Impact Factor: 9.9 ISSN-L: 2544-980X

Analysis of Some Methods for Determining a Print Attack Into a Biometric Personal Identification System

Abdukadirov Bakhtiyor [1]

Annotation: The article analyzes and evaluates the state of the problem of detecting a printed attack, false input data in the biometric identification system. The existing methods of replacing the biometric properties of registered users are discussed, as well as methods of combating counterfeiting in biometric systems using motion analysis, analysis of local movements on the face and recognition of facial images based on the assessment of facial vitality. The directions of research to improve the effectiveness of methods for combating false input data are identified.

Key words: face recognition, biometric system, biometric authentication system, person identification system.

1. Introduction. Most modern face recognition systems are based on image brightness and are equipped with a simple camera. The preferred anti-counterfeiting method is to use the system without this equipment. It is easy to integrate into existing face recognition systems.

The types of fraudulent attacks on biometric identification systems are listed in [1], and some of the attack detection methods are published below.

Determining the viability of facial images is a very important process in biometric identity authentication, but this concept has not yet been fully explored. In particular, there are several approaches to this topic in the analysis of faces: [2] When distinguishing live faces from fake faces in the study, a depth map is built by restoring the three-dimensional structure of movement. This depth map will be constant in photographs even if the image is in motion, in which case the living face will give different depth values. In this case, fake faces are assessed using a motion-based method.

2. Definition of a print attack.

The approach presented in [3] combines face part detection and optical flow assessment to determine the viability of a face in authentication systems. In the case of a live face sequence, the specific trajectory of the facial parts is used to distinguish it from false faces. This used a tunable optical flow called linear optical flow. It is based on optical flow approaches that can distinguish between point movement and line movement. As the name suggests, it only specializes in linear motion. The linear optical flux approach, which requires only three images, is a light energy-based optical flux technique fully implemented using two-dimensional Gabor filters.

Comparison of optical fluxes based on the model [4] using Gabor functions was combined in logarithmic polar grids [5], [6] and in a support vector machine to identify parts of the face. Gabor filters are a class of powerful face recognition functions [6], [7].

The biometric authentication system recommended for the facial trajectory assessment system is a separate component aimed at determining viability. It analyzes a sequence of facial images taken with a digital camera, and makes it possible to identify the face as alive or as a craft.

The basic idea here is based on the assumption that a three-dimensional face produces an accurate two-dimensional movement that is stronger in the central parts of the face, such as the nose, than in the outer areas of the face, such as the ear. Ideally, the outer and inner parts are additionally moved in

opposite directions in terms of determining the vitality of the face. This situation is shown in Figures 1 and 2, respectively, in which the head is slightly tilted to the left. Figure 2 shows the horizontal linear optical flow, here only the optical current in the horizontal direction is estimated from the sequence of images shown in Figure 1. The focal parts of the face and their movement are shown as rectangles.

Fig. 1. An example of a sequence of face images.

In other words, body parts closer to the digital camera act differently than those farther from the living face. This assumption requires at least a partial rotational movement of the head, which we consider to be natural and undesirable human behavior. On the contrary, a photograph of the specified face creates constant movement in different parts of the face.

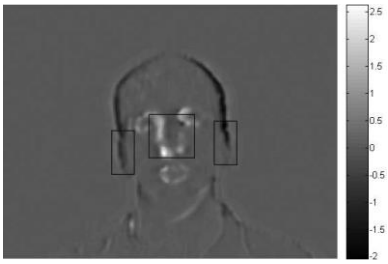

Fig. 2. Horizontal linear optical flow with rectangles denoting focused areas.

Optical flow estimation and face recognition were used to apply these functions. This is based on the Gabor decomposition model [4], as well as an intuitive approach through pattern matching of the optical flow. By knowing the position of parts of the face and comparing how fast they move relative to each other and in which direction they are moving, you can distinguish a live face from a photograph.

The result is based on some assumptions and simplifications of linear optical flow. First, as mentioned, the linear optical flow approach can only handle linear motion, which is called normal motion. Second, when evaluating the components of velocity, the lines are assumed to be horizontal or vertical. Based on the linearity of these simplifications, especially horizontally and vertically oriented lines are regarded as the dominant structure within a known range of scales. It is assumed that these properties are stable enough for space-time analysis. This allows us to reduce the problem of three-dimensional minimization to a two-dimensional level. Linear optical flow is performed using Gabor filters.

