A Novel Face Spoofing Detection Method based on Gaze Estimation

Lijun Cai, Chunshui Xiong, Lei Huang and Changping Liu

Institute of Automation Chinese Academy of Sciences, Beijing, China

Abstract. Since gaze is a kind of behavioral biometrics which is difficult to be detected by the surveillance due to the ambiguity of visual attention process, it can be used as a clue for anti-spoofing. This work provides the first investigation in research literature on the use of gaze estimation for face spoofing detection. Firstly, a gaze estimation model mapping the gaze feature to gaze position is established for tracking user's gaze trajectory. Secondly, gaze histogram is obtained by quantifying and encoding the gaze trajectory. Finally, information entropy on gaze histogram suggests the uncertainty level of user's gaze movement and estimates the liveness of the user. Our basic assumption is that the gaze trajectory of genuine access has higher uncertainty level than that of attack. Therefore, the greater the entropy, the more probable the user is genuine. Experimental results show that the proposed method obtains competitive performance in distinguishing attacks from genuine access.

1 Introduction

Due to the requirement of information security, face spoofing detection is attracting more and more attention and research nowadays. Generally speaking, there are three common manners to spoof face recognition system: photograph, video and 3D model of a valid user. Among them, photograph and video faces are the most popular because invaders can easily obtain the faces of valid users through mobile phones or surveillance cameras. With the aid of modern technology, 3D face composition is no more difficult. For example, the service of ThatMyFace.com can realizes 3D face reconstruction and model order by uploading a front and side photos. Compared with real faces, photograph faces are planar, as well as having quality degradation and blurring problems. Video faces are reflective and 3D face models are rigid. Based on these clues, face anti-spoofing techniques can be roughly classified into three categories: motion based methods, texture based methods and fusion methods.

Motion based anti-spoofing methods hypothesize that planar objects move significantly different with real faces, which are 3D objects. K.Kollreider et al. [1] present a lightweight novel optical flow to analyze the trajectories of certain parts of a real face against a fake one. Bao et al. [2] estimate four basic types of optical flow field and heuristically detect attacks by calculating the difference degree. Anjos et al. [3] compute the correlations between personal's head movements and scene context based on the pixel difference of adjacent two frames.

Later, the same authors present a similar method [4] based on motion direction correlation instead of pixel intensity. In addition to involuntary head movement, other liveness traits, such as eye-blinks or mouth-movements, are also used for spoofing detection. Pan et al. [5] formulate blink detection as an undirected conditional graphical framework and propose to use scene context information to avoid video replay.

Another commonly used facial clue is texture analysis. The key idea is that the local micro textures are changed during image recapture. Jukka et al. [6] adapt multi-scale local binary pattern and nonlinear support vector machine to classify real and fake faces. Later, the same authors [7] propose to fuse texture and shape features for spoofing detection. Tan et al. [8] propose two strategies to extract the essential information of a live human face or a photograph by Lambertian model and train a complex classifier. Komulainen et al. [9] introduces the first investigation on the use of dynamic texture for face spoofing detection.

Motion based methods can effectively distinguish photographs from genuine access, while invalid to warped photograph and video attacks. Texture based methods can effectively obtain the discriminative models for differentiating real and fake faces, while can't take full advantage of adjacent frames information. Nowadays, more and more researchers are focusing their attention on the fusion methods which can defense multiple kinds of attacks by complementary advantages. Yan et al. [10] propose three clues including non-rigid motion, face-background consistency and imaging banding effect to conduct an effective face spoofing detection. Komulainen et al. [11] present the complementary countermeasures by studying fusion of motion and texture.

Besides above methods, multi-mode information [12–14] and multi-spectra [15–17] also offer useful clues for spoofing detection. However, they require extra devices or user cooperation.

Therefore, non-intrusive methods without extra devices and human cooperation are preferable in practice, since they can be embedded into a face recognition system, which is usually only equipped with a generic webcam. Gaze is a kind of biometric metrical information which can avoid spoofing with following characteristics [18]. Firstly, it does not require physical contact between user and device. Secondly, gaze is difficult to be obtained by surveillance camera and other equipment. Ali et al. [19–21] present the first time to use gaze clue for anti-spoofing, in which user is required to follow a moving point showed on the computer screen. Features based on the collinearity of gaze are used to discriminate between genuine access and attack. Experiments show that these methods are effective on small scale collected database by screening samples. However, they are invalid for still photographs and uncooperative users. What's more, the process of collecting samples lasts 130s, which is far beyond the users' patience. To my knowledge, except for the methods proposed by Ali et al. [19–21], there is no other work to introduce gaze into face spoofing detection.

