International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

A Survey on Anti-Spoofing Techniques for Face and Fingerprint Modalities

Sukhchain Kaur[1], Reecha Sharma[2]
[1,2]Department of Electronics and Communication, Punjabi University Patiala, India

***Abstract*- The need for automation of the identity recognition process for a vast number of applications resulted in great advancement of biometric systems in the recent years. Yet, many studies indicate that these systems suffer from vulnerabilities to spoofing (presentation) attacks: a weakness that may compromise their usage in many cases. A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access. The goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of anti-spoofing, with special attention to the mature and largely deployed face and fingerprint modalities.**

***Keywords*- Security, Anti-spoofing, EER (Equal Error Rate), TER (Total Error Rate), FSA (False Spoof Acceptance), FLR (False Live Rejection).**

I. INTRODUCTION

As modern means of communication increase in their potential and receptiveness, they instigate additional demands in terms of security. Biometric recognition is a new technology that has become the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric-based solutions are able to provide trustworthy financial transactions and personal data privacy. Biometric authentication has been considerable improvement in reliability and accuracy, with some of the traits offering better performance.

However, in spite of these advantages, biometric systems have some drawbacks, including: (i) the lack of secrecy (e.g. everybody knows our face or could get our fingerprints) and (ii) the fact that a biometric trait cannot be replaced. Furthermore, biometric systems are vulnerable to external attacks which could decrease their level of security. Among the different vulnerabilities analyzed, intensive research efforts have been focused on the study of *direct* or *spoofing* attacks.

Spoofing is a purely biometric vulnerability that is not shared with other IT security solutions. Therefore, spoofing consists in using an artificial trait to imitate a different user or to create a new genuine identity. Several scenarios are typically conceived for spoofing attacks depending on the type of biometric system considered. (*i*) Verification system: Spoofing is carried out at the time of authentication by presenting to the sensor a fake physical copy of the genuine's user trait. Such artefact is acquired and matched to the enrolled real template of the genuine user. (*ii*) Verification system/Identification system in closed set: Spoofing may also be performed at the enrolment stage by generating a new identity with an artifact (not necessarily imitating any real user's trait) which can later be used by different users to access the system. (*iii*) Identification system in open set: Typically this case corresponds to look-up systems where a new identity is created using the spoofing artefact to avoid being found in a watch list (e.g., to obtain a VISA for illegally entering a country).

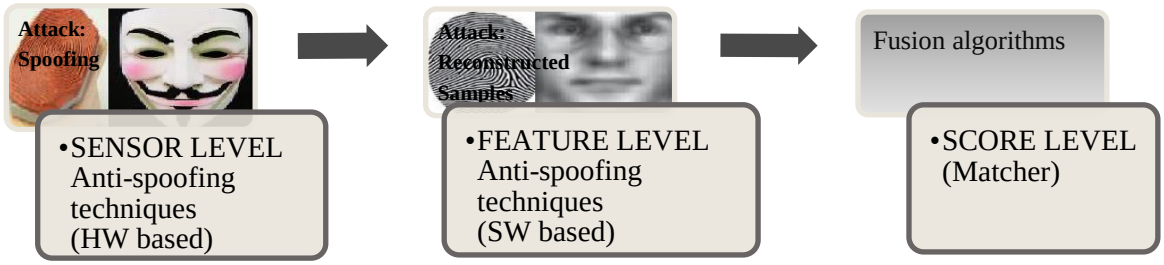

FIGURE 1. General diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated (sensor-level, feature-level and score-level). Also displayed are the two different type of attacks for which anti-spoofing techniques may offer protection: spoofing and attacks carried out with synthetic or reconstructed samples.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Given the above spoofing definition, an *anti-spoofing* method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artefacts containing a biometric trait. From a general perspective, anti-spoofing techniques may be classified into one of three groups depending on the biometric system module in which they are integrated.

