IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A Review: Face Liveness Detection

Dhananjay Garud[1], Dr. S.S. Agrawal[2]

ME Student, Signal Processing (E&TC), SKN COE, Pune, India[1]

Assistant Professor, E&TC, SKN COE, Pune, India[2]

Abstract: In order to develop security systems for identity authentication, face recognition (FR) technology has been applied. One of the main problems of applying FR technology is that the systems are especially vulnerable to attacks with spoofing faces. To defend from these attacks and to enhance the reliability of FR systems, many anti-spoofing approaches have been recently developed. A secure system needs Liveness Detection in order to guard against such spoofing. In this paper various face liveness detection methods are discussed which are used to avoid these attacks. This helps to create a robust and accurate system to avoid spoofing attacks. The main aim of this work is to give a simple for future generation for more secured liveness detection approach.

Keywords: Biometric technology, Face Recognition, Face Liveness Detection, Spoofing Attack.

I. INTRODUCTION

With latest technology, for security purposes various methods are developed for industrial security. Some known methods for identification are face recognition. Hand-writing verification. Hand geometry, retinal, finger print recognition and iris scanner. Compared to other techniques face recognition is simple, user friendly and easier for detection than other methods. So face detection is widely used in industries for identification. As FR system only identifies a user it unable to identify a live person or a fake person i.e. face recognition system can easily spoofed by using photos, videos or masks.

So for securing face recognition system face liveness detection is key technique which can easily avoids spoofing attack. Liveness is nothing but differentiating the feature space into live and non-live face. Attackers try number of spoofs in the biometric system. Liveness detection makes face recognition system more secure that improve the performance of system. It is challenging task for FR system to find real and fake face against the spoofing attack.

Classification of attack is based on what verification proof is used, such as photo, recorded video or 3-D face module with abilities of eye blinking, lip movement and various facial expressions and so on. Liveness detection for face recognition system based various methods as, motion based, frequency spectrum based or quality based. Various methods are used for face liveness detection.

In the next section, a review of the most interesting face liveness detection methods is presented. Then, a discussion is presented citing the advantages and disadvantages of various face liveness detection approaches. Finally, a conclusion is drawn.

II. LITERATURE SURVEY

There are many approaches implemented in Face Liveness Detection.

In this section, some of the most interesting liveness detection methods are presented.

A. Using Eye Blinking

Gang Pan et al.[1] presented a real-time liveness detection approach against photograph spoofing in face recognition, by recognizing spontaneous eyeblinks, which is a non-intrusive manner. Eye blinking is very complex structure to understand. The goal of this face liveness detection method is to resist the spoofing attack in non-intrusive manner without any external hardware except a generic camera. Physiological activity of eye blink is to instantaneously close and open eye lids, it helps to spread the tears across and removes irritants from surface. Normally blinking rate of human being is around 15 to 30 eyeblinks per minute, that is human blinks once after every 2 to 3 seconds and blink time is about 205 millisecond's. So generic camera can easily capture face video with more than 15 frames per second, so interval between frames is not more than 70 milliseconds. Then camera can capture two or more frames at the time of face in looking in camera. It makes a clue to use eyeblinking to use against face spoofing.

Images are captured by digital camera are represented as temporal sequence of images which are independent on state of previous image but blinking is opening and closing of lids which is dependent process. For this method author assumes that sequence in independent which is helpful for recognition. HMM produces observations to produce joint probability tractably assuming that there is an underlying sequence of states drawn from a finite state set. Features of images can be regarded as the observations, and the eye state label is for the underlying states. HMM makes two independence assumptions to model the joint probability tractably. It assumes that each state depends only on its immediate predecessor, and that each observation variable depends only on the current state.

An eyeblink activity can be represented by an image sequence S consisting of T images, where S = {I ,i =1,...,T}. The typical eye states are *opening* and *closing*. In addition, there is an ambiguous state when blinking from open state to close or from close state to open. We

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

define a three-state set for eyes, Q = {a : open, γ : close, ß : ambiguous}. Thus, a typical blink activity can be described as a state change pattern of

$$a \rightarrow ß \rightarrow \gamma \rightarrow ß \rightarrow a.$$

B. Using Motion Based Counter

Anjos et al.[2] propose a new technique of counter-measure solely based on foreground/background motion correlation using optical flow.

Proposed algorithm is based on similar principles as those established in head rotation using optical flow field. It tries to detect motion correlations between the head of the user trying to authenticate and the background of the scene, which indicates the presence of a spoofing attack. Instead of working with averaged intensities as in it, proposed method uses fine-grained motion direction for deriving the correlation between these two regions.

