

Live Face Detection Method Based on Local Binary Pattern and Bandelet

Haiqing Liu, Shuhua Hao, Yuancheng Li, Xiang Li and Jie Ma

Abstract —Face recognition system is exposed to video replay attacks and photo spoofing attacks along with the extensive use of identity authentication technology. Spoofing attack happens when an attacker tries to disguise as a legitimate user with permissions to spoof authentication system by replaying the recorded videos of legitimate users or utilizing the printed photos of legitimate users. Inspired by the differences between image acquisition and playback, printing properties, and light emission models, this paper proposes a live face detection method based on local binary pattern and Bandelet. The replayed video images and the printed face images usually contain characteristics that are easy to be detected by texture detection and frequency domain analysis. The proposed method analyzes the differences between live faces and photo faces in texture, at the same time it utilizes Bandelet to analyze face images with multi-scale analysis and extracts the high-frequency sub band coefficients as feature vectors to train Extreme Learning Machine (ELM) to classify and recognize. The algorithm is verified on the public CASIA_FASD, print-attack and replay-attack datasets, well known Face Anti-Spoofing Databases, and the experimental results show that the method reduces the computational complexity and improves the detection accuracy.

Index Terms—liveness detection; Bandelet transform; replay attack; authentication technology

I. INTRODUCTION

IN recent years, biometric authentication has attracted more and more attention, such as the safety assessment and vulnerability assessment. As a convenient user authentication technology, face recognition only needs regular cameras and a face detection application, so it has been widely applied to various scenarios under the efforts of many researchers. To give some examples, we can mention entrance guard systems, access security checks, criminal detection, the banking system, etc. However, face recognition system detects human faces through the analysis of the tactic flat images, so the system is easy to be spoofed by replayed videos or printed photos. In a real application scenario, the identity authentication system mainly faces three common spoofing methods [1].

1) Photo spoofing [2]: It is one of the most convenient spoofing methods to access the photos of legitimate users. The spoofer bends and rotates the printed photos in front of

image acquisition devices to simulate the real legitimate users, which can spoof the authentication system.

2) Video spoofing [3]: The video of legitimate users is a more threatening spoofing tool, and it can be acquired by the secret cameras. Compared with photos, videos have characteristics of head movements, facial expressions, blink, etc. and their effects are similar to the real human faces.

3) 3D model spoofing: Make a 3D model for the human faces of legitimate users, which can simulate the blink, talking, head movements of real people [2-4]. Compared with the photo spoofing and video spoofing, 3D model spoofing is more threatening, but forging the live 3D model is more difficult. So, photo spoofing and video spoofing are the most used methods of identity authentication spoofing.

In this paper, our goal is to use a better algorithm to distinguish between real and fake faces. We propose a novel live face detection method, based on local binary pattern and Bandelet that extracts texture features from living bodies and photos, and then trains ELM classifier to identify authenticity. Finally, the result is verified on the public CASIA_FASD database, print-attack and replay-attack databases. Our experimental results show that the proposed algorithm performs well on all datasets.

The contribution of this article can be summarized as follows. We proposed a fusion method of LBP and Bandelet algorithm for countering spoof attacks in face recognition. We optimize the basic LBP and Bandelet algorithm to extract the features from face image respectively. Then we fuse the features and put them into the ELM classifier for training and learning. Our method finally is verified and evaluated on public CASIA-FASD, print-attack and replay-attack datasets, and the results show that the proposed approach outperforms the other methods in spoof detection.

The rest of this paper is organized as follows: Section II presents related works about face spoofing detection. Section III introduces the details of our live face detection method, the local binary pattern, Bandelet decomposition, and the ELM classifier. Section IV shows our experimental results. Finally, we conclude the paper in section V.

II. RELATED WORKS

Currently, many scholars in China and the rest of the world are committed to the study of the liveness detection problem, and there are already many live detection methods that are presented in the international conferences and journal articles. Presently, the live detection methods applied to face recognition mainly include the following categories:

This work was supported in part by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry ([2013]693).

All the authors come from the school of Control and Computer Engineering in North China Electric Power University.

Haiqing Liu (email: hqliu@ncepu.edu.cn), Shuhua Hao (email: shhao@ncepu.edu.cn (new), hsh0218hsh@163.com (old)). Yuancheng Li (Corresponding author, Email: ycli@ncepu.edu.cn).

