Volume 8, No. 7, July – August 2017



International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

REAL TIME FACE LIVENESS DETECTION WITH IMAGE QUALITY AND TEXTURE PARAMETER

Ningthoujam Sunita Devi Department Of Computer Science Assam University Silchar, India Dr.K. Hemachandran Department Of Computer Science Assam University Silchar, India

Abstract: Face Biometric systems are vulnerable to spoofing attacks. The activeness of face recognition has raised concerns about face spoof attacks, where a printed photo or video of an authorized persons face could be used to gain access to facilities or service. Hence, we present a novel approach based on analyzing facial image quality and face image texture for detecting whether there is a live person or a fake person. The proposed approach analyzes the spoof face detection based on video and print out image. Two different feature are extracted (chromatic moment and Local Binary Pattern (LBP)) from the face image. Extracted feature are fed into Classifier, SVM classifier trained for different face spoof attack (i.e. printed photo and played video) is used to distinguish between real and fake face.

Keywords: Spoofing, Liveness Detection, Feature Extraction

1. INTRODUCTION

The digital face recognition technique has been a very active research area in the biometric system, for the last few decades and they are being widely used in applications like attendance monitoring and security systems. However, the conventional Face recognition system is not sufficient for security reason because it can't distinguish between 'live' and 'fake' faces. The drawback of face recognition is an easy way to spoof face recognition system by face printout image such as using portrait photographs. A secure system needs a liveness detection function in order to guard against spoofing. Liveness detection has been a widely used research topic in fingerprint recognition and iris recognition communities. So, the use of liveness detection in face recognition approaches will eliminate the drawback of identifying 'live' and 'fake' face during recognition process. Generally, liveness and non liveness detection for face recognition is performed according to the facial movement, the system is able to analyze face parts movement or facial expression, especially the movement of lips and eyes such as blinking to detect fake and real face [1], [2]. Tanzeem et.al.[3] have constructed a depth map by recovering 3D structure from motion and implemented a system that combines face recognition and speaker identification modules for person recognition. Jain et.al.[3] have evaluated a new integrated method for live face detection. It defined two descriptor i.e. high frequency descriptor and frequency dynamics descriptor to implement live face detector. High frequency descriptor is very effective to prevent in small size fake image. Frequency dynamics descriptor is more successful to discover a large size face image in front of a camera. Gang et.al [4] presented a real-time liveness detection approach against photograph spoofing in face recognition, by recognizing spontaneous eye blinks, in a nonintrusive manner. Anjos et.al. [5] Proposed a new technique of counter measure solely based on foreground/background motion correlation using optical

flow. Maatta et. al. [6] presented a novel approach based on analyzing facial image textures for detecting whether there is a live person in front of the camera or a face print by analyzing the texture of the facial images using multi-scale local binary patterns (LBP). Jang et.al [7] proposed a method consists of four steps: (1) locating the components of face; (2) coding the low-level feature respectively for all the components; (3) deriving the high-level face representation by pooling the codes with weights derived from fisher criterion; (4) concatenating the histogram from all components into a classifier for identification. It gives an appropriate performance of difference between genuine faces and fake faces. Li et.al. [3] Presented a structure and movement information of live face, an effective live face detection algorithm. This method is based on the analysis of Fourier spectra of a single face image or face image sequences. Libin et.al. [8] Proposed an approach to detect the face liveness by using the blurriness and investigating the focus distance between the face and the background. The focus distance should be the same for the photo or video, while the distance should be different for a real person.

In this paper, we present a real-time and non-intrusive method to address the spoofing attacks based on Image quality and texture analyses for discriminating fake face and the live faces generated from a generic webcam. For the Image quality analysis, we have carried out Chromatic moments based method [9] which exploits imperfect color rendering of printer or LCD screen; and color diversity distortion due to limited color resolution of printer or LCD screen. Moreover, widely used Local Binary Pattern (LBP) [9] based description method has been employed for analyzing the textures on the given facial images. In addition, the fused information of the decision values from the frequency based classifier and the texture based classifier has also been utilized for detecting the fake faces. Previous fake face detection methods which try to supplement only the face recognition systems dealt with 2-D paper masks generated by photo-printing on photographic

papers or conventionally printing on general printing papers. However, the proposed method expands its scope by considering both the face recognition and facial occlusion detection systems. Therefore, in the experiments, attacks made by using faces on the magazines or caricature images are also taken into account.