In this paper, we propose a novel and appealing approach for face spoofing detection based on gaze estimation, which is non-intrusive and doesn't require extra device and user cooperation. Because of the ambiguity of the visual at-

tention process, real faces has higher uncertainty level of gaze trajectory in a period of time compared with the fake faces. Our key idea is to make a statistical analysis on gaze trajectory for liveness estimation by gaze tracking. This work provides the first investigation in research literature on the use of gaze estimation for face spoofing detection. Extensive experimental analysis on databases show that gaze estimation offers a new and effective tool for anti-spoofing.

2 General Framework

The general framework of the proposed method is illustrated in Fig. 1, which consists of two sections: establishment of gaze estimation model and spoofing detection.

In the first section, gaze estimation model mapping gaze feature to gaze position, a 2D coordinate, on the computer screen is established. This paper formulates the model as a nonlinear regression problem. In the second section, spoofing detection based on gaze estimation is conducted. It includes three stages: (I) gaze tracking, (II) gaze quantification and encoding, and (III) liveness estimation. Firstly, a video clip lasting 3-5 seconds of a test user is obtained and gaze trajectory (the gaze locations of each frame in the video clip) can be estimated according to the gaze estimation model. Secondly, quantification and encoding of gaze trajectory is performed to form the gaze histogram, which is convenient for statistics and robust to attacks of warped photograph. Finally, information entropy of the gaze histogram is used to analyze the uncertainty level of gaze trajectory and estimate the liveness of test user. Our hypothesis is that compared with attacks, the gaze uncertainty level of genuine accesses are higher. Therefore, the greater the information entropy value is, the more probable the user is judged to be a genuine access.

3 Gaze Estimation Model

The existing gaze estimation methods can be roughly classified into two categories: feature-based methods and appearance-based methods. Feature-based methods [22, 23] map the gaze feature (for example iris outline, pupil, cornea) to gaze position. However, this kind of methods generally require high quality camera, even multiple light sources. Appearance-based [24, 25] methods firstly locate eye region, then directly map the whole eye region to gaze position, which takes full advantage of gaze information. Considering our proposed method is conducted under the condition of the nature light and a generic camera, in this paper we choose appearance-based method to establish the gaze estimation model.

3.1 Data Collection

To obtain training data for gaze estimation model, we develop a system on a desktop composed of a 19-inch computer screen with 1440×900 resolution and

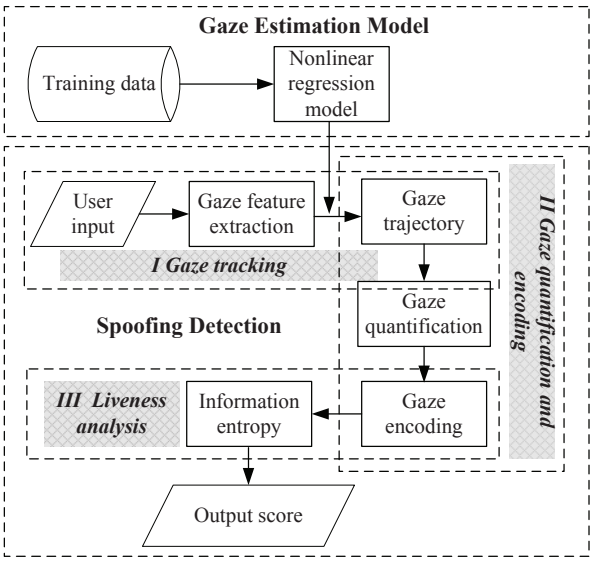
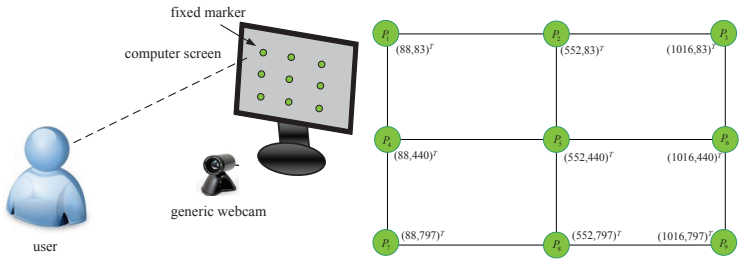


Fig. 1. System architecture.

a generic webcam with 640×480 resolution. The user is asked to sit in front of the computer screen (about 50cm-60cm) and keep his head stable with the help of a chinrest. There are nine fixed makers on the computer screen. The setup of our system is shown in Fig. 2(a) and the positions of markers are illustrated in Fig. 2(b).

In the process of data collection, the system captures the user's frontal appearance while his gaze is focusing on the each marker shown on the screen. In this paper there are 50 users and 30 images are captured at each marker for each user, totally 13500 frontal images. By artificially removing eye-closed images, there are 12698 frontal images left. Considering the negative effect of optical reflection, users are required to remove glasses during the data collection.



