Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, 11-14 July 2010

ANTI-SPOOFING SYSTEM FOR RFID ACCESS CONTROL COMBINING WITH FACE RECOGNTION

BING-ZHONG JING, PATRICK P. K. CHAN, WING W. Y. NG, DANIEL S. YEUNG

Machine Learning and Cybernetics Research Center, School of Computer Science and Engineering, South China University of Technology, 510006, Guangzhou, China
E-MAIL: patrickchan@ieee.org

Abstract:

RFID has been widely adopted in access control as an identity identification technology. This system can be combined with the face recognition technique to avoid the RFID is used by unauthorized people. However, this approach also suffers a drawback that someone may try to deceive the security system by presenting a photo of the real card owner. In this paper, we propose a method ensuring that such kind of spoof can be rejected. After a frontal face has been detected, the facial object will be tracked by optical flow algorithm until a profile is detected. Experimental results show that the proposed mechanism can improve the validity of the access control system effectively.

Keywords:

Face recognition, RFID, adaboost, optical flow

1. Introduction

Radio Frequency Identification (RFID) is a wireless technology which uses radio waves to edit data in an identification chip [1]. The identification chip which is called a RFID tag stores its own ID and a small amount of application data that can be retrieved by RFID readers [2]. RFID technology has been widely adopted in many areas, such as physical distribution, traffic control, automatic tolls collection, product tracking, identification and access control, etc [3].

Among those applications, access control with RFID has drawn much attention nowadays for its advantage that it allows convenience contactless access. Using an RFID key card to open an electronic lock, the first RFID based access control system was invented by Charles Walton in 1973 [4]. However, card based or key based access controls share the same problem that anyone who picked or stolen the card could get access granted to the real owner. With the wide spreading application of RFID, its security threats affect people's daily life more seriously.

Biometrics, which refers to the automatic identification of individual identity by exploiting one's physiological characteristics, such as faces, iris, fingerprints, and gait etc. [5], [6], is another approach for security systems, since biometric data are unique and stable for individuals. Facial data is unique personal privacy information, which is permanently associated with a person [7]. Therefore, by combining the RFID access control system with face recognition technology, this problem can be solved to some extent. However, the common face recognition system does not know whether the face presented in front of the camera is a real human's face or just on a photo. In this paper, we propose an access control system embedded with face recognition subsystem as well as an anti-spoof mechanism which can reject such delusion.

In the following sections, Section 2 describes the current researches on anti-spoofing techniques and adaboost face detection as well as the optical flow algorithm. The security system combining anti-spoofing subsystem is shown in Section 3 and tested in Section 4. Finally, we conclude our work in Section 5.

2. Key Concepts

In this section, we introduce recent development of anti-spoofing technology and provide the brief descriptions of adaboost algorithm and optical flow method for face tracking.

2.1. Recent Development of Anti-spoofing Technology

Several methods have been developed to avert attacks of photograph spoofing. Assuming a photograph would generate a constant depth map while a real human face will produce a varying one, T. Choudhury and B. Clarkson suggested a method of constructing a relative depth map by tracking facial landmarks: the eyes and the mouth [8]. But there is no further research from then. But when the head is still, it is hard to estimate the depth map and the yielding result is very sensitive to the lighting condition and noise

978-1-4244-6527-9/10/$26.00 ©2010 IEEE

produced by the camera. Non-rigid deformation and appearance change is a distinct characteristic of live face comparing to photograph. Some systems designed to evaluate facial expression changes or movements, especially the eye-blinking on a statistical models and the motion of lips [9], [10]. But the reliable performance of these systems needs high quality input video. K. Kollreider detected facial organ motion information by analyzing optical flow field for liveness judgment [11]. But it would be vulnerable to photo blending and translation of photo. There are some approaches involving the speech modality, trying to detect the fake face attacks by exploiting the fused audio-visual features [12], [13]. One of this is M. I. Faraj and J. Bigun's study based on the possibility of recognizing utterances (digits 0-9) from lip motion [14]. But this also requites high resolution videos. Li suggested exploiting Fourier spectrum to classify live faces and fake face attacks and claimed that the high frequency components of the photograph is less than those of live face images [15].

