Face spoofing detection using Local binary patterns and Fisher Score

CONFERENCE PAPER · MAY 2015

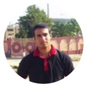
DOI: 10.1109/CEIT.2015.7233145

Azeddine Benlamoudi

Université Kasdi Merbah Ouargla

Abdelkrim Ouafi

Université de Biskra



Salah Eddine Bekhouche

Université de Biskra

Face spoofing detection using Local binary patterns and Fisher Score

Azeddine Benlamoudi*, Djamel Samai*, Abdelkrim Ouafi†, Salah Eddine Bekhouche†, Abdelmalik Taleb-Ahmed‡,
and Abdenour Hadid§
*Laboratory of LAGE, University of Ouargla, Algeria
Email : be.azzeddine@gmail.com, Samai.djamel@gmail.com
†Laboratory of LESIA, University of Biskra, Algeria
Email: ou_karim@yahoo.fr, salah@bekhouche.com
‡LAMIH, UMR CNRS 8201 UVHC, University of Valenciennes, France
Email: Abdelmalik.Taleb-Ahmed@univ-valenciennes.fr
§Center for Machine Vision Research, University of Oulu, Finland

***Abstract*—Todays biometric systems are vulnerable to spoof attacks made by non-real faces. The problem is when a person shows in front of camera a print photo or a picture from cell phone. We study in this paper an anti-spoofing solution for distinguishing between 'live' and 'fake' faces. In our approach we used overlapping block LBP operator to extract features in each region of the image. To reduce the features we used Fisher-Score. Finally, we used a nonlinear Support Vector Machine (SVM) classifier with kernel function for determining whether the input image corresponds to a live face or not. Our experimental analysis on a publicly available NUAA and CASIA face anti-spoofing databases following the standard protocols showed good results.**

***Keywords*—biometric, spoofing, LBP, Fisher-Score, SVM**

I. Introduction

Nowadays we are experiencing an increasing demand for highly secure identification and personal verification technologies. This demand becomes even more apparent as we become aware of new security breaches and transaction frauds [1]. The main reason is that a biometric sample is a face represented in a digital image, which is intrinsically highly reproducible by several means like printed photos and electronic portable devices capable of showing images and videos [2].

Unfortunately, research in countermeasures to this type of attack has not kept-up-even if such threats have been known for nearly a decade. There seems to exist no consensus on best practices, techniques or protocols for developing and testing spoofing-detectors for face recognition[3].

The proposed approach in this paper focused in LBP overlapping algorithm with fisher score for reduced histogram .Overlapping algorithm divides the image in nine blocks, in each block we applied $LBP^{u2}_{16,2}$ to extract the features and then we concatenated feature histograms in one histogram. Then we used a nonlinear SVM classifier to determine if the input image is real or not.

The rest of the paper is organized as follows: SectionI is an introduction to face recognition and anti spoofing. SectionII discusses related works on anti spoofing attacks. SectionIII describes our approach in details. The experimental results, database used in our tests and a comparison with many related works are summarized in SectionIV. Finally a conclusion and future works are given in sectionV.

II. Related work

Anti-spoofing for 2-D face recognition systems can be coarsely classified into 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection [4].

The first one interests in detecting clues generated when two dimensional counterfeits are presented to the system, for example photos or video clips [5]. Kollreider et al. [6] evaluated the trajectories of selected part of the face from a short sequence of images using a simplified optical flow analysis followed by a heuristic classifier. The same authors in [7] introduced a method to fuse these scores with liveness properties such as eye-blinks or mouth movements. Bao et al. [8] proposed the detection of attacks produced with planar media using optical flow based on motion estimation.

Li et al. [9], used a Fourier spectra to compare the hard-copies of client faces and real accesses. Li et al's. method works well for down-sampled of the print-photo attack identity, but it fails for higher-quality images sometimes.

Liveness detection tries to capture signs of life from user images by analyzing spontaneous movements that cannot be detected in photographs, such as eye blinking. The authors in [2]and [10] brought a real-time liveness detection specifically against photo-spoofing using spontaneous eye-blinks, which are supposed to occur once every 2-4 seconds in humans.

