Face spoofing detection using Multi-Level Local Phase Quantization (ML-LPQ)

A. Benlamoudi*, D. Samai*, A. Ouafi†, SE. Bekhouche†, A. Taleb-Ahmed‡, and A. Hadid§
*Universit Kasdi Merbah Ouargla, Laboratoire de Gnie Elctrique,
Facult des Nouvelles Technologies de lInformation et de la Communication, Ouargla, 30000, Algeria
Email : benlamoudi.azeddine@univ-ouargla.dz, samai.djamel@univ-ouargla.dz
†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*—Biometric technologies are becoming the foundation of an extensive array of highly secure identification and verification solution. Unfortunately, biometric systems are vulnerable to attacks made by persons showings photo, video or mask to spoof the real identity. In this paper we study a solution for those problems. We try to make solution to face spoofing for distinguishing between real face and fake one. Our approach called Multi-Level Local Phase Quantization (ML-LPQ) is focused in Local Phase Quantization (LPQ) descriptor for extracting features on face region of interest. In our approach, we use three levels for the LPQ descriptor to extract features and LibSVM for classification. Our experimental analysis on a publicly available CASIA face anti-spoofing database give us good result compared to other approaches using the same protocol.**

***Keywords*—biometrics, spoofing, ML-LPQ, CASIA , LibSVM**

I. Introduction

Recent search in biometrics technologies show that are vulnerable to attack by fake fingerprints, static facial images, static iris images [1] ...etc. Among these techniques, face spoofing is the most used in these attacks by showing (picture, video and mask) at the place of the real person because face recognition system are not able to differentiate between real face and fake one.

Generally fake faces are divided into two classes: positive and negative. The first one (positive) is known as the genuine face. The second one (negative) named the spoof face based on photographs or record videos [2], as we use in this paper see fig 1.

In the next section, we present the state-of-the-art in face anti spoofing for facial biometrics. In our work, we used CASIA anti spoofing database [3] so we describe only the related works on the same database.

Javier et al [4], 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.

Tiago et al [5], introduced a method focus on dynamic texture extensions of the highly popular local binary pattern operator (LBP). The general idea of proposed approach is learn and detect the facial micro-textures, this approach is called LBP-TOP.

Benlamoudi et al [6], 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 [7], 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.

Maatta et al [8], proposed cascade structure for face spoofing detection using upper and medium body detection depending on Histograms of Oriented Gradients (HOG) descriptor for determine if there is spoof or not.

Santosh et al [9], developed an algorithm called Dynamic Mode Decomposition (DMD) to capture liveness on motion. The same authors propose a classication pipeline consisting of DMD, Local Binary Patterns (LBP) and Support Vector Machines (SVM) with a histogram intersection kernel.

Di et al [10], proposed an algorithm based on Image Distortion Analysis (IDA) robust face spoof detection algorithm. The IDA feature vector is formed with four different features (specular reection, blurriness, chromatic moment, and color diversity). Also the proposed method depending in multi-frame face spoof detection in videos using a voting based scheme.

Jianwei et al [11], proposed a method consists of : locating the components of face, coding the low-level features respectively for all the components, deriving the high-level face representation and concatenating the histograms from all components. All these steps named Component Dependent Descriptor.

The rest of the paper is organized as follows: Section I introduces and discusses related works on face anti spoofing attacks. Section II presents Database used in our tests. Section III describes our approach in details. The experimental results and a comparison with many related works are summarized in Section IV. Finally a conclusion and future works are given in section V.

II. CASIA Face Anti-Spoofing Database

The CASIA database[3] [1] 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. There fore 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 see fig 1.

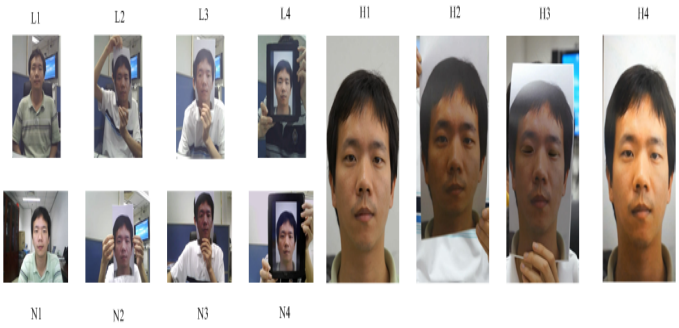

Fig. 1: One complete video set for an individual subject of CASIA Face Anti-Spoofing Database.

