LIVENESS DETECTION USING FREQUENCY ENTROPY OF IMAGE SEQUENCES

Ting-Wei Lee, Gwo-Hwa Ju, Heng-Sung Liu, Yu-Shan Wu

Computer Vision Group, Business Customer Solutions Lab., Chunghwa Telecommunication Laboratories
No. 99, Dianyan Rd., Yangmei City, Taoyuan County 32601, Taiwan (R.O.C.)
E-mail: {finas, jgh, lhs306, yushanwu}@cht.com.tw

ABSTRACT

Spoofing attack (or copy attack) is a fatal threat for biometric authentication systems. In this paper, we present a novel liveness detection method based on frequency entropy of image sequences against the photograph spoofing. By splitting the color video of face region into RGB channels, we can obtain the time sequences of each color channel. Then, three RGB sequences are analyzed through Independent Component Analysis (ICA) algorithm to eliminate the cross-channel image noises. Moreover, the Fast Fourier Transform (FFT) is further applied to these signals to get the power spectra of each RGB channels. Finally, the power spectra are verified through the entropy calculation to validate the liveness or photo attack. The experimental results demonstrate the superiority of the proposed method, which has an accuracy of more than 95%.

Index Terms— Liveness detection, entropy

1. INTRODUCTION

Some biometric features, such as fingerprints or face images, could be used in liveness detection. The work by Shankar Bhausaheb Nikam *et al* [1] detected spoof fingerprint attacks in fingerprint biometric systems by using various classifiers and voting rule. In face biometric systems, Zhiwei Zhang et al [2] also trained a Genuine-or-Fake face classifier previously to distinguish a live face or a photograph. Another derivative application of face image is detecting eye-blink, like Gang Pan *et al* [3]; they considered that the participant was alive if he blinked, but the success of eye-blink technology highly depended on the accuracy in locating eye region. The work presented here improves the defects in the previous studies. We did not need training classifier previously. In addition, since it was hard to locate the eyes area accurately, the proposed method uses the whole face image to identify a live face or a photograph.

Another biometric feature for liveness detection is physiological signal. T. Kathikeyan *et al* [4] proposed an integrated system using IRIS and Electroencephalogram biometric with Liveness detection. But the EEG recognition may cause discomfort because the participants have to wear medical equipment on their heads to collect the verification data. Moreover, a useful physiological signal is heart pulse to prevent spoofing attack. However, the participants also have to wear adhesive gel patches or chest straps that could cause skin irritation and discomfort. To overcome those problems, Wim Verkruysse *et al* [5] brought up the concept of measuring Plethysmographic signals remotely. It was the first study about heart rate estimation using computer vision technique. By analyzing the RGB signal in frequency, the cardiac pulse could be estimated correctly. In 2010, Ming-Zher Poh *et al* [6] proposed the further research in non-contact cardiac pulse measurements. They improved the heart pulse detection rate proposed previously by Wim Verkruysse *et al*.

What we observed was that using the method proposed by Ming-Zher Poh *et al* could not distinguish a live face or photo correctly because we still could get the heart pulse data like the human had in photo attack experiments. Hence, in this paper, we further improve the performance by developing a rule according to the frequency entropy to resist photo attack.

The organization of the paper is as follows. In Section 2 our proposed method is presented. Experimental environment and results are shown in Section 3. Finally, we present our conclusions in Section 4.

2. THE PROPOSED METHOD

The flowchart of the proposed liveness detection approach is shown in Fig. 1. The method works by first detecting the face regions from the continuous input frames, as explained in Section 2.1. We then normalize the RGB signals separately (Section 2.2) and we could get the power spectrum of each normalized signal by applying ICA and FFT (Section 2.3). Finally we develop an anti-spoofing method by analyzing the entropy in certain frequency range (Section 2.4). The following sections describe each of the steps in detail.

2.1. Face detection

In this section, we adopted the Viola and Jones [7] method, which was commonly used in detecting face, to localize the

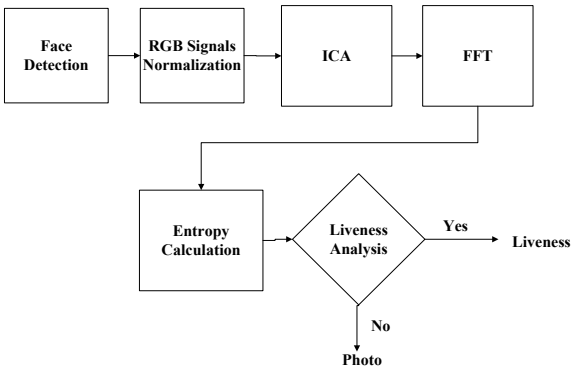

Fig.1 Flowchart of the proposed method

face region in videos. This algorithm uses Haar-like features and Adaboost technique to train with positive and negative examples and then formed a cascade of boosted classifier. OpenCV library [8] provides programmer with this boosted classifier publicly. Unfortunately, there are shadows or bangs around the face region at times which may cause decreasing the accuracy of experimental results. For that reason, the system selected the center 60% width and 80% height of the face region to avoid this problem..