(a) Setup of data collection (b) The locations of nine markes

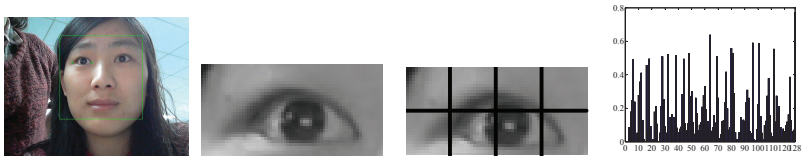
Fig. 2. Data collection system for gaze estimation.

3.2 Gaze Feature Extraction

We want to find a function that map the gaze feature to the corresponding marker on the computer screen. In this paper gaze feature is obtained based on micro-texture analysis of eye image.

Firstly we introduce an eye image extraction method consisting of two steps: eye corners detection and eye region alignment. In the first step, the face region and inner and outer eye corners are detected by adaptive boosting algorithm [26] (Fig. 3(a), left eye is used in this paper). In the second step, to deal with small head motion, an additional alignment procedure is performed. Firstly we define an eye image template with 64×32 size, and the location of inner eye corner is (54, 20) and outer corner (9, 20). The aligned eye image is obtained by rotating and scaling the face region based on the locations of eye corners in template (Fig. 3(b)).

In the procedure of feature extraction, to fully use the micro-texture difference between fake faces and real faces, the eye image is divided into $r \times c$ subregions (4×2 in this paper, Fig. 3(c)) and for each subregion dual histogram local binary pattern (DH-LBP) [27] is extracted as feature. The feature of eye image is formed by concatenating features of subregions (Fig. 3(d)). DH-LBP is the improved version of LBP and its local texture descriptor reduces the dimensions of LBP as well as maintains the discriminate ability.



(a) (b) (c) (d)

Fig. 3. Data collection system for gaze estimation. (a) Face and eye corners detection. (b) Eye image (64×32). (c) Uniform partition of eye image. (d) Gaze feature (128D)

3.3 Model Building and Solving

Given data set $\{x_i, y_i\}_{i=1}^{N}$, $x_i \in R^n$ ($n = 128$) is gaze feature and $y_i = (p_{x,i}, p_{y,i})^{\mathrm{T}} \in R^2$ is the corresponding gaze position (one of the fixed markers in Fig. 2(b)), $N = 12698$ is the data number. Considering gaze estimation under non-high quality camera is a complex nonlinear problem, we use regression model in the following to establish the function f mapping gaze feature to gaze position.

$$y = f(x) = (w \cdot \phi(x)) + b \tag{1}$$

where $(\cdot)$ denotes the inner product in the mapped feature space of the input space via a nonlinear map function ϕ. Here, we adapt the robust SVR (Support Vector Regression) technique and libSVM toolbox [28] to solve the model.

4 Spoofing Detection Based on Gaze Estimation

In this section, we describe in details our proposed spoofing detection method based on gaze estimation. Our hypothesis is that compared with photograph, video and 3D model, the gaze trajectory of real faces has higher level of uncertainty. Information entropy is used to evaluate the the uncertainty level and estimate the liveness of user. The proposed method has three main steps: gaze tracking, gaze quantification and liveness estimation.

4.1 Gaze Tracking

Firstly we define two nouns used later in this paper: training interface and test interface. Both of them refer to the computer screen that user focus on in the process of training or test. Differently, training interface indicates the computer screen adapted in Fig. 2(a) for gaze estimation model, and test interface indicates the one adapted in test phrase. Since the establishment of gaze estimation model is offline, training interface and test interface may have different resolutions. Considering the mapping of two different resolutions, for the same user, the predict gaze trajectories are different, but the relative gaze positions are invariable.

1)Test interface has the same resolution with the training interface. Assuming there are M frontal images captured for the user in front of camera, by extracting gaze feature, we can directly get the gaze trajectory $\{\hat{y}_i = (\hat{p}_{x,i}, \hat{p}_{y,i})^{\mathrm{T}}\}_{i=1}^{M}$ according to function f obtained by solving equation (1).

2)Test interface has the different resolution with the training interface. In this case, we should perform affine transformation on $\{\hat{y}_i = (\hat{p}_{x,i}, \hat{p}_{y,i})^{\mathrm{T}}\}_{i=1}^{M}$ to get the final gaze trajectory. Assuming the final gaze trajectory is $\{\hat{z}_i = (\hat{q}_{x,i}, \hat{q}_{y,i})^{\mathrm{T}}\}_{i=1}^{M}$ and the affine transformation matrix is $T = \left(\begin{smallmatrix} a_{00} & a_{01} & b_{00} \\ a_{10} & a_{11} & b_{10} \end{smallmatrix}\right)$, we have

$$\begin{aligned} (\hat{z}_1 \cdots \hat{z}_M) &= T(\hat{y}_1 \cdots \hat{y}_M) \\ &= \begin{pmatrix} a_{00} & a_{01} & b_{00} \\ a_{10} & a_{11} & b_{10} \end{pmatrix} \begin{pmatrix} \hat{p}_{x,1} & \cdots & \hat{p}_{x,M} \\ \hat{p}_{y,1} & \cdots & \hat{p}_{y,M} \\ 1 & \cdots & 1 \end{pmatrix} \end{aligned} \tag{2}$$

T can be obtained by three pairs of corresponding points between training interface and test interface.