III. PROPOSED APPROACH

In this section, we explain our approach of face anti-spoofing based in three steps: face preprocessing, feature extraction and classification. Face Anti-spoofing is a technique used for differentiate between fake face and real face. The first one is (photographe, video or mask) of the user and the second one isthe real person. In below, we explain our approached in detail.

A. Face preprocessing

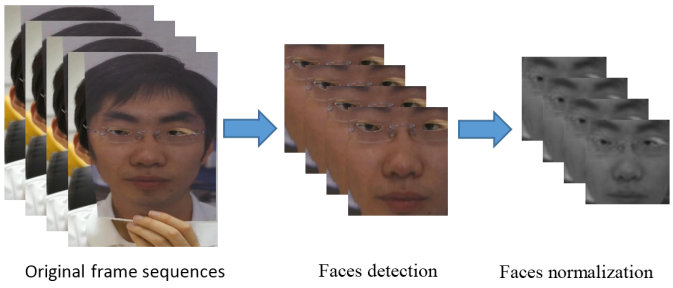

Fig. 2: Face preprocessing

In each frame of our video, first we detect the face and eyes localization in this face, then we use those eyes location to calculate the distance between them to adjust and crop the Region Of Interest (ROI). For more detail, you can see [12] [13]. Finally we normalize the croped face into a (128 x 128) pixel images see fig 2.

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

B. Feature extraction

The local phase quantization (LPQ) method is based on the blur invariance property of the Fourier phase spectrum [14]. It uses the local phase information extracted using the 2-D DFT or, more precisely, a short-term Fourier transform (STFT) computed over a rectangular M-by-M neighborhood at each pixel position x of the image f(x) dened by:

$$F(u,x) = \sum_{y \in N_x} f(x-y) e^{-j2\pi u^T y} = w_u^T f_x \qquad (1)$$

where w_u is the basis vector of the 2-D Discrete Fourier Transforms (DFT) at frequency u, and f_x is another vector containing all M^2 image samples from N_x [9].

For this subsection we used the local phase quantization (LPQ) as descriptor of features extraction. Depending on LPQ, we compared Multi-level Local Phase Quantization (ML-LPQ) and Multi-Blocks Local Phase Quantization (MB-LPQ).

1) MB-LPQ: We divided the face ROI (region of interest) into (n x n) sub-blocks and applied the Local Phase Quantization (LPQ) features on each sub-block n= 1, 2, 3, 4, and 5. This method is called multi block Local Phase Quantization (MB-LPQ) (see fig 3).

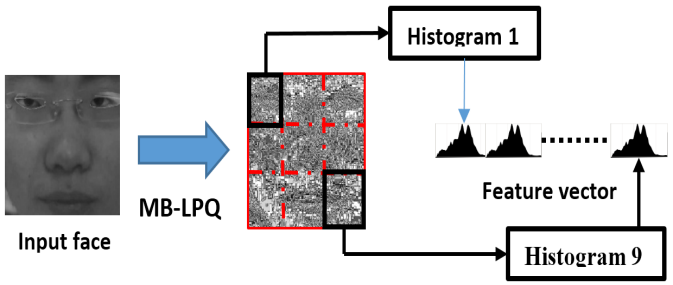

Fig. 3: Example of MB-LPQ features extraction with (n = 3 x3 sub-blocks).

2) ML-LPQ: The main idea of ML-LPQ is to extract features from different (MB-LPQ) divisions and then combine them. In other words, extracting features from the whole image, then dividing the image into 2^2 sub-blocks and extracting the features from each sub-blocks and so on until we reach the intended level. The nal result of ML-LPQ is $1^2 + 2^2 + 3^2 + ... + n^2$ histograms[15]. We combine these histograms to get the feature vector. Figure 4 explains our approach.

We explained before how we used MB-LPQ and ML-LPQ to extract the features from image. So we need now to explain how to use those histogram in video because our data bases contain only the video. Each video is divided in multiple frame and on each frame our approach is used and the feature in terms of histogram is extracted, then the mean of all histograms is calculated. Finally fisher score selection [16] is used on the mean of all histograms to reduce the bin histogram (see fig 5).

