint reproducing that one of an authorized user.

Recent studies have shown that the security of fingerprint recognition systems is questionable with using artificial re- productions. In 2002, Matsumoto *et al.* [6] have conducted experimental *spoofing* research by creating gummy (gelatin) fingers to attack fingerprint verification systems. They reported a vulnerability evaluation of 68%-100% for cooperative users and 67% for not-cooperative users (when data were extracted from latent fingerprints). In 2006, Galbally *et al.* [7] pre-sented a statistical evaluation of two fingerprint verification systems using two different sensors (thermal and optical) against attacks with gummy fingers. More recently, in [8] thecontribution was focused on evaluating the robustness of an ISO minutiae-based system against attacks in which gummy fingers were generated from reconstructed fingerprint images exploiting the information stored in the template.

Initial research has shown the efficiency of image processing and pattern recognition to discriminate between live and fake fingers. Over the last few years, several methods to face spoof attacks at sensor level have been proposed. One of the first efforts in liveness detection was reported in [9], in which a ridge signal algorithm using the periodicity of sweat and sweat diffusion pattern was implemented to detect fake fingerprints. Later, the same technique but with a wavelet-based technique was proposed in [10]. The existing software-based solutions may belong to three types of categories [2]

- Perspiration-based method: the perspiration phenomenon is a typical *dynamic* property of a live finger and it can be detected by using multiple fingerprint images consequently acquired. This approach presents a certain sensitivity to the environment, the pressure of the finger and the time interval. An interesting method based on perspiration pattern and perspiration changes in live finger was presented by Abhyankar and Schuckers in [11]. Live fingers present a distinctive spatial moisture pattern that evolves in time across the ridges due the presence of the pores. This method uses wavelet analysis of the entire fingerprint image to isolate the changing perspiration pattern. The effectiveness of the algorithm depends on efficient extraction of the evolving pattern from images acquired in two appropriate different times.
- Skin deformation-based method: distortions due to the pressure and rotation of the finger on a sensor produce different elastic characteristics of the materials. Liveness can be detected by comparing these distortions through static features. Recently, the elastic deformation due to the contact of the fingertip with a plane surface was studied by Chen *et al.* in [12], since a fake fingerprint presents different deformations than a live one. The elastic behaviour of a live and a fake finger was analyzed by using a mathematical model relying on the extraction of a specific and ordered set of minutiae points.
- Image quality-based method: in general, a fake fingerprint image does not have a good quality as a live one. The important idea to detect liveness by checking quality was implemented by Moon in [13]. He proposed a fast and convenient wavelet-based algorithm based on the computation of the standard deviation of the fingerprint image.

To capture the needed details, the methods mentioned earlier make the system complex. To alleviate these problems, a texture-based method using a single image was proposed by Nikam and Agarwal in [3]. Their work focuses on the obser- vation that real and fake fingerprint images present different textural properties useful for vitality detection. In particular, authentic fingerprints exhibit non-uniformity of gray levels along ridges due to the presence of sweat pores and the perspiration phenomenon, while the characteristics of artificial materials, such as gelatin or silicon, do not change for surfaces of spoof fingers, they show high uniformity of gray levels along ridges. Moreover, since texture involves the spatial distribution of the gray levels, the analysis of spatial statistics of the image gray levels assumes a significant importance. This texture perception aspect was extensively studied by Julesz in the context of texture discrimination [14].

III. THE PROPOSED APPROACH

Liveness detection problem is treated as a two class clas- sification problem (live/fake). Given an input

fingerprint, the vitality information is represented by a set of features that are exploited to train a pattern classifier. Such classifier is able to compute the probability of the image vitality. This section describes the three categories of static fingerprint textural features adopted in our approach.

The texture of an image describes visual information re- lated to local spatial variations of gray level intensities and orientations [3]. For example, the image of a wooden surface is not uniform but presents variations of intensities which generate repeated patterns called *visual texture*. The patterns may result from physical surface properties such as roughness, orientations or reflectance differences depending on the color on a surface [15]. Two-dimensional histograms are used as reasonable texture analysis tools.

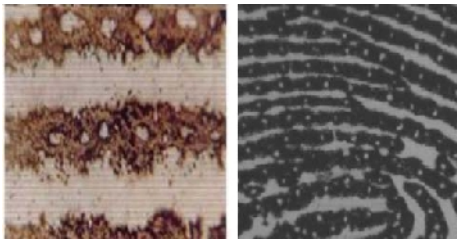

Fig. 1. The image on the left shows a photographical example of pores. The image on the right is output from a high resolution sensor (1000dpi) that captures the location of pores in detail. Both are taken from [16].

- Signal processing methods: refers to features extracted from filtered images.