2.2. Normalization of the RGB signals

Given the selected face region, we calculated the RGB traces through the following formulas to be the image features. The $R(t), G(t)$ and $B(t)$ three signals respectively mean the sum of the pixel values in red, green and blue channels at the time t. $E(\cdot)$ is the mean value and $STD(\cdot)$ is the standard deviation of pixel values in a period of time T. We normalized the three signals to be $R'(t), G'(t)$ and $B'(t)$ called RGB traces.

$$R^{\wedge\prime}(t) = (R(t) - E(R))/STD(R), \quad (1)$$
$$G'(t) = (G(t) - E(G))/STD(G), \quad (2)$$
$$B^{\wedge\prime}(t) = (B(t) - E(B))/STD(B), \quad (3)$$

where $t = 1,2, \dots, T$.

2.3. ICA and FFT

To eliminate the cross-channel noises caused by the environment interference, we adopted the Independent Component Analysis (ICA) [9] to deal with this problem. ICA is a method of Blind Source Separation (BSS), which is developed to solve the cocktail-party problem in audio signal processing. By applying ICA algorithm to the RGB traces, we could get three much clearer signals. The ICA algorithm used in this system is called Joint Approximation Diagonalisation of Eigen-matrices (JADE) [10]. This code is published publically and can be downloaded on website [11].

After removing the noises by ICA , we then used the Fast Fourier Transform (FFT) to produce the power spectra and analyzed entropies of three signals individually. Using the final result of the analysis, we could successfully distinguish whether the participant was alive or not. In the next section we explain the following concept in detail.

2.4. Liveness analysis

Assuming the power spectrum values of RGB traces are $X_\theta = \{x_1, \dots, x_T\}$, $\theta \in \{R, G, B\}$. The entropy of X_θ was calculated by the formula (4) shown below:

$$Entropy(X_\theta) = -\sum_{i=1}^{T} p(x_i)\, logp(x_i), \quad (4)$$
$$p(x_i) = x_i / \sum_{i=1}^{T} x_i, \quad (5)$$

where $p(x_i)$ means the probability of x_i.

Table 1 A typical example of entropies in liveness and in photo attack experiments

	Liveness experiment	Photo experiment
entropy of R	4.77	5.13
entropy of G	2.86	5.16
entropy of B	5.06	5.04

Table 1 is a typical example of experimental results that shows the entropies of power spectra of the individual RGB signals in liveness and in photo attack experiments. We could find that the maximum entropy and minimum entropy in liveness experiment have more significant difference than that in photo attack experiment.

According to the observation above, we generalize a discriminative linear formula shown in (6) for distinguishing live face and photo. Then the live face would satisfy the principle shown in (7).

$$\mathrm{Th} = ((maxE - minE)/maxE), \quad (6)$$
$$Lx = \begin{cases} 1 & if\ Th > C \\ 0 & otherwise \end{cases}, \quad (7)$$
$$maxE = Max\{Entropy(X_\theta)\}, \quad (8)$$
$$minE = Min\{Entropy(X_\theta)\}. \quad (9)$$

Lx means the liveness or spoofing photo (1 or 0).The *maxE* and *minE* mean the maximum and minimum entropies of power spectra of the individual RGB signals. The subtract value was normalized by dividing the *maxE*. *C* is the threshold and set to be 0.05 in our experiments.

3. EXPERIMENTAL RESULSTS

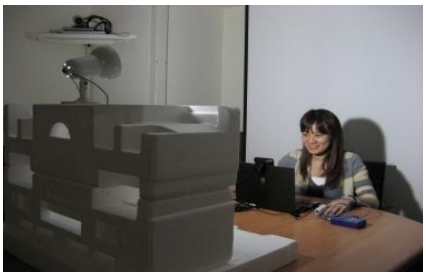

Fig.2 The setting of the experimental environment.

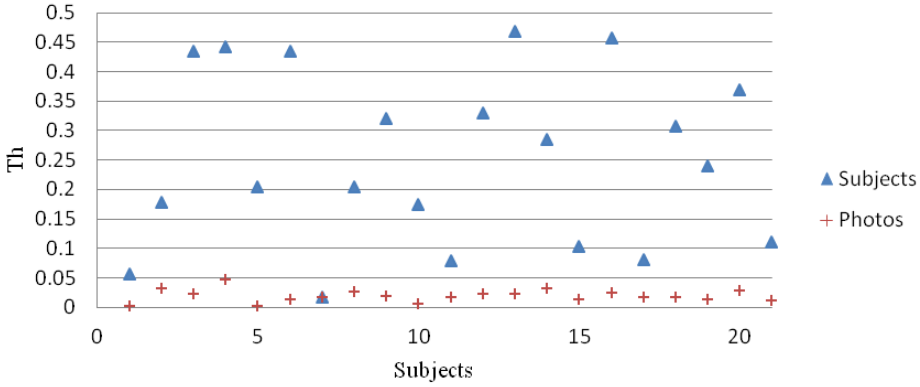

Fig.3 The entropies analysis of 21 subjects and spoofing photos in Experiment 3.1