C. Classification

A Support Vector Machine (SVM) performs classification by finding the hyper plane that maximizes the margin between

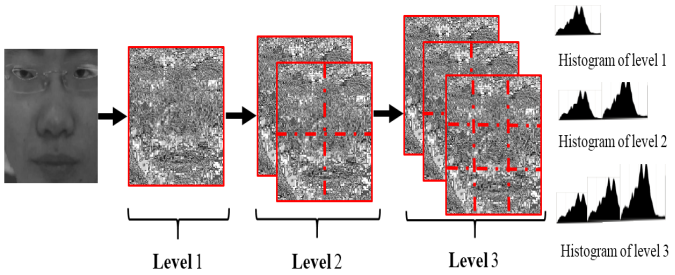

Fig. 4: Example of our approach ML-LPQ features extraction with (n = 3 level).

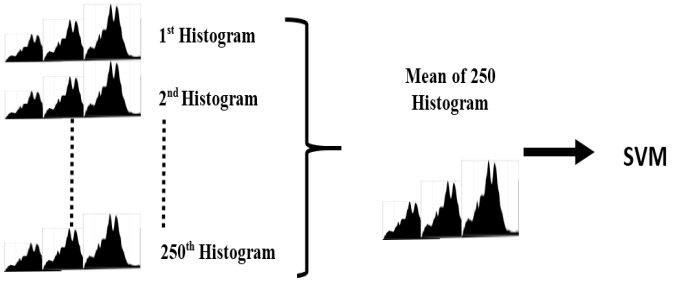

Fig. 5: Example of mean of all histograms.

two classes. The vectors (cases) that define the hyper plane are called the support vectors.

In our experiments, to classify each subject (video) into real/fake one, we use Library Support Vector Machine (lib-SVM)[2] with a linear option [17]. SVM is constructed for every pair of classes by training it to discriminate the two classes. We use 4 fold for selection the C parameter of linear lib-SVM. For determining whether the input video corresponds to a live or not. The SVM classifier is first trained using a set of positive (real faces) and negative (fake faces) samples from the dataset.

IV. EXPERIMENTAL ANALYSIS

We evaluated the proposed approach in CASIA Anti spoofing database[3]. 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 imaging qualities (Low, High and normal) 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 classication we used 240 video samples as a train and 360 as a test.

In our experimente to obtain the best results, we consider the different Local Phase Quantization LPQ parameters. LPQ with 5 x 5 local window size gives the best results. We use LPQ on overall test because it have all qualities and attacks.

[2]https://www.csie.ntu.edu.tw/ cjlin/libsvm/

We take on each step N numbers of frames and calculate the EER for comparing which number of frames give the best results. After this comparison we decided to take 250 frames on each video. The table I shows the compared result.

TABLE I: Comparison of number of frames in term of (EER)

Number of frame	EER (%)	Number of frame	EER (%)
5	25.86	**125**	15.38
10	22.25	**150**	15.98
15	19.24	**175**	16.06
25	17.90	**200**	14.98
50	20.03	**225**	14.54
75	16.97	**250**	13.98
100	18.93	**275**	14.39

After the comparison and decision, the number of frames used in our approach is 250 frame per video. For now, we go to compare our approach using Multi-Block Local Phase Quantization MB-LPQ with and without fisher score, and also Multi-Level Local Phase Quantization ML-LPQ with and without fisher score. The table II and table III show the compared results of MB-LPQ and ML-LPQ respectfully.

TABLE II: Comparaison between the diffrent MB-LPQ

MB-LPQ divisions	EER (%) without fisher score	EER (%) with fisher score
1 x 1	**13.98**	**13.31**
2 x 2	15.94	15.47
3 x 3	17.72	15.95
4 x 4	21.19	18.59
5 x 5	14.30	13.96

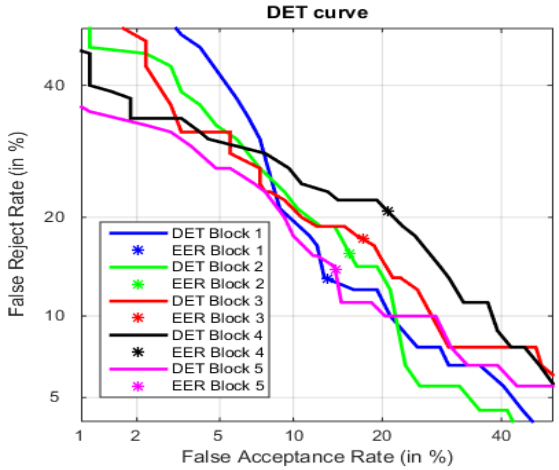

Fig. 6: DET of MB-LPQ without fisher score.