A. Image quality analysis based methods

As an example of image quality analysis method, D. Gong et al. proposed a new feature descriptor called common encoding model for heterogeneous face recognition, which is able to capture common discriminant information, such as the large modality gap [5]. I. Kim proposed a novel approach to robustly find the spoofing faces using the highlight removal effect, which is based on the reflection information. Because the spoofed face image is recaptured by a camera, it has additional light information [6]. D. Wen et al. proposed an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector [7]. M. Uzair et al. proposed a hyperspectral face recognition algorithm using a spatio-spectral covariance for band fusion and partial least square regression for classification. Moreover, they extended 13 existing face recognition techniques, for the first time, to perform hyperspectral face recognition [8]. Galbally et al. extracted 25 features from an image such as peak signal-to-noise ratio and structural similarity index to detect subtle image quality [9]. Karubgaru et al. solved the feature extracted method by "increasing" the data available from the original image using several preprocesses, such as, image mirroring, colour and edges information [10].

B. Move option based methods

Shervin et al. proposed a multiscale dynamic texture descriptor based on binarized statistical image features on three orthogonal planes (MBSIF-TOP) that is effective in detecting spoofing attacks and showing promising performances compared with existing alternatives [11]. Pan et al. have conducted live detection by blink actions [12]. Santosh T et al. have proposed a classification pipeline consisting of DMD, local binary patterns (LBPs), and support vector machines (SVMs) with a histogram intersection kernel. A unique property of DMD is its ability to conveniently represent the temporal information of the entire video as a single image with the same dimensions as those images contained in the video [13]. W. Yin et al. explored the issue of face anti-spoofing with good performance in accuracy by utilizing optical flow vector on two types of attacks: photos and videos shown on high-resolution electronic screens. The key idea is to calculate the displacement of the optical flow vector between two successive frames of a face video and obtain a displacement sum of a certain number of frames [14]. Many scholars were studying video sequences and dynamic descriptors that were extracted from video sequences [15-16]. Besides, Zhang Yu et al. improved the Piecewise Aggregate Approximation (PAA) method, and proposed a Hierarchical Clustering technique (HC-PAA) [17].

C. Texture based methods

N. Werghe et al. presented a novel approach for fusing

shape and texture local binary patterns (LBPs) on a mesh for 3D face recognition. Using a recently proposed framework, they computed LBP directly on the face mesh surface, then they construct a grid of the regions on the facial surface that can accommodate global and partial descriptions [18]. K. Patel et al. analyzed the image distortion of the print and replay attacks using different: 1) intensity channels (R, G, B, and grayscale); 2) image regions (entire image, detected face, or facial component between nose and chin); and 3) feature descriptors. They developed an efficient face spoof detection system on an Android smartphone. Their studies of Android face spoof detection system involving 20 participants showed that the proposed approach worked very well in real application scenarios [19]. Pereira et al. applied a local binary pattern (LBP) to the X-Y, X-T and Y-T dimensions to analyze the texture of time and space [20]. T. Edmunds et al. proposed an original approach was that the fake face detection process occurs after the face identification process. Having access to enrollment data of each client, it becomes possible to estimate the exposure transformation between a test sample and its enrollment counterpart [21].

Table I Comparative of different face spoof detection methods

Type	Mechanism	Strengths	Limitations
Image quality analysis [5-10]	Image quality analysis of different attack image	Good generalization ability Fast response	Different classifiers needed for different spoof attacks
Move option [11-17]	Get the dynamic description in the video sequence	Good generalization ability	Slow response High computational complexity
Texture [18-21]	Analyze image static texture information	Fast response Low computational complexity	Vulnerable to the variations in acquisition conditions

Although much work has been directed towards tackling issues related to face spoofing detection, there is still significant room for improvement for anti-spoofing methods in face recognition [22]. Table I shows some advantages and disadvantages of the three methods listed in this article. In this paper, we proposed live face detection method based on local binary pattern and Bandelet. This method doesn't need users' active cooperation, so it has certain concealment. At the same time, the dimensions of extracted features are not high, while it reduces the time and the algorithm complexity.

III. LIVE FACE DETECTION METHOD BASED ON MULTISCALE ANALYSIS

It could be very difficult for us to distinguish the live faces in the photos accurately with our eyes, as shown in Figure 1. In fact, live faces are complicated non-rigid 3D objects, while photo faces or video faces are flat rigid objects, so they can differ in light reflection and shadow. Photo faces usually contain the defects of printing quality, and this difference can be detected well by utilizing texture details.

A. Local Binary Pattern

Local binary pattern is a kind of operator used to describe the local texture features of images. Obviously, its function is feature extraction, and the extracted features are the texture features of images and they are local texture features. As show in Figure II, the original LBP operator is defined in the window of 3x3 pixels. The window's center pixel is regarded as a threshold and is compared with the grey values of eight adjacent pixels. If the surrounding pixel value is greater than the center pixel value, then the position of this pixel is marked as 1, otherwise is marked as 0. In this case, eight points in a



Figure I. Live faces in the CASIA database (a), photo faces (b) and video faces (c).

