Face Anti-Spoofing combining MLLBP and MLBSIF

A. Benlamoudi†, ME. Zighem.†,F. Bougourzi ‡, *SE. Bekhouche, A. Ouafi† and A. Taleb-Ahmed**
† LAGE Laboratory, University of Ouargla, Algeria, ‡ Laboratory OF LTII, University of Bejaia, Algeria, †LESIA Laboratory, University of Biskra, Algeria, *LAMIH Laboratory, UMR CNRS 8201 UVHC, University of Valenciennes, France

***Abstract* —The Face recognition applications are the used way of authentication identity verification of mobile payment. This popularity of face recognition is easy to raise concerns about face spoof attacks; use photo or video of an authorized person's face to access to facilities or services. We propose an efficient and more robust algorithm for face spoof detection based-on combination between MLLBP and MLBSIF. An ensemble classifier, consisting of Lib-SVM classifiers using different face spoof attacks (e.g., printed photo and replayed video) to trained our model which is used to distinguish between genuine and spoof faces. We tested our approach on CASIA FASD database. Our proposed approach conduct a good result compared with the state of art.**

***Keywords* — Face recognition, Anti-spoofing, CASIA, MLLBP, MLLPQ**

I. INTRODUCTION

Biometrics human characteristics and traits can successfully allow to identification people authentication. For these reasons, it can be used for access control and global security system. Several biometric modalities have applied to person recognition, ranging from traditional fingerprint to face, iris, and, more recently, vein and blood flow. Simultaneously, various spoofing attacks techniques have been created to defeat such biometric systems. A spoofing attack occurs when someone tries to bypass a face biometric system by presenting a fake face in front of the camera. However, the abundance of still face images or video sequences on the internet has made it particularly easy to access a person's facial data compared to other modalities.

The literature of spoofing detection discuss two types of spoofing attacks, namely print and replay. Print attack uses printed photographs of a subject to spoof 2D face recognition systems, while replay attack presents a video of a live person to evade liveness detection. Moreover, the relatively low cost of launching a face spoof attack has made the face spoofing problem even more common. The media used for spoofing a face recognition system vary from low quality paper prints to high quality photographs, as well as video streams played in front of the biometric authentication system sensor.

Depending on the type of features used for information extraction and representation, face anti-spoofing literature techniques can be classified into liveness and texture analysis based approaches. Liveness techniques primarily encode signs of vitality, such as eye blinking and mouth movements. Texture based approaches rely on the observation that face frames of a real person exhibit some unique spatiotemporal properties when compared to spoofed frames, now we will present some famous works:

Zhang et al. [1] used a set of difference-of-Gaussian filters to choose a specific frequency band, to be used as the features for discriminating real accesses from spoofing attempts.

Javier et al [2] proposed novel approach based on Image Quality Assessment (IQA). The authors used 14 image quality features extracted from one image, which work well in real time application.

Pereira et al. [3] proposed an anti-spoofing solution based on the dynamic texture, a spatiotemporal version of the original LBP. Results showed that LBP-based dynamic texture description has a higher effectiveness than the original LBP.

Benlamoudi et al [4], proposed an approach named Local Binary Pattern overlapping using features reduction with fisher score (LBP overlapping with fisher score). The method focused on texture of facial in each frame, which gives a real or fake frame. Then with voting method they give the global result of video if it is a real or fake one.

Samarth et al [5], presented a framework focused in motion magnification and multi-feature on video. The authors used a configuration of Local Binary Pattern and Motion estimation using Histogram of Oriented Optical Flow to encode texture and motion.

Yang et al. [6] used component analysis for liveness detection using Fisher criterion analysis for pooling evidence from informative regions of the face.

Inspired by the aforementioned observations, we propose, in this work, a new anti-spoofing method based on combining Multi-Level Local Binary Pattern (MLLBP) and Multi-Level Binarized Statistical Image Features (MLBSIF). In our approach we divided the Regions of interest (ROI) in multiple blocks with multi-level presentation and apply the two descriptor LBP and BSIF then then we extracted histograms from each block after that we concatenated the histograms to form the final

descriptors, then we combine the finale descriptors of MLLBP and MLBSI to distinguish between real and fake faces. Extensive experiments on benchmark database, namely CASIA face anti-spoofing.

We organize the remaining of this paper as follows. Section I discusses introduction and state-of-the-art methods for face spoofing attack detection. Section II presents our method for spoofing attack detection. Section III shows and discusses the experimental protocol and the obtained results. Finally, Section IV concludes the paper and discusses possible future work.