TABLE III: Comparaison between different levels of ML-LPQ

ML-LPQ Level	EER (%) without fisher score	EER (%) with fisher score
1	13.98	13.31
2	14.93	14.34
3	**12.97**	**11.39**
4	13.26	12.47
5	15.85	12.85

We compared now the Multi-Block Local Phase Quantization (MB-LPQ) with Multi-Level Local Phase Quantization

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

methodes scenario	Low(1)	Normal(2)	High(3)	Warped(4)	Cut(5)	Video(6)	Overall(7)
IQA [4]	31.7	22.20	05.60	26.10	18.30	34.40	32.40
DoG baseline [3]	13.00	13.00	26.00	16.00	06.00	24.00	17.00
LBP$^{u2}_{8,1}$ [5]	11.00	17.00	13.00	13.00	16.00	16.00	16.00
LBP overlapping fisher [6]	07.20	08.80	14.40	12.00	10.00	14.70	13.10
Multi-LBP [7]	12.77	16.66	26.66	15.55	25.55	17.77	17.77
Mag-Multi-LBP [7]	07.22	13.33	29.44	14.44	22.22	13.33	15.74
HOOF [7]	16.66	30.00	26.11	15.55	17.77	38.88	21.11
Mag-HOOF [7]	17.22	33.33	22.77	12.22	20.00	36.60	22.22
HOOF + Multi-LBP [7]	09.44	20.55	16.66	10.00	16.66	24.44	15.55
Mag-HOOF + Mag-Multi-LBP [7]	06.11	23.33	13.88	10.00	14.44	20.00	14.44
CDD [11]	01.50	05.00	02.80	06.40	04.70	00.30	11.80
MB-LPQ(our)	16.31	22.36	11.34	14.20	13.65	10.46	13.98
MB-LPQ fisher (our)	13.37	13.12	08.45	12.11	11.43	07.61	13.31
ML-LPQ(our)	14.83	08.95	05.41	15.83	10.01	10.06	12.97
ML-LPQ fisher (our)	12.49	08.96	05.22	13.62	09.66	10.10	**11.39**

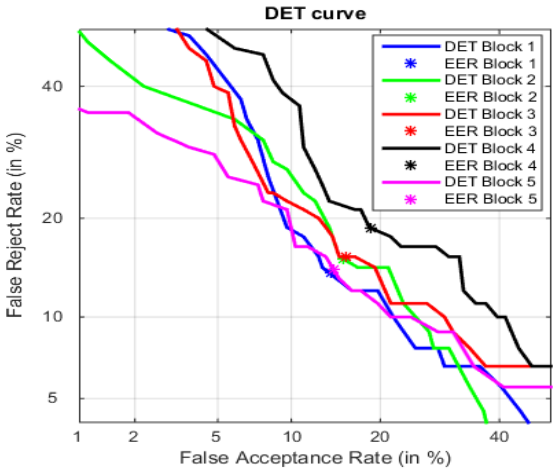

Fig. 7: DET of MB-LPQ with fisher score.

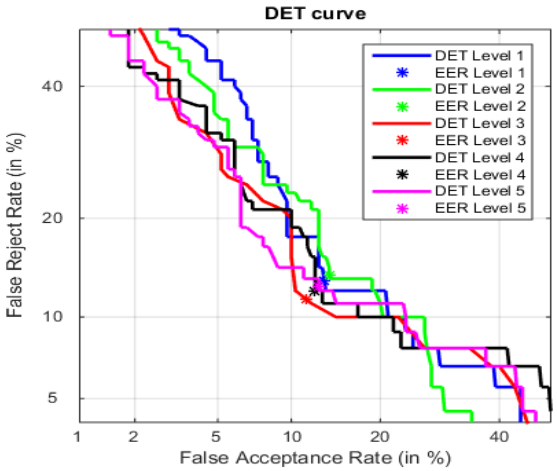

Fig. 9: DET of ML-LPQ with fisher score (3 level).