4.2 Gaze Quantification and Encoding

The quantization step is important because it not only simplify the statistics for gaze trajectory of real faces but also may robust to that of warped photograph attack. Gaze codebook is firstly constructed as base points for further quantification. In this paper gaze codebook is obtained by performing affine transformation on the nine fixed makers belonging to the training interface of Fig. 2(a). Given

$\{P_1, \cdots, P_9\}$ presented in section 2.1 and transformation matrix T obtained in section 4.1, we have

$$(Q_1 \cdots Q_9) = T \begin{pmatrix} P_1 & \cdots & P_9 \\ 1 & \cdots & 1 \end{pmatrix} \tag{3}$$

$\{Q_1, \cdots, Q_9\}$forms the gaze codebook. Then, gaze quantification is performed by classifying each gaze position of gaze trajectory to its nearest Q_i and gaze encoding is conducted by voting and normalization to form gaze histogram.

4.3 Liveness Estimation

In information theory, entropy is the indicator of information quantity. The greater the entropy is, the larger quantity the information contains. In this paper, we use information entropy to estimate the liveness of user. The greater the information entropy is, the higher the uncertainty level of gaze trajectory is, and the more probable the user is judged as a live person.

For gaze histogram $H = \{p_1, p_2, \cdots, p_9\}$ satisfying $\sum_{i=1}^{9} p_i = 1, 0 \leq p_i \leq 1$, according to the definition of information entropy

$$entropy = -\sum_{i=1}^{9} p_i log(p_i) \tag{4}$$

if $\exists\ p_{i_0} = 1$, then $entropy = -\sum_{i=1}^{9} p_i log(p_i) = -p_{i_0} log(p_{i_0}) = 0$. if $\exists\ \{0 < p_{i_k} < 1\}_{k=1}^{l}, 1 < l \leq 9$, $entropy = -\sum_{i=1}^{9} p_i log(p_i) = -\sum_{k=1}^{l} p_{i_k} log(p_{i_k}) > 0$. $entropy = log(9) \approx 2.1972$ obtains the maximum if and only if $p_1 = p_2 = \cdots = p_9 = \frac{1}{9}$.

By above analysis, if the user keeps gaze still in a period of time, then $entropy = 0$. If he moves his attention and changes the gaze, then $entropy > 0$, and if the user casts his gaze on the neighborhood of each Q_i uniformly, then $entropy$ gets the maximum.

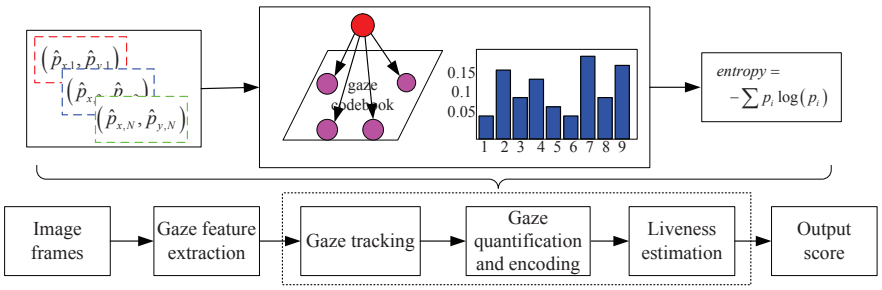


Fig. 4. The flowchart of the proposed spoofing detection algorithm.

To sum up, for a test user, our proposed spoofing detection method based on gaze estimation includes the following procedures: 1) Capture video frames of user from generic webcam. 2) Gaze feature extraction. 3) Spoofing detection based on gaze trajectory analysis: gaze tracking, gaze quantification and encoding, and liveness estimation. 4) Output entropy as liveness score. Fig. 4 shows the flowchart of the proposed method.

5 Experiments

5.1 Evaluation of Gaze Estimation Model

Gaze error [25] is commonly used to evaluate the gaze estimation model.

$$error = arctan\left(\frac{\|y - \hat{y}\|_2}{d_{user}}\right) \tag{5}$$

where $\|y-\hat{y}\|_2$ represents the Euclidean distance between real and predict value, and d_{user} refers to the distance between user's eye with computer screen.

