Spoofing Face Detection based on Spatial and Temporal Features Analysis

Chin-Lun Lai*, Jun-Horng Chen
Communication Engineering Department
Oriental Institute of Technology
New Taipei City, Taiwan
{fo001, jhchen}@mail.oit.edu.tw

Jing-Ying Hsu, Chih-Hong Chu
Advanced Technology Center, DBG
Wistron Corporation
New Taipei City, Taiwan
{Jingying_Hsu, Markov_Chu}@wistron.com

***Abstract*—In this paper, an intuitive spoofing face detection method is proposed to increase the reliability of face recognition systems. Via the simple spatial-temporal spectral analysis and border edge detection, people with fake face as the recognition system input will be pick out efficiently and effectively. Experimental results show that the proposed method is competitive and practical to be implemented in the portable equipments with face recognition function to improve the system reliability.**

Keywords—spoofing face detection; spatial-temporal analysis; smart TV; portable devices

I. INTRODUCTION

Face recognition technology had been rapidly developed and widely used in various fields these years [1] as ID retrieval or security control. Although the performance of face recognition systems is quite satisfactory and are convenient for most applications, some well known problems should be addressed and solved first for the practical systems. Spoofing face attack is one of the serious problems which decrease the reliability of a face recognition system. Thus, to protect the authentication process, face recognition systems must be able to reject the use of a copy version instead of the live face. This function, overall, is called liveness or spoofing face detection [2]. Face spoofing can be mainly classified into three types: 2D static paper mask, pre-recorded video, and 3D face models with abilities of eye blinking, lip moving, and face expressions [3]. Among these cheating methods, 2D mask with static photos or displayed videos are the easiest to be used than 3D models thus relevant researches are developed to resist such attacks [4-6]. Although there exist high reliability exploring devices to verify a live face such as ultra-violet cameras, thermal-imaging cameras, stereo cameras and so on, a single and simple camera is preferred due to the cost consideration.

In this paper, a life face detection method is proposed to against the face spoofing by flat photos and videos. The proposed algorithm is based on analyzing the spatial and temporal features around the detected face region (DFR). By observing that there exists distribution difference of lighting between the live faces and displayed masks due to optical influence, a simple but is efficient and affective analyzing methodology is used to analyze the distribution variation from spatial-temporal domain thus to tell fake faces from the real ones.

This paper is organized as follows. In next section, the proposed spoofing face detection method is described. Section III gives the experimental results and discussions, while the conclusion is presented in the last section.

II. PROPOSED SPOOFING FACE DETECTION METHOD

The flowchart of the proposed spoofing face detection method is shown in Fig. 1 and is described in detailed as follows.

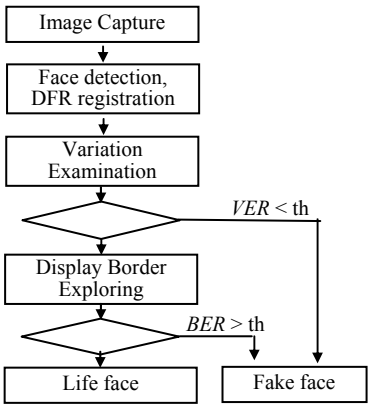

Fig. 1. The flowchart of the proposed spoofing detection system

A. Face detection and region registration

First, a face detection function should be applied to pick out the face candidate for post processing. Although there exist various face detection algorithms, popular learning machine like Adaboost structure is often adopted due to its high efficiency, accuracy, and less limitations. Once a face is targeted, the DFR corresponding to that face should be registered for further analysis. The DFR can be defined as

$$DFR(x,y,t)=\begin{Bmatrix}1,\ x\in x_c\pm\Delta x, y\in y_c\pm\Delta y, t\le t+\Delta t\\ 0,\ \text{others}\end{Bmatrix} \quad (1)$$

where (x_c, y_c) is the center of the candidate face block, Δx, Δy are the width and height ration of face block respectively, while Δt represents the observing time interval. Once the DFR cube is obtained, it is used in the consecutive analysis process.

