

Face Spoofing Detection From Single Images Using Active Shape Models with Stasm And LBP

Azeddine Benlamoudi*, Djamel Samai*, Abdelkrim Ouafi†, Abdelmalik Taleb-Ahmed‡, Abdenour Hadid§, and Salah Eddine Bekhouche†

*Laboratory of LAGE, University of Ouargla, Algeria. be.azeddine@gmail.com ,Samai.djamel@gmail.com

†Laboratory of LESIA, University of Biskra, Algeria. ou_karim@yahoo.fr, salah@bekhouche.com

‡LAMIH, UMR CNRS 8201 UVHC, University of Valenciennes, France Abdelmalik.Taleb-Ahmed@univ-valenciennes.fr

§Center for Machine Vision Research, PO Box 4500, FI-90014 University of Oulu, Finland. hadid@ee.oulu.fi

Abstract—Besides the recognition task, today's biometric systems need to cope with additional problem: spoofing attacks, like presenting a photo of a person(client) to camera. We study in this paper an anti-spoofing solution for distinguishing between 'live' and 'fake' faces. In our approach we focused in face detection using Viola-Jones algorithm and Active Shape Models with Stasm for locating landmarks. Then, we apply Local Binary Patterns (LBP) operator to extract the features in each region of the image. Finally, we use 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 database NUAA, showed excellent results compared to existing methods.

Keywords—BIOMETRIC, SPOOFING, STASM, LBP, SVM, NUAA.

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 (laptops and even cellular phones have nowadays wide and very good quality screens) [2].

In the context of face biometrics, an impostor tries to access the system as a valid user with three approaches [3]:

- Showing photography of a valid user
- Showing a video of a valid user, or
- Showing a 3D facial model of a valid user

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[4].

Commonly cited papers refer to the problem of photo attack detection in two major complementary directions [2], [5], [6]:

- Static analysis, based on the fundamental idea that during the manufacturing process of a photo attack

a certain loss of information occurs and also peculiar noise is introduced .

- Video analysis, that tries to detect, as humans do, facial physiological clues like blinks, mouth movements and changes in facial expression.

The proposed approach in this paper focused in face detection using Viola-Jones algorithm [7] and Active Shape Models with Stasm [8]. We used Viola-Jones algorithm to detect the face and stasm to locate the eyes. The difference in face detection between our approach and [9], is that in ours we use stasm to locate the eyes and [9] they used eye detection algorithm (aligned by the nose and the eyes). Then we applied the LBP operator to extract the features and used a nonlinear SVM classifier to determine if the input image is real or not.

The rest of the paper is organized as follows: Section 2 discusses related works on anti spoofing attacks. Section 3 presents the Database used in our tests. Section 4 describes our approach in details. The experimental results and a comparison with many related works are summarized in Section 5. Finally a conclusion and future works are given in section 6.

II. RELATED WORK

Anti-spoofing for 2-D face recognition systems can be coarsely classified in 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection [10].

The first one interests in detecting clues generated when two dimensional counterfeits are presented to the system, for example photos or video clips [11]. Kollreider et al. [12] 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 [13] introduced a method to fuse these scores with liveness properties such as eye-blinks or mouth movements. Bao et al. [14] proposed the detection of attacks produced with planar media using optical flow based on motion estimation.

Exploring the input image data is to take advantage of texture patterns that may look unnatural by counter measures. Li et al. [15], used a Fourier spectra to compare the hard-copies of client faces and real accesses. Li et al. method works well for down-sampled of the print-photo attack identity, but it is fail for higher-quality sometimes.

On liveness detection tries to capture signs of life from the user images by analyzing spontaneous movements that cannot be detected in photographs, such as eye blinks. The authors in [2] and [16] 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.

Juka et al. [17] proposed an approach based on learning texture features from single images using LBP, Gabor wavelet and HOG. In [18] the same authors presented a novel approach based on analysing the texture of the facial images using multi-scale local binary patterns (LBP), LPQ and Gabor wavelets. Tiago et al. [6] 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 [19] the same authors analyzed three recently published countermeasures (Correlation with frame differences, LBP countermeasure, LBP-TOP countermeasure). Chingovska et al. [20] inspected the potential of texture features based on LBP and its variations on three types of attacks: printed photographs, photos and videos. William et al. [4] 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).

We propose in this paper a new approach based on face detection using Viola-Jones algorithm for detection the face and Active Shape Models with Stasm for locating Landmark. These Landmarks help us to crop the essential part of the face, then we apply LBP operator to extract features and then SVM classifier.