In this experiment, we compare adapted nonlinear model solved by SVR with linear model solved by least square method. Experiment is performed by separating the collected data in section 2.1 into two parts: 30 persons for training gaze estimation model and 20 persons for test. Fig. 5 illustrates the average gaze error on nine makers of 20 test users. Experimental results show that nonlinear model has lower average gaze error. Compared with SVR, 1) Least square method is sensitive to outer points of fitting curve. 2) Least square method only minimizes the empirical risk and doesn't generalize well. It should be noted that all the existing gaze estimation model presented under the condition of nature light and a generic webcam can be embedded into our spoofing detection method.

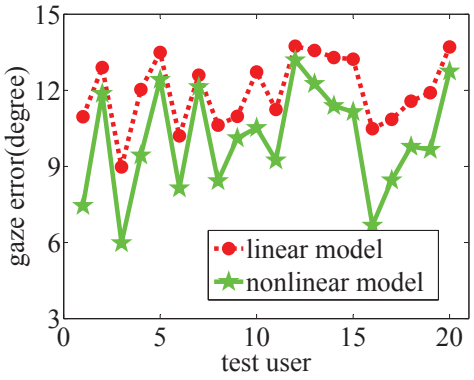


Fig. 5. Average gaze error of 20 test users by linear and nonlinear regression model.

5.2 Gaze Analysis of Real Faces under Involuntary State

This section studies the gaze change of real faces under involuntary state. Involuntary state means that there is no interference from outside. We collect 24 video clips with 15fps (Frames Per Second) from 24 users , and each clip lasts about 10s (Second). Different from the setup showed in Fig. 2(a), the video collection setup has no fixed markers on the computer screen. Considering the detection efficiency, we choose time window with 15 frames for evaluation. Fig. 6 gives the entropy values for each time window of 24 users.

Experimental results show that different users have different uncertainly level of gaze trajectory. For example, user 1-4, 5, 8, 10, 12, 16 and 21 change their gaze in the first 1s. However, user 18-20 and 24 keeps gaze still during all the 10s. Therefore, to ensure the efficiency of applicant system, extra stimulus showed on the test interface is needed to attract the attention of genuine access for gaze change, which avoids mistakenly judging the real faces as attacks.

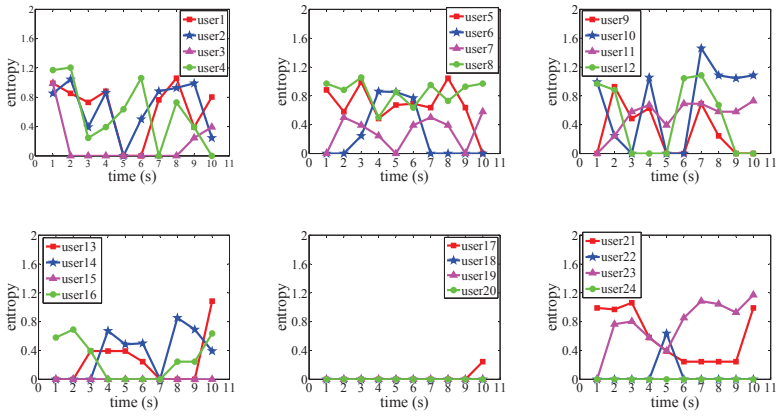


Fig. 6. The variation of gaze directions under user's involuntary state.

5.3 Effectiveness of Proposed Spoofing Detection Method

To my knowledge, there is no suitable database which is public available to evaluate our proposed method. In this section, we construct two databases by combing self-collected data with parts of two public databases. CASIA [29] and Replay-Attack [30] are commonly used databases for evaluating spoofing detection methods. They contain samples with multiple qualities (low quality, low quality and high quality) and multiple forms (photograph, iPhone and iPad play). However, the positive samples (sample with real faces) of the two databases keep gaze direction unchanged, which is unfit for proposed method. On the

other side, the diversity of negative samples (samples with fake faces) in these two databases facilitates to verify algorithm generalization. Therefore, in this paper we substitute the positive samples by self-collection for that of two public databases and retain the negative samples of two public databases to form two new ones: Gaze-CASIA and Gaze-Replay-Attack.

Database and Test Protocol. The self-collected data include three subsets: G-Train (50 subjects), G-Devel (30 subjects) and G-Test (30 subjects). Subjects belonging to different subsets have no intersection. One video clip for each subject lasting about 10s is collected. Different with training data collected for gaze estimation model in section 2.1, G-Train is collected for contrast experiments, because the compared method used in this paper has training stage for classifier. The data collection setup is similar to Fig. 2(a): a computer screen with the same or different resolution with training interface and a generic webcam with 640×480 resolution. The difference is that in Fig. 2(a), there are nine fixed markers on the computer screen, while in this section, random points is set to appear on computer screen for attacking user's attention and changing live user's gaze direction as soon as possible. It is noted that we don't force users to follow the trajectory of random points, which means that our proposed method doesn't require user's cooperation. Gaze-CASIA and Gaze-Gaze-Replay-Attack databases are constructed as follows.

