INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Face spoofing detection using LBP descriptor and ensemble subspace discriminant classifier

Shahna J. S
shahna737@gmail.com
Marian Engineering College,
Thiruvananthapuram, Kerala

Minnu Jayan C
minnu.j@gmail.com
Marian Engineering College,
Thiruvananthapuram, Kerala

ABSTRACT

Recently, automatic face recognition has become a realistic target of biometrics research. Face fake attacks are truly a threat to face recognition systems. Exploration on non-invasive software based face spoofing detection schemes have been mainly concentrated on the analysis of the luminance information of the face images, accordingly discarding the chroma component, which can be very useful for discriminating fake faces from genuine ones. In this paper, we present a novel approach based on analyzing joint color-texture information of the facial image from the luminance and the chrominance channels using color local binary pattern (LBP) descriptor. Particularly the feature histograms are extracted from each image band separately. The resulting feature histograms are concatenated into an enhanced feature histogram inorder to obtain an overall reproduction of the facial color texture. The final feature vector is fed to an ensemble subspace discriminant classifier and it describes whether there is a live person in front of the camera or a fake one. Also, we determine the performance measures of an ensemble classifier and compare with SVM.

Keywords: *Face recognition, Spoofing detection, LBP, Color-texture analysis, and Ensemble subspace classifier.*

1. INTRODUCTION

Nowadays, most of the existing face recognition systems are susceptible to spoofing attacks [1] through which unauthorized attackers try to access illegal authorities by exhibiting fake faces of an authorized client. Significant consequences may occur if these attacks succeed, yet unfortunately, there still lack effective anti-spoofing techniques. While attackers can obtain a client's face images by using portable digital cameras or simply downloading from the internet, and fake faces can be easily produced, for example, printing photos or showing videos on a laptop. Fake faces like photos and video playbacks are not easy to implement but also usually quite effective in spoofing a face recognition system [3]. For instance, in [2], the Windows XP and Vista laptops of Lenovo Asus and Toshiba come with built-in webcams and embedded biometric systems that authenticate users by scanning their faces. Although, in 2009, the Security and Vulnerability Research team of the University of Hanoi (Vietnam) has demonstrated at Black Hat 2009 conference, the world's premier technical security conference, how to easily spoof and bypass these systems (Lenovo's Veri face III, Asus' Smart Logon V1.O.0005, and Toshiba's Face Recognition 2.0.2.32- each set to its highest security level) using fake facial images of the legitimate user and thus gaining access to the laptops. This vulnerability is now listed in the National Vulnerability Database of the National Institute of Standards and Technology (NIST) in the US. This single example reveals the risks in current face recognition systems, which suggest a rapid need for addressing spoofing attacks to enhance the security and robustness of face recognition systems, and to bring the technology into practical use.

Fig-1: Cropped and normalized example face images from the CASIA FA dataset. From left to right: real faces and the corresponding cut photo and video replay attacks

Assuming that there are characteristic dissimilarities between genuine faces and artificial material that can be observed in single images or a sequence of images, many anti-spoofing techniques analyzing static and dynamic facial appearance properties have been proposed. The key idea is that an image of a fake face passes through two different camera systems and a printing system or a display device, thus it can be mentioned too as a recaptured image. Therefore, the observed fake face image is likely to have lower image quality compared to a genuine one captured in the same conditions due to lack of high-frequency information [5]. The recapturing process discussed above suggests also inherent dissimilarity in the color information between a genuine face and a fake face image. This is owing to the used spoofing medium like printed photograph, display device or mask dependant gamut and other deformities in the in the color reproduction, e.g. printing defects or noise signatures. The camera used for capturing the targeted face sample will also lead to imperfect color reproduction contrast to the authorized biometric sample. Furthermore, images tend to look different when they are printed or displayed using different devices. In order to maintain the color and appearance perception over the different device, color mapping algorithms can be applied on the source image to map it's out of gamut color into the color gamut of a specific output device. Anyway, these kinds of mapping functions can cause variations between the texture of original and the output images [5].