III. DATABASE AND PROTOCOL

In our work, we used the publicly available NUAA Photograph Imposter Database. The NUAA database, proposed by Tan et al. [9] 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, and the latter consists of 3362 live and 5761 non-live samples (c.f. Tab I).

| NUAA dataset | | Session1 | Session2 | Session3 | Total |
|--------------|----------|----------|----------|----------|-------|
| Training Set | Client | 889 | 854 | | 1743 |
| | Imposter | 855 | 893 | | 1748 |
| Test Set | Client | 0 | 0 | 3362 | 3362 |
| | Imposter | 0 | 0 | 5761 | 3362 |
| Total | | 1744 | 1747 | 9123 | 12614 |

TABLE I: Number of images in the training set and test set.

The data provided in this dataset consists of grayscale face images cropped using the Viola-Jones detector, and normalized to 64 x 64 pixels aligned by the nose and the eyes. Tan et al. [9] used the normalized images in their experiments to perform a direct comparison with their results. We used in our test the same set of images (c.f. fig 1) and also images that we've cropped using our method explained in (section 4-c).



Fig. 1: . Illustration of the 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 from a photo.

IV. OUR APPROACH

Using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years. So there is big problem when a person showing in front in camera the prints photo because it can look very similar to the images captured from live faces (cf. Fig. 1).

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. The proposed method adopts face detection using Viola-Jones algorithm [7], and Active Shape Models with Stasm [8]. Viola-Jones algorithm is used to get all the face needed for Stasm which locates landmarks. Then we used the coordinates of eyes to rotate and crop the face. In each bloc 3x3 of cropped image we applied LBP operator [21], for describing the micro-textures. Each vector in its own transformed feature space is then fed to a non linear SVM classifier. The individual SVM outputs determine whether there is a real face or a fake one in front of the camera. We describe below each step in detail.

A. Viola-Jones algorithm

The Viola and Jones algorithm is a method for detecting an object in a digital image, proposed by Paul Viola and Michael Jones in 2001 [7]. Originally invented to detect faces, it may also be used to detect other types of objects such as cars or aircraft.

We use Viola-Jones in our approach to detect the face. The question here is why we didnt use Stasm directly. When we used Stasm directly in large images with small face we cant find the correct face, so we must apply Viola-Jones to detect the face first (c.f fig.2.a), because viola really good in face detection with any pictures has faces.

B. Active Shape Models with Stasm

Stasm is a software package for locating landmarks using Active Shape Models (ASMs). The package comes pre-configured for locating landmarks in faces. We need Stasm only for localization of eyes (Coordinates). To rotate the face we must depend on coordinates of eyes (See fig.2.b).

C. Crop and normalzide the face

For adjust and crop the face, we need to calculate the distance between the two eyes (distance A)(c.f fig.2.c). So to