In this study, the evaluation of the trajectory lines of several parts of the face using optical flow is the main innovation of the proposed system. Liveness detection successfully separated a sequence of live faces from fake face photos with less than 1% error in the test data. Although the proposed linear optical flux method is limited to estimating line speed, it can provide reliable measurements in assessing facial vitality. It also shows the possibility of a quick way to determine the center of the face using optical flow control. Defining facial parts according to the model-based Gabor classification of traits is resistant to common mistakes such as glasses and facial hair. This system has been rated in the XM2VTS database with up to 10% scale variations.

Although the method of detecting parts of the face by assessing the optical flow gave the above results of effectiveness, this method has several disadvantages in detecting a printed attack, primarily because this method is not comparable with modern databases of fake faces.

3. LOCAL ACTIONS ON THE FACE.

In general, a person can easily distinguish a living face from a photograph, because a person can easily distinguish many physiological signs of life, such as changes in facial expression, mouth movement,

head rotation, changes in eye movements. However, it is very difficult for a computer to recognize these differences even in an unrestricted environment.

From a static point of view, an important difference between a live face and a photograph is that a live face is a completely three-dimensional object, and a photograph can be viewed as a two-dimensional plane. [8] used a motion structure that provides information about the depth of the face to distinguish between a living person and a still photograph with this natural feature. The disadvantage of image depth data is that it is difficult to estimate the depth data when the person's head is stationary, and the estimation noise is also very sensitive to lighting conditions, making it unreliable.

Another distinguishing feature of a live face compared to photography is that a live face experiences slight deformations and changes in appearance, such as changes in mouth movements and facial expressions. Accurate and reliable detection of these changes usually requires high quality login information or user input. In [9], the optical flow to the video input was used to obtain data on facial movements to assess the liveliness of the face, but it is weak for the properties of depth and bending of the photograph. Several researchers have used multimodal Face-Voice approaches [10, 11], using lip movement during speech to detect false signals. This method requires a voice recorder and user interaction. The interactive approach was tested in [12] and required the user to move precisely in the form of head movement.

Below we will consider a method for detecting fake attacks in the ID system by blinking an eye.

Blinking is a physiological activity that occurs when the eyelid is quickly opened and closed. Although the blink rate can vary depending on factors such as fatigue, emotional stress, behavioral category, sleep duration, eye injury and illness, in [13] the researchers reported that the resting blink rate of the human eye is 15 to 30 per minute. ... That is, a person opens and closes his eyes every 2-4 seconds, and the average duration of eye blinking is about 250 milliseconds. Modern conventional cameras can easily shoot video of a face at a frame rate of at least 15 frames per second, that is, the interval between frames does not exceed 70 milliseconds. Thus, a conventional camera can easily capture two or more frames in the blink of an eye while looking at a face camera. Blinking can be used as a key to prevent false attacks. The advantages of the blinking method can be listed as follows:

1. it can be done easily, usually without user interaction;
2. no additional equipment is required;
3. eye blinking is a distinctly prominent character of a live face in a photograph of a face, which would be very useful for determining liveliness only from a conventional camera.

To detect a false attack on a person's identification system, eye blink detection is primarily modeled as a logical inference in a conditionally random field structure [14], which allows relationships to be established at a large distance between observations and situations. Eye closure is a specific measurement derived from a flexible enhancement algorithm that is included in the context model to ensure computational efficiency and accuracy. Extensive experiments have been carried out to demonstrate the effectiveness of the proposed approach.

To simplify the output complex and at the same time to increase efficiency, the blinking behavior was simulated in an undirected structure of a conditionally random field, including differential measurement of eye states. One of the advantages of the proposed method is that it allows one to weaken the assumption of the conditional independence of the observed data.

Effective weak classifiers must be trained to calculate eye closure. A total of 1016 images with closed eyes (positive samples) and 1200 images with open eyes (negative samples) were used during the training stage. This does not take into account the difference between the left and right eyes. All samples are scaled to a base resolution of 24×24 pixels. Some positive patterns of closed eyes are shown in Figure 3. 50 weak classifiers were selected to calculate the degree of occlusion.

The center of the left and right eyes is automatically localized for each frame using the facial key point localization system developed by the OMRON Facial Team to evaluate the parameters of the

conditional eye blink model both during the testing phase and during the training phase. For training, images of the eyes are extracted and normalized, the size of which is determined by the distance between the two eyes.