3x3 window can produce an 8-bit unsigned number, and then the LBP value of this window can be obtained to reflect the texture information of this area.

After the original LBP was brought up, researchers increasingly proposed various improvements and optimizations to get an LBP operator where there are P sampling points in the circular area with R in radius: LBP uniform pattern, LBP rotation invariant pattern, LBP equivalent pattern, etc.

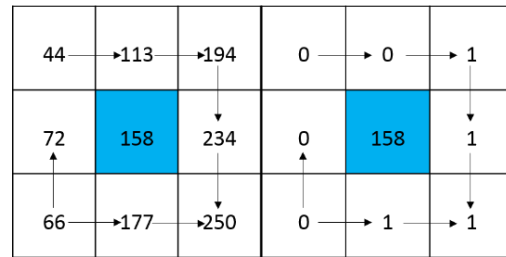


Figure II. The processing of LBP

Apparently, the above extracted LBP operator can get an LBP code in each pixel. Then, the obtained original LBP features are still an image after extracting the original LBP operator from an image. However, the objects in this image have been converted to secondary features, which cannot be directly applied to the discriminant analysis. We can see that this feature is closely relevant to the position information from the above analysis. So it can have a considerable deviation due to non-aligned positions if we directly conduct discriminant analysis on this feature of two images. Later, the researchers found that an image can be divided into several sub areas and LBP features are extracted from each pixel in each sub area, and then, statistical histograms of LBP features are established in each sub area. In this way, each sub area can be described by a statistical histogram. The whole image is composed of several statistical histograms. For example, an image with 100x100 pixels is divided into 100 sub areas with 10x10 pixels, and the size of each sub area is 10x10 pixels. LBP features are extracted from each pixel in each sub area, and then, statistical histograms are established. In this way, the image has 10x10 sub areas and 10x10 statistical histograms. This image can be described by these 10x10 statistical histograms. After that, we can judge the similarity between two images by various similarity measure functions.

At present, the LBP local texture extraction operator has been successfully applied to fingerprint recognition, character recognition, face recognition, license plate recognition and other fields.

B. Bandelet Decomposition

The main idea of constructing Bandelet transform [23] is to define geometric features in images as a vector field, rather than a set of common edges. And the vector field denotes the local regularity direction of gray value variations in an image spatial structure. Bandelet base is not predetermined, and it is chosen according to the optimization of final application results. A. Lutz et al. proposed the quick search method of the optimal base in Bandelet variation.

Live face detection method based on local binary pattern and bandelet

For geometric regularity images, geometric flows are parallel within a local scope. The wavelet transform is essentially the convolution of wavelet function and the original image, and the wavelet function can be regarded as the fuzzy kernel in this sense, so wavelet transform has a smoothing effect on the original image. This smoothing effect makes the image to have the regularity of direction that is vertical with the geometric flow, and it makes that the positioning of geometric flow doesn't need to be strictly accurate, being allowed to have a certain deviation. In view of the difficulties of accurate positioning of image edge line, this regularity makes it convenient to position geometric flow rapidly.

Image segmentation adopts the binary segmentation method which Donoho adopted in wedgelet. Firstly, a square image is equally divided into 4 sub areas, and then, each sub area is equally divided into 4 sub areas in the next layer of segmentation, until the size of sub areas at the bottom layer reaches the minimum preset. The segmentation result can be shown by quadtree; each sub area corresponds to one node of the quadtree, as shown in Figure III. When the width of an image is 1, and the width of the sub area is $(1/2)^n$, the depth of the quadtree node corresponding to the sub area is n.

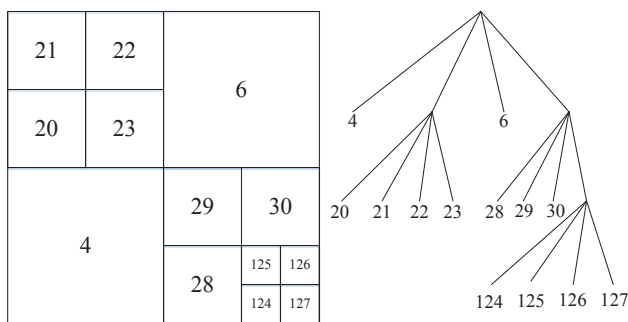


Figure III. Binary tree decomposition diagram

C. The Proposed Live Face Detection Method

As for texture feature detection, this paper proposes a live face detection method based on LBP and Bandelet to solve this problem. The flowchart of this method is shown in Figure IV.

Step 1 Convert the face image to be detected into a grayscale image, remove the redundant color information and keep the texture information.