2. PROPOSED SYSTEM

The overall structure of the proposed liveness detection system is shown in figure 1. The proposed approach first detects the face and cropped and normalized into a 120 X 120 pixel image. Then the chromatic moment and Local Binary Pattern (LBP) of the normalized face image are extracted and are concatenated to make the feature vector to represent the face. Finally SVM will be used as a classifier to detect the liveness of the face image.

3. FACE DETECTION

Face detection is focus on the detection of frontal human faces from the image or video. It is analogues to object detection. For the present work, Viola Jones face detection algorithm has been used for detection of faces from the image as well as from the video. The Viola Jones face detection algorithm is fast and accurate approach used universally for detection of faces. This algorithm consists of Haar Features, Integral Image, Adaboost machine learning method and Cascading classifier[10].

$$\sum_{1 \leq i \leq N} \sum_{1 \leq j \leq N} I(i, j) \mathbf{1}_{p(i, j) \text{ white}} - \sum_{1 \leq i \leq N} \sum_{1 \leq j \leq N} I(i, j) \mathbf{1}_{p(i, j) \text{ black}}$$

The Variations in the black and white portion of the image are detected by using Haar like features. It is a scalar product between image and Haar like templates defined as:

Where, *I* and *P* denote the image and pattern of the same size $N \times N$. Before feature extraction, image is normalized with mean and variance to compensate the effect of different illumination. Typical Haar templates used in this algorithm are shown in Fig. 2.



Fig. 2 (a) Two rectangle Feature (b) Three rectangle feature and (c) Four rectangle feature. The Integral image is the outline of the pixels values in the original image. The integral image II of I defined holds for all $N_1 \le N_2 and N_3 \le N_4$.

$$\sum_{N1 \le i \le N2} \sum_{N3 \le j \le N4} I(i, j) = II(N_2, N_4) - II(N_2, N_3 - 1) - II(N_1 - 1, N_4) + II(N_1 - 1, N_3 - 1)$$

The integral image *II* defined as:

$$II(i, j) = \left\{ \sum_{0, 1 \le S \le i} \sum_{1 \le t \le j} I(s, t), 1 \le i \le N.and. 1 \le j \le N.and \right\}$$

The face region in the image is around the image center and manually marked with specified facial location with nose tip. A rectangle, bounding the face, is then generated according to the landmark position.

The Adaboost machine learning method facilitates the fast and easy computation by discarding undesirable background of the image. The Algorithm 1 describes the working of Adaboost machine learning method.

Algorithm 1:

Step 1: Given image is in the form (a_1, b_1) (a_n, b_n) Step 2: $b_1 = 0, 1$ for negative and positive examples. Step3: Initialize the weights x_1 , $i = \frac{1}{2m}, \frac{1}{2l}$ for $b_i = 0.1$ respectively, Where m and l are number of positive and negative respectively.

Step4: For t=1T:

1. Normalize the weights.

$$\mathbf{X}_{t,i} = \frac{x_{t,i}}{\sum_{f=1}^{n} x_{t,i}}$$

X_t is the probability distribution

2. For each feature j, train a classifier y_j which is restricted to use a single feature. The error is evaluated with respected to

 $\mathbf{x}_{t}, \mathbf{E}_{t} = \sum_{i} x_{i} |\mathbf{y}_{j}(\mathbf{a}_{i}), \mathbf{b}_{i}|$ (1)

- 3. Choose the classifier y_t with lowest error E_t
- 4. Update the weights $x_t + l.i = x_{t-i} B_t^{1-ei}$ Where $e_i=0$ if a_i is classified correctly, $e_i=1$ otherwise and $B_t = \frac{et}{1-et}$
- 5. The final strong classifier is x(a) = 1

$$\sum_{t=1}^{T} 1l_t \ x_t(a) \ge \frac{1}{2} \sum_{t=1}^{T} l_t \tag{2}$$

Where
$$l_t = \log \frac{1}{B^2}$$

The Viola Jones algorithm has cascade of stages to detect the face as shown in fig.3. The candidate face is detected if it passes conditions of all stages of classifier



Fig. 3 Cascading stages of Viola Jones Algorithm.