1.1 SENSOR-LEVEL TECHNIQUES-

Usually referred to in the literature by the term *hardware-based* techniques. These methods add some specific device to the sensor in order to detect particular properties of a living trait (e.g., facial thermogram, blood pressure, fingerprint sweat, or specific reflection properties of the eye). As shown in Fig. 2, such techniques are integrated in the biometric sensor. In general, hardware-based approaches measure one of three characteristics, namely: (*i*) intrinsic properties of a living body, including physical properties (e.g., density or elasticity), electrical properties (e.g., capacitance, resistance or permittivity), spectral properties (e.g., reflectance and absorbance at given wavelengths) or even visual properties (e.g., colour and opacity); (*ii*) involuntary signals of a living body which can be attributed to the nervous system. Good examples are the pulse, blood pressure, perspiration, pupillary unrest (hippus), brain wave signals (EEG) or electric heart signals; (*iii*) responses to external stimuli, also known as *challenge-response* methods, which require the user cooperation as they are based on detecting voluntary (behavioural) or involuntary (reflex reactions) responses to an external signal.

Examples of such methods can be the pupil contraction after a lighting event (reflex), or the head movement following a random path determined by the system (behavioural). Multibiometric anti-spoofing is based on the hypothesis that the combination of different biometrics will increase the robustness to direct attacks, as, in theory, generating several fake traits is presumed to be more difficult than an individual trait.

1.2 FEATURE-LEVEL TECHNIQUES-

Usually referred to in the literature by the term *software-based* techniques. In this case the fake trait is detected once the sample has been acquired with a standard sensor. As such, features used to distinguish between real and fake traits are extracted from the *biometric sample* (usually images, as in the case of face, or some kind of time-functions, as in the case of speech), and not directly from the human body as in the case of sensor-level techniques. These methods are integrated after the sensor, usually functioning as part of the feature extractor module (as shown in Fig. 2).They can be further classified into *static* and *dynamic* anti-spoofing methods, depending on whether they work with only one instance of the biometric trait, or with a sequence of samples captured over time. Although they may present some degradation in performance, in general, static features are preferable over dynamic techniques as they usually require less cooperation from the user, which makes them faster and less intrusive.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

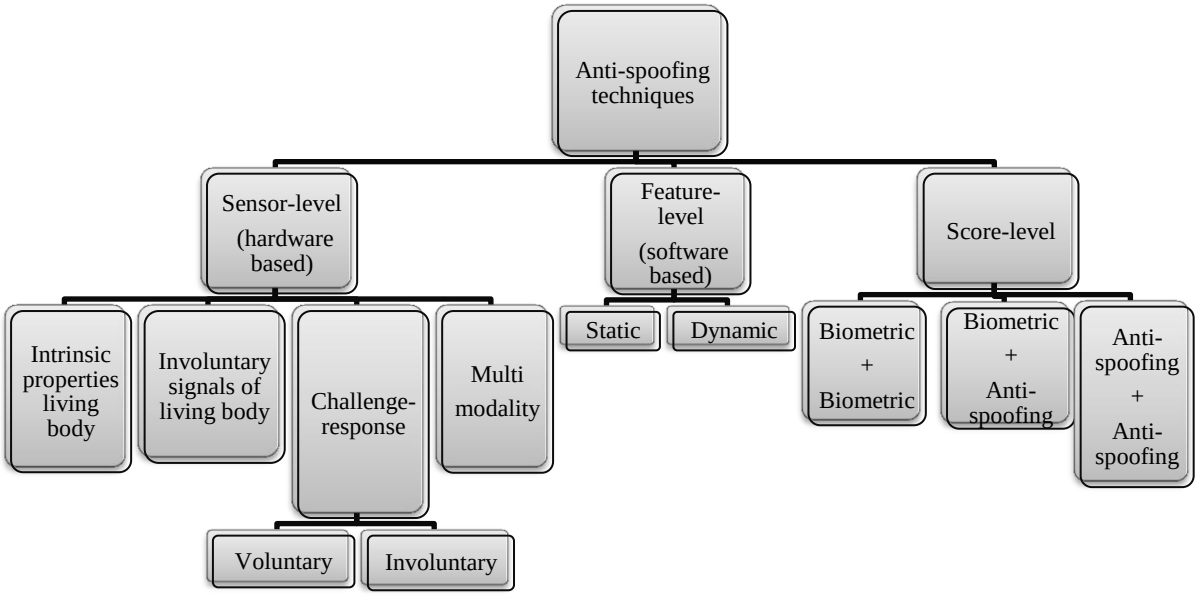

FIGURE 2. GENERAL CLASSIFICATION OF ANTI-SPOOFING METHODS CONSIDERED IN THE PRESENT ARTICLE WITH THE THREE MAIN GROUPS DEPICTED IN FIG. 1: SENSOR-LEVEL, FEATURE-LEVEL AND SCORE-LEVEL TECHNIQUES