Influence by image quality assessment, characterizations of printing artefacts and by differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. Actually, face prints usually contain printing quality defects that can be well detected using color – texture patterns [2]. Texture analysis of grey scale face images can provide adequate way to demonstrate to the recapturing artefacts of fake faces if the image resolution is good enough to capture the fine details of the observed face. Anyway, if we take close look at the cropped facial images of the genuine human face and corresponding fake ones, it is basically impossible to obviously name any textural difference between them, because in the input image resolutions are not high enough [5]. The human eye is truly much sensitive to luminance than to chroma, thus fake faces still look very similar to the genuine ones when the same facial images are shown in color [1].

2. PREVIOUS WORKS

Depending on the distinct types of prompts, face spoof detection methods are categorised into five groups. They are (1) Motion Related Methods (2) Texture Related Methods (3) Image Quality Related Methods (4) Image Distortion Analysis Related Methods (5) Methods Related on Other Prompts.

2.1 Motion Related Methods

These methods are depicted to adverse printed photo attacks. These methods attempt to capture the subconscious motion of organs and muscles in a live face, like eye blink, mouth movement and head rotation. The authors established a method for blinking based liveness detection using Conditional Random Fields [CRF]. CRF's holds long-range contextual dependencies among the observation sequence. Motion is a relative feature across video frames. So, these methods have better generalization ability. The main constraint is that it takes rather long time to gather the stable vitality features for face spoof detection. It is easy to complicate these methods by other irrelevant background motions [4].

2.2 Texture Related Methods

Texture Related methods are formulated to oppose both replay video attack and printed photo attack. A single image is only required for the spoofing detection. These methods have poor generalization ability because these can be easily over fitted to one specific illumination and imagery condition. The basic advantages are fast response and low computational complexity. The authors introduced a component-based face coding approach for liveness detection. In this method, a Holistic Face (H-FACE) is created by enlarging the detected face and dense low level features for example LBP, LPQ, HOG, etc.. are extracted for all the components. They have used a component-based approach which gives better performance when compared to the methods that uniformly divide the image into grids [4].

2.3 Image Quality Analysis Related Methods

For describing information characteristics no face specific information has been examined in this method. This method points at depicting a generic liveness detection method across various biometric modalities. The authors introduced a biometric liveness detection method for iris, fingerprint and face images. Here 25 general image quality features are examined which contains full-reference and non-reference measures. This method has improved generalization ability, fast response and low computational complexity. The features are selected based on performance, complementarity, complexity and speed [4].

2.4 Image Distortion Analysis Related Methods

Depending on the light reflection of the object at specified area, the major distortions in a spoof face image contain: (1) specular reflection from the printed paper surface or LCD screen (2) image blurriness owing to camera defocus (3) image chromaticity and contrast distortion owing to faculty colour rendering of printer or LCD screen and (4) colour diversity distortion owing to restricted colour resolution of printer or LCD screen. The author established an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). Various classifiers are used for different face spoof attacks. Experimental results on two public-domain face spoof databases like REPLAY-ATTACK, CASIA FASD and the MSU MFSD database generated by the author shows that the proposed approach exceeds the new methods in spoof detection. The recommended approach could enhance the generalization ability under cross-database scenarios [4].

2.5 Methods Related On Other Prompts

Face spoof aids using prompts obtained from sources other than 2D intensity image like 3D depth, IR image, spoofing context and voice have also been proposed. The main limitation of this method is that it imposes the further requirements on the system or user. For example, the methods that use IR images demand an additional IR sensor and the method depending on voice needs a speech analyzer. Because of these methods have a narrower application range. The author introduced a novel face liveness detection approach to oppose spoofing attacks by improving sparse 3D facial structure. From the given face video, they first detect facial landmarks and then select the key frames. The frames which are auspicious to recover facial structure are called as key frames. From the selected key frames sparse 3D facial structures are recovered. At last, an SVM classifier is trained to distinguish between genuine and fake faces [4].

