2015 IEEE Symposium Series on Computational Intelligence

A Preliminary Study on Identifying Fabrication Material from Fake Fingerprint Images

Ajita Rattani[1], Zahid Akhtar[2] and Gian Luca Foresti[2]
[1] University of Missouri at Kansas City, U.S.A.
Email: rattania@umkc.edu
[2]University of Udine, Udine, Italy.
Email: {zahid.akhtar, gianluca.foresti}@uniud.it

***Abstract*—Existing studies suggest the vulnerability of fingerprint verification system against spoof attacks. A spoofing attack occurs when an adversary mimics the biometric trait of another individual for illegitimate access and advantages. Liveness detection algorithms aim to detect live fingerprint samples from the fake artifact. A variety of materials, such as latex, gelatine and silicone, can be used to fabricate fake fingerprint samples. Continuous advancement in the spoofing techniques will lead to the introduction of new materials for fake fingerprint fabrication. However, the performance of these liveness detection algorithms severely degrade when new spoof materials are encountered during the operational stage. Therefore, there is a need for automatic detection of the fabrication material from fake fingerprint images. To this aim, this work investigates texture descriptors such as LBP, BSIF, BGP and GLCM for automatic detection of the fabrication material from fake fingerprint images.**

I. Introduction

Fingerprint recognition systems for person identification have proliferated over the past few decades [1]. Fingerprint recognition system is often required for government-controlled activities such as border crossings, as well as by private institutions such as banks. Moreover, many mobile devices now use fingerprints instead of passwords (e.g., iPhone 5s). Despite the recent progress, fingerprint recognition systems can be compromised through malicious attacks at many points within the system [2], [3]. In particular, they are vulnerable to many a spoof attack, which consists in submitting to the system an artefact fingerprint [4], [5], [6]. The spoofed/fake fingers can be fabricated using commonly available materials (e.g., latex) with the fingerprint ridges of an individual engraved on the surface [7], [8], [9]. These fake fingers can then be used by an adversary to launch a spoof attack by placing them on a fingerprint sensor and claiming the identity of another individual. The success rate of such spoof attacks can be up to 70% [7], [6], [9].

In fact, spoofing attacks have great practical relevance because they don't require advanced technical skills; therefore, the potential number of attackers is large [10]. Likewise, spoofing attacks are a major issue for companies selling biometric-based identity management solutions. For instance, in 2013, doctors at the Ferraz de Vasconcelos hospital in Brazil were caught using fake silicone fingers to defraud the hospital's biometric punch-in clock to get overtime [11]. Fingerprint liveness detection algorithms have been proposed as a quintessential anti-spoofing mechanism against spoof attacks [6], [8].

A fingerprint liveness detection method aims at discriminating live fingerprint samples from spoof artifacts [12]. Despite recent advances, the state-of-the-art in fingerprint liveness detection is not mature enough. This is because of the high error rates associated with current liveness detection algorithms [4], [13]. Further, the performance of these liveness detectors is significantly degraded during the operational stage, when spoofs are generated using materials not used during the training stage. Similarly, majority of liveness detectors do not account for the variations introduced by different sensors and datasets [10].

Reported studies [13], [14], [15] suggest a three fold increase in the error rate of the fingerprint liveness detector when spoofs using new materials (not used during the training stage) are encountered during the operational stage, thus suggesting the limited interoperability of existing liveness detectors across materials, sensors and datasets. Very few methods have been developed that are robust to variations instigated by the spoof fabrication materials, sensors and datasets [6], [7], [11]. However, Rattani et al. [5], [6], [7] and Akhtar et al. [10] recently devised schemes to improve the interoperability of liveness detection algorithms across spoof fabrication materials and sensors.

With the evolvement of the spoof attacks, it is likely that new materials will be discovered to launch spoof attacks, thus the nature of attack is unpredictable. As the liveness detector cannot be trained against spoofs generated using all the possible fabrication materials [7], it becomes necessary to automatically detect new spoof materials [5], [6], [7], [11]. The liveness detector can be retrained to new spoof materials to minimize any security risk posed by new spoof materials.

The problem of fingerprint liveness detection and identification of spoof fabrication materials is exacerbated by two facts. First, standard sensors are not able to distinguish images of a real fingerprint from those of an artificial replica. Second, there is often no obvious cue, visual or otherwise, that a captured image is coming from a spoof attack. In order to detect and mitigate vulnerabilities related to spoof fabrication materials or techniques, *digital spoof-material fingerprinting* methods may be applicable.