4. FEATURE EXTRACTION

The chromatic moment and Local Binary pattern is used as a feature extraction technique to extract the unique face feature. Due to its good strength in low computational complexity and measurement, Local Binary Pattern (LBP) has been choose for invariant to monotic changes in gray scale, which makes it robust against illumination changes and computationally very fast. Based on these feature extractions, efficient and rather robust face spoof detection is achieved.

a) CHROMATIC MOMENT

The facial images which are recaptured may show a different color distribution when compared with the color of genuine face images. This difference is due to the imperfect color distribution property of printing and display media. This chromatic degradation was explored in [11] for detecting the recaptured images, but its effectiveness in spoof face detection is unknown. Since the absolute color distribution is dependent on illumination and camera variations, it is proposed to devise an invariant feature to detect abnormal chromaticity in spoofed faces. That is, we first convert the normalized facial image from the RGB space into the HSV (Hue, Saturation, and Value) space and then compute the mean, deviation, and skewness of each channel as a chromatic feature. Since these three features are equivalent to the three statistical moments in each channel, they are also referred to as chromatic moment features. Besides these three features, the percentages of pixel in the minimal and maximal histogram bins of each channel are used as two additional features.

Ningthoujam Sunita Devi et al, International Journal of Advanced Research in Computer Science, 8 (7), July-August 2017,730-735



Fig .4 represent the chromatic moments difference between real and fake faces. (a) and (b) show the Hue, Saturation, and value components for real and fake images with their histogram. The abnormality of the histogram for the spoof face can be measured by the three chromatic moments.

b) Local Binary Pattern

The Local binary pattern (LBP) texture analysis operator, developed by Ojala et al. [9] is defined as a gray-scale invariant texture measure, derived from a general definition of texture in a local neighborhood. It is a powerful means of texture description and among its properties in real-world applications are its discriminative power, computational simplicity, and tolerance against monotonic gray-scale changes. The operator worked with the 3 X 3 neighbors of a pixel, using the value of the center pixel as a threshold.



Fig 5. The Basic Calculation of LBP operator

The LBP operator was extended to use neighborhood of different sizes and deal with textures at different scales. Defining the local neighborhoods as a set of sampling points evenly spaced on a circle centered at the pixel to be labeled allows any radius and number of sampling points. By circular neighborhood and bilinear interpolating values at non-integer pixel coordinates allow any radius and number of pixels in the neighborhood [6]. The following notation (P,R) is used for pixel neighborhood to refer to P sampling point on a circle of radius R as shown in Figures, shows an example of a circular neighborhood.

$$LBP_{P,R} = \sum_{P=0}^{P-1} s(g_P - g_C) 2^P$$

Where g_P and g_C denote gray levels of centered pixel and its neighbor respectively, P is the number of neighbors pixel; R is the radius of the circular neighbor set. Below Figure describes on how to employ the neighboring pixels regarding the P and R. The use of various values for P and R enabled the analysis of the multiresolution texture. This work utilized the uniform LBP, and P and R were set to 8 and 1, respectively.



Fig 6 The circular (8, 1), (8, 2) and (16, 2) neighborhoods. The pixel values are bilinear interpolated whenever the sampling point is not in the center of a pixel.







Fig 7: Feature vector extraction process based on LBP (a) original facial image (b) LBP-coded images (c) histogram of the LBP-coded image.

The process of acquiring the LBP feature vector from a given facial image is shown in fig. 7. The Figure. 4(a) is the original facial image, (b) shows the LBP-coded images (c) shows the exploited feature vector for the classification.

5. LIVENESS DETECTION SCORE

A nonlinear Support Vector Machine (SVM) with radial basis function kernel is used to determine whether the input face image corresponds to a live or fake face. The SVM classifier is trained using a set of positive (Live faces) and negative (Fake faces) samples. Chromatic moment and LBP are used for features extraction of input face image and extracted features are fed into the trained SVM and recognize the input image as live face and in the case of opposite, it is discriminated to the Fake Face based on the threshold value, (*th*).

6. EXPERIMENTAL RESULT

The experiments are carried out on windows 8 operating system with Intel core i3 3110M processors and 4GB RAM by using MATLAB 7.0 software. We evaluate the proposed face liveness detection model using CASIA FASD and NUAA databases, for the experiments. The details of the databases considered for experiments are tabulated in Table 1. The chromatic moments and Local Binary Pattern (LBP) features are concatenated to make the feature vector of the image.