In this work, we focus on web-cam videos of low resolution to propose a robust method of spoofing detection.

2.2. Adaboost Face Detection

Adaboost face detection bases on cascaded detector by Viola and Jones is one of the best detect methods currently available in terms of speed and reliability [16]. Weak classifiers are constructed by Haar-like features which shown in Figure 1 are easy to compute.

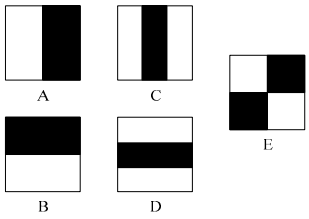


Figure 1. Prototypes of Haar-like features. White areas have positive weights and black areas have negative.

The integral image at location (x, y) of a given image can be represented as

$$S(x,y)=\sum_{x'\le x,y'\le y} i(x',y') \tag{1}$$

where $i(x,y)$ is the original image. And the integral image can be calculated in one pass over the original image by using the following pair of recurrences.

$$ii(x,y)=ii(x,y-1)+i(x,y) \tag{2}$$

$$S(x,y)=S(x-1,y)+ii(x,y) \tag{3}$$

Adaboost algorithm is one kind of self-adaptation boosting algorithms. By using this algorithm, weak classifiers can be combined into a strong classifier. The basic idea of adaboost algorithm is that when the classifier distributes certain sample correctly, the weight of these samples reduces; when a misclassification occurs, these samples' weight increase. Therefore, the algorithm is pushed to focus these difficult training samples in the following training circulations and merges the weak rules to be a strong one finally.

2.3. Optical Flow

Optical Flow is the pattern of apparent motion of objects, surfaces, and edges in a visual scene caused by the relative movement between an observer and the scene [17], [18], [19], which can be used as a technology of object tracking and motion segmentation.

Sequences of adjacent images allow the estimation of motion which the optical flow methods are trying to calculate by partial derivatives with respect to the spatial and temporal coordinates. Assume that two consecutive images are taken at times t and $t+dt$ at every voxel position.

One of the assumptions that optical flow methods are rested on is brightness constancy, which can be given:

$$I(x,y,t)=I(x+dx,y+dy,t+dt) \tag{4}$$

The second assumption is temporal persistence. By this, the image constraint at $I(x,y,t)$ with Taylor series can be:

$$\begin{aligned} &I(x+dx,y+dy,t+dt)\\ &=I(x,y,t)+\frac{\partial I}{\partial x}dx+\frac{\partial I}{\partial y}dy+\frac{\partial I}{\partial t}dt+o(dx,dy,dt) \end{aligned} \tag{5}$$

According to (4) and (5), it follows that:

$$\frac{\partial I}{\partial x}dx+\frac{\partial I}{\partial y}dy+\frac{\partial I}{\partial t}dt=0 \tag{6}$$

or

$$\frac{\partial I}{\partial x}\frac{dx}{dt}+\frac{\partial I}{\partial y}\frac{dy}{dt}+\frac{\partial I}{\partial t}\frac{dt}{dt}=0 \tag{7}$$

which the same as:

$$\frac{\partial I}{\partial x}V_x+\frac{\partial I}{\partial y}V_y+\frac{\partial I}{\partial t}=0 \tag{8}$$

where V_x, V_y are the x and y components of the velocity (optical flow of $I(x,y,t)$) and $\frac{\partial I}{\partial x}$, $\frac{\partial I}{\partial y}$ and $\frac{\partial I}{\partial t}$ are the derivatives of the image at (x,y,t) in the corresponding directions. Thus we have:

$$I_xV_x+I_yV_y=-I_t \tag{9}$$

This raises a problem that there are two unknowns for

any given pixel for this single equation, which is known as the aperture problem of the optical flow algorithms. To solve this problem, additional constraints are needed. Different constraints lead to different optical flow algorithms.