We define 'digital spoof material fingerprinting' as the process of identifying the source material used to fabricate spoof attacks, regardless of the image content. In other words, 'digital spoof material fingerprinting' provides the ability to

978-1-4799-7560-0/15 $31.00 © 2015 IEEE
DOI 10.1109/SSCI.2015.61

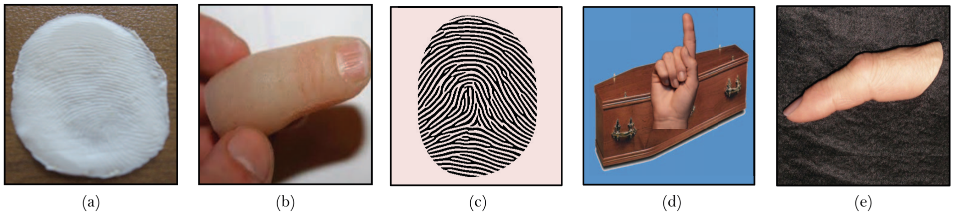


Fig. 1. Examples of fingerprint spoofing based on: (a) 2-D (flat) fake fingerprint using Silicone (b) synthesized 3-D fake fingerprint (c) reverse-engineered fingerprint image (d) cadaver fingerprint (e) finger cut from the user.

identify or validate the source material that was used to fabricate spoof attack, also called as *source material identification*. This technique i.e., 'source material identification' could be used for analyzing distinguishing characteristics in images due to different spoof fabrication material's imperfections [5], [6], [7]. All spoof fabrication materials and techniques have different characteristics and are also subject to manufacturing imperfections, resulting from inconsistencies during the production process. Such characteristics and fabrications errors/imperfections manifest as noise or texture changes in the ensuing image (which are often undetectable to human observers) and can be detected and characterized by machine learning, computer vision or image processing algorithms for the purpose of 'source material identification'.

In this paper, our focus is on "fingerprinting" fake fingerprint fabrication materials. In particular, the aim of this work is to design a scheme for automatic detection of the fabrication material from the fake fingerprint images. Such a classifier will facilitate the detection and automatic adaptation of the liveness detector to novel spoof materials.

This paper is organized as follows. Section II list different characteristics of fake fabrication materials and techniques that lead to performance differences. Section III outlines the features used for material detection. Section IV discusses the experimental protocol and experimental results. A conclusion is drawn in Section V.

II. Fingerprint Spoofing

In this section, we first give a short illustration of fingerprint spoofing methods, and then summarize spoof fabrication materials' characteristics.

A. Fingerprint Spoofing Methods

A fingerprint recognition system can be fooled by (see Fig. 1) (a) a 2-D (flat) fake fingerprint of a genuine user; (b) a synthesized 3-D fake fingerprint of a genuine user; (c) a reverse-engineered fingerprint image from template of a genuine user; (d) a cadaver fingerprint of a genuine user; (e) a dismembered finger from a genuine user.

Fake fingerprint could be fabricated either by 'consensual/cooperative/direct casts' or 'non-consensual/noncooperative/ indirect casts' method using easily available materials[1] like latex, gelatin and so on [8], [13]. In a non-consensual method fake fingerprints are fabricated from latent finger-marks on daily use product or sensors; hence, the cooperation of the user is not required. While, a consensual procedure [2] (i.e., with the consent and collaboration of the user) for fake fingerprint fabrication consists of the following steps: (i) a user is asked to press his finger against a soft material, such as wax, play-doh or plaster, to create a mould that holds a negative impression of the fingerprint; (ii) a casting (fabrication) material such as liquid silicon, wax, gelatin, or clay is poured on the mould; and (iii) after the liquid solidifies, the cast is lifted from the mould and is used as a fingerprint replica or fake finger [5], [6], [7].

B. Spoof Fingerprint Fabrication Materials

Rattani and Ross in [6], [7] mention that fabrication material should have high elasticity and very low shrinkage to avoid reduction in the volume as the cast cools and solidifies. Further, the authors [6], [7] also identified different characteristics exhibited by fabrication different materials as mentioned below. Note that studies in [6], [7] did not propose any scheme for automatic detection of the fabrication material from fake fingerprint images.