(1)Gaze-CASIA is composed of two subsets: training set and test set. Their positive samples are G-Train and G-Test respectively, and the negative samples are the same with that in CASIA database (L2, L3, L4, N2, N3, N4, H2, H3 and H4, each with 20 and 30 subjects for training and test sets). L, N and H refer to low-quality camera, normal-quality camera and high-quality camera respectively . 2, 3 and 4 refer to warped photograph, photograph removing eye region and video. Thus, L2 means photograph attack in front of a low-quality camera, and so on.

(2)Gaze-Replay-Attack database is composed of three subsets: training, validation and test. Positive samples are G-Train, G-Devel and G-Test respectively, and negative samples are the same with that in Replay-Attack database. Validation is used for selecting parameters. Details are shown in Table 1.

For Gaze-Replay database, to verify the effectiveness of proposed method on samples with diverse qualities, we present four scenarios similar to [29].

scenario 1: {G-Train+G-Test, L2, L3, L4};

scenario 2: {G-Train+G-Test, N2, N3, N4};

scenario 3: {G-Train+G-Test, H2, H3, H4};

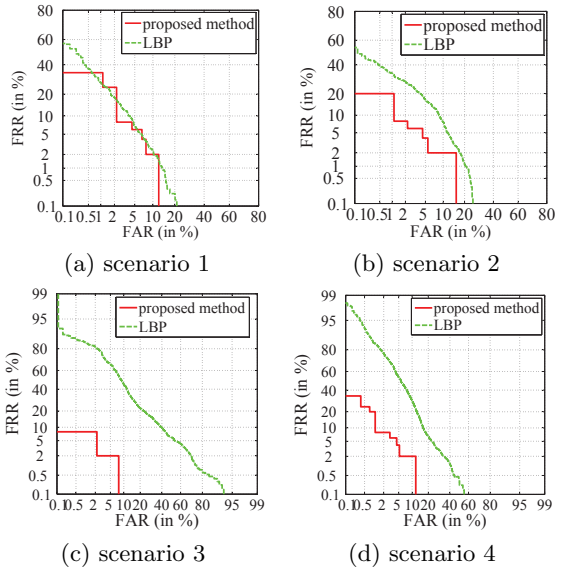
scenario 4: {G-Train+G-Test, L2, L3, L4, N2, N3, N4, H2, H3, H4}. DET (Detection-Error Trade-off) curve and EER (Equal Error Rate) [29] are adapted for evaluation on each scenario. EER is the value when FRR (False Rejection Rate) equals to FAR (False Acceptance Rate).

For Gaze-Replay-Attack database, FAR, FRR and HTER (Half Total Error Rate) [30] on test set should be given under the threshold selected by minimizing EER on validation set.

Table 1. The decomposition of Gaze-Replay-Attack database. The numbers indicate how many videos are included in each subset (the sums indicate the amount of hand-based and fixed-support attacks).

Type	Train	Devel	Test	Total
Real-access	50	30	50	130
Print-attack	$30 + 30$	$30 + 30$	$40 + 40$	$100 + 100$
Phone-attack	$60 + 60$	$60 + 60$	$80 + 80$	$200 + 200$
Tablet-attack	$60 + 60$	$60 + 60$	$80 + 80$	$200 + 200$
Total	350	330	450	1130

Contrast Experiments. Because there is no similar methods proposed before, we can't compare our proposed method with the state of the arts on the public available databases. To verify the effective of our method, on the constructed databases Gaze-CASIA and Gaze-Replay-Attack, classical LBP-based spoofing detection method [6] is used for comparison. Fig. 7 and Table 2 are the DET curves and EER of two compared methods under four scenarios of Gaze-CASIA database.



(a) scenario 1 (b) scenario 2

(c) scenario 3 (d) scenario 4

Fig. 7. DET curves under the different scenarios of the Gaze-CASIA database.

Table 2. EER under different scenarios of Gaze-CASIA database.

Scenario	1	2	3	4
LBP	0.0558	0.0821	0.2096	0.1288
Proposed method	0.0489	0.0378	0.0211	0.0359

Experimental results show that compared with LBP-based method, proposed method gets lower FAR and FRR under scenario 2, 3, and 4. By contrast, the difference of two methods under scenario 1 are not apparent. It expresses that compared with low-quality photo and video, proposed method works better with high-quality camera. Because high-quality camera offers clear image, thus face region and eye corners can be detect accurately.

Table 3 gives the compared performance on Gaze-Replay-Attack database. Experimental results show that proposed method works better. The FAR doesn't reach 0% may because the glasses reflectivity brings mistaken judgement.