B. *Variations examination on spatial-temporal domain*

A significant clue for distinguishing a live face from fake is the gray value distribution variation on spatial temporal domain. Due to the image difference in a certain time interval for a live face, it is easy to tell static masks (photo or picture mask) from a live one. The variance energy ratio (*VER*) in the DFR can be used to exam the lifeness and is defined as

$$VER = \frac{\sum R_d(x,y)}{\sum_{x,y} R_{eye}(x,y)} \tag{2}$$

where R_{eye} denotes the region of detected eyes, while R_d represent the corresponding pixels in R_{eye} which with difference during the time interval. If *VER* is less than a given threshold than a fake face is said to be found.

C. *Display boarder exploring*

Observing that no matter the fake face is presented by a picture, photo, or videos, the discontinuity phenomenon exists between the foreground face region and background scene. Therefore, the flat mask can be easily detected by line segment detection on spatial domain. Pixels in DFR are undergone the edge operation first and the corresponding result is passed to a line detection operation. After that, the border energy is calculated to determine whether a potential display exists or not. The border energy ratio (*BER*) can be defined as

$$BER = \frac{\sum_i L_i(x,y)}{\sum_{x,y} B_D(x,y)} \tag{3}$$

where B_D denotes the border of the DFR, L_i denotes the vertical and horizontal line segment i which locate in DFR but outside the detected face block. If *BER* is greater than a given threshold than an obvious display border is said to be found.

III. Experimental Results and Discussions

Since there is no public database for live face detection, several faces under different conditions are constructed to evaluate the proposed algorithm. These conditions include static face picture/photo with both simple and complex background, as well as pre-recorded face videos under simple and complex background. Related parameters are described as follows. The photo is printed out to A4 size. The pre-recorded face videos is 640*480 and is displayed by IPAD. The webcam resolution is 2M pixels and the test platform is a PC with I5 core. The Δt is set as 10 successive frames at 10 frames/s capturing rate, while Δx and Δy are set to be 150%. The threshold value of *VER* and *BER* are set to be 0.3.

Up to now, 20 test samples including photos, pictures, and recorded videos are used for system evaluation. The test result of live face is shown in Table 1 and some examples of the experimental results are shown in Fig. 2. It is observed that no matter the fake face is shown by photo or video, the spoofing attack can be detected successfully.

IV. Conclusions

This paper presents an intuitive method to against the spoofing face attack. By simply analyzing the spatial-temporal content of DFR, static face photos as well as dynamic face videos can be efficiently selected out from a live face. Experimental results show that the proposed method is effective and practical. In future research work we will deal with the spoofing attack by 3D models with moving eyes, lip, and facial expressions.

Acknowledgment

This research was supported by Advanced Technology Center of Wistron Corporation, Taipei, Taiwan.

TABLE I. Liveness Test Results

	Displayed Types		
	video	***picture***	***photo***
Test No.	10	4	6
Fail No.	1	0	0
FAR	0.05		

Fig. 2. Examples of live face test results. first row: printed face photo; second row: face video in iPAD, with different background.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar. "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp.4-20, 2004.

[2] Schuckers, Stephanie AC., "Spoofing and anti-spoofing measures," *Information Security Technical Report*, vol. 7, no. 4, pp. 56-62, 2002.

[3] Li, Jiangwei, et al. "Live face detection based on the analysis of fourier spectra." *Defense and Security*, *International Society for Optics and Photonics,* pp. 296-303, 2004.

[4] Ng, Ee-Sin, and Alex Yong-Sang Chia. "Face verification using temporal affective cues." *IEEE 21st International Conference on Pattern Recognition (ICPR),* 2012.

[5] Pinto, Allan da Silva, et al. "Video-Based Face Spoofing Detection through Visual Rhythm Analysis." *IEEE 25th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI),* 2012.

[6] Määttä, J., A. Hadid, and M. Pietikäinen. "Face spoofing detection from single images using texture and local shape analysis." *Biometrics*, IET 1.1, pp.3-10, 2012.