1) *Differences in artifacts:* Different fabrication materials possess different potential to hold a ridge and valley pattern [6], [7]. This can result in fabrication errors. Further, due to differences in the elasticity of materials, non-linear deformations may be introduced when pressure is applied by an adversary while presenting the fake finger to the sensor. Fig. 2 shows examples of fake fingerprint samples corresponding to five different fabrication materials (from LivDet 2011 [13]). Fabrication errors and non-linear deformations (an example indicated using red circle and white square) are quite evident in the case of silgum, woodglue and ecoflex.
2) *Differences in image quality:* Due to the presence of organic molecules in fabrication materials that tend to agglomerate, noise components are observed in the acquired fake fingerprint images [16], which may vary across materials [6], [7]. Consequently, quality of the fake fingerprint samples may vary across fabrication materials. Fig. 3 shows the difference in the range of quality values (obtained using the Image Quality of Fingerprint (IQF) freeware developed by MITRE[2]) across spoof samples generated using

[1] http://www.lumidigm.com/liveness-detection/: Fifty seven materials and variants have been recognized for fake fingerprints.

[2] http://www2.mitre.org/tech/mtf/

different fabrication materials. It can be seen that silgum and woodglue produced spoofs of relatively low quality. On the contrary, the quality of the spoofs generated using latex is quite similar to that of live fingerprint samples. The performance of the liveness detection algorithm significantly degrade when spoofs generated using new materials are encountered during the operational stage due to the aforementioned reasons. Therefore, it becomes beneficial to automatically detect the fabrication material of the fake fingerprints.

III. Texture Features used for Material Detection

Here, we discuss the image descriptors used in this study to extract the fabrication material characteristics from fake fingerprint image.

- **Binary Gabor Patterns (BGP)[17]**: These are efficient and effective multi-resolution approach to gray-scale and rotation invariant texture classification. Given a texture image, it is first convolved with J Gabor filters sharing the same parameters except the parameter of orientation. Then by binarizing the obtained responses, J bits are obtained at each location. Then, each location can be assigned a unique integer, namely rotation invariant binary Gabor pattern (BGPri), formed from J bits associated with it using a rule. The classification is based on the image's histogram of its BGPris at multiple scales.
- **Binary Statistical Image Features (BSIF)[18]**: This method for constructing local image descriptors which efficiently encode texture information and are suitable for histogram based representation of image regions. The method computes a binary code for each pixel by linearly projecting local image patches onto a subspace, whose basis vectors are learnt from natural images via independent component analysis, and by binarizing the coordinates in this basis via thresholding. The length of the binary code string is determined by the number of basis vectors. Image regions can be conveniently represented by histograms of pixels' binary codes.
- **Grey level Co-occurence Matric (GLCM)[19]**: A statistical method of examining texture that considers the spatial relationship of pixels is the gray-level co-occurrence matrix (GLCM), also known as the gray-level spatial dependence matrix. The GLCM functions characterize the texture of an image by calculating how often pairs of pixel with specific values and in a specified spatial relationship occur in an image, creating a GLCM, and then extracting statistical measures from this matrix. Some of the features include contrast, correlation, energy and homogeneity.
- **Local Binary Patterns (LBP)[20]**: The LBP feature vector, in its simplest form, is created in the following manner: Divide the examined window into cells (e.g. 16x16 pixels for each cell). For each pixel in a cell, compare the pixel to each of its 8 neighbors (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise. Where the center pixel's value is greater than the neighbor's value, write 1. Otherwise, write 0. This gives an 8-digit binary number (which is usually converted to decimal for convenience). Compute the histogram, over the cell, of the frequency of each number occurring (i.e., each combination of which pixels are smaller and which are greater than the center). Optionally normalize the histogram. Concatenate (normalized) histograms of all cells. This gives the feature vector for the window.

IV. Experiments

In this section, we provide experimental protocol and evaluation procedure of the proposed method to detect fabrication material from fake fingerprint images.

Database:

LivDet11 [13]: We exploited the same data set that was used to evaluate fingerprint liveness detection algorithms in the Second International Competition on Fingerprint Liveness Detection (LivDet11)[3]. This data set consists of 1000 live and 1000 fake fingerprint images each in training and test set, respectively. All images collected using the Biometrika sensor have been used in this study. These live images are obtained from 100 subjects with 10 samples from distinct finger per subject for each set (training and test). The fake fingerprints are fabricated using the following materials: gelatine, silicone, woodglue, ecoflex and latex. For each of these five materials, 200 images are fabricated from 20 subjects for each set.