Table 3. Performance on Gaze-Replay-Attack database (%).

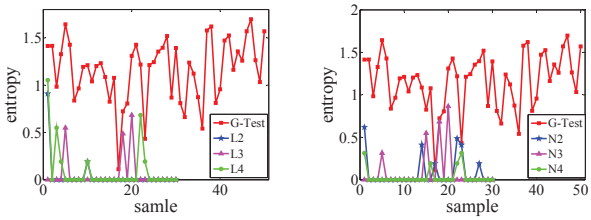
Method	Devel		Test		
	FAR	FRR	FAR	FRR	HTER
LBP	26.43	26.43	19.47	5.13	12.30
Proposed method	1.50	1.50	6.50	2.00	4.25

5.4 Is Entropy A Good Indicator?

This section verifies the effectiveness of bringing into information entropy into our proposed method. Fig. 8 and Fig. 9 illustrate the entropy values of samples in two databases and show that entropy values of real faces (G-Test in Fig. 8(a)-(c) and Fig. 9(a), (e)) are averagely higher than that of fake faces (L2-L4, N2-N4, H2-H4 in Fig. 8(a)-(c) and Fig. 9 (b)-(d), (f)-(h)). Considering the fact that compared with attacks, genuine accesses have higher uncertainty level of gaze trajectory. Experimental results show that the hypothesis of proposed method matches the real case, therefore, entropy is a good indicator.

6 Conclusion and Future Work

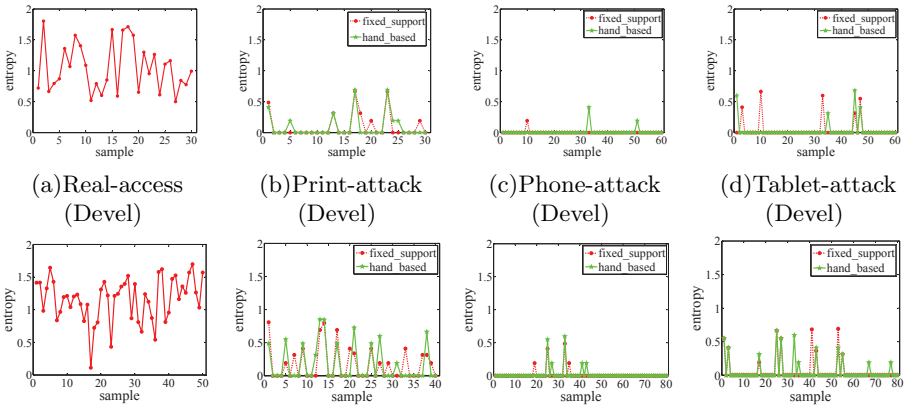
In this paper we propose a novel spoofing detection method based on gaze estimation. To the best of my knowledge, it is the first time to present this kind of method for preventing the fake faces based on gaze tracking and analysis. Due



(a) scenario 1 (b) scenario 2

(c) scenario 3 (d) scenario 4

Fig. 8. The entropy values of Gaze-CASIA database.



(a)Real-access (Devel) (b)Print-attack (Devel) (c)Phone-attack (Devel) (d)Tablet-attack (Devel)

(e)Real-access (Test) (f)Print-attack (Test) (g)Phone-attack (Test) (h)Tablet-attack (Test)

Fig. 9. The entropy values of Gaze-Replay-Attack database.

to the ambiguity of visual attention process, real faces have no fixed gaze trajectory within a period of time. Our key idea is that compared with photograph, video and 3D model, gaze trajectory of real face has higher level of uncertainty. The proposed spoofing detection method contains three key stages: gaze tracking, gaze quantification and decoding, and liveness estimation. Gaze tracking is performed based on gaze estimation model to form gaze trajectory. Gaze quantification and decoding of gaze trajectory offers convenient way for statistics and is robust to attack of warped photograph. Information entropy is a good indicator to estimate the liveness of user. Experimental results on constructed databases show that the proposed method can effectively distinguish the attacks from genuine accesses. How to prevent video attacks with gaze changing is the future issue we will research on.