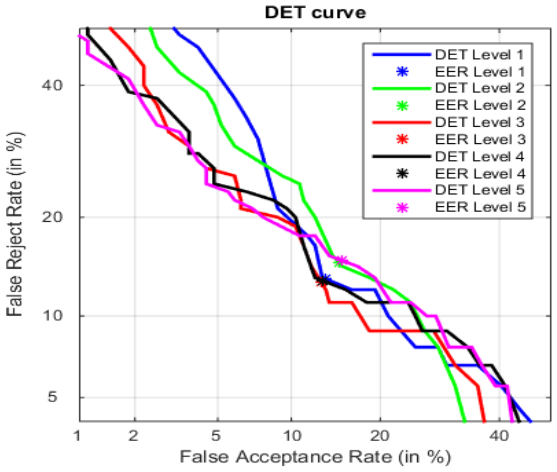

Fig. 8: DET of ML-LPQ without fisher score (3 level).

(ML-LPQ). The Both descriptors are used with and without fisher score. As we see in table (II) and DET curves (6 and 7), MB-LPQ with fisher score, EER is 13.31 % is good compared the MB-LPQ without fisher score MB-LPQ, EER is 13.98 %. After that in table (III) and DET curves (8 and 9), ML-LPQ with fisher score, EER = 11.39 % is good compared to ML-LPQ without fisher score, EER = 12.97 %. Finally outcome Multi-Level Local Phase Quantization (ML-LPQ) with fisher score our approach is the best compared to all our test before.

Now after discussion of our result and outcome that ML-LPQ with fisher score gives the good result. To test the robustness of our system, we start now comparing our approach with state-of-art on CASIA face anti spoofing database, which already have 7 scenario are namely the low quality (1), normal quality (2) and high quality (3). Three fake face attacks are implemented, which include warped photo attack (4), cut photo attack (5) and video attack (6), the last scenario is overall test (7) which have all type of qualities and attacks. The table below shows the comparison of results between the state-of-art and the 7 scenario of CASIA databases. Finally for

more comparison we show the DET curves of all descriptors, MB-LPQ and ML-LPQ with and without fisher score of all scenarios.

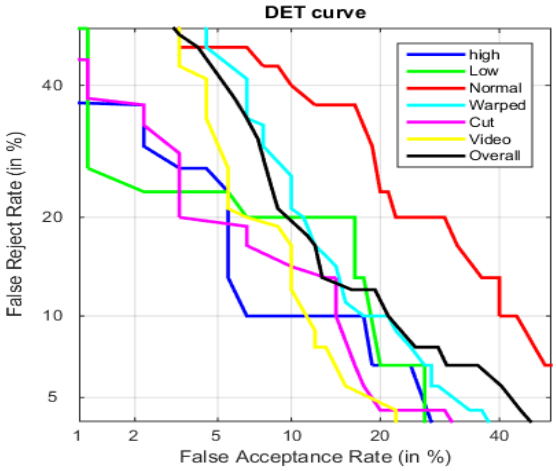

Fig. 10: DET of MB-LPQ without fisher score, 7 scenario.

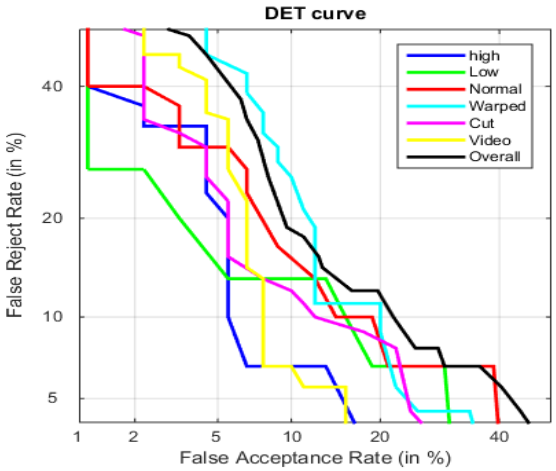

Fig. 11: DET of MB-LPQ with fisher score, 7 scenario.