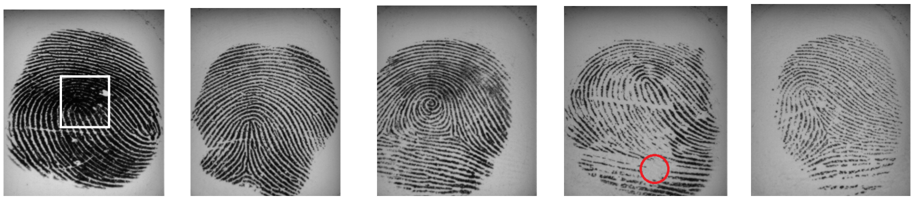
Protocol and Performance metrics: Following the LivDet2011 protocol as adopted in , we used 1000 live and 1000 fake images to train the proposed classifier, and the remaining 1000 live and 1000 fake images were reserved as the test set, which is used uniquely to gauge the generalization performance of the proposed material-detector.

(a) *Training stage*: During the training stage of the material detector, a set of n feature vectors $\mathbf{X} = \{\mathbf{x_1}, \mathbf{x_2} \ldots \mathbf{x_n}\}$ extracted from both live and spoof samples, along with their corresponding class labels $\{y_1, y_2, \ldots y_n\}$ where $y_i \in \{c_1, c_2, \ldots, c_K\}$ are used to train a multi-class AdaBoost. Spoofs generated using different materials have different class labels $(c_1 \ldots c_{K-1})$. Live samples are assigned a separate class (c_K). Thus, there are K classes, where $K-1$ is the number of spoof materials represented in the training set. The Adaboost algorithm [21] (adaptive boosting) is an ensemble learning method which combines multiple weak classifiers to form a single strong classifier as:

$$y(\mathbf{x}) = \sum_{t=1}^{T} \alpha_t h_t(\mathbf{x}) \tag{1}$$

where $h_t(\mathbf{x})$ refers to the weak classifiers operating on the feature vector $\mathbf{x}$, T is the number of weak classifiers, $y(\mathbf{x})$ is the classification output and α_t is the corresponding weight for each weak classifier.

[3] http://people.clarkson.edu/projects/biosal/fingerprint/index.php



(a) EcoFlex (b) Latex (c) Gelatine (d) Silgum (e) WoodGlue

Fig. 2. Examples of fake fingerprint images (from the LivDet 2011 [13] database) corresponding to five different fabrication materials. The artifacts introduced (an example indicated using circle and square) are typically quite prominent for silgum, woodglue and ecoflex materials, taken from [5], [7].

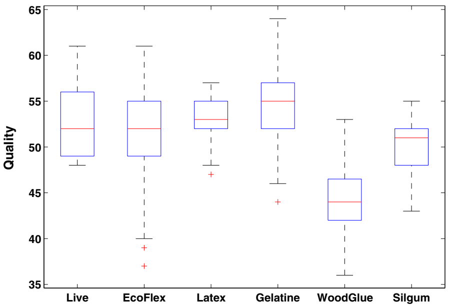


Fig. 3. Box-plot of the quality measures computed for 200 live and 200 fake fingerprint samples (acquired using Biometrika sensor) fabricated using five different materials from the LivDet 2011 dataset [13], taken from [5], [7].

The weak classifiers are generated after extracting a texture descriptor from the image. The following descriptors are considered in this work: Grey Level Co-occurence Matrix (GLCM) [19], Binary Statistical Image Features (BSIF) [18], Binary Gabor Patterns (BGP) [17] and Local Binary Patterns (LBP) [20].

For each of these descriptors, several weak classifiers are defined and iteratively added until a total of $T = 200$ (see equation (1)) weak classifiers are generated. Thus, the AdaBoost classifier for a particular descriptor is an ensemble of these 200 weak classifiers. Note that each of these descriptors is independently incorporated into an AdaBoost framework for implementation of the fabrication material-detector.

(b) *Testing stage*: For each input sample $(\bar{\mathbf{x}}_\mathbf{i})$ encountered during the operational phase, the label of the input sample $\left(p(c_k|\bar{\mathbf{x}}_\mathbf{i}) \text{ for } k = 1 \ldots K\right)$ belonging to each of the K classes is computed.

(c) *Performance metrics*: The performance of the fabrication material-detector is assessed using the following performance metrics: Correct detection rate (CDR): the proportion of fingerprint samples whose material has been correctly detected. False detection rate (FDR): the proportion of the fingerprint samples whose materials have been falsely identified. Confusion matrices to allow visualization of the performance of the material-detector in correctly identifying the material or falsely classifying as another material.