II. PROPOSED APPROACH

Our face anti spoofing approach consists in four steps which are: face alignment, presentation, features extraction and classification. First in the face alignment step, we detect the face and localize the eyes then cropped the faces, after that we normalize all faces using the center of the eyes points. In the presentation step, we divided the ROI to multiple blocks with Multi- Level presentation. After that we apply two descriptors Local Binary Pattern (LBP) and Binarized Statistical Image Features (BSIF) in each blocks and concatenate it to one finale histogram the we combine the two finale histograms to one which represents the features of our approach. Finally, we use the Lib-SVM to classify the input video to real or fake face.

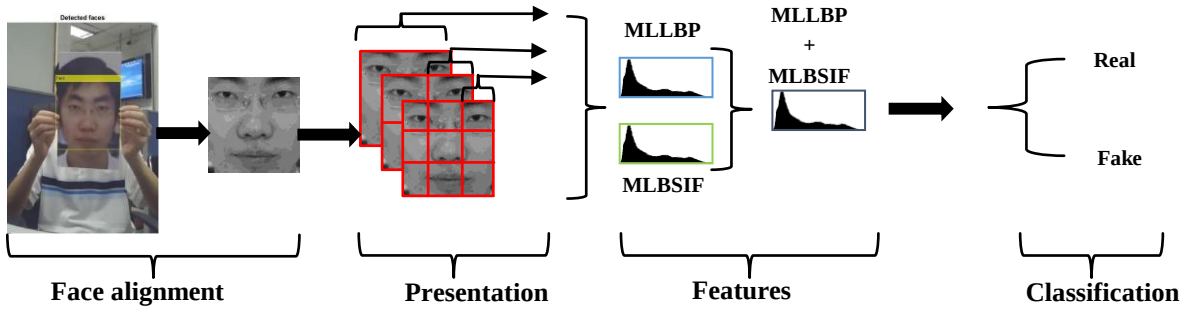

Fig 1 Our Proposed approach

A. *Face alignment*

Face is widely used for identity verification. In our system, we detected the face by using viola and jones algorithm and localized the center of the eyes using the Pictorial Structure (PS) algorithm, then we used these points to rotate and crop the Face ROI (for more detail see [7]) finally, we normalized the ROI into [64x 64].

B. *Presentation*

The main idea of Multi-Level (ML) [8] is to extract features from different Multi-Block divisions then combine them. In other words, extracting features from the whole image, then divide the face into 2^2 sub-blocks and extracting the features from each sub-blocks [9] and so on until reach the intended level. The result of ML is $1^2+ 2^2+ 3^2+... + n^2$ histograms. We combined these histograms to get the features vector. Figure 4 explains our approach.

C. *Features extraction*

In this paper, we used two famous features extraction algorithms, which are Local Binary Pattern (LBP) and Binarized Statistical Image Features.

The original LBP operator works in 3×3 neighborhood, each pixel can be labeled by using the center value as a threshold and considering the result as a binary number.

$LBP_{P,R}$ is almost used for pixel neighborhoods and it is refers to P sampling points on a circle of radius R. The value of the LBP code of a pixel (x_c, y_c) is given by:

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

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:

$$S(x) = \begin{matrix} 1 & x \geq 0 \\ 0 & otherwise \end{matrix} \quad (2)$$

A Binarized Statistical Image Feature (BSIF) [] is an image descriptor that describes each pixel's neighborhood, which constitutes a patch, by a binary code. In the beginning, BSIF computes the convolution of the image patch with a set of filters, then the responses are binarized. Each element of binary code b (i.e., b = (b_i) , (I = 1,..n)) is obtained by comparing a response with a threshold at zero. Consequently, the length of the bit string is fixed by the number of the used filters. Notice that these filters are learned from a training set of natural image patches by maximizing the statistical independence of the filter responses. To illustrate these steps, for a given image patch X of size (k * k) pixels and a linear filter $Ø_i$ of the same size, the filter response r_i , corresponding to the bit value b_i Then each bit b_i , is obtained as follows:

$$r_i = \sum_{u=1}^{k} \sum_{v=1}^{k} \Phi_i(u,v) X(u,v) \quad (3)$$

Then each $b_i = \begin{matrix} 1 & r_i \rangle 0 \\ 0 & otherwise \end{matrix}$ (4)

In order to obtain the local and the global properties of image texture, we divided the face ROI into ML to obtain the histogram of features from each sub-block. Therefore, we had one vector consisting histograms of MLBSIF features and did the same procedure for MLLBP. Finally, we combined MLBSIF and MLLBP features.

D. *Classification*

We extracted the features with combining MLLBP and MLBSIF from our training set, which we used to learn our classifier, Support Vector Machine (SVM), to recognize the spoofing faces. In this paper, we used Lib-SVM [9] classifier.