3. PROPOSED SYSTEM

In this section, we will discuss the proposed approach in detail. To better demonstrate the effectiveness of the proposed approach in this work is depending on Color Texture Analysis. Face spoofing attacks are mostly accomplished by displaying the targeted face using prints or video screens. Attack attempts with low facial texture quality for e.g. mobile phone can be perceived by analyzing the texture and the quality of the gray-scale images. Anyway, it is sensible to assume that fake faces of higher quality are harder or nearly difficult to detect using only luminance information of webcam-quality images [1].

Auspiciously, the color reproduction of various display media for e.g. photographs, video displays, and masks is confined compared to genuine faces. Thus, the presented fake faces affected from spoofing medium dependant color. Moreover, a recaptured face image is likely to contain local variations of color owing to other imperfections in the reproduction process of the targeted face. Both the display medium dependant color gamut signatures and the local chroma variations can be distinguished by analyzing the color texture of the chroma channels. After all the chrominance channels are separated from the luminance information, they are more tolerant of conditions are reasonable [1]. We aim to analyze how the prior idea can be used for face anti illumination variation assuming that the retrieval spoofing. We explore which color models provide the most useful microtexture representation by extracting LBP descriptions from the YCbCr color space.

3.1. Color Spaces

RGB is the widely used color space for sensing, representing and displaying color images. But, its application in image analysis is quite limited owing to the high correlation between the three color components (red, green and blue) and the imperfect separation of the luminance and chrominance information [1]. In this work, we examine the color space YCbCr to explore the color texture information. It is based on the separation of the luminance and the chrominance information. The YCbCr space separates the RGB components into luminance(Y), Chrominance blue (Cb), Chrominance-red (Cr) [1]. The texture information of the chrominance components in the color space illustrates apparent disparities between the real faces and fake ones. The dissimilarity of the corresponding LBP descriptions is also significant, although the resemblance between the descriptions of real faces remains same [5].

3.2. Texture Model

The LBP descriptor is a highly discriminative gray scale texture descriptor. For each pixel in an image, a binary code is determined by thresholding a circularly symmetric neighborhood with the value of the central pixel. Finally, a histogram is generated to assemble the occurrences of different binary patterns. The LBP is applied to each color band. The derived histograms are concatenated to form the final color descriptor [1]. The notation (Q, R) is normally used for pixel neighborhoods to mention to Q points on a circle of radius R. The computation of the LBP code can be easily done in a single scan through the image [2]. The value of the LBP code of a pixel (xc, yc) is given by:

$$LBP_{Q,R} = \sum_{p=0}^{Q-1} h(gq - gc)2\text{^}p, \qquad (1)$$

Where gc corresponds to the gray value of the central pixel (xc, yc), gq refers to the gray values of Q equally spaced pixels on a circle of radius R, and h describes a thresholding function as follows:

$$h(x) = \begin{cases} 1, x \geq 0; \\ 0, \text{otherwise.} \end{cases} \qquad (2)$$

LBP pattern has described a uniform if its binary code consists of at most two transitions from 0 to 1 or from 1 to 0 [5].

Algorithm

- The random subspace samples data from the original feature set and constructs a base classifier on each subset. The ensemble assigns a class label by majority voting.
- Let g={x1, x2,...xn} be the set of n features. To construct an RS ensemble with L classifiers, collect L samples with size M, drawn without replacing ment from a uniform distribution over X.
- Each feature subset describes a subspace of X with cardinality M.
- The classifier is trained by base classifier K-nearest neighbor. The final ensemble decision is made by majority vote.