Maatta et al. [11] proposed an approach based on learning texture features from single images using LBP, Gabor wavelet and Histogram of Oriented Gradients (HOG). In [12], the same authors presented a novel approach based on analyzing the texture of the facial images using Multi-Scale Local Binary Patterns (MSLBP), Local Phase Quantization (LPQ) and Gabor wavelets. Freitas et al. [13] proposed a novel countermeasure against face spoofing. This approach uses an operator called Local Binary Patterns from Three Orthogonal Planes (LBP-TOP) that combines space and time information into a single descriptor with a multi-resolution strategy. In. [14], the same authors analyzed three recently published countermeasures

(Correlation with frame differences, LBP countermeasure, LBP-TOP countermeasure). Chingovska et al. [15] inspected the potential of texture features based on LBP and its variations on three types of attacks: printed photographs, photos and videos. Schwartz et al. [3] introduced an anti-spoofing solution based on a set of low-level feature descriptors exploring both spatial and temporal information using Partial Least Squares (PLS). Galbally et al [16] used new approach called image quality assessment (IQA) suitable for real-time spoofing detection.

III. PROPOSED APPROACH

In this section, we explain our approach of anti-spoofing used to differentiate between live faces and fake ones. The block diagram of our anti-spoofing approach can be seen in Fig. 2. First, we detect the face using Viola-Jones algorithm [17] and we then apply the Active Shape Models with Stasm [18] to locate landmarks. These landmarks help us to adjust and crop the faces. After that we divided the face image into 3x3 overlapping regions, and we applied LBP operator on each region. The local 243-bin histograms from each region are computed and collected into a single 2187-bin histogram and after that, we applied fisher score for reducing the number of histogram bins. Finally, we used a non-linear SVM classifier with radial basis function kernel for determining whether the input image corresponds to a live face or not.We describe below each step in detail.

A. Face preprocessing

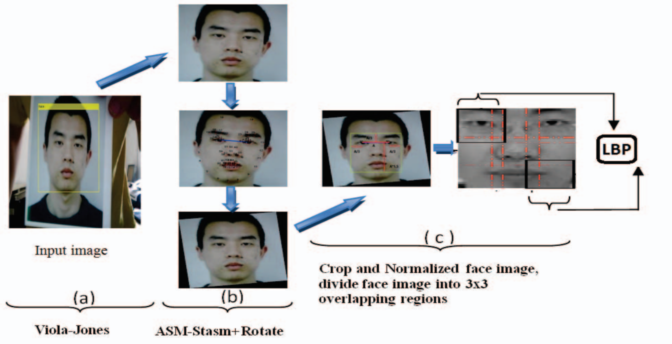


Fig. 1: Face preprocessing

1) Viola-Jones algorithm: To detect the faces we used Stasm. When we used Stasm directly on large images which have small faces the system fails to detect the faces. So, we must apply Viola-Jones [17] to detect the faces first, then we can apply Stasm in detected faces to locate lanmarks (see fig1-(a)).

2) Active Shape Models with Stasm : Stasm is a software package for locating landmarks using Active Shape Models (ASMs). We used Stasm only for eyes localization to rotate the face[19] (see fig1-(b)).

3) Crop and normalize the face: To adjust and crop the face, we need to calculate the distance between the eyes (named distance A). This distance (A) is used to crop the face as follows: [(A+2A/3) * (A/3+3A/2)][20]. We normalize then the cropped face into a (64 x 64) pixel images. In order to extract the local features of the face image, we divided it into 3x3 overlapping regions and applied the LBP on each bloc (see fig1 (c)).

B. Feature extraction using LBP

The LBP is an image operator which transforms an image into an array or image with more detail. The basic LBP, introduced by Ojala et al.[21], was based on the assumption that texture has locally two complementary aspects, a pattern and its strength.

The original LBP works in a 3x3 pixel block of image. The pixels in this block are thresholded by its center pixel value, multiplied by powers of two and then summed to obtain a label for the center pixel. As the neighborhood consists of 8 pixels, a total of 2^8=256 different labels can be obtained depending on the relative gray values of the center and its neighborhood.

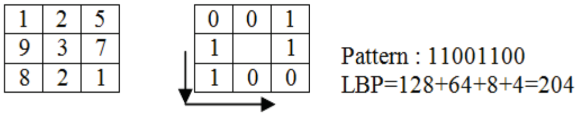


Fig. 3: The basic LBP operator.