Results:

The confusion matrices of the material-detector implemented using GLCM, BSIF, LBP and BGP, respectively, are shown in the Tables I - IV for five fabrication materials and live fingerprint class. From these tables, it can be observed that Latex (66.5%) and Gelatine (64.0%) obtained the highest detection rate using LBP and BSIF-based image descriptors, respectively. Further, live samples can be easily distinguished from fake ones with the detection rate upto 94%.

However, the average correct detection rate for each material is low and unacceptable for real-time implementation. This suggest that these state-of-the-art descriptors are not very efficient in detecting the fabrication material from the fake fingerprints. In practical scenarios where nature of attacks can never be a priori known. Thus, a particular emphasis should be put on generalized liveness detection methodologies that have potential to detect varying or previously unseen spoofing attacks. Hence, the texture analysis should be combined with other characteristics such as coarseness analysis of the surface of fake fingerprint samples and noise residual for error rate reduction to acceptable level.

V. Conclusion

It is a well-know fact that fingerprint recognition systems are vulnerable to spoof attacks, which has led to the great advances in fingerprint anti-spoofing technologies, especially fingerprint liveness detection methods. Despite recent advances, counteracting fingerprint spoof attacks has proven to be a challenging task due to variations in spoof fabrication materials and techniques. In fact, recent studies suggest a three fold increase in the error rate of a fingerprint liveness detector on encountering spoofs generated using materials that were not used during the training stage. Therefore, in this paper, we designed a scheme for automatic detection of the fabrication materials from the fake fingerprint images, which may be used for novel spoof material detection and then to update the liveness detector. The proposed automatic spoof material detection scheme obtains a correct detection rate upto 67% depending upon the material and the features. This preliminary work suggests high error rate exhibited by state-of-the-art textural descriptors in detecting fabrication material from spoof fingerprint images. Future work will involve investigating new features such as noise residual and coarseness analysis and their fusion with the textural descriptors to reduce the error rate of the fabrication material-detector to acceptable level.

References

[1] J. Galbally et al., *Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition*, IEEE TIP, pp. 710-724, 2014.

TABLE I. Confusion matrix of the material-detector based on multi-class adaboost using GLCM for five fabrication materials; EcoFlex, Gelatine, Latex, Silgum, WoodGlue and the Live samples.

	Ecoflex [%]	Gelatine [%]	Latex [%]	Silgum [%]	WoodGlue [%]	Live [%]
Ecoflex	43.5	19.0	6.5	0.5	0.0	30.5
Gelatine	16.0	40.0	23.5	1.0	8.0	11.5
Latex	0.0	20.5	56.5	9.0	0.0	14.0
Silgum	0.0	18.0	0.0	37.5	3.5	41.0
WoodGlue	0.0	5.0	0.0	0.0	32.5	62.5
Live	2.0	6.8	1.8	4.3	3.3	81.8

TABLE II. Confusion matrix of the material-detector based on multi-class adaboost using BSIF for five fabrication materials; EcoFlex, Gelatine, Latex, Silgum, WoodGlue and the Live samples.

	Ecoflex [%]	Gelatine [%]	Latex [%]	Silgum [%]	WoodGlue [%]	Live [%]
Ecoflex	10.0	38.5	21.0	2.0	1.5	27.0
Gelatine	3.0	64.0	25.0	7.0	5.0	96.0
Latex	1.5	32.0	12.5	3.5	2.5	48.0
Silgum	0.0	13.0	24.0	12.0	9.5	41.5
WoodGlue	0.0	8.5	7.0	0.5	21.5	62.5
Live	0.4	2.1	0.0	1.7	2.1	93.7

TABLE III. Confusion matrix of the material-detector based on multi-class adaboost using BGP for five fabrication materials; EcoFlex, Gelatine, Latex, Silgum, WoodGlue and the Live samples.

	Ecoflex [%]	Gelatine [%]	Latex [%]	Silgum [%]	WoodGlue [%]	Live [%]
Ecoflex	20.0	20.5	27.0	2.5	2.0	28.0
Gelatine	3.0	35.5	13.5	4.0	12.5	31.5
Latex	0.5	14.5	55.0	3.5	8.0	18.5
Silgum	1.0	17.0	20.5	24.5	14.5	22.5
WoodGlue	0.5	3.5	2.0	1.0	44.0	49.0
Live	0.5	4.9	1.0	3.7	2.6	87.3

TABLE IV. Confusion matrix of the material-detector based on multi-class adaboost using LBP for five fabrication materials for five fabrication materials; EcoFlex, Gelatine, Latex, Silgum, WoodGlue and the Live samples.