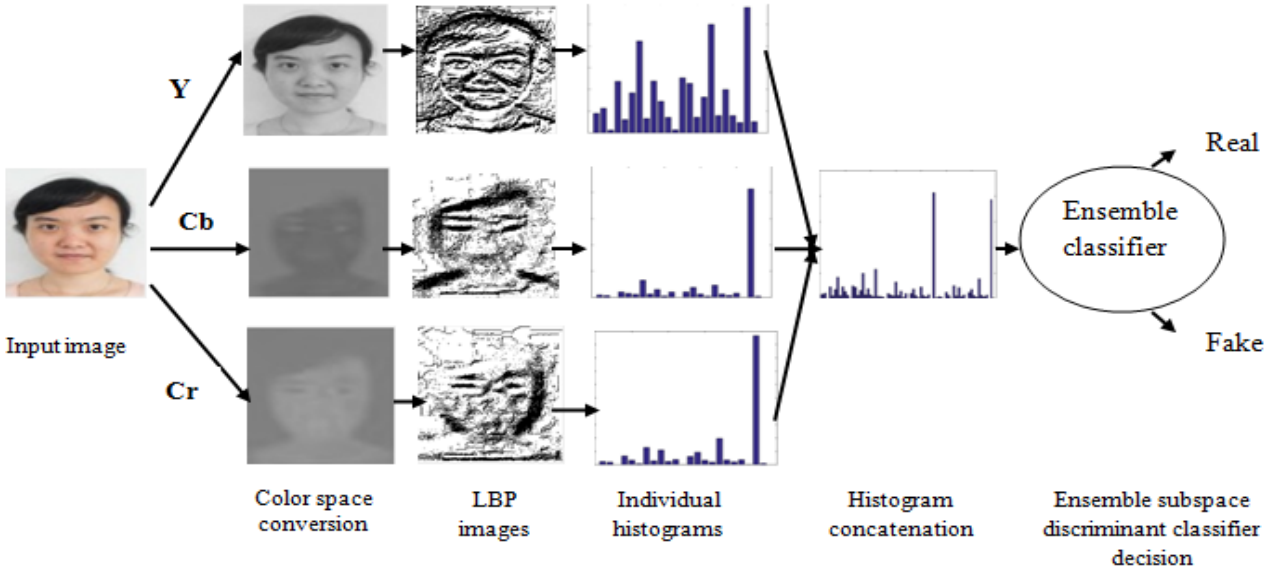

Fig-2: The face is first detected, cropped and normalized into a 200x200pixel image. Then, we converted to YCbCr color space and apply $LBP_{8,1}$ operator on corresponding chrominance channels of the face image. Then, we compute histograms from the whole face image using LBP operators. After that, we concatenated the histograms. Finally, we use an ensemble subspace discriminant classifier for determining whether the input image corresponds to a live face or not.

3.3. Classification

Once the enhanced histograms are determined, we use an ensemble subspace discriminant classifier for detecting whether the input image corresponds to a live face or not [2]. It learns from a set of classifiers and assembles the prediction from those various classifiers. The classification results are dependent on these individual classifiers by averaging the output probabilities. The classifier is trained by base classifier k-nearest neighbor.

4. RESULT

The analysis of the proposed method has been done in this section. By feeding the extracted features to an ensemble subspace discriminant classifier, the efficiency of the system has been computed. Then testing has been performed to get the response of the classifier over the test dataset. The experiment was conducted by using MATLAB (R2015a). To evaluate the effectiveness of our proposed anti-spoofing technique, we considered the CASIA FAS dataset.

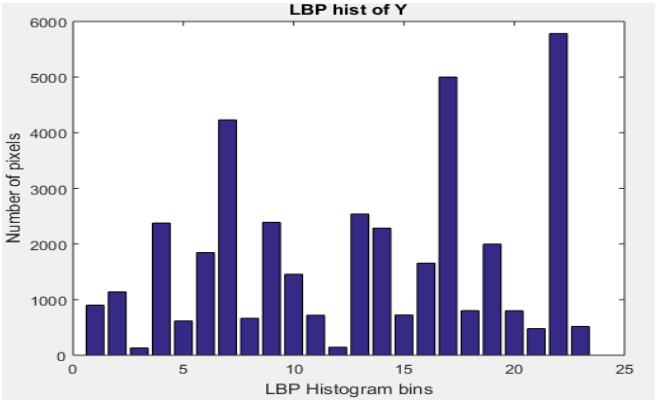

Fig-3: LBP histogram of Y channel

Fig-3 indicates the LBP histogram of Y channel of the real face image.