III. Experiment and Results

A. *CASIA FASD database*

We evaluated the proposed approach in CASIA Anti spoofing database [1]. Which has a significant improvement in data collection compared with previous databases. This database mainly focuses on the variation of collected data, trying to provide a comprehensive collection. Specifically, CASIA contains 50 genuine subjects, and fake faces made from records of the genuine faces with three image qualities (Low, normal and High) and three fake face attacks (warped, cut and video). Each subject contain 3 genuine and 9 fake, so CASIA have 600 videos. Finally the test protocol have 7 scenarios (High, Low, Normal, Warped, Cut, Video and Overall) for a thorough evaluation from all possible aspects. For the anti-spoofing classification, we selected 240 video samples as a train and 360 as a test.

B. *Effectiveness of combining texture and representation*

To obtain the better result Equal Error Rate (EER), we consider the different LBP and BSIF parameters, LBP with u2, P = 8 and R =1, BSIF features are obtained using eight filters of size 7 × 7. We also, compared different MB and ML level representation with level three. For fair comparison, we combined between LBP+BSIF, MBLBP+MBBSIF and MLLBP+MLBSIF. Finally, all these experiments are evaluated by lib-SVM based on two-class SVM and. The results showed in Table 1 and Figure 2.

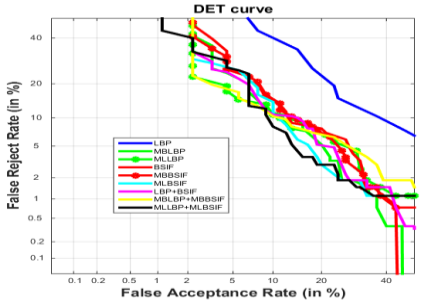

TABLE 1: COMPARISON TEXTURE AND REPRESENTATION.

Methods	***EER %***
LBP	21.29
MBLBP	10.55
MLLBP	10.37
BSIF	11.85
MBBSIF	11.48
MLBSIF	10.65
LBP+BSIF	10.37
MBLBP+MBBSIF	10.18
MLLBP+MLBSIF	09.81

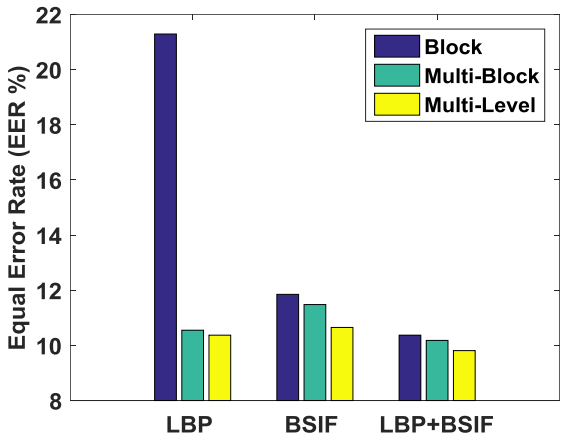

Fig. 2. Comparison between texture and representation.

C. *Comparison with state of the art*

Tables 2, 3 and 4 provide a comparison with the state-of-art of face spoofing detection techniques proposed in the literature, which show that our proposed approach outperforms the state-of-the-art algorithms on the challenging CASIA FASD database in both video and frame based evaluations. Our approach also achieves very competitive performance.

TABLE 2: DIFFERENT QUALITIES.

Methods	***Normal***	***low***	***High***
IQA	22.20	31.70	**05.60**
DoG baseline	13.00	13.00	26.00
LBP	17.00	11.00	13.00
LBP overlapping fisher	**08.80**	07.20	14.40
M-HOOF + M-M-LBP	23.33	06.11	13.88
MLLPQ	08.96	12.49	05.22
MLLBP+MLBSIF	09.93	**06.56**	07.36

As noted earlier, the CASIA FASD data contains three different qualities, which are low, normal and high qualities of image sequences. In addition, different media used for spoofing attacks. The media used for spoofing attacks are warped paper, cut paper and videos played on an iPad. In this section, we analyze the effects of quality of image sequences and spoofing media on the system performance. In this experiment, the training and testing data selected from the relevant data; three different qualities (low, normal and high) and three different media (warped photo, cut photo and video attacked) examined separately.

The results of the analysis for the MLLBP+MLBSIF in Table. 2. Similar to the figure, with low quality image sequences, the proposed systems achieve relatively low equal error rates. With increasing image quality, the performance of all three systems degrade. The hypothesis is that one of the discriminating factors between the spoofing attacks and real accesses is the high frequency content of image sequences, which are likely to be attenuate in spoofing attacks. However, as the high frequency content of spoofing attacks strengthened by increasing the device quality, the ability to distinguish them from genuine accesses diminished. Further investigation is needed to fully characterize the effect of

quality on performance. It is pertinent also to examine the possibility of degrading the quality artificially, or deliberately using a poor quality device, to achieve better detection performance.