	Ecoflex [%]	Gelatine [%]	Latex [%]	Silgum [%]	WoodGlue [%]	Live [%]
Ecoflex	20.5	17.0	33.0	1.0	0.0	28.5
Gelatine	1.0	39.0	25.5	0.0	2.0	32.5
Latex	0.5	7.0	66.5	0.5	0.5	25.0
Silgum	3.5	26.0	16.0	17.5	7.5	29.5
WoodGlue	0.0	11.0	11.5	0.0	46.5	31.0
Live	0.3	5.1	0.7	2.6	1.4	89.9

[2] Z. Akhtar, *Security of Multimodal Biometric Systems against Spoof Attacks*, PhD thesis, University of Cagliari, Italy, 2012.

[3] A. Rattani, N. Poh, *Biometric system design under zero and non-zero effort attacks*, International Conference on Biometrics, pp.1-8, 2013.

[4] D. Gragnaniello et al., *Local contrast phase descriptor for fingerprint liveness detection*, Pattern Recognition, vol. 48, no. 4, 2015.

[5] A. Rattani, W. Scheirer, A. Ross, *Open Set Fingerprint Spoof Detection Across Novel Fabrication Materials*, IEEE Transactions on Information Forensics And Security (TIFS), 2015.

[6] A. Rattani, A. Ross, *Automatic adaptation of fingerprint liveness detector to new spoof materials*, IEEE Int'l Joint Conference on Biometrics (IJCB), pp.1-8, 2014.

[7] A. Rattani, A. Ross, *Minimizing the impact of spoof fabrication material on fingerprint liveness detector*, IEEE International Conference on Image Processing (ICIP), pp.4992-4996, 2014.

[8] S. Marcel, M. Nixon, and S. Z. Li, *Handbook of Biometric Anti-Spoofing*, Springer, 2014.

[9] T. Matsumoto et al., *Impact of artificial "gummy" fingers on fingerprint systems*, In Proc. of SPIE Opt. Sec. Counterfeit Deterrence Tech. IV, pages 275-289, 2002.

[10] Z. Akhtar, C. Micheloni, G. L. Foresti, *Correlation based fingerprint liveness detection*, Int'l Conf. on Biometrics (ICB), pp.305-310, 2015.

[11] Z. Akhtar, C. Micheloni, G. L. Foresti, *Biometric Liveness Detection: Challenges and Research Opportunities*, IEEE Security & Privacy Magazine, 2015.

[12] Z. Akhtar, C. Micheloni, C. Piciarelli, G. L. Foresti, *MoBio_LivDet: Mobile biometric liveness detection*, IEEE Intl Conf. on Advanced Video and Signal Based Surveillance, pp.187-192, 2014.

[13] D. Yambay et al., *LivDet 2011 - fingerprint liveness detection competition*, In Proc. of IEEE Intl. Conf. on Biometrics, pp. 208-215, 2012.

[14] B. Tan et al.,, *The effect of environmental conditions and novel spoofing methods on fingerprint anti-spoofing algorithms*, In Proc. of IEEE Intl. Workshop on Information Forensics and Security, pp. 1-6, 2010.

[15] E. Marasco, C. Sansone, *On the robustness of fingerprint liveness detection algorithms against new materials used for spoofing*, In Proc. of Intl. Conf. on Bio-Inspired Sys. and Signal Proc., pp. 553-558, 2011.

[16] Y. Moon et al., *Wavelet based fingerprint liveness detection*, Electronic Letters, 41:11121113, 2005.

[17] L. Zhang and Z. Zhou and H. Li, *Binary gabor pattern: An efficient and robust descriptor for texture classification*, Proc. of IEEE Intl. Conf. on Image Processing, FL, USA, 2012.

[18] J. Kannala and E. Rahtu, *BSIF: Binarized statistical image features*, ICPR, 1363-1366, 2012.

[19] R. M. Haralick and K. Shanmugan and I. Dinstein, *Textural Features for Image Classification*, IEEE Trans. on Systems, Man, and Cybernetics, 3:610-621, 1973.

[20] T. Ojala and M. Pietikinen and T. Menp, *Multiresolution gray-scale and rotation invariant texture classification with Local Binary Patterns*, IEEE PAMI, 24(7):971-987, 2002.

[21] Y. Freund and R. E. Schapire, *A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting*, Journal of Computer and System Sciences, 55:119-139, 1997.