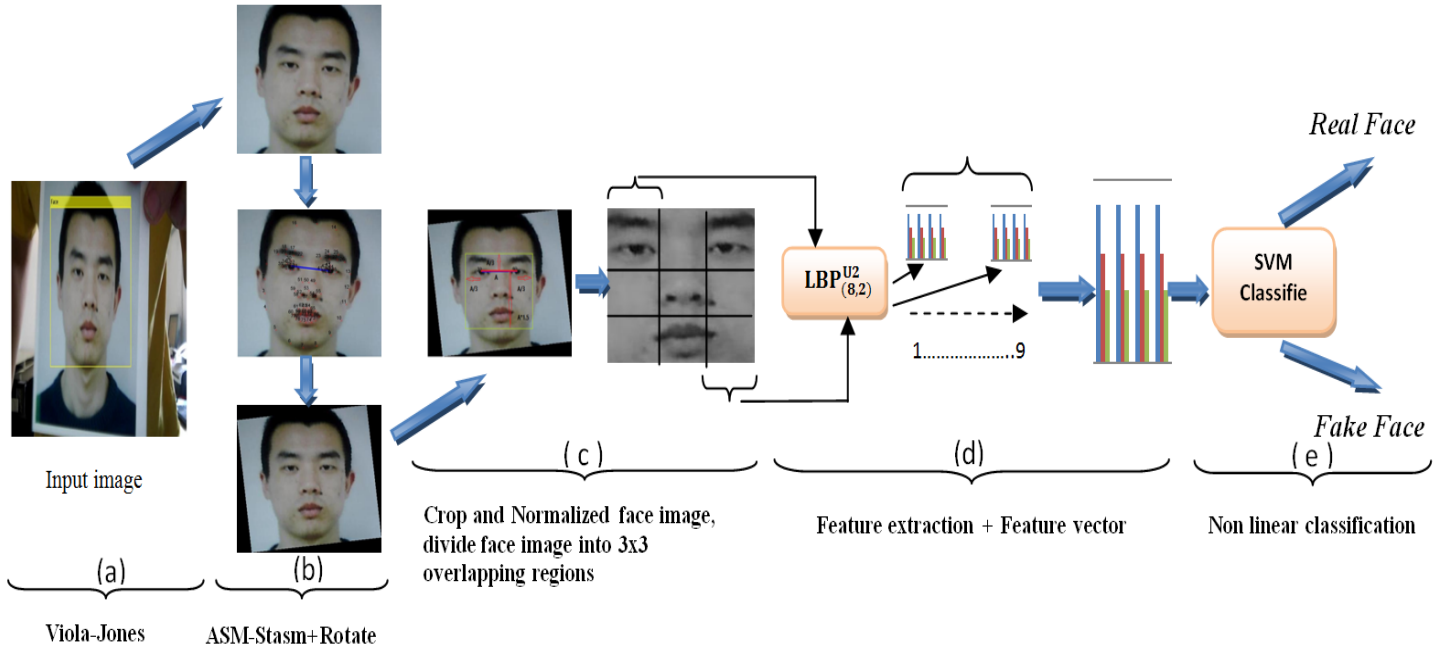


Fig. 2: The proposed approach : (a) Viola-Jones algorithm, (b) Active Shape Models with Stasm, (c) Crop and normalize the face, (d) Feature extraction using LBP and (e) Non-linear SVM classifier for determining a real face or fake.

crop the face, we used the distance A. Then we normalized the cropped face into a (64 x 64) pixel images. In normalized face image we used the histogram equalization, for adjusting image intensities to enhance contrast. After that we added noise (salt and pepper) and applied median filter on the image to denoise it. 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.

D. Feature extraction using LBP

The LBP is an operator which transforms an image simple 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 threshold 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 the pixels in the neighborhood [22]. Fig 3 illustrates the principle of basic LBP operator.

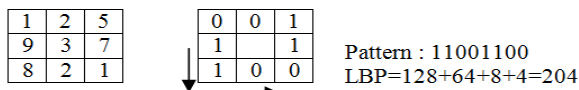


Fig. 3: The basic LBP operator.

The LBP 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[22]:

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

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:

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

Another extension of the original LBP 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, divided the face image into 3x3 overlapping regions, we used $LBP_{(8,2)}^{U2}$ operator on each region. The local 59-bin histograms from each region are computed and collected into a single 531-bin histogram.

E. 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 called the support vectors.

In our experiments, Once the enhanced histograms are computed, 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.

V. EXPERIMENTAL ANALYSIS

We evaluated the proposed approach on the NUAA Photograph Imposter Database [9]. In our experiments we used Matlab2013b, beginning with Viola-Jones Algorithm to locate all components of the Face images. Using Stasm on detected face image, we have localized of eyes. The coordinates of the eyes are used to adjust, and then to crop the face as explain before (c.f section 4.c). All cropped faces are resized to a consistent size 64x64.

We also divided the normalized faces in 9 block with over lapping algorithm before applying $LBP_{(8,2)}^{U2}$ to extract the local features in each region of the image. In this step, we computed the histogram of each block to get 59 bin histograms. We collected then these histograms in a simple one of a 531 bin. For classification, we used SVM classification.

We applied our approach using face detection without Stasm using the same image normalization in NUAA data bases in one hand. In other hand, we calculated the results using the Viola Jones algorithm and Active Shape Model with Stasm. Also, for 107 images not detected by Stasm, we have used a manual detection by manual calculation of coordinates of eyes needed to crop the face.

We compared our results with those of the state of art : LBP+Gabor+HOG [3], LBP [5], LPQ [5], Bad Illumination Conditions [24]. For fair comparison, we used the same protocol with other authors: 1743 live images, 1748 non-live, for train and 3362 live and 5761 non-live samples for test.

The performance of the three detection (without Stasm, with Stasm, and manual) with texture operators LBP in terms of Receiver Operating Characteristic (ROC) curves and Detection Error Tradeoff (DET) curve are shown in (Fig.4 and Fig. 5).