 Table 1. The number of persons and the images per person from each dataset

CASIA			
Total Image	170		
	Traning	53	
	Testing	117	
	Real	Print	Mobile
	43	51	23
NUAA			
Total Image	9371		
	Training	3312	
	Testing	6059	
	Real	Imposter	
	3362	2697	

In this work, The False Accept Rate (FAR) and False Reject Rate (FRR) of the proposed recognition approach were computed to determine the threshold value (*th*) for liveness detection. Also the Receiver operating characteristic (ROC) and accuracy of the system were presented as an assessment of the proposed liveness detection approach. The performance of the proposed liveness detection approach of CASIA and NUAA databases is shown in table 2.

Table 2:	FAR,	FRR,	and	accuracy	at	different	threshold
value.							

Name	CASIA Database				
Database					Accuracy
	Real	Prin	t	Mobile	Accuracy
	Image	Imag	ge	Image	
	96%	90%		91%	97.39%
Name	NUAA Database				
Database					Accuracy
	Real		Im	poster	Accuracy
	98.8%		100)	99.95%

From table 2 it is observed that, the system achieved the recognition accuracy of 97.39% and 99.95% by using the CASIA and NUAA face databases respectively. The Accuracy is calculated as:

$$Accuracy = (1 - \frac{FAR + FRR}{2}) \times 100$$

The figure 5 represents the ROC curve of the proposed approach. The curve is drawn between False Accept Rate (FAR) vs True Accept Rate (TAR)(TAR=100-FRR) at different threshold value (*th*). The performance of the proposed approach show that it is suitable for the liveness detection system.





Fig 8: The ROC curve of the database (a) Casia Database (b) NUAA Database for the proposed system.

7. COMPARISON TO TEXTURE APPROACH

To evaluate the proposed liveness detection approach, the performance of the proposed approach compared with the performance of the Andre et.al [6]. The results are shown in Table 3. It is observed from table 3 that the proposed approach out performs existing approach in terms of liveness detection accuracy. The advantage of the proposed system is that it can detect spoof attack using video as well as photo.

 Table 3: Compared the proposed system with the existing system

	Accuracy	
Andre et.al	CASIA database	94.8%
[6]	NUAA database	96.7%
The proposed	CASIA database	97.39%
system	NUAA database	99.95%

8. CONCLUSION

In the present work, real time face liveness detection method based on image quality and texture parameters has been proposed. In order to employ the difference in image quality and texture in live and fake face images, image quality and texture information are exploited by using chromatic moments and Local Binary Pattern (LBP) respectively. The SVM has been used as a classifier. Experimental results show that the proposed method can efficiently classify the real and fake faces of the considered database. The system achieved the liveness detection accuracy 97.39% and 99.95% with CASIA and NUAA databases respectively. The ROC curves also demonstrate the efficacy of the proposed approach of liveness detection.

REFERENCE

- L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-Based Live Face Detection Using Conditional Random Fields," Adv. Biometrics, pp. 252–260, 2007.
- [2] H.-K. Jee, S.-U. Jung, and J.-H. Yoo, "Liveness detection for embedded face recognition system," Int. J. Biomed. Sci., vol. 1, no. 4, pp. 235–238, 2006.
- [3] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," Def. Secur., vol. 5404, pp. 296–303, 2004.
- [4] G. Pan et al., "Eyeblink-based Anti-Spoo ng in Face Recognition from a Generic Webcamera," 11th IEEE ICCV, Rio Janeiro, Brazil, Oct., vol. 14, p. 20, 2007.
- [5] M. M. Chakka, A. Anjos, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, 2014.
- [6] M. anda andtta , J., A. Hadid, and M. Pietika andinen, "Face spoofing detection from single images using texture and local shape analysis," Biometrics, IET, vol. 1, no. 1, pp. 3–10, 2012.
- [7] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," Proc. - 2013 Int. Conf. Biometrics, ICB 2013, 2013.
- [8] F. L. Detection and F. Faces, "Face Liveness Detection By Focusing on Frontal Faces and Image Backgrounds," pp. 13– 16, 2014.
- [9] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 971–987, 2002.
- [10] M. Chaudhari, S. Shanta, and G. Vanjare, "A review on Face Detection and study of Viola Jones method," Int. J. Comput. Trends Technol., vol. 25, no. 1, pp. 54–61, 2015.
- [11] Chen, Yuanhao, et al. "Automatic classification of photographs and graphics." Multimedia and Expo, 2006 IEEE International Conference on. IEEE, 2006.