Step 2 Extract the local binary pattern features and statistical features of high-frequency coefficients in Bandelet transform from the converted grayscale image.

The process of getting local binary pattern features is:

- 1) Divide the detected window into several sub areas (for example, the size of every sub area is 16x16 pixels).
- 2) Compare every pixel in the sub areas with its eight neighborhood pixels (upper left, left middle, lower left, upper right, etc.), which can be carried out in accordance with the clockwise or counter-clockwise order.

- 3) If the surrounding pixel value is greater than the center pixel value, then the position of this pixel is marked as 1, otherwise, is marked as 0. In this case, an 8-bit binary number is obtained and converted to a decimal number to be as the feature of this area.
- 4) Establish histograms for every sub area.
- 5) At this time, the histograms can be normalized.
- 6) Have all the histograms of sub areas connected in series, and then the features of the detected window are obtained.

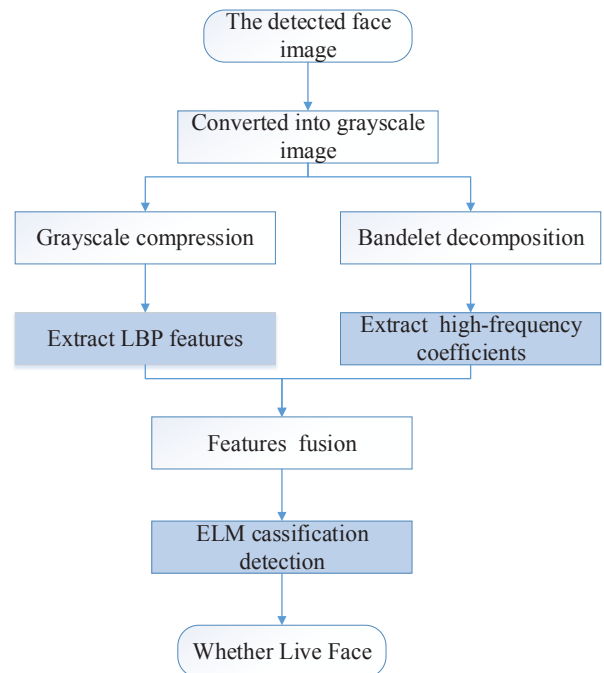


Figure IV. Flowchart of live face detection method based on LBP and Bandelet.

The process of getting statistical features of high-frequency coefficients in Bandelet transform is:

- 1) Input: grayscale image, quantization threshold T.
- 2) Conduct 2D wavelet transform on the image, orthogonal and biorthogonal wavelet transform can be used.
- 3) Establish quadtree segmentation for each sub band respectively, and get the best geometric flow directions of segmentation areas.
- 4) Conduct Bandelet transforms on each Bandelet area and get Bandelet coefficients.
- 5) Arrange Bandelet coefficients into matrix form according to a particular way.
- 6) Output: quadtree, the best geometric flow direction, Bandelet coefficients.

D. Extreme Learning Machine

We have conducted a statistical analysis and classification of the above two kinds of features. In this paper, basic ELM is adopted as the classifier. ELM, proposed by Guangbin Huang [24], is an algorithm to solve the single hidden layer neural networks. Under the condition of ensuring learning accuracy,

the most obvious feature of ELM is to run faster than traditional learning algorithms for the traditional neural networks, especially for single-hidden layer feed forward neural networks (SLFN). ELM is a new type of fast learning algorithm, for the single-hidden layer neural network, and it can initialize the input weights and bias randomly to get the corresponded output weights.

For a single hidden layer neural network (as shown in Fig. 3), assume that there are N random samples (X_i, t_i) , where $X_i = [x_{i,1}, x_{i,2}, \dots, w_{i,n}]^T \in R^n$, $t_i = [t_{i,1}, t_{i,2}, \dots, t_{i,m}]^T \in R^m$. n is the dimension of each feature vector X and m is the length of output vector t (m is 1 here because face detection is a binary classification problem, and t_i is 0 or 1). A single hidden layer

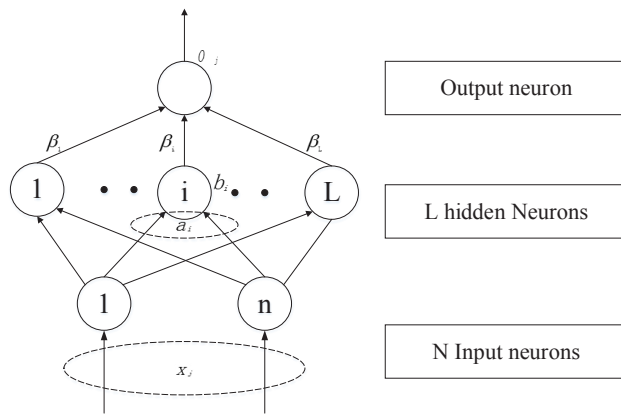


Figure V. SLFN: additive hidden nodes.