1.3 SCORE-LEVEL TECHNIQUES-

Recently, a third group of protection methods which fall out of the traditional two-type classification (software- and hardware-based), has started to be analyzed in the field of fingerprint anti-spoofing. These protection techniques, much less common than the previous two categories, are focused on the study of biometric systems at *score-level* in order to propose fusion strategies that increase their resistance against spoofing attempts.

Due to their limited performance, they are designed as supplementary measures to the sensor-level and feature-level techniques presented above, and are usually integrated in the matcher (as shown in Fig. 2). The scores to be combined may come from: *i*) two or more unimodal biometric modules; *ii*) unimodal biometric modules and anti-spoofing techniques; or *iii*) only results from anti-spoofing modules.

TABLE 1.
Coarse comparison between the types of anti-spoofing techniques .

TYPE	SUBTYPE	Performance	Low cost	User friendly	Non-invasive	Protection vs other attacks
Sensor level	Intrinsic properties	High	Medium	Low	Low	Low
	Involuntary signals	High	Low	Low	Low	Low
	Challenge response	High	Low	Low	Low	Low
	Multi-modality	Medium	Low	Medium	Medium	Low
Feature level	Static	Medium	Medium	Medium	High	Medium
	dynamic	Medium	Medium	Low	Low	Medium
Score level	Biom.+biom.	Very low	Medium	Medium	High	Low
	Biom.+Anti-spoofing	Very low	Medium	Medium	High	Low
	Anti-spoofing+Anti-spoofing	Very low	Medium	Medium	High	Low

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

II. LITERATURE SURVEY

2.1 Fingerprint Anti-Spoofing Techniques Review-

2.1.1 Feature Level Techniques (Static)-

In 2005, Y.S. Moon et al. Proposed a simple and effective approach for fingerprint liveness detection based on the wavelet analysis of the finger tip surface texture. In the proposed approach, they treat the surface coarseness as a kind of Gaussian white noise added to the images. A finger tip image is first denoised using the wavelet based approach. The noise residue (original image – denoised image) was then calculated. Coarser surface texture tends to result in a stronger pixel value fluctuation in the noise residue. Thus, the standard deviation of the noise residue can be used as an indicator to the texture coarseness.

In 2006, Aditya Abhyankar et al. proposed an algorithm provides a faster technique for doing a liveness test which relies on only one fingerprint image.The approach is based on underlying texture and density of the fingerprint images.The algorithm combines the features derived from multiresolution texture analysis as well as derived from local ridge frequency analysis.The features are further processed using FCM and error rates were calculated. Based on the association of all the points to particular type of a class, the classification rates were calculated.Advantages of this method were that it is purely software based and only requires one image.

In 2007, C. Jin et al. proposed a fake finger detection approach based on band-selective Fourier spectrum.The ridge-valley structure of the fingerprint produces a ring pattern around the center in the Fourier spectral image and a harmonic ring pattern in the subsequent ring. Both live and fake fingerprints produce these rings, but with different amplitudes in different spatial frequency bands. Typically, live fingerprints show stronger Fourier spectrum in the ring patterns than the fake. The proposed method classifies the live and the fake fingerprints by analyzing the band-selective Fourier spectral energies in the two ring patterns. The experimental results demonstrate this approach to be a promising technique for making fingerprint recognition systems more robust against fake-finger-based spoofing vulnerabilities.

In 2008,S. Nikam et al. presented a new texture-based method which is based on the observation that, real and spoof fingerprints exhibit different textural characteristics. Local binary pattern (LBP) histograms are used to capture these textural details.

Wavelet energy features characterising ridge frequency and orientation information are also used for improving the efficiency of the proposed method. Advantage of this method was that it do not require extra hardware to detect liveness.

In 2009, S. Nikam et al. Presented textural measures based on gray level co-occurrence matrix (GLCM) are used to characterize fingerprint texture. This is based on structural, orientation, roughness,smoothness and regularity differences of diverse regions in a fingerprint image. Wavelet energy signature is also used to obtain texture details. GLCM texture features and wavelet energy signature are independently tested on three classifiers: neural network, support vector machine and K-nearest neighbor.