Some popular methods include Block-based methods, which minimize sum of squared differences or sum of absolute differences, or maximize normalized cross-correlation; Lucas-Kanade method, a method regards image patches and an affine model for the flow field; and Horn-Schunck method based on global smoothness constraint [20], [21], [22] and so on.

Optical flow methods can be divided to two groups: dense optical flow and sparse one, which is more practical than the previous one because of lower computational cost. Lucas-Kanade method is one widely-used sparse optical flow which is used in the face tracking module in this work.

3. Description of the Anti-spoofing System

The procedure of spoofing detection of the proposed anti-spoofing system and how it combines with the current RFID access control system will be described in this section.

3.1. Steps of the Anti-spoofing System

Since a human face is rigid three-dimension object, it has discernible difference between observing from the front and the lateral. On contrast, a photo of human face cannot have a similar property due to its nature of a plane. The anti-spoofing system detects human faces in the video sequences captured by its camera when a user approaches to the access control system and passes the RFID identification. The image of the user will be capture in order to identify whether the user is owner of the RFID card. Before this procedure, the system has to decide whether the image is captured from a live human, or just a photo.

Once the system detects a face image, it has the location of that face in the same time. Also, the current image is a frontal image. In order to get the user's profile, the system will require the user to turn right (or left). When the user is turning his/her face, the system will keep tracking the location of the face, until the profile is detected. Then the anti-spoof test is passed.

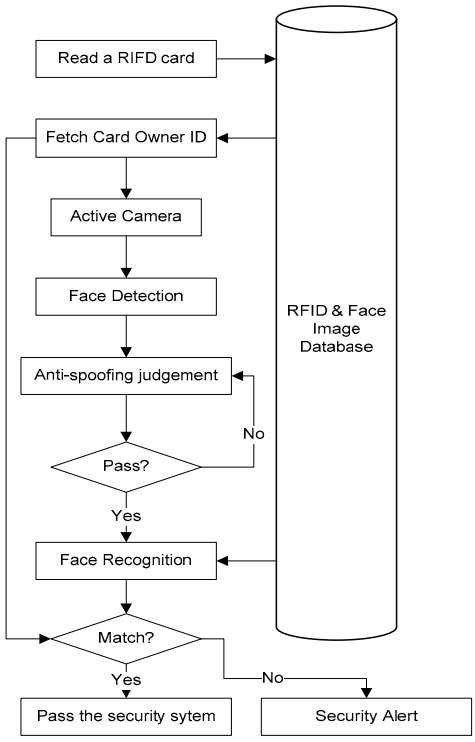


Figure 2. Flow chart of the security system

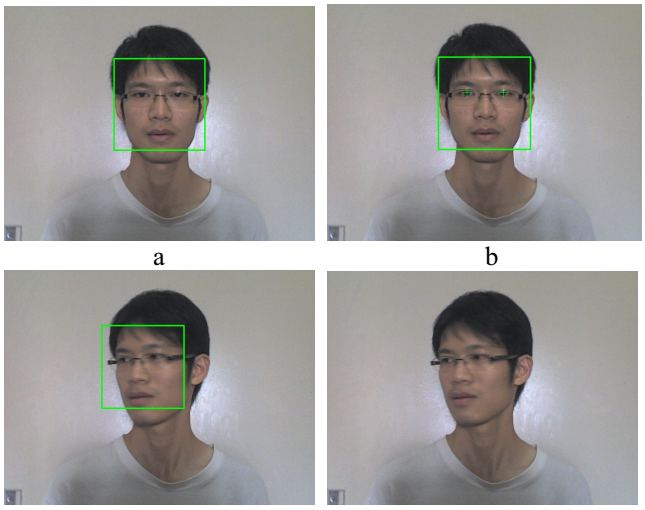
3.2. Frontal Face Detection

The security system is shooting video after the system retrieved data of an RFID card and each frame of the video passes to the face detection module. Once someone is coming towards the system, the face will be detected and located by the face detection module.