neural network with L hidden nodes can be expressed as:

$$\sum_{i=1}^L \beta_i g(W_i \cdot X_j + b_i) = O_j, j = 1, \dots, N, \quad (1)$$

in this formulation, $f(x)$ is active function, $W_i = [w_{i,1}, w_{i,2}, \dots, w_{i,n}]^T$ is the weight of the input, β_i is the weight of the output, b_i is the bias of the i th transient node. $W_i \cdot X_j$ represents the inner-product of W_i and X_j .

The target of Single layer neural network is to minimize the error of the output, which can be represented as

$$\sum_{j=1}^N \|o_j - t_j\| = 0, \quad (2)$$

there are some β_i, W_i and b_i that are qualified for

$$\sum_{i=1}^L \beta_i g(W_i \cdot X_j + b_i) = t_j, j = 1, \dots, N, \quad (3)$$

which can be represented by a matrix

$$H\beta = T, \quad (4)$$

where H is the output of the transient node, β is the weight of output, and T is the expected value of output.

$$H(W_1, \dots, W_L, b_1, \dots, b_L, X_1, \dots, X_L) = \begin{bmatrix} g(W_1 \cdot X_1 + b_1) & \dots & g(W_L \cdot X_1 + b_L) \\ \vdots & & \vdots \\ g(W_1 \cdot X_N + b_1) & \dots & g(W_L \cdot X_N + b_L) \end{bmatrix}_{N \times L} \quad (5)$$

$$\beta = \begin{bmatrix} \beta_1^T \\ \vdots \\ \beta_L^T \end{bmatrix}_{L \times m}, \quad T = \begin{bmatrix} T_1^T \\ \vdots \\ T_N^T \end{bmatrix}_{N \times m}$$

In order to train a single transient layer network, \hat{W}_i, \hat{b}_i and $\hat{\beta}_i$

$$\|H(\hat{W}_i, \hat{b}_i)\hat{\beta}_i - T\| = \min_{W_i, b_i, \beta_i} \|H((w_i, b_i)\beta) - T\| \quad (6)$$

where, $i = 1, \dots, L$. The inference process above can be summarized as the following minimize loss function.

$$E = \sum_{j=1}^N (\sum_{i=0}^L \beta_i g((W_i \cdot X_j + b_i) - t_j))^2 \quad (7)$$

Some traditional algorithms based on gradient descent methods can be used to solve this problem, but the basic learning algorithm based on gradient needs to adjust all the parameters in the process of iteration. As opposed to this, in the ELM algorithm, once the input weights and hidden layer bias are randomly determined, the output matrix H of hidden layer is only determined. Training a single hidden layer neural network can be transformed into solving a linear system and the output weights can be determined.

IV. EXPERIMENTAL RESULTS

In order to test the algorithm's ability to identify live faces and fake faces, we use the public face database CASIA_FASD, print-attack and replay attack to test.

A. Print-attack Dataset

The print-attack dataset contains a short video of valid access and spoof attacks to 50 different identities. The spoof attack that is emphasized in this dataset is print attack only, whereby an impostor presents a printed photograph of the targeted identity in order to falsify the access to a face biometric authentication system. This dataset includes two different scenarios: (i) controlled background (the background is uniform) and (ii) adverse background (a non-uniform background). These scenarios provide a valid simulation of the attack environment. Table II shows the number of video in the print-attack dataset.

Table II. Number of videos in the print-attack dataset

Type	Train	Develop	Test	Total
Real-access	60	60	80	200
Phone-attack	90+90	90+90	120+120	200+200
Table-attack	240	240	320	800

B. Replay-Attack Dataset

The replay-attack dataset consists of 200 videos of valid access (with 375 frames each), and 1000 videos of attack attempts (with 240 frames each). As shown in Table III, the dataset is divided into three partitions, namely development, training and testing set. The development set is used for estimating the threshold value and training set is used for estimating any model parameters.

Table III Number of videos in the replay-attack dataset

Type	Train	Develop	Test	Total
Live	60	60	80	200
Print-attack	30+30	30+30	40+40	100+100
Phone-attack	60+60	60+60	80+80	200+200
Table-attack	60+60	60+60	80+80	200+200
Table-attack	360	360	480	1200

Live face detection method based on local binary pattern and bandelet

Each of these sets is generated by a video gallery of 15 clients for development and training, and 20 clients for testing. This means that the training and testing sets are disjoint and completely independent of each other.