From the results, we can notice that the three descriptors performed quite well. The equal error rates (EER), shown in Table II, indicates that the detection with Stasm (EER= 2.4) is better than without Stasm (EER= 3.9). For the manual detection of 107 image not detected by Stasm (EER= 0.6) gives best results. So, we have to develop an algorithm to detect automatically any coordinate of eyes.

| Methods | Accuracy % | EER | AUC |
|----------------------------------|------------|-----|--------|
| Bad Illumination,Conditions [24] | 93 | 8.2 | - |
| LBP overlapping,blocks[18] | - | 2.9 | 0.99 |
| LBP+Gabor+HOG,[11] | 98 | 1.1 | 0.999 |
| Without_stasm | 97.31 | 3.9 | 0.9930 |
| With_stasm | 98.41 | 2.4 | 0.9975 |
| With_stasm(correction manual) | 99.61 | 0.6 | 0.9998 |

TABLE II: Performance comparison between our proposed approach and the best results in [17], [18], [24] on the same database and using the same protocol.

VI. CONCLUSION AND FUTUR WORK

Face biometric systems are vulnerable to spoofing attacks and photographs are the most common sources of spoofing attacks. Indeed, face prints usually contain printing quality defects that can be well detected. The surface properties of real faces and prints are also different.

We proposed in this work, an approach for anti-spoofing detection based on Active Shape Models with Stasm and LBP that discriminate live faces from fake ones.

Our approach tested on NUAA Photograph Imposter Database witch contains several real and fake faces showed excellent results compared to many previous works. On future work we will try to test our approach with another data base and to find a method replacing the manual method for locating landmarks on images which have hard position.

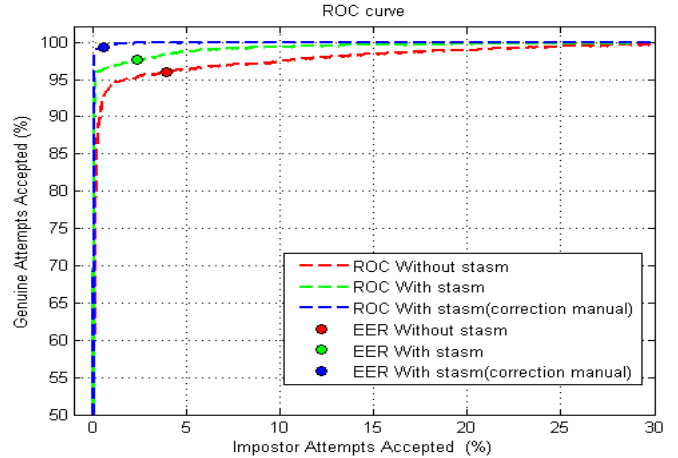


Fig. 4: Performance (ROC curves) of the proposed approach without Stasm,with Stasm, and manual.

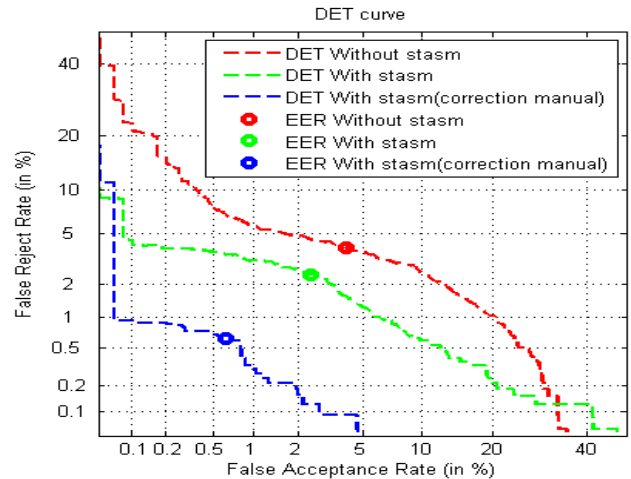


Fig. 5: Performance (DET curves) of the proposed approach without Stasm, with Stasm, and manual.



Fig. 6: Examples of anti-spoofing classification (Real: blue, Fake: yellow and wrong classification: red)

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] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 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. 1–511.
- [8] S. Milborrow and F. Nicolls, "Locating facial features with an extended active shape model," in *Computer Vision-ECCV 2008*. Springer, 2008, pp. 504–513.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcam," in *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on*. IEEE, 2007, pp. 1–8.
- [17] 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.
- [18] 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.
- [19] T. de 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.
- [20] 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.
- [21] T. Ojala, M. Pietikainen, and T. Maenpää, "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] M. Pietikäinen, A. Hadid, G. Zhao, and T. Ahonen, *Computer vision using local binary patterns*. Springer, 2011, vol. 40.
- [23] M. A. Hearst, S. Dumais, E. Osman, J. Platt, and B. Scholkopf, "Support vector machines," *Intelligent Systems and their Applications, IEEE*, vol. 13, no. 4, pp. 18–28, 1998.
- [24] 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.