The $LBP_{(P,R)}$ operator used a circular neighborhood. The notation (P, R) is generally used for pixel neighborhoods to refer to sampling points and circle of radius. So the calculation of the $LBP_{(P,R)}$ codes can be easily done. The value of the LBP code of a pixel (x_c, y_c) is given by:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \qquad (1)$$

where g_c corresponds to the gray value of the center pixel (x_c, y_c), g_p refers to gray values of P equally spaced pixels on a circle of radius R , and s defines a thresholding function as follows:

$$s(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & otherwise. \end{cases} \qquad (2)$$

In our work we considered another extension of the original $LBP^{U2}_{(P,R)}$ called uniform patterns where a uniformity measure of a pattern is used: U (pattern) is the number of bitwise transitions from 0 to 1 or vice versa when the bit pattern is considered circular.

When, When dividing the face image into 3x3 overlapping regions, we used $LBP^{U2}_{(16,2)}$ operator on each region. The local 243-bin histograms from each region are computed and collected into a single 2187-bin histogram.

C. Features histogram reduction using fisher score

Fisher score [22] is one of the most known method for feature selection. The idea in fisher score is to select each feature independently according to its scores under the Fisher criterion. We used fisher score in our approach to reduce the bin histograms and keep the best of histogram bins.

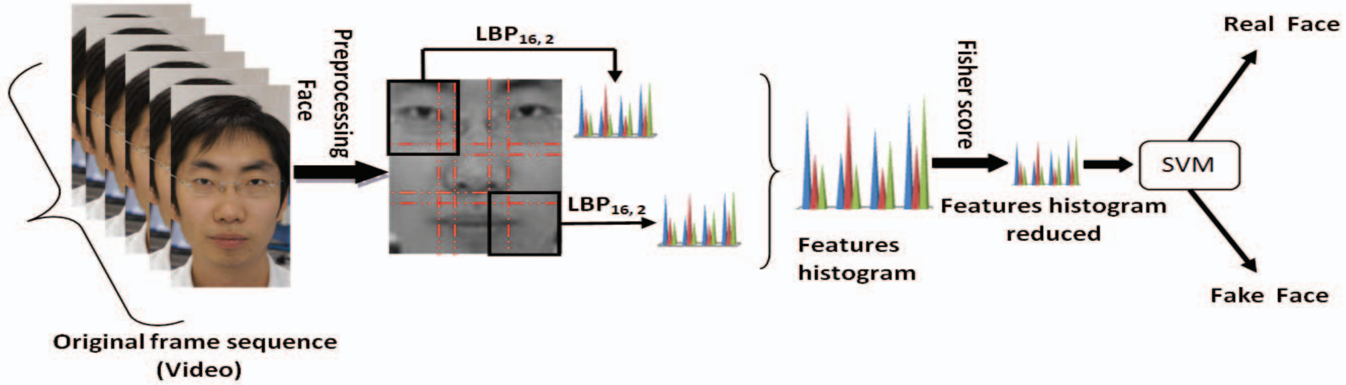


Fig. 2: The proposed approach

D. Classification

A Support Vector Machine (SVM) performs classification by finding the hyper plane that maximizes the margin between two classes. The vectors (cases) that define the hyper plane are called the support vectors.

In our experiments, once the enhanced histograms are computed and reduced, we use a nonlinear SVM classifier [23] with radial basis function kernel for determining whether the input image corresponds to a live face or not. The SVM classifier is first trained using a set of positive (real faces) and negative (fake faces) samples from the dataset.

IV. Results & discussion

We evaluated the proposed approach on the NUAA Photograph Imposter[24] and CASIA face anti-spoofing[25] databases.

A. Setup

To validate the proposed idea and compare the results against the state of-the-art, we used two data sets: publicly available NUAA Photograph Imposter[24] and CASIA face anti-spoofing[25] databases.

1) NUAA Photograph Imposter Database: The NUAA database[1], proposed by Tan et al. [24] comprises images extracted from videos of 15 subjects captured in three sections and contains attempts of attack based on hand-held printed photos. This dataset is divided into training and test sets. The former has 1743 live images and 1748 non-live ones, and the latter consists of 3362 live and 5761 non-live samples.

2) CASIA Face Anti-Spoofing Database: The CASIA database[2] contains 50 genuine subjects, and fake faces are made from the high quality records of the genuine faces. Three imaging qualities are considered, namely the low quality, normal quality and high quality. Three fake face attacks are implemented, which include warped photo attack, cut photo attack and video attack. Therefore each subject contains 12 videos (3 genuine and 9 fake), and the final database contains 600 video clips (240 for train and 360 for test). Test protocol is provided, which consists of 7 scenarios for a thorough evaluation from all possible aspects.