  – *Individual pore spacing:* extensive research has shown that pore patterns are unique to each individ- ual [17]. A photo-micrograph of pores is shown in Figure 1. 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 algo- rithm proposed in [9], the 2-dimensional fingerprint image was mapped to 1-dimensional signal which represents the gray-level values along the ridges. This technique lets to quantify the perspiration phe- nomenon 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 denoised 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 spacial frequency of the pores was 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:

$$SM = \sum_{k=11}^{33} f(k)^2 \qquad \ldots(1)$$

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

$$f(k) = (\mathrm{i}=1 \;/_{p=1}\; S_{1i}(p)e)n \qquad \cdots(2)$$

$$_{1i} = S_{1i} - mean(S_{1i}) \qquad \ldots(3)$$

where n is the total number of individual ridges and S_{1i} is the individual ridges from the first image.

– *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 [17]. Ma- terials used to make fake fingers such as

silicon or gelatin consist of organic molecules which tend to agglomerate, thus the surface of a live finger is generally smoother than an artificial one [13].

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, we have treated the surface coarseness as a kind of Gaussian white noise added to the image. Firstly, the image was denoised 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 Figure 2 shows a human finger tip image while Figure 3 shows a fake fingertip made of silicon. By comparing the two noise residues, we can see the difference.

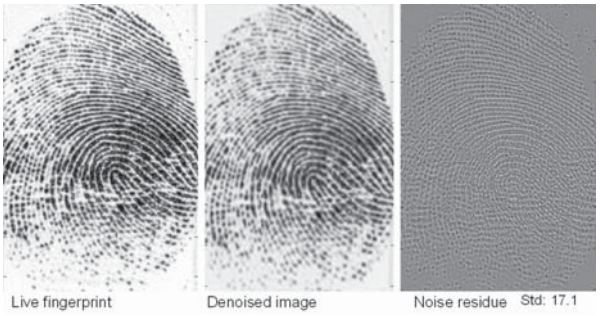

Fig. 2. Wavelet-based de-noising of a human fingertip whose image was taken from Biometrika database.

Fig. 3. Wavelet-based de-noising of a fake fingertip made of silicon, whose image was taken from Biometrika database.

- First order statistics: measure the likelihood of ob- serving 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, the set of first order statistical properties used in this work are as follows [17]:

– Energy:

$$e = \sum_{n=0}^{N-1} H(n)^2 \quad \ldots(4)$$

Entropy:

$$S = -\sum_{n=0}^{N-1} H(n) \log H(n) \quad \ldots(5)$$

– Median:

$$M = \arg\min \; H(n)|n - a| \quad (6)$$

– Variance:

$$\sigma^2 = \sum_{n=0}^{N} (n - \mu)^2 H(n) \quad \ldots(7)$$

– Skewness:

$$\gamma_{1=1/\sigma^3} \sum_{n=0}^{N-1} (n - \mu)^3 H(n) \quad \ldots(8)$$

– Kurtosis:

$$\gamma_{2=1/\sigma^3} \sum_{n=0}^{N-1} (n - \mu)^4 H(n) \quad \ldots(9)$$

– Coefficient of variation:

$$Cv = \frac{\sigma}{\mu} \quad \ldots(10)$$

- Intensity-based features: from the intensity distribution perspective, among the 256 different possible intensities, the spoof and cadaver fingerprints images are distributed in the dark (<150) [18]. 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 Figure 4 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 the gradient of the gray-level matrix of the image.

IV. EXPERIMENTS

A. Datasets

Our experimental phase was carried out by using three databases Biometrika, CrossMatch and Identix composed by live and spoof fingerprint images.

They have been taken from the Liveness Detection Compe- tition 2009 and each one of them is composed by two subsets, one for training and the other one for testing the algorithm. Biometrika

training dataset consists in 520 silicone images and 520 live images (13 subjects x 20 acquisitions x 2 frames), with 2 time-series (0 sec and 5 sec). The corresponding test.

Fig. 4. Gray level uniformity analysis in fingerprint images: high level value for a real fingerprint and low for a spoof. The image was taken from [3].

Table I. Datasets For Training.

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

Set consists in 1440 silicone images and 1440 live images (37 subjects x 20 acquisitions x 2 frames), with 2 time-series (0 sec and 5 sec). CrossMatch training dataset consists in 500 live images and 500 fake images produced by using silicone, gelatin and PlayDoh, with 2 time-series (0 sec and 2 sec). The corresponding test set consists in 1500 live images and 1500 fake images produced by using silicone, gelatin and PlayDoh, with 2 time-series (0 sec and 2 sec). Identix training dataset consists in 375 live images and 375 spoof images produced y using silicone, gelatin and PlayDoh, with 2 time-series (0 sec and 2 sec). The corresponding test set consists in 1125 live images and 1125 spoof images produced by using silicone, gelatin and PlayDoh, with 2 time-series (0 sec and 2 sec). The details about the data collection are shown in the tables 1 and 2. Table 3 reports details about the sensors used for LivDet 2009 Competition.