V. CONCLUSION AND FUTUR WORK

In this paper, we studied a solution for face spoof detection, practically in seven scenario of CASIA anti spoofing database (CASIA ASD). In fact the most authors in face spoof detection used texture or motion based features. We propose Multi-Level Local Phase Quantization algorithm (ML-LPQ) with fisher score to play a role face anti spoofing detection tol give us local features when LPQ base give global features. In our approache used three level LPQ so we needed to use fisher score to selecte and reduce the bin histograms. We used Lib-SVM classifier to train different spoof attacks and determinate if it is a real video or not. Evaluations on CASIA database show that the proposed approach gives best results compared to the state-of-the-art in overall test which have all qualities and attacks. Our suggestions for future work on face spoof detection is trying to make our system robust for all databases and get a unic training model for all face spoof detection.

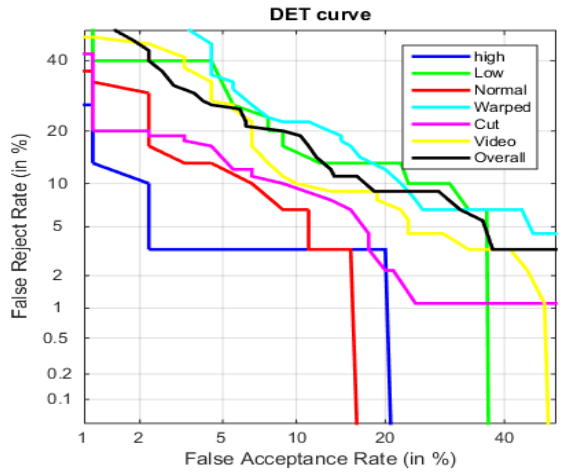

Fig. 12: DET of ML-LPQ without fisher score (3 level), 7 scenario.

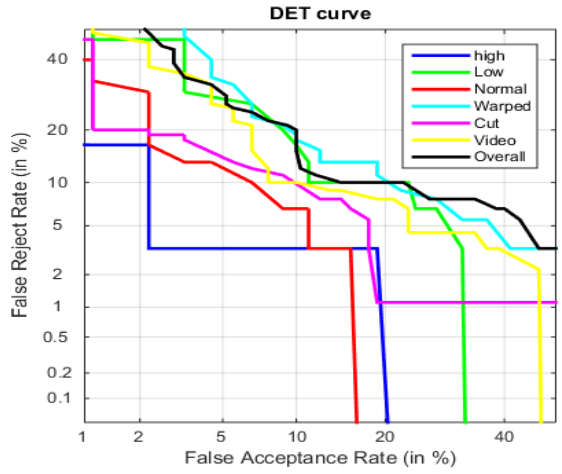

Fig. 13: DET of ML-LPQ with fisher score (3 level), 7 scenario.

REFERENCES

[1] P. V. Reddy, A. Kumar, S. Rahman, and T. S. Mundra, "A new antispoofing approach for biometric devices," *Biomedical Circuits and Systems, IEEE Transactions on*, vol. 2, no. 4, pp. 328–337, 2008.

[2] S. Parveen, S. Ahmad, S. Mumtazah, M. Hanafi, W. Adnan, and W. Azizun, "Face anti-spoofing methods." *Current Science (00113891)*, vol. 108, no. 8, 2015.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing," in *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 2013, pp. 1–8.

[9] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. Ho, "Detection of face spoofing using visual dynamics," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 4, pp. 762–777, 2015.

[10] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 4, pp. 746–761, 2015.

[11] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in *Biometrics (ICB), 2013 International Conference on*. IEEE, 2013, pp. 1–6.

[12] 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.

[13] 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.

[14] V. Ojansivu and J. Heikkilä, "Blur insensitive texture classification using local phase quantization," in *Image and signal processing*. Springer, 2008, pp. 236–243.

[15] S. Bekhouche, A. Ouafi, A. Benlamoudi, A. Taleb-Ahmed, and A. Hadid, "Facial age estimation and gender classification using multi level local phase quantization," in *International Conference on Control, Engineering and Information Technology (CEIT2015)*, 2015.

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

[17] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011, software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.