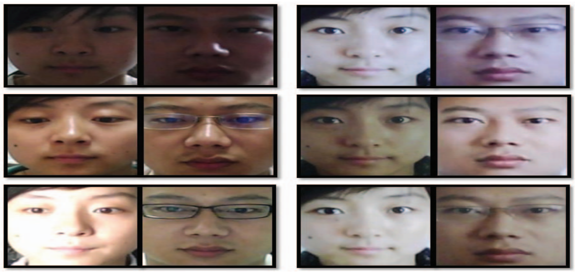


Fig. 4: . Illustration of samples from the database. In each column (from top to bottom) samples are respectively from session 1, session 2 and session 3. In each row, the left pair are from a live human and the right are from a photo.

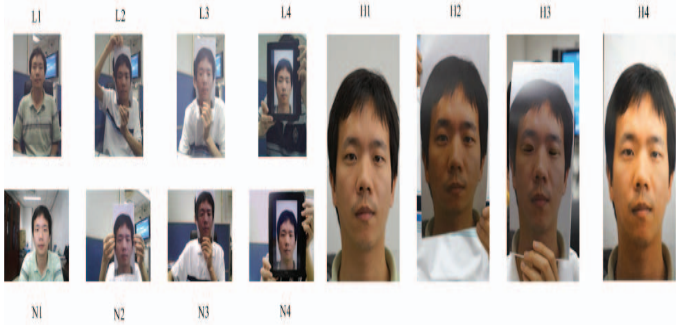


Fig. 5: One complete video set for an individual subject of CASIA Face Anti-Spoofing Database.

In our experiments, we used Viola-Jones algorithm to locate all components of the face images and Stasm for localizing the eyes. The coordinates of the eyes are used to rotate and to crop the face. All cropped faces are resized to a consistent size 64x64. Then, we divided the face into nine blocks to apply the overlapping algorithm (see Fig. 2). On each block we apply $LBP^{U2}_{(16,2)}$ which gives an histogram of 243 bin. All histograms are then concatenated into a single histogram of 2187 bin. Finally, we use fisher score for reducing

[1] http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html

[2] http://www.cbsr.ia.ac.cn/english/FaceAntiSpoofDatabases.asp

histograms.

To classify the faces, we use SVM classifier with a non-linear RBF kernel. The parameters of the SVM classifier were determined using a grid search.

B. Results

In this section, we give results of our approach compared with the state of the art. The performance evaluation of the studied anti-spoofing algorithm are measured in terms of the Equal Error Rate (EER).

1) Results on NUAA Photograph Imposter Database: We compared our results with those of the state of art : LBP+Gabor+HOG [26], LBP [27], LPQ [27], Bad Illumination Conditions [28]. For fair comparison, we used the same protocol (see table I)

The performance of our approach with LBP texture operator in terms (EER), indicates that our approach gives best results compared to the stat of art. figur 7 shows the DET curve and the figure 6 shows the ROC curve in NUAA data base.

TABLE I: Performance comparison between our proposed approach and the best results in [28], [12], [11] on the same database NUAA and using the same protocol.

Methods	EER%
Gabor [12]	09.50
Bad Illumination Conditions [28]	08.20
LPQ [12]	04.90
LBP overlapping Blocks [12]	02.90
LBP+Gabor+HOG [11]	01.10
LBP Without_Stasm	03.95
LBP Without_Stasm_Fisher	03.83
8_1_Stasm	03.21
8_1_Stasm_Fisher	03.12
8_2_Stasm	02.32
8_2_Stasm_Fisher	02.25
16_2_Stasm	01.84
16_2_Stasm_Fisher	**01.00**
16_2_Stasm_M_fisher(correction manual)	**00.61**

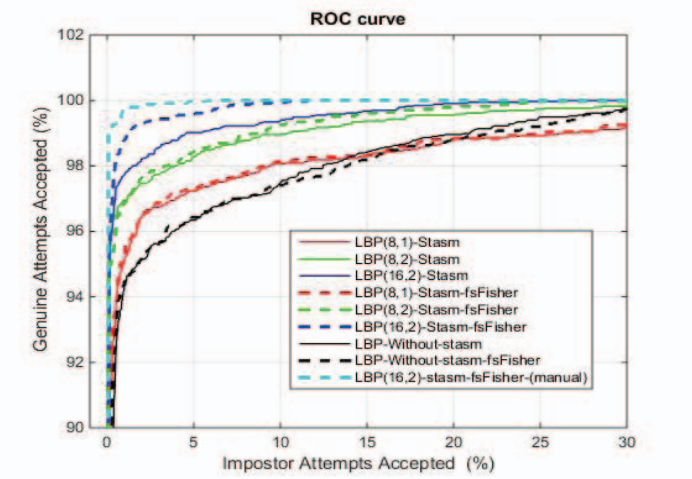


Fig. 6: Performance (ROC curves) of the proposed approach without (Stasm-Fisher) and with (Stasm-Fisher).