B. Procedure

We performed the following steps.

- 1. *Feature extraction*. Table 4 reports the 12 features we have considered and for each feature the time needed for the extraction process.

Table 2. Datasets For Testing.

Database	Subjects	Live Images	Fake Images	Frames
Biometrika	37	1440	1440	0 and 5 sec
Identix	125	1125	1125	0 and 2 sec
CrossMatch	191	5100	1500	0 and 2 sec

Table 3. Fingerprint Sensors Used For LivDet.

Scanners	Model No.	Resolution (dpi)	Image size
Biometrika	FX2000	569	(312x372)
Identix	DFR2100	686	(720x720)
CrossMatch	Verifier 300 LC	500	(480x640)

Table 4.. Time Required For Extracting Our Features When the Algorithm is Running On *Core Duo T8100 2,1 Ghz Intel* ProCessor.

Feature	Average Extraction Time
Gradient	0.06 sec
Energy	0.15 sec
Entropy	0.02 sec
Mean	0.02 sec
Variance	0.02 sec
Skewness	0.06 sec
Kurtosis	0.06 sec
Coefficientofvariation	0.02 sec
Stdofresidualnoise	0.59 sec
PoreSpacing	1 sec
*GrayLevel*1	0.02 sec
*GrayLevel*2	0.02 sec

Table 5. Selected Features For Each Database.

Featur	Biometrik	CrossMatc	Identix
Gradie	x	x	x
Energ		x	x
Entrop	x		x
Mea	x	x	x
Variance		x	x
Skewness		x	x
K		x	x
CoefficientOfV	x	x	x
StdResidualNoise	x	x	x
PoreSpacing	x	x	
*GrayLevel*1		x	
*GrayLevel*2	x		x

V. RESULTS AND DISCUSSION

For each sensor, the set of more discriminative features was used to train the classifier. In this section, we analyse the fingerprint images in the space of some features belonging to the three categories we have considered in the current paper. The Figures 5, 6, 7 and 8 correspond to the entropy, the mean, the variance and the coefficient of variation of the fingerprint image. These three first statistics present a good separability between the classes live and fake. The standard deviation of the residual noise also presents a good separability, as the Figure 9 shows.

Finally, Figure 10 and Figure 11 report the two intensity- based features, the Gray Level 2 and the gradient of the fingerprint image.

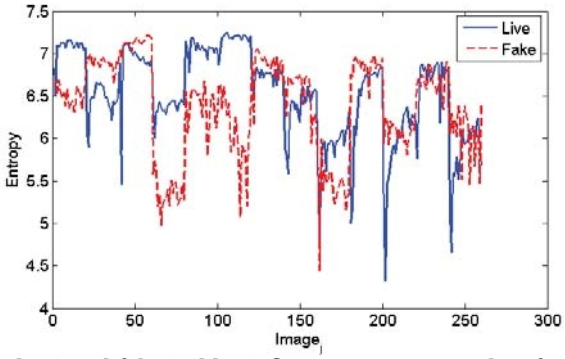

Fig. 5. Entropy for live(blue line) and fake(red line) fingerprint images taken from Biometrika database.

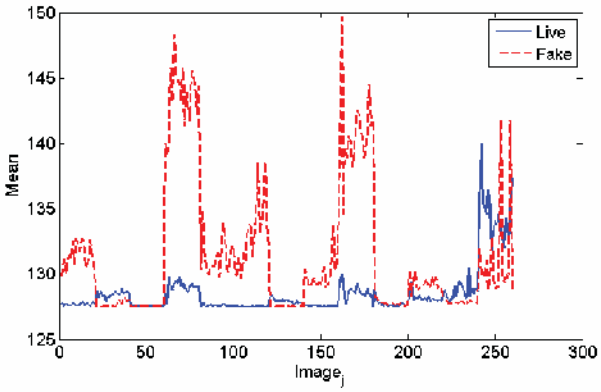

Fig. 6. Mean for live(blue line) and fake(red line) fingerprint images taken from Biometrika database.

To evaluate the classification performance, we have adopted the following parameters, used during the Liveness Detection
2009 Competition

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

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

Table 6 shows the performance achieved by the best algorithm submitted to the LivDet09 Competition, while Table 7 reports the error rate achieved with our method. As we can see, the average error rate of our approach, 12.47% outcomes the value of the best algorithm proposed during the LivDet09 Competition (14.6%). Performances depend on the technology of the sensor used to acquire the fingerprint images. We have achieved the higher percentage accuracy on *Biometrika* and *Identix* datasets by using a Multilayer Perceptron, while on *CrossMatch* dataset, a decision tree worked efficiently. Table 8 reports a comparison between the proposed algorithm and those presented during the LivDet09 Competition. Note that classification performance depends on the technology of the sensor, in particular it is affected by the resolution factor.