C. CASIA-FASD dataset

Compared to other live face detection databases, CASIA-FASD database contains more abundant real face and fake face sample types. As shown in Table IV, there were a total of 50 people registered in the database. Each registered person corresponded to 12 face video sequences, including three real face videos and nine fake face videos. Three real face videos were collected by a low-quality USB webcam, a high-quality USB webcam and a webcam of model Sony NEX-5 respectively.

All the videos in the database were collected in an uncontrolled environment, and the background areas were complex and changeable. In order to fully consider different ways of attack, fake face sample types were more abundant in the database. First, high-resolution images of each target face were displayed on different media, including common A4 printing papers, glossy photo papers, and a high-resolution display frequency. After that, the face eye area printed on A4 papers was removed to simulate the blink attack method. The database was divided into training set and testing set, where the training set is composed of 240 video sequences from 20 targets and the test set is composed of 360 video sequences from other 30 targets. Take the rest samples which never participated in the training as the test set and the image numbers of train set and test set are shown in Tab. 1. We took the remaining samples, which never participated in the training, as the test set. The details of the test set and the training set are shown in Table IV.

Table IV Face images of train set and test set in CASIA database

Quality	Size	Train data			
		Liveness face	Spoof face		
			Bend	Cut	Video
high	640×480	20	20	20	20
medium	480×640	20	20	20	20
low	920×1080	20	20	20	20
Total		60	60	60	60

Test data					
	Size	Liveness face	Spoof face		
			Bend	cut	video
		high	640×480	30	30
medium	480×640	30	30	30	30
low	920×1080	30	30	30	30
Total		90	90	90	90

In order to test the validity of the algorithm, this paper extracts LBP features of real and fake faces and wavelet features to classify and train ELM. Its detection accuracy is shown in Table V. This paper also adds the Bandelet features to LBP features and tests its detection accuracy for real and fake faces, as also shown in Table V.

From Table V, we can see that with the local binary pattern as the basic features, combined with Bandelet analysis, has an effect on the detection accuracy on CASIA dataset. It is noticed that using Bandelet analysis increases the feature dimension, which leads to improvement in the detection accuracy of the system significantly, from 93.87% to 97.97%; although the basic LBP features are easy to compute, its feature dimension 59 is greater than 12 under the analysis of LBP in comparison with Bandelet, which increases the system cost. The detection accuracy of LBP features which adds Bandelet analysis is 97.97%, and it is significantly greater than the detection accuracy of basic LBP features at 93.87%.

Table V. Comparison of LBP in combination with Bandelet features and other features

Samples	TP	TN	Detection accuracy	Feature dimensions
Basic LBP features	93.55%	94.06%	93.87%	59
Gray-level co-occurrence matrix	96.44%	91.13%	94.27%	8
All LBPV	91.84%	86.39%	88.03%	256
Uniform LBPV	88.13%	86.25%	86.95%	59
DoG (Curvature Driven Diffusions)			97.7%	512
LBP in combination with Bandelet	96.03%	95.88%	97.97%	12

Where TP denotes the detection accuracy of positive samples and TN denotes the detection accuracy of negative samples.

Compared with ALL LBPV and Uniform LBPV, LBP features under the analysis of Bandelet have obvious advantages. It reduces the feature dimensions and complexity of the algorithm, and at the same time it improves the detection accuracy. The detection accuracy of the proposed method declines, but the algorithm complexity reduces significantly compared with gray-level co-occurrence matrix and wavelet features. Therefore, reducing the algorithm complexity, while maintaining the detection accuracy, will be our future research focus.

Also, we compare the other method in Table V, Gray-level co-occurrence matrix and DOG methods has also been widely used in the extraction of image texture. Compared with the text algorithm, the size of DOG is too large and the computational complexity is large. Although the dimensions of co-occurrence gray matrix are small, the accuracy is not high.

Next, we compare the performance of LBP, Bandelet and Bandelet-LBP on three datasets. The images in Fig.8 show the ROC curves of Bandelet-LBP, LBP and Bandelet. The performance of proposed algorithm is better than the base LBP and Bandelet on three dataset. Figure VIa shows the overall performance when trained and tested on CASIA dataset. Figure VIb shows the overall performance when trained and tested on print-attack dataset. Figure VIc shows the performance on replay-attack dataset. In these three datasets, the Bandelet-LBP features perform the best, and our method is more robust on three datasets than LBP and Bandelet features.