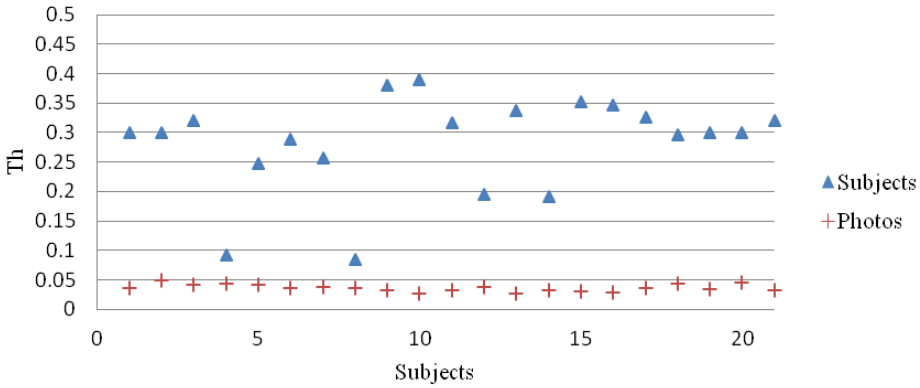

Fig.4 The entropies analysis of 21 subjects and spoofing photos in Experiment 3.2

Fig.2 shows the experimental environment in our laboratory. To establish our photo-spoofing database, we recorded 21 participants (15 males and 6 females). The participants were asked to seat in front of a laptop and recorded videos by web camera. The laboratory we selected was indoor place under compact fluorescent lamp without outdoor lighting. The length of each video is about 1 minute with 320x240 resolutions and frame rate 20fps. One frame extracted from video clip was taken as spoofing photo. The testing program was written by C/C++ based on Borland C++ 6.0 platform.

3.1. Observation time: 1 minute

The participants recorded 1 minute video and the length of observation window time was 1 minute. In other words, we had 1200 feature points for each RGB trace and only get one result eventually. The spoofing photo, a frame extracted from the video clip, also recorded 1 minute video and used the same experimental steps.

The experimental results are shown in Fig.3. According to the Fig.3, we found that there existed an apparent boundary 0.05 between subjects and spoofing photos. The threshold in the principle is 0.05. When the final result was above 0.05, we determined the observed object is alive; otherwise it is a spoofing photo. This judgment was verified

by the rule mentioned in Section 2.4. There is only one exception under the 0.05.

3.2. Observation time: 15 seconds

In this experiment, we shortened the observation window time to 15 seconds but the length of video was still 1 minute. We shifted the observation window in every 2 seconds, that is to say, we had 13 seconds overlap in every observation window. Through 1 minute video, the 23 results (i.e. Th) were produced. We averaged over 23 numbers to be the final results and adopted the principle in Section 2.4 to detect liveness. Fig.4 shows the experiment results. The threshold 0.05 also works in this experiment. The accuracies of the experiments are summarized in Table 2.

Table 2 the accuracy rates of different observation time

	1 minute	15 seconds
Accuracy rate	95.24%	100%

4. CONCLUATIONS

In this paper, we present a novel method for the liveness detection based on frequency entropy of image sequences. Our method does not expect the user to perform unfriendly behavior like eye blinking which is the condition judgment of liveness in the previous work. By combining the ICA and FFT frequency analysis of the face images sequence, the liveness detection can be effectively solved from the verification of the entropy of power spectrum. The experimental results of 21 subjects show the promising results of more than 95% accuracy.

5. REFERENCES

[1] S.B. Nikam, and S. Agarwal, "Fingerprint liveness detection using curvet energy and co-occurrence signatures," *IEEE CGIV*, pp. 217-222, 2008.

[2] Zhiwei Zhang, Dong Yi, Zhen Lei and S.Z. Li, "Face liveness detection by learning multispectral reflectance distributions," *IEEE FG*, pp. 436-441, 2011.

[3] Gang Pan, Zhaohui Wu, and Lin Sun, "Liveness detection for face recognition," I-Tech, 2008.

[4] T. Kathikeyan, and B. Sabarigiri, "Countermeasures against iris spoofing and liveness detection using electroencephalogram (EEG)," *IEEE ICCCA*, pp. 1-5, 2012.

[5] Wim Verkruysse, Lars O Svaasand, and J Stuart Nelson, "Remote plethysmographic imaging using ambient light," *Opt Express*, vol. 16, no. 26, 2008.

[6] Ming-Zher Poh, Daniel J. McDuff, and Rosalind W. Picard, "Non-contact automated cardiac pulse measurements using video imaging and blind source separation," *Opt Express*, vol. 18, no. 10, 2010.

[7] P. Viola, and M. Jones, "Rapid object detection using a boosted cascade of simple features," *IEEE CVPR*, pp. 511-518, 2001.

[8] Intel, "Open source computer vision library; http://sourceforge.net/projects/opencvlibrary/", 2001.

[9] Aapo Hyvärinen, and Erkki Oja, "Independent component analysis: algorithms and applications," *Neural Networks*, 2000.

[10] Jean-François Cardoso, "High-order contrasts for independent component analysis," *Neural Computation*, pp. 157-192, 1999.

[11] http://bsp.teithe.gr/members/downloads/Jade.html