In 2009, J. Galbally et al. presented a novel fingerprint parameterization for liveness detection based on quality measures. In the first step the fingerprint was segmented from the background, for this purpose, Gabor filters are used as proposed in. Once the useful information of the total image was separated, ten different quality measures were extracted which will serve as the feature vector that will be used in the classification. Prior to the classification step, the best performing features were selected depending on the sensor that was used in the acquisition. Once the final feature vector has been generated the fingerprint was classified as real or fake.The proposed solution proves to be robust to the multi-sensor scenario.

In 2009, S. Nikam et al. developed a single-image-based method using newly introduced curvelet transform to detect vitality. The main benefit of curvelets is their capability of representing a curve as a set of superimposed functions of various lengths and widths. Textural measures based on curvelet energy and co-occurrence signatures were used to characterize fingerprint image. All texture features (energy, co-occurrence and fused signatures) provide better results than the wavelet based and power spectrum-based methods in related works.

In 2010, E. Marasco et al. proposed a novel software-based solution for liveness detection based on static features coming out from the visual texture of the image. Since it was observed that textural characteristics of real fingerprints are different from those of spoof fingerprints, this 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

This algorithm has been tested for three different types of scanner technologies. An important advantage of this method was that it does not require additional hardware, this reduces the cost of the fingerprint biometric system.

In 2012, L. Ghiani et al. presented feature-level fusion of several fingerprint liveness detection algorithms, beside the proposal of a novel algorithm, based on the local phase quantization of the fingerprint images. However, no works studied the possibility of combining different feature sets, thus exploiting the eventual complementarity among them.So the proposed system is another step ahead with respect to the state-of-the-art, by pointing out that current fingerprint liveness detection algorithms cannot be adopted individually, but their combination, carefully handled, can help in improving the performance, thus allowing their integration in current fingerprint verification systems.

In 2013, L. Ghiani et al. introduced the use of BSIF, a textural analysis algorithm, in fingerprint liveness detection.

The idea behind BSIF was to automatically learn a fixed set of filters from a small set of natural images, instead of using handcrafted filters such as in LBP and LPQ. The proposed approach for fingerprint representation consists of apply learning, instead of manual tuning, to obtain statistically meaningful representation of the fingerprint data.

In 2015, D. Gragnaniello et al. proposed a new local descriptor for fingerprint liveness detection. The input image was analyzed both in the spatial and in the frequency domain, in order to extract information on the local amplitude contrast, and on the local behavior of the image, synthesized by considering the phase of some selected transform coefficients.These two pieces of information are used to generate a bi-dimensional contrast-phase histogram, used as feature vector associated with the image. After an appropriate feature selection, a trained linear-kernel SVM classifier makes the final live/fake decision.

TABLE 2.
Summary of the most relevant Fingerprint anti-spoofing techniques.

Fingerprint anti-spoofing techniques				
Feature level techniques				
Reference	**Subtype**	**Features and methodology**	**Sensor**	**Error**
2005, Y.S. Moon et al. [1]	Static	Texture / Wavelet	Optical	FLR=0%;FSA=0%(Th=25)
2006, Aditya Abhyankar et al. [2]	Static	Texture / Statistics	Optical Capacitive Electrooptical	EER=2.7% EER=3.5% EER=7.7%
2007, C. Jin et al. [3]	Static	Texture / Fourier	Optical	FLR=23%;FSA=12%
2008,S. Nikam et al. [4]	Static	Texture / LBP; Wavelet	Optical	TER=3%-6%
2009,S. Nikam et al. [5]	Static	Texture / Curvelet	Optical	TER=1.82%-5.65%
2009, J. Galbally et al. [6]	Static	Quality / Gabor Filters	Optical	TER=7%
2009,S. Nikam et al. [7]	Static	Texture/ Curvelet	Optical	TER=1.78%-5.65%
2010, E. Marasco et al. [8]	Static	Texture; Perspiration/ Fourier;Wavelet	Optical	FLR=12.6%;FSA=12.3%
2012, L. Ghiani et al. [9]	Static	Texture/ LPQ	Optical	EER=2.3%
2013, L. Ghiani et al. [10]	Static	Texture/ BSIF	Optical	TER=7.22%
2015, D. Gragnaniello et al. [11]	Static	Texture/ LCPD	Optical	TER=5.7%