The viability measurement uses three types of detection levels to measure proximity properties. The eye detection rate is the ratio of the number of correctly detected blinks to the total number of flashes in the test data, where the left and right eyes are calculated respectively.

Figure 3. Some of the positive eye-closure samples, note that it includes the wearing of glasses.

As each eye blinks, the left and right eyes open and close. If the blinking of the left or right eye is correctly detected with each blink, it will be possible to detect a living face. Thus, the frequency of detection of two eyes in this case is defined as the ratio of the number of correctly detected blinking movements to the total number of blinking movements in the test data, where the blinking of two eyes is simultaneously calculated as a single blinking movement.

Figure 4. Samples from the blinking database. The first row is for no glasses, the second row is with thin rim glasses, the third row for wearing black frame glasses, and the fourth row with upward view.

Conclusion.

While wearing glasses and bottom-up viewing differently affects the effectiveness of this approach, this approach shows good effectiveness: the average frequency for one eye is 88.8%, and the average frequency for two eyes is 95.7%.

The advantages of the eye blinking method are that there is no need for additional equipment and significant activity in detecting false attacks. While it is concluded that detecting fake attacks by flickering behavior detection is effective based on the above results, it should be noted that this method is only useful when detecting a typed attack, the presence of flickering eyes in the registered user's video frames may make this method less effective.

REFERENCES

1. Sh. Fazilov, S. Radjabov, B. Abdukadirov. The problem of detecting fake access in biometric identification systems. Muhammad al-Xorazmiy avlodlari 3(13):16-23, Tashkent, 2020.
2. T. Choudhury, B. Clarkson, T. Jebara, A. Pentland. Multimodal person recognition using unconstrained audio and video. In 2nd International Conference on Audio-Visual Biometric Person Authentication, Washington D.C, 22–23 March 1999.
3. *Kollreider, K., Fronthaler, H., Bigun, J.* Evaluating Liveness by Face Images and the Structure Tensor // Automatic Identification Advanced Technologies, 2005. – Fourth IEEE Workshop on. 17–18 Oct. – 2005. – P. 75–80.
4. J. Bigun, H. Fronthaler, K. Kollreider. Assuring liveness in biometric identity authentication by real-time face tracking. In CIHSPS2004 - IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, Venice, Italy, 21-22 July, pages 104–112. IEEE Catalog No.04EX815, ISBN 0-7803-8381-8, 2004.
5. F. Smeraldi, J. Bigun. Facial features detection by saccadic exploration of the Gabor decomposition. In International Conference on Image Processing, ICIP-98, Chicago, October 4-7, volume 3, pages 163–167, 1998.
6. F. Smeraldi, J. Bigun. Retinal vision applied to facial features detection and face authentication. Pattern Recognition Letters, 23:463–475, 2002.
7. B. Duc, S. Fischer, J. Bigun. Face authentication with Gabor information on deformable graphs. IEEE Trans. on Image Processing, 8(4):504–516, 1999.
8. T.Choudhury, B.Clarkson, T.Jebara, A.Pentland, Multimodal person recognition using unconstrained audio and video, AVBPA'99, pp.176-181, Washington DC, 1999.
9. K.Kollreider, H.Fronthaler, J.Bigun, Evaluating liveness by face images and the structure tensor, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, pp.75-80, 17-18 Oct. 2005.
10. Robert W. Frischholz, Ulrich Dieckmann, BioID: A Multimodal Biometric Identification System, IEEE Computer, vol. 33, no. 2, pp.64-68, February 2000.
11. Girija Chetty, Michael Wagner, Multi-level Liveness Verification for Face-Voice Biometric Authentication, Biometrics Symposium 2006, Baltimore, Maryland, Sep. 19-21, 2006.
12. R.W.Frischholz, A.Werner, Avoiding Replay-Attacks in a Face Recognition System using Head-Pose Estimation, IEEE International Workshop on Analysis and Modeling of Faces and Gestures (AMFG'03), pp.234- 235, 2003.
13. Kazuo Tsubota, Tear Dynamics, Dry Eye. Progress in Retinal and Eye Research, vol.17, no.4, pp565-596, 1998.
14. J.Lafferty, A.McCallum, F.Pereira, Conditional Random Fields: Probabilistic Models for Segmenting and Labeling Sequence Data. ICML'01, pp.282-289, 2001.