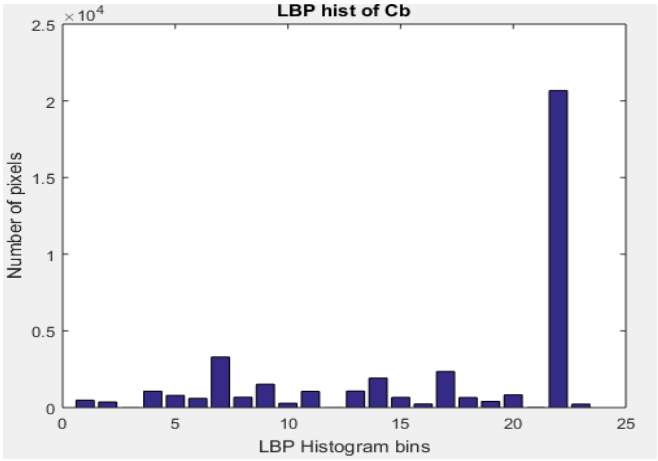

Fig-4: LBP histogram of Cb channel

Fig-4 indicates the LBP histogram of Cb channel of the real face image.

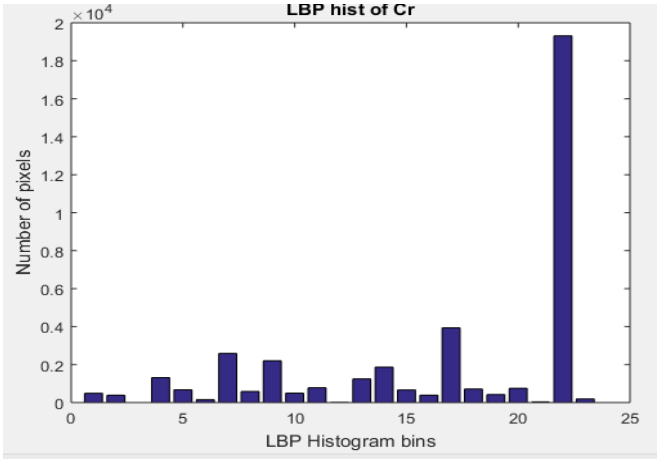

Fig-5: LBP histogram of Cr channel

Fig-5 indicates the LBP histogram of Cr channel of the real face image.

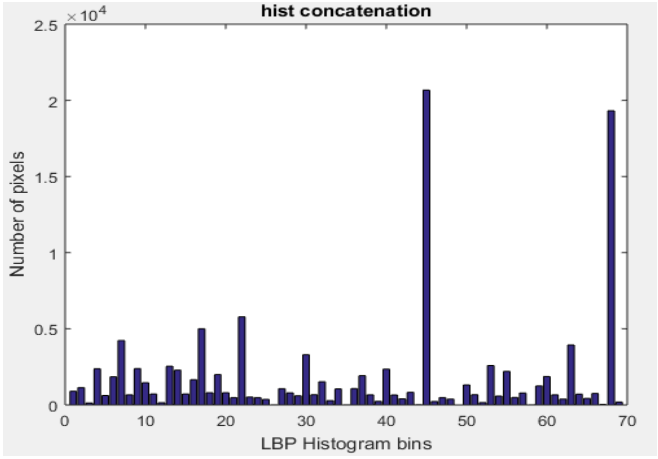

Fig-6: LBP histogram concatenation

Fig-6 indicates the LBP histogram concatenation of real face image.

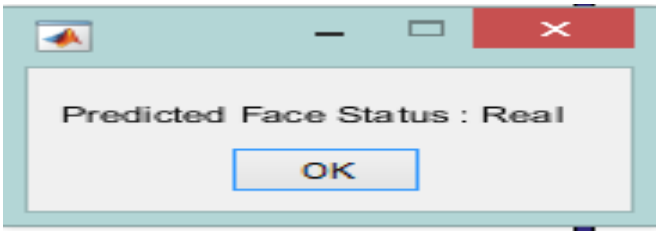

Fig-7: Output from Ensemble classifier

Fig-7 is the output from an Ensemble Subspace Discriminant Classifier.