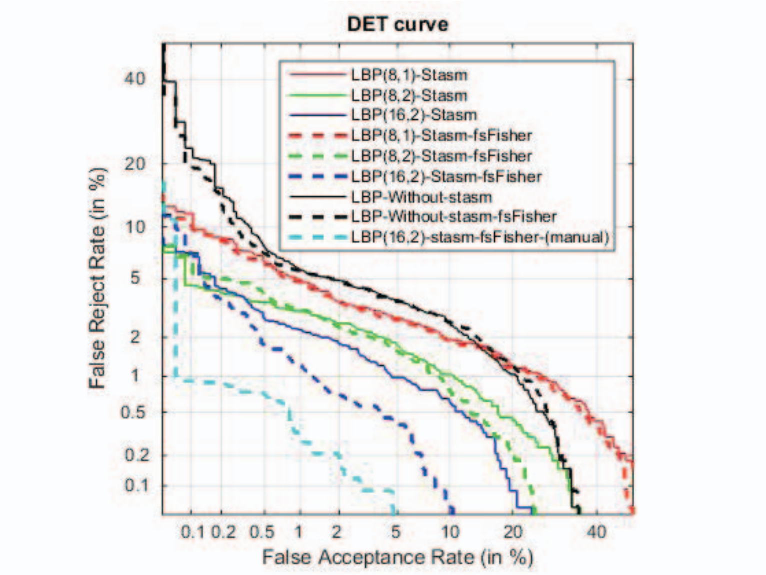


Fig. 7: Performance (DET curves) of the proposed approach without (Stasm-Fisher) and with (Stasm-Fisher).

2) Results on CASIA Face Anti-Spoofing Database: The database has only two totally independent datasets train and test.For fair comparison, we used the same protocols reported in [25]. The results presented in our paper in term of EER are computed as two test, the first test used per-Frame and the second test per-video. Finally the first test gives us score of image real or fake and the second test gives score of video real or not (see table II).

The databases have seven scenarios to train and test, because the main purpose is to investigate the possible effects of different fake face types and imaging qualities. which are: low (1), normal (2) and high quality (3),warped photo (4), cut photo (5), video attacks (6) and overall test (7). The results of each scenario are reported as Equal Error Rate (EER) in (TableII).

TABLE II: Comparison of the results (in EER %) between our proposed approach and the stat of the art on CASIA data base.

Scenario	(1)	(2)	(3)	(4)	(5)	(6)	(7)
IQA [16]	31.7	22.2	5.6	26.1	18.3	34.4	32.4
DoG baseline [25]	13	13	26	16	6	24	17
LBP [29]	11	17	13	13	16	16	16
Our	**7.2**	**8.8**	14.4	**12**	10	**14.7**	**13.1**

When using NUAA database, we have obtained an EER = 1% which represents the best result compared to the other works (table I). In the case of CASIA database (table II), we got good results for low and normal quality (EER=7.2% and 8.8%), but in high quality the results are poor compared to Freitas Periara et al [29]. For warped photo and attack video, our results are good compared to other groups. In addition, when using cut photo our results are a little low compared to Zhang et al [25]. In conclusion, the overall test in our work is better than the others in the case of texture algorithm.

V. CONCLUSION AND FUTUR WORK

We proposed in this work, an approach for anti-spoofing detection based on LBP and Fisher Score that discriminate live faces from fake ones.

Our approach tested on NUAA Photograph Imposter and CASIA Face Anti-Spoofing Databases which contains several real and fake faces showed promising results compared to many previous works.

As future work we will try to test our approach on other databases and find a new method working well on high quality images or videos.