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

2.2 Face Anti-Spoofing Techniques Review-

2.2.1 Feature Level Techniques (Static)-

In 2010, X. Tan et al. presented a novel method for liveness detection against photo spoofing in face recognition. They investigated the different nature of imaging variability from a live human or a photograph based on the analysis of Lambertian model, which leads to a new strategy to exploit the information contained in the given image. Further ,some current illumination-invariant face recognition algorithm can be modified to collect the needed latent samples, which allows us to learn a sparse nonlinear/bilinear discriminative model to distinguish the inherent surface properties of a photograph and a real human face. Experiments on a large photo imposter database show that the proposed method gives promising photo spoof detection performance, with advantages of realtime testing, non-intrusion and no extra hardware requirement.

In 2012, Z. Lei et al. released a face anti-spoofing database with diverse attacks to serve as an evaluation platform in the literature. The database contains 50 genuine subjects, and the fake faces are produced from the high quality records of the genuine faces. Three imaging qualities and three kinds of fake face attacks are included. They also designed a test protocol which consists of 7 scenarios to provide a thorough analysis of different factors which may affect the anti-spoofing accuracy. Further,designed a DoG+SVM algorithm to explore high frequency information to classify genuine and fake faces, which serves as the baseline algorithm.

In 2012, I. Chingovska et al. introduces REPLAY-ATTACK, a novel spoofing attack database containing three types of possible attacks: printed photographs, and photos and videos displayed on electronic screens of different sizes using three different media and two different recording conditions. The database includes a protocol for training, development and testing purposes, and also proves the vulnerability of a baseline face recognition system to its attacks. Secondly, it proposed a simple and easily reproducible LBP based face spoofing counter-measure and explored its efficiency against a variety of attacks.

Further, they concluded that LBP, with _15% Half Total Error Rate, show moderate discriminability when confronted with a wide set of attack types.

In 2012, A. Hadid et al. proposed an approach for spoofing detection based on learning texture features and gradient structures from single images that discriminate live face images from fake ones. The proposed approach analyses the texture and gradient structures of the facial images using a set of low-level feature descriptors, fast linear classification scheme and score level fusion.In addition, the texture features that are used for spoofing detection can also be used for face recognition.This provides a unique feature space for coupling spoofing detection and face recognition. This attack-specific countermeasure obtained excellent results under various fake face attacks, especially under video replay attacks.

In 2013, J. Komulainen et al. proposed to approach the problem of face spoofing as a set of attack-specific subproblems that are solvable with a proper combination of complementary countermeasures. Inspired by how we humans can perform reliable spoofing detection only based on the available scene and context information, this work provides the first investigation in research literature that attempts to detect the presence of spoofing medium in the observed scene. The proposed approach consists of a cascade of an upper-body and a spoofing medium detector that are based on histogram of oriented gradients descriptors and linear support vector machines.

In 2015, L. Feng et al. proposed an extendable multi-cues integration framework for face anti-spoofing using a hierarchical neural network, which can fuse image quality cues and motion cues for liveness detection. Shearlet was utilized to develop an image quality-based liveness feature. Dense optical flow was utilized to extract motion-based liveness features. A bottleneck feature fusion strategy was able to integrate different liveness features effectively. The proposed approach was evaluated on three public face antispoofing databases. A half total error rate (HTER) of 0% and an equal error rate (EER) of 0% were achieved on both REPLAY-ATTACK database and 3D-MAD database. An EER of 5.83% was achieved on CASIA-FASD database.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

TABLE 3.
Summary of the most relevant Face anti-spoofing techniques.