The direction of objects in the scene is estimated using OF techniques. The use of OF is expected to grant more precise estimation of motion parameters between the regions of interest in the scene, assuring that motion cues are related in direction and do not come from unrelated phenomena, as it could happen in RS3. Instead of lump-summing intensities, OFC quantizes, histograms, normalizes and directly compares motion direction vectors from the two regions of interest in order to provide a correlation score, for every analyzed frame.

The feature extraction has four steps, The input consists of the OF horizontal and vertical velocity estimates, but also uses the face bounding boxes available in the database to separate features from the face and background regions.

From those inputs, the algorithm performs the following steps:

1. First compute the direction θ of motion for every pixel using the horizontal and vertical orientations according to a simple Cartesian to polar coordinate transformation.
2. The histogram computation unit calculates the normalized histograms for face and background regions solely based on the quantised angle for every flow field frame.
3. The next block in the feature extraction computes the χ^2 distance, between the angle histograms of face and background regions.
4. The windowing unit averages the $\chi 2$ scores over a window size of N frames, with a possible specified overlap size (also in number of frames).

The scores computed from the windowing unit are fed to the binary classifier, which detects the spoofing attacks based on a threshold on the EER tuned at the development set.

Newly introduced method requires the estimation of OF fields or other direction-oriented features on the target images, but can dramatically improve the accuracy of spoofing detectors.

Specifically, they attempted to detect motion correlations between the head of the user and the background that indicate a spoofing attack. Although these approaches are conceptually simple, multiple frames are required to track face components, which leads to an increase in the detection time, and highly cooperative user actions are also required.

C. Based on Extraction of Micro-texture

Maatta *et al.* [3] attempted to extract micro textures by using the multiscale local binary patterns (LBP), which are frequently treated as a liveness clue. Inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection, they propose to approach the problem of spoofing detection from texture analysis point of view. Indeed, face prints usually contain printing quality defects that can be well detected using texture features. Hence, this method presents 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. The proposed approach analyzes the texture of the facial images using multi-scale local binary patterns (LBP). Compared to many previous works, proposed approach is robust, computationally fast and does not require user-cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition. Extensive experimental analysis on a publicly available database showed excellent results compared to existing works.

D. Based on Analysis of Fourier Spectra

Wang et.al.[5] presented an effective live face detection algorithm is presented based on the analysis of Fourier spectra of a single face image or face image sequences. Fake faces includes screen of video device, photo, paper and so on, their structure is very different from live face. As all this media are have 2-D structure while live faces have 3-D structure. According to Lambertian model[6], the face image can be described as

$$I(x,y) = \rho(x,y)n(x,y)^T s \qquad (1)$$

Where, ρ is the albedo (surface texture) of face, $n(x,y)^T$ is the surface normal (3D shape) of the object (the same for all objects of the class), and s is the point source, which can vary arbitrarily. Due to 2-D planar structure of photograph $n(x,y)^T$ is a constant. So for same illumination conditions, live ness can be determined by the albedo and surface normal and only albedo is enough for fake face. Such differences lead to their difference in reflectivity of light, with which frequency distribution of an image changes. Which results in, the size of fake image is usually smaller than that of live face. If fake faces are held before the camera, many details of image may loss. This all brings a great difference between live face and fake face image by using 2D Fourier spectra.

Fourier spectra of live face image has much less high frequency components than spectra of fake face image as shown in fig1.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

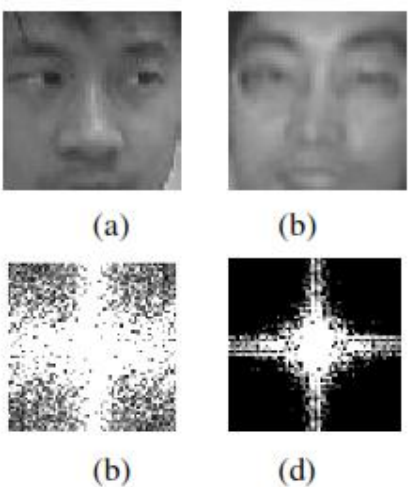

Figure 1. Difference between live face and fake face in frequency domain: (a) A live face image; (b) A fake face image; (c) 2D Fourier spectra of (a); (d) 2D Fourier spectra of (b).