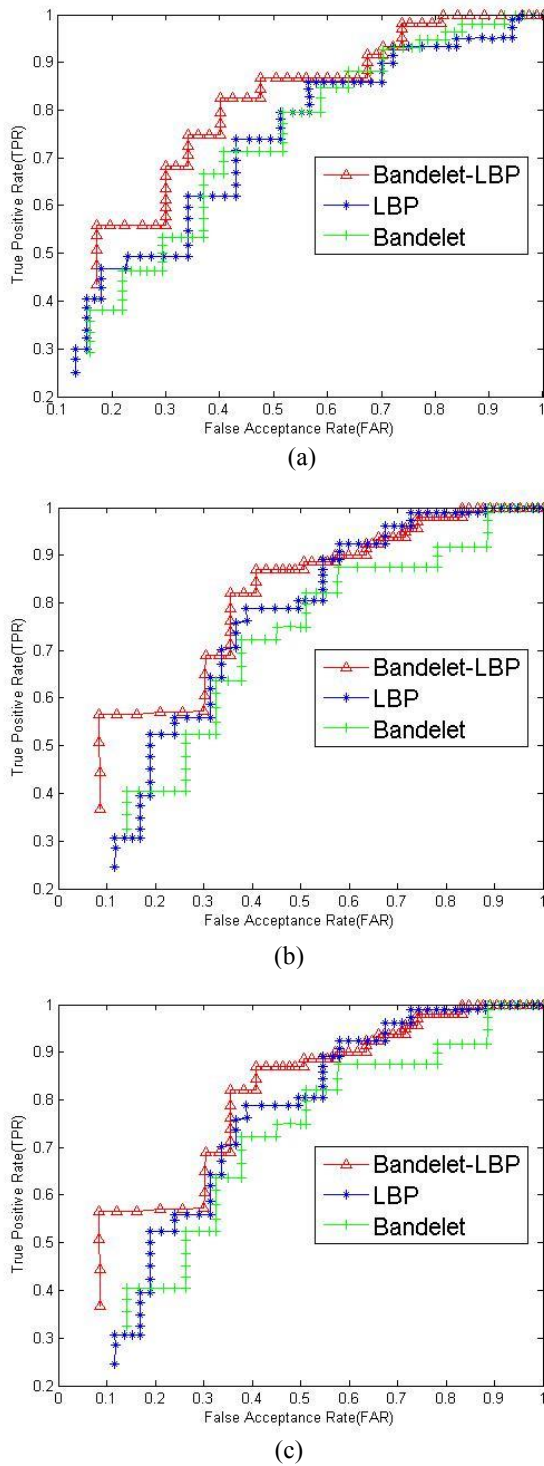


Figure VI Comparison of ROC curves of different algorithm on three datasets. (a) print-attack dataset (b) CASIA dataset (c) replay-attack dataset.

V. CONCLUSION

This paper proposed a live face detection method based on Bandelet analysis under the analysis of texture feature differences among live faces, photo faces, and video faces. This method conducts a Bandelet analysis on grayscale images of faces and extracts local binary pattern features based on the Bandelet

analysis. The feature of the image is obtained by divided into 100 blocks and set the weight value, which can enhance the important characteristics of the image and reduce the noise impact. Finally, the characteristics of the two algorithms are fused, and the learning and classification are entered into ELM. Experimental results show that the algorithm can reduce the computational complexity and improve the detection accuracy. But in practical applications, there are many interference factors to be considered, such as the influence of illumination condition and high-resolution cameras which are used to shoot face photos and videos. This will be in the focus of our future research.