References

1. Kollreider, K., Fronthaler, H., Bigun J.: Non-intrusive liveness detection by face images. Image and Vision Computing **27** (2009) 223–244
2. Bao, W., Li, H., Li, N., Jiang, W.: A liveness detection method for face recognition based on optical flow field. In: Proc. Int. Conf. Image Analysis and Signal Processing (2009) 233–236
3. Anjos, A., Marcel, S.: Counter-measures to photo attacks in face recognition: a public database and a baseline. In: Proc. IJCB (2011) 1–7
4. Anjos, A., Mohan, M., Marcel, S.: Motion-based counter-measures to photo attacks in face recognition. Institution of Engineering and Technology Journal on Biometrics, to be published (2014)
5. Pan, G., Sun, L., Wu, Z., Wang, Y.: Monocular camera-based face liveness detection by combining eyeblink and scene context. J. of Telecommunication Systems **47** (2011) 215–225
6. Jukka, M.P., Hadid, A., Pietikinen, M.: Face spoofing detection from single images using micro-texture analysis. In: Proc. IJCB (2011) 1–7
7. Maatta, J., Hadid, A., Pietikainen, M.: Face spoofing detection from single images using texture and local shape analysis. IET Biometrics **1** (2012) 3–10
8. Tan, X., Li, Y., Liu, J., Jiang, L.: Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: Proc. ECCV (2010) 504–517
9. Komulainen, J., Hadid, A., Pietikainen, M.: Face spoofing detection using dynamic texture. In: Proc. ACCV Workshop (2013) 146–157
10. Yan, J.J., Zhang, Z.W., Lei, Z., Yi, D., Li, S.Z.: Face liveness detection by exploring multiple scenic clues. In: Proc. Int. Conf. Control Automation Robotics and Vision (2012) 188–193
11. Komulainen, J., Hadid, A., Pietikainen, M., Anjos, A., Marcel, S.: Complementary countermeasures for detecting scenic face spoofing attacks. In: Proc. ICB (2013) 1–7
12. Frischholz, R.W., Dieckmann, U.: Bioid: A multimodal biometric identification system. Computer **33** (2000) 64–68
13. Eveno, N., Besacier, L.: Co-inertia analysis for "liveness" test in audio-visual biometrics. In: Proc. Int. Symp. Image and Signal Processing and Analysis (2005) 257–261
14. Chetty, G., Wagner, M.: Liveness verification in audio−video speaker authentication. In: Proc. Australian Int. Conf. Speech Science and Technology (2004) 363–385

15. Pavlidis, I., Symosek, P.: The imaging issue in an automatic face/disguise detection system. In: Proc. IEEE workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications (2000) 15–24
16. Zhang, Z.W., Yi, D., Lei, Z., Li, S.Z.: Face liveness detection by learning multispectral reflectance distributions. In: Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition and Workshops (2011) 436–441
17. Kim, Y., Na, J., Yoon, S., Yi, J.: Masked fake face detection using radiance measurements. J. of the Optical Society of America A **24** (2009) 760–766
18. Sireesha, M.V., Vijaya, P.A., Chellamma, K.: A survey on gaze estimation techniques. In: Proc. Int. Conf. VLSI, Communication, Advanced Devices, Signals and Systems and Networking (2013) 353–361
19. Ali, A., Deravi, F., Hoque, S.: Liveness detection using gaze collinearity In: Proc. Int. Conf. Emerging Security Technologies (2012) 62–65
20. Ali, A., Deravi, F., Hoque, S.: Directional sensitivity of gaze-collinearity features in liveness detections. In: Proc. Int. Conf. Emerging Security Technologies (2013) 8–11
21. Ali, A., Deravi, F., Hoque, S.: Spoofing attempt detection using gaze colocation. In: Proc. Int. Conf. Biometrics Special Interest Group (2013) 1–12
22. Sigut, J.F., Sidha, S.A.: Iris center corneal reflection method for gaze tracking using visible light. IEEE Trans. on Biomedical Engineering **58** (2011) 411-419
23. Villanueva, A., Cabeza, R.: Evaluation of corneal refraction in a model of a gaze tracking system. IEEE Trans. on Biomedical Engineering **55** (2008) 2812–2822
24. Williams, O., Blake, A., Cipolla, R.: Sparse and semi-supervised visual mapping with the S3GP. In: Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition (2006) 230–237
25. Feng, L., Sugano, Y., Takahiro, O., Sato, Y.: Inferring human gaze from appearance via adaptive linear regression In: Proc. ICCV (2011) 153–160
26. Viola, P., Jones, M.: Robust Real-time Face Detection. Int. J. of Computer Vision **57** (2004) 137–154
27. Ma, W.H., Huang, L., Liu, C.P.: Advanced local binary pattern descriptors for crowd estimation. In: Proc. Pacific-Asia Workshop on Computational Intelligence and Industrial Application (2008) 958–962
28. Chang, C.C, Lin, J.C.: LIBSVM: a library for support vector machines. ACM Trans. on Intelligent Systems and Technologies **2** (2011) 1–27 Software available at http://www.csie.ntu.edu.tw/ cjlin/libsvm
29. Zhang, Z.W., Yan, J.J., Liu, S.F., Lei, Z., Yi, D., Li, S.Z.: A face antispoofing database with diverse attacks. In: Proc. IAPR Int. Conf. Biometrics (2012) 26–31
30. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing In: Proc. Int. Conf. Biometrics Special Interest Group (2012) 1–7