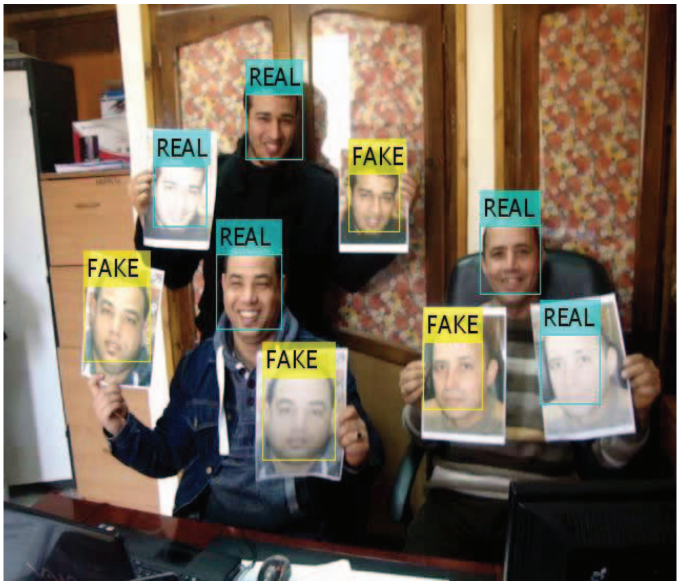


Fig. 8: Examples of anti-spoofing classification (Real: blue and Fake: yellow)

REFERENCES

[1] F. L. Podio, "Biometrics technologies for highly secure personal authentication," *National Institute of Standards and Technology, http://whitepapers. zdnet. com/search. aspx*, 2001.

[2] G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," *Recent advances in face recognition*, pp. 109–124, 2008.

[3] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–8.

[4] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–7.

[5] O. Kahm and N. Damer, "2d face liveness detection: An overview," in *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the*. IEEE, 2012, pp. 1–12.

[6] K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating liveness by face images and the structure tensor," in *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on*. IEEE, 2005, pp. 75–80.

[7] K. Klaus, H. Fronthaler, and J. Bigun, "Verifying liveness by multiple experts in face biometrics," in *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on*. Ieee, 2008, pp. 1–6.

[8] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in *Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on*. IEEE, 2009, pp. 233–236.

[9] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in *Defense and Security*. International Society for Optics and Photonics, 2004, pp. 296–303.

[10] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on*. IEEE, 2007, pp. 1–8.

[11] 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, 2012.

[12] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–7.

[13] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Lbp-top based countermeasure against face spoofing attacks," in *Computer Vision-ACCV 2012 Workshops*. Springer, 2013, pp. 121–132.

[14] T. Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in *Biometrics (ICB), 2013 International Conference on*. IEEE, 2013, pp. 1–8.

[15] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the*. IEEE, 2012, pp. 1–7.

[16] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in *Pattern Recognition (ICPR), 2014 22nd International Conference on*. IEEE, 2014, pp. 1173–1178.

[17] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, vol. 1. IEEE, 2001, pp. I–511.

[18] S. Milborrow and F. Nicolls, "Locating facial features with an extended active shape model," in *Computer Vision–ECCV 2008*. Springer, 2008, pp. 504–513.

[19] S. Bekhouche, A. Ouafi, A. Taleb-Ahmed, and A. Hadid, "Facial age estimation using bsif and lbp," in *Proceeding of the first International Conference on Electrical Engineering ICEEB14*, in press.

[20] A. Benlamoudi, D. Samai, A. Ouafi, A. Taleb-Ahmed, S. E. Bekhouche, and A. Hadid, "Face spoofing detection from single images using active shape models with stasm and lbp," in *Proceeding of the Troisime CONFERENCE INTERNATIONALE SUR LA VISION ARTIFICIELLE CVA 2015*, in press.

[21] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 24, no. 7, pp. 971–987, 2002.

[22] R. Duda, P. Hart, and D. Stork, *Pattern Classification*, 2nd ed. John Wiley & Sons, New York, 2001.

[23] M. 8.4 and S. T. 9.1. Natick, Massachusetts: The MathWorks Inc., 2014, united States.

[24] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Computer Vision–ECCV 2010*. Springer, 2010, pp. 504–517.

[25] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *Biometrics (ICB), 2012 5th IAPR International Conference on*. IEEE, 2012, pp. 26–31.

[26] B. Toth and U. C. von Seelen, "Liveness detection for iris recognition," in *The Presentation Sheet of NIST Workshop, Biometrics and E-Authentication over Open Networks*, 2005.

[27] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli, "Fusion of multiple clues for photo-attack detection in face recognition systems," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–6.

[28] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in *Image Processing (ICIP), 2011 18th IEEE International Conference on*. IEEE, 2011, pp. 3557–3560.

[29] T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikäinen, and S. Marcel, "Face liveness detection using dynamic texture," *EURASIP Journal on Image and Video Processing*, vol. 2014, no. 1, p. 2, 2014.