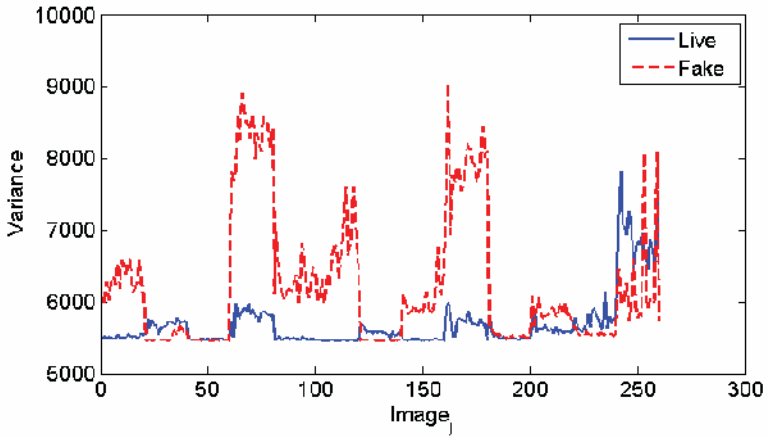

Fig. 7. Variance for live(blue line) and fake(red line) fingerprint images taken from Biometrika database.

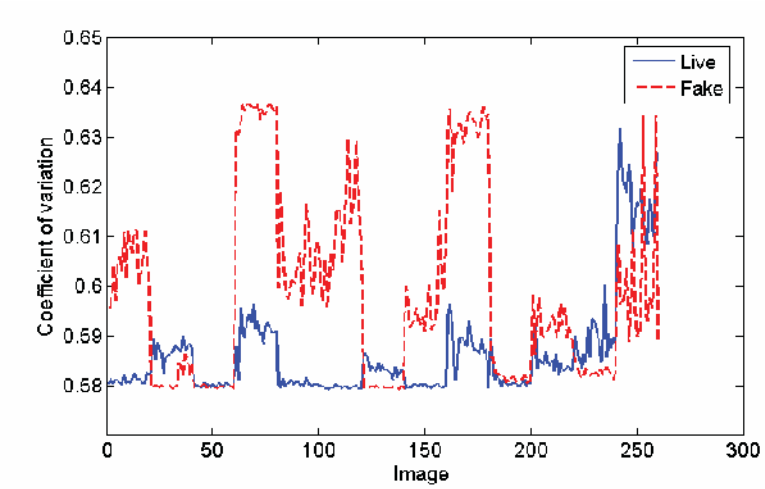

Fig. 8. Coefficient of variation for live(blue line) and fake(red line) fingerprint images taken from Biometrika database.

VI. CONCLUSIONS

We propose a novel algorithm for liveness detection to be integrated in fingerprint scanners. Since it was observed that textural characteristics of real fingerprints are different from those of spoof fingerprints, our approach combines multiple features derived from texture analysis, such as the first order statistics, the standard deviation of the residual noise, ratios between gray-level values, etc. This algorithm has been tested for three different types of scanner technologies. An important advantage of our method is that it does not require additional hardware, this reduces the cost of the fingerprint biometric system. Moreover, the required information can be extracted from only one image, this makes faster the overall authentication process since the user does not have to scan twice his finger.

REFERENCES

[1] J. Galbally, J. Fierrez, , and J. Ortega-Garcia. Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In *Proc. Spanish Workshop on Biometrics, SWB*, June 2007.

[2] H. Kim C. Jin and S. Elliott. Liveness detection of fingerprint based on band-selective fourier spectrum. *Information Security and Cryptology*, 4817:168–179, 2007.

[3] S. B. Nikam and S. Agarwal. Curvelet-based fingerprint anti-spoofing. *Signal, Image and Video Processing*, 4(1):75–87, January 2009.

[4] G. Marcialis P. Coli and F. Roli. Analysis and selection of features for the fingerprint vitality detection. *Structural, Syntactic and Statistical Pattern Recognition*, 4109:907–915, 2006.

[5] G. Marcialis et al. First international fingerprint liveness detection competition - livdet 2009. *Lecture Notes in Computer Science*, 5716:12–23, August 2009.

[6] K. Yamada T. Matsumoto, H. Matsumoto and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. *Optical Security and Counterfait Deterrence Techniques IV*, 4677:275–289, January 2002.

[7] J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador. On the vulner- ability of fingerprint verification systems to fake fingerprint attacks.

[8] J. Galbally, R. Cappelli, A. Lumini, G. González de Rivera, D. Maltoni, J. Fiérrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct attacks using fake fingers generated from iso templates. *Pattern Recognition Letters*, 31(8):725–732, 2010.