REFERENCES

- [1] Z. Boulkenafet, J. Komulainen, A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis", *IEEE Transactions on Information Forensics and Security*, 2016, pp. 1818-1830.
- [2] W. Kim, S. Suh, J. Han, "Face Liveness Detection From a Single Image via Diffusion Speed Model" *IEEE Transaction on Image Processing*, 2015, pp. 2456-246.
- [3] D.F. Smith, A. William, B.C. Lovell. *Face Recognition on Consumer Devices: Reflections on Replay Attacks*. *Information Forensics and Security IEEE Transaction on*. 2015, pp. 736-745.
- [4] N. Erdogmus, S. Marcel, "Spoofing Face Recognition With 3D Masks". *IEEE transactions on information forensics and security*, 2014, pp. 1084-1097.
- [5] D. Gong, Z. Li, W.L. Huang, X.L. Li, D. Tao. *Heterogeneous Face Recognition: A Common Encoding Feature Discriminant Approach*. *IEEE Transaction on circuits and system for video technology*. 2017. pp. 2079-2089.
- [6] I. Kim, J. Ahn, D. Kim, *Face Spoofing Detection with Highlight Removal Effect and Distortions*. *IEEE International Conference on Systems*. 2016. pp. 1-6.
- [7] D. Wen, H. Han, A.K. Jain. *Face Spoof Detection With Image Distortion Analysis*. *IEEE Transaction on forensics and security*. 2015. pp. 746-761.
- [8] M. Uzair, A. Mahmood, A. Mian. *Hyperspectral Face Recognition With Spatiospectral Information Fusion and PLS Regression*. *IEEE Transactions on image processing*. 2015. pp. 1127-1137.
- [9] J. Galbally, S. Marcel, J. Fierrez, *Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition*, *IEEE Transactions on Image Processing*, 23 (2014) 710-724.
- [10] S. Karungaru, M. Fukumi, N. Akamatsu. *Face recognition in colour images using neural networks and genetic algorithms*. *International Journal of Computational Intelligence and Applications*, 2005, pp. 55-67.
- [11] S.R. Arashloo, J. Kittler, W. Christmas, *Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features*, *IEEE Transaction on information and security*, 2015, pp. 2396-2407.
- [12] G. Pan, L. Sun, Z. Wu, S. Lao, *Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Web camera*, in *IEEE International Conference on Computer Vision*, 2007, pp. 1-8.
- [13] Santosh T, Norman P, David W, et al. *Detection of Face Spoofing Using Visual Dynamics*. *IEEE Transaction on Information Forensics and Security*. 2015. pp. 762-777.
- [14] W. Yin, Y. Ming, L. Tian. *A face anti-spoofing method based on the optical flow field*. *2016 IEEE 13th International Conference on Signal Processing (ICSP)*. 2016. pp. 1333-1337.
- [15] A. Pinto, H. Pedrini, W.R. Schwartz, A. Rocha, *Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes*. 2015. pp. 4726-4740.
- [16] W. Paier, M. Ketterm, A. Hilsmann, P. Eisert, *A Hybrid Approach for Facial Performance Analysis and Editing*. *IEEE Transaction on circuits and system for video technology*. 2017. pp. 784-797.

Live face detection method based on local binary pattern and bandelet

[17] Z. Yu, G. Michael, B. Chris, C. Jun, X. Yong. Hybrid hierarchical clustering-piecewise aggregate approximation, with applications. *International Journal of Computational Intelligence and Applications*. 2016. p 165019(26 pp).

[18] N. Werghi, C. Tortorici, S. Berretti, A. D. Bimbo. Boosting 3D LBP-Based Face Recognition by Fusing Shape and Texture Descriptors on the Mesh. 2016. pp. 964-979.

[19] K. Patel, H. Han, A.K. Jain, Secure Face Unlock: Spoof Detection on Smartphones. *IEEE Transaction on information and security*. 2016. pp. 2268-2283.

[20] T.D.F. Pereira, J. Komulainen, A. Anjos, J.M.D. Martino, A. Hadid, M. Pietikäinen, S. Marcel, Face liveness detection using dynamic texture, *Eurasip Journal on Image & Video Processing*, 2014 (2014) 1-15.

[21] T. Edmunds, A. Caplier, Fake Face Detection Based on Radiometric Distortions. *IEEE Conference Publications*. 2016, pp, 1-6.

[22] Z. Akhtar, C. Micheloni and G. L. Foresti, "Biometric Liveness Detection: Challenges and Research Opportunities," in *IEEE Security & Privacy*, vol. 13, no. 5, pp. 63-72, Sept.-Oct. 2015.

[23] A. Lutz, K. Grace; N. Messer. Bandelet transformation based image registration. 2015 *IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*. 2015. pp. 1-6.

[24] L.L.C. Kasun, H. Zhou, G.B. Huang, and C.M.Vong, "Representational Learning with Extreme Learning Machine for Big Data", *IEEE Intelligent Systems*, 2013, pp. 31-34.



Haiqing LIU, acquired engineering PHD degree in Computer Application Technology from Wuhan University on December 2001. She went to WPI (Worcester Polytechnics Institute) in USA as a visiting scholar for 1 year since April 2004. She was employed as an associate professor and master’s supervisor by Wuhan University since October 2002, and transferred to Control and Computer Engineering Academy in NCEPU (North China Electric Power University) later in May 2005. She has been engaged in research

and development work related to Software Engineering, Database and Artificial Intelligence since 1988.



Shuhua HAO, master degree candidate in North China Electric Power University, Beijing, China. Her research interests include power system and spooling face recognition.



Yuancheng Li, received the Ph.D. degree from University of Science and Technology of China, Hefei, China, in 2003. From 2004 to 2005, he was a postdoctoral research fellow in the Digital Media Lab, Beihang University, Beijing, China. Since 2005, he has been with the North China Electric Power University, where he is a professor and the Dean of the Institute of Smart Grid and Information Security. From 2009 to 2010, he was a postdoctoral research fellow in the Cyber Security Lab, college

of information science and technology of Pennsylvania State University, Pennsylvania, USA.