TABLE 3: DIFFERENT MEDIA.

Methods	***Warped***	***Cut***	***Video***
IQA [2]	26.10	18.30	34.40
DoG baseline [1]	16.00	06.00	24.00
LBP[3]	13.00	16.00	16.00
LBP overlapping fisher[4]	12.00	10.00	14.70
M-HOOF + M-M-LBP[5]	10.00	14.44	20.00
MLLPQ[10]	13.62	09.66	10.10
MLLBP+MLBSIF	**09.89**	**03.45**	**10.04**

Regarding the effect of spoofing media, examination of Table. 3 reveals that system perform well on the warped, photo attacks and video. As expected, the error rates decrease when the spoofing media are face prints, in which eyes positions are cutout and blinking performed. We conclude that blinking plays an important role for distinguish between the spoofing attacks and the real accesses. However, the error rates for the cut photo are better than the other rate that can explain the limited quality of the video displays and reflections from an iPad screen, both of which make it easier to discriminate an attack from a real access request.

TABLE 4: OVERALL TEST.

Methods	***Overall test***
IQA	32.40
DoG baseline	17.00
LBP	16.00
LBP overlapping fisher	13.00
M-HOOF + M-M-LBP	14.44
MLLPQ	11.39
MLLBP+MLBSIF	**09.81**

Finally, we compare the proposed approach (MLLBP+MLBSIF) in the overall test scenarios of the CASIA FASD database with other existing approaches reported in the literature. The results showed in Table 4 and Figure 3. The following observations from the table. The proposed approach based on MLLBP+MLBSIF descriptors compares very favorably to the existing approaches. We observe that the combining representation in ML technique achieves the lowest error rate in the overall test scenario among other competitors.

IV. CONCLUSION

In this paper, we described a novel method for face anti-spoofing based on MLLBP+MLBSIF features extraction. The experimental results showed that the combination of MLLBP and MLBSIF features provide a better performance than the previous methods in the case of whole CASIA FASD database. We used Lib-SVM classifier to train different spoof attacks then we can test if the person is real or not. Our future suggestion is to use many databases to train our model to improve our result.

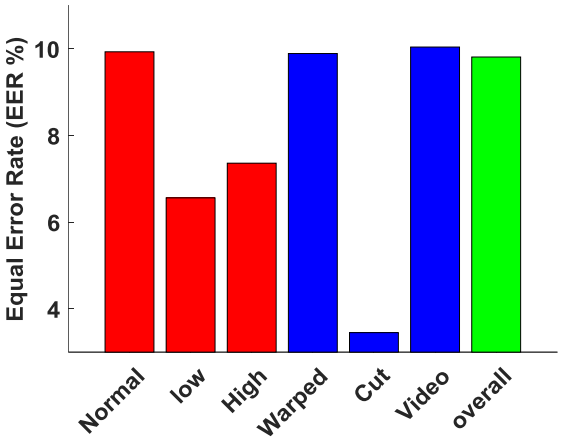

Fig. 3. COMPARISON OF EER'S (%) OF DIFFERENT METHODS ON THE CASIA FASD.

REFERENCES

[1] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks." in ICB, A. K. Jain, A. Ross, S. Prabhakar, and J. Kim, Eds. IEEE, 2012, pp. 26–31.

[2] 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.

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

[4] A. Benlamoudi, D. Samai, A. Ouafi, A. Taleb-Ahmed, S. E. Bekhouche, and A. Hadid, "Face spoong detection using local binary patterns and fisher score," in International Conference on Control, Engineering and Information Technology CEIT2015, in press.

[5] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Face anti-spoofing via motion magnification and multi-feature videolet aggregation," 2014.

[6] J. Yang, L. Zhen, L. Shengcai, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proceedings of IAPR International Conference on Biometrics, 2013, pp. 1–7.

[7] 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.

[8] S. E. Bekhouche, A. Ouafi, A. Benlamoudi, A. Taleb-Ahmed and A. Hadid, "Facial age estimation and gender classification using multi-level local phase quantization," 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT), Tlemcen, 2015, pp. 1-4.

[9] S. E. Bekhouche, A. Ouafi, A. Benlamoudi, A. Taleb-Ahmed and A. Hadid, " AUTOMATIC AGE ESTIMATION AND GENDER CLASSIFICATION IN THE WILD," International Conference on Automatic control, Telecommunication and Signals (ICATS'15), 2015, pp. 1-5.

[10] A. Benlamoudi, D. Samai, A. Ouafi, S. Bekhouche, A. Taleb-Ahmed, A. Hadid, Face spoofing detection using multi-level local phase quantization (mllpq), International Conference on Automatic control, Telecommunication and Signals (ICATS'15) (2015) 1,6.