E. Using Component Descriptor

Yang et al [4]. extracted micro textures in the regions of face components, e.g., eyes and nose. They propose a component-based face coding approach for liveness detection. The proposed method consists of four steps: (1) locating the components of face; (2) coding the low-level features 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 histograms from all components into a classifier for identification. The proposed framework makes good use of micro differences between genuine faces and fake faces. Meanwhile, the inherent appearance differences among different components are retained.

F. Face Liveness Detection By Focusing on Frontal Faces and Image Backgrounds

Libin Yang [7] observes an images with focusing on nose and background are different from images with focus on nose and ear. Blurriness increase by focusing on ear and background on user as compared with focusing on ear and nose, this difference gives accurate and robust method for face liveness detection.

Sum Modified Laplacian (SML) [8] is a common measurement for focus effects. SML measures the distance between any objects and the focused plane. SML computed using second derivative in x and y directions and using modified Laplacian as shown in equations,

$$\mathrm{ML}(x,y) = \left|\frac{\partial^2 I}{\partial x^2}\right| + \left|\frac{\partial^2 I}{\partial y^2}\right| \quad (2)$$

For computation of partial derivatives

$$ML(x,y) = |2I(x,y) - I(x-step,y) - I(x+step,y)| + |2I(x,y) - I(x,y-step) - I(x,y+step)| \quad (3)$$

$$SML(x,y) = \sum_{x=i-N}^{x=i+N}\sum_{y=j-N}^{y=j+N} \begin{matrix} ML(x,y) \\ For\ ML(x,y) > T \end{matrix} \quad (4)$$

Since, T is predefined threshold point.

In this method the blurriness difference between the frontal faces and the image backgrounds will be compared twice. First, take two consecutive photos for a user. One is focused on the nose and the other is focused on the image background. If the face is real, it is obvious that the frontal face is clearer than the background when focusing on the nose. Likewise, the background will be clearer when focusing on the background. While for fake faces, displayed by tablet or photo, face may be little clearer than the background because there may be focusing effects of tablet or photo quality.

After taking the images, separate the face and the background from the image and apply Local SMQT Features and Split up Snow Classifier [9] to extract a human face from a recaptured image. After extraction SML for every point of frontal face is compute and find the average SML value for frontal face. Similarly for background find average SML value for both left and right side using same method. Then find the difference between average value of SML between frontal face and background. For each user we get two difference values as focus on nose and background. Difference value for focus on nose should positive and close to zero for a real and fake face respectively and difference value for focus on background should be negative and close to zero for real and fake face respectively.

Table 1 Advantages and Disadvantages of liveness detection approaches

Liveness Indicator / Clue	Advantages	Disadvantages
Texture	Easy to implement No need of user collaboration	Images with low texture information Dataset must be diverse.
Motion	Independent of texture Hard to spoof by 2D image No need of user collaboration	Needs video Difficult to use when video has low motion activity Can be spoofed by 3D mask.
Life Sign	Difficult to spoof using 2D image or 3D mask. Independent of texture	user collaboration needed Depends on face part detection

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5183

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

III. CONCLUSION

Here, liveness detection approaches are categorized based on the type of liveness indicator used to assist the liveness detection of faces. Three main types of indicators were mainly used: motion, texture and life sign. This work helps to generate robust and highly secure liveness detection method. Discussed methods are based on motion, texture and life sign of user which is used for face liveness detection and discussed some advantages and disadvantages which makes easy to select method of working for future work.

REFERENCES

[1] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[2] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014.

[3] J. Maatta, A.Hadid, M.Pietikainen, Face Spoofing Detection From Single images Using MicroTexture Analysis, Proc. Intn Joint Conference on Biometrics,2011, Washington, D.C., USA.

[4] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IEEE Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.

[5] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identificat., pp. 296–303, Aug. 2004.

[6] R.Basri, D.W. Jacobs, "Lambertian Reflectance and Linear Subspaces", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(2): 218 – 233

[7] Libin Yang, "Face Liveness Detection by Focusing on Frontal Faces and Image Backgrounds", Proceedings of the 2014 International Conference on Wavelet Analysis and Pattern Recognition, Lanzhou, 13-16 July, 2014

[8] Nayar, Shree K., and Yasuo Nakagawa. "Shape from focus." Pattern analysis and machine intelligence, IEEE Transactions on 16, no. 8 (1994): 824-831.

[9] QU, Xiao-bo, Jing-wen YAN, and Gui-de YANG. "Sum-modified-Iaplacian-based multifocus image fusion method in cycle spinning sharp frequency localized contourlet transform domain." Optics and Precision Engineering 13, no. 2 (2005)

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5183