Table-1: Performance measures between SVM and Ensemble classifier

RATES AND THRESHOLDS	SVM CLASSIFIER	ENSEMBLE CLASSIFIER
AT MINIMUM HTER		
Half Total Error Rate	0.6500	0.5000
Threshold	1.3000	1
False Rejection Rate	0.8667	0.6667
Verification Rate	0.1733	0.3333
False Acceptance Rate	0	0
AT EER		
Half Total Error Rate	0.6500	0.5000
Threshold	2.6026	2.0002
False Rejection Rate	0.4333	0.3333
Verification Rate	0.7367	0.6667
False Acceptance Rate	0.8667	0.6667

5. ACKNOWLEDGEMENT

I also acknowledge my gratitude to all other faculty members of the department of Electronics and Communication Engineering.

6. CONCLUSION

In this paper, we proposed a novel approach for detecting face spoofing using a color-texture analysis. The color image representations can be used for describing the intrinsic disparities in color- texture. The effectiveness of the different color- texture representations was examined by extracting color LBP features from the individual image channels. Also, it improves the generalization capabilities of color-texture analysis based face spoofing detection. Finally, an ensemble subspace discriminant classifier determines whether the input image is live one or not.

Also, the project work concentrates on determining the performance measures of an ensemble classifier and comparing with SVM classifier.

7. REFERENCES

[1] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in Proc. IEEE Int. Conf. Image Process. (ICIP), Sept.2015, pp.2636-2640.
[2] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in Proc. Int. Joint Conf. Biometrics (IJCB), Oct. 2011, pp.1-7.
[3] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis," IET Biometrics, vol. 1, no. 1, pp. 3-10, Mar. 2012.
[4] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," in Proc. IEEE Int. Conf. Image Process. (ICIP), vol. 11, no. 8, Aug. 2016, pp. 1818-1830.
[5] Yan Li, Ke Xu, Qiang Yan, Yingjiu Li, and Robert H.Deng, "Understanding osn-based facial disclosure against face authentication systems," in Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, New York, NY, USA, 2014, ASIA CCS '14, pp. 413–424, ACM.
[6] Reshma Rajan and Ani Sunny "Detecting Face Spoof Using IDA Features and Colour Texture Analysis," ISSN: 0974-5572, vol. 10, pp.309-317, 2017.
[7] P. Kayal, S. Kannan "An Ensemble Classifier Adopting Random Subspace Method based on Fuzzy Partial Mining," in Indian Journal of Science and Technology, Vol 10(12), DOI: 10.17485/ijst/2017/v10i12/104975, March 2017.
[8] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in Proc. IAPR/IEEE Int. Conf. Pattern Recognit. (ICPR), Aug. 2014, pp. 1173–1178.
[9] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 746–761, Apr. 2015.
[10] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May/Jun. 2010, pp. 3425–3428.
[11] 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. 11th Eur. Conf. Comput. Vis., VI (ECCV), 2010, pp. 504–517.
[12] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A faceantispoofing database with diverse attacks," in Proc. 5th IAPR Int. Conf. Biometrics (ICB), Mar./Apr. 2012, pp. 26–31.
[13] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IAPR Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.
[14] T. de Freitas Pereira et al., "Face liveness detection using dynamic texture," EURASIP J. Image Video Process., vol. 2014, no. 1, pp. 1–15, Dec. 2014.
[15] A. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Face spoofing detection through visual codebooks of spectral-temporal cubes," IEEE Trans. Image Process., vol. 24, no. 12, pp. 4726–4740, Dec. 2015.
[16] N. Bonnier,"Contribution to spatial gamut mapping algorithms," M.S. thesis, Lab. Commun. Process. Inf. (LTCI), Télécom ParisTech, Paris, France, Sep. 2008.
[17] J. Y Choi, K. Plataniotis, and Y. M. Ro,"Using colour local binary pattern features for face recognition," in Proc. IEEE Int. Conf. Image Process. (ICIP), Sep. 2010, pp. 4541–4544.
[18] J. Komulainen, A. Hadid, M. Pietikäinen,, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in Proc. IAPR Int. Conf. Biometrics, Jun. 2013, pp. 1–7.