Face anti-spoofing techniques				
Feature level techniques				
Reference	**Subtype**	**Features and methodology**	**Attack**	**Error**
2010, X. Tan et al. [12]	Static	Face texture using the lambertian model	Photo	15%
2012, Z. Lei et al. [13]	Static	Face texture frequency analysis using Difference of Gaussian(DOG) filters	Photo, Video	15%
2012, I. Chingovska et al. [14]	Static	Face texture using LBP's	Photo, Video	15%
2012, A. Hadid et al. [15]	Static	Texture +shape combining LBP's + Gabor wavelets +HOG	Photo	0.5%
2013, J. Komulainen et al. [16]	Static	Context-based using upper body and spoof spot detection	Photo, Video	3%
2015, L. Feng et al. [17]	Static	Image quality and motion cues using NN	Photo, Video	5.83%

III. CONCLUSION

This paper presents various countermeasures that are used in literature to deflect the spoofing attacks for face and fingerprint modalities. From the discussed methods of anti-spoofing it can be concluded that the feature level techniques are easy to establish as they does not require additional sensor and features extracted from standard datasets consisting of live and fake samples are used to develop the countermeasure. Further, Static features are preferable over dynamic as they require lesser user cooperation, faster and less intrusive.

Also from the literature, Liveness detection techniques in which the recent feature extraction algorithms such as LBP, HOG, LPQ, GLCM, Gabor wavelets extract features from public available databases which are then given to classifier show excellent results in terms of lower values of error rates.

REFERENCES

[1] Y. Moon, J. Chen, K. Chan, K. So., and K. So. Woo," Wavelet based fingerprint liveness detection" Electronic Letters 41, 2005,pp. 1112–1113.

[2] A.Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques" in Proceedings of the IEEE International Conference on Image Processing (ICIP'06),2006,pp. 321–324.

[3] C. Jin, H. Kim, and S. Elliott., "Liveness detection of fingerprint based on band-selective Fourier spectrum" Information Security and Cryptology 4817 (2007),pp. 168–179.

[4] S. Nikam and S. Agarwal, "Local binary pattern and wavelet-based spoof fingerprint detection" International Journal of Biometrics 1, 2 (2008),pp. 141–159.

[5] S. Nikam and S. Agarwal, "Co-occurrence probabilities and wavelet-based spoof fingerprint detection" International Journal of Image and Graphics 9, 2 (2009),pp. 171–199.

[6] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Fingerprint liveness detection based on quality measures" in Biometrics, Identity and Security (BIds), 2009,pp. 1–8.

[7] S. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing" Signal, Image and Video Processing 4, 1 (January 2009), pp. 75–87.

[8] E. Marasco and C. Sansone, "An anti-spoofing technique using multiple textural features in fingerprint scanners" in Proceedings of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMs'10),2010,pp. 8–14.

[9] L. Ghiani, G. Marcialis, and F. Roli, "Experimental results on the feature-level fusion of multiple fingerprint liveness detection algorithms" in Proceedings of the ACM Workshop on Multimedia and Security,2012.

[10] L. Ghiani, A. Hadid, G. Marcialis, and F. Roli., "Fingerprint liveness detection using binarized statistical image features" in Proceedings of the IEEE 6th International Conference on Biometrics: Theory, Applications, and Systems (BTAS'13),2013.

[11] D. Gragnaniello, Diego, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. "Local contrast phase descriptor for fingerprint liveness detection." Pattern Recognition 48, no. 4 ,2015,pp. 1050-1058.

[12] X. Tan, Y. Li, J. Liu, and L. Jiang, ``Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. Eur.Conf. Comput. Vis. (ECCV), vol. LNCS 6316. 2010, pp. 504-517.

[13] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, ``A face antispoofing database with diverse attacks," in Proc. IAPR Int. Conf. Biometrics (ICB), Mar./Apr. 2012, pp. 26-31.

[14] I.Chingovska, A. Anjos, and S. Marcel, ``On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG), Sep. 2012, pp. 1-7.

[15] J. Määttä, A. Hadid, and M. Pietikäinen, ``Face spoofing detection from single images using texture and local shape analysis," IET Biometrics,vol. 1, no. 1, pp. 3-10, Mar. 2012.

[16] J. Komulainen, A. Hadid, and M. Pietikainen, ``Context based face anti-spoofing," in Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl.Syst. (BTAS), Sep./Oct. 2013, pp. 1-8.

[17] Feng, Litong, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, and Kwok-Wai Cheung. "Integration of image quality and motion cues for face anti-spoofing: A neural network approach." Journal of Visual Communication and Image Representation 38 ,2016,pp. 451-460.