The adaboost algorithm takes rectangle feature, a kind of simple feature which can describe eyes and nose, as characteristic vector of face to construct a classifier, is employed to detect human faces. However, under some unusual circumstances, a non-faced object which has some similar patterns as a face would be recognized as a face incorrectly. Therefore, to solve this problem, a multi-feature detector, which combines by a face detector and two eyes detectors, is used.

This multi-feature detector has a side-effect which shows in Figure 3. In common cases, we wish the detector is highly robust. Therefore, the detector must be designed to tolerate a relative wide range of head rotation. However, if we request a more stable result of face recognition, we need a stricter angle range of face images. The multi-feature detector can meet this requirement. And this will also benefit the anti-spoofing mechanism because this will enlarge the disparity between the frontal face and the

profile.



a b c d

Figure 3. Face detection by adaboost algorithm.
a. b. A precise frontal face can be detected by both common adaboost face detector and multi-feature face detector; c. and d. A lenient frontal face can pass the common face detector but not the multi-feature one.

3.3. Face Tracking

After taking a frontal face image and before capturing a profile image, the system must track the detected object, in order to assure these two images are attained from the same person. By matching feature points of two consecutive frames, optical flow algorithm can estimate the velocity of the tracking object (Figure 4). Admittedly, optical flow algorithm is computation-consuming. But the face location is the only region the algorithm needs to run and the optical flow algorithm we chose is LK algorithm, a sparse optical flow. As a result, the complication and tracking effect of sparse optical flow based on LK algorithm are satisfying. Although when the object rapidly moves, the stability of LK algorithm will become bad [18], [24], this decrease precision can be utilized in our system as a signal of stop tracking, because in our assumption, a normal behavior of human's head is not moving or rotating dramatically. Every pair of points matched between two sequential frames can be regarded as a vector. In a successful tracking, the variance of these vectors generated by optical flow should be low, for nearly all feature points in the previous frame will move in a similar velocity to the next frame. When the variance is high, which may be affected by dramatic move of user or sudden change of lighting condition, the tracking is regarded as fail and the system will inform the user to redo this anti-spoofing procedure.

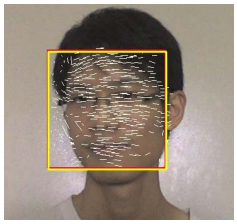
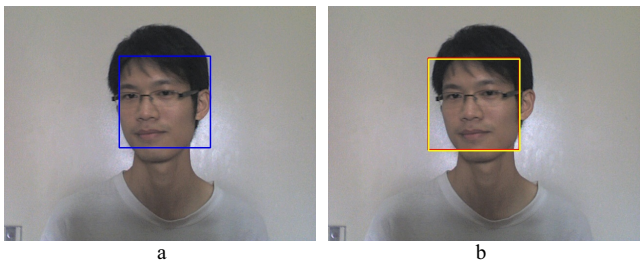


Figure 4. An example of optical flow tracking

3.4. Profile Detection



a b

Figure 5. a. The face image is detected as a profile by a single profile detector; b. The face image is detected as a frontal face by a two-pass detector.

The process of profile detection is identical with the frontal one. Because of the relatively wide range of angle tolerance ability of the detector we mentioned in section 3.2 and a stricter profile image we are aiming at, we detect profile in two passes: firstly, the image is passed to the frontal face detector to decide whether it is a frontal face; if the image was rejected by the frontal face detector, the next step is passing the image to the profile detector. If there are 3 frames passed the profile detector in 5 consecutive frames, the profile of the user is detected which means the user passes the anti-spoofing system; else, tracking image contains neither frontal face nor profile one, face tracking will be ceased and the user needs to try to pass the anti-spoofing system once again. Figure 5 shows the difference between a single profile detector and the two-pass method. The face image of Figure 5 should not be classified as a profile according to our commonsense. Therefore, the two-pass detector has classified the face images as a frontal face which is more precise than the single method. Even though the image has to pass two face detectors, a frontal one and a profile one respectively, the computational cost of this two-pass method is still satisfied because only the tracking area needs to be detected.

4. Experiments

In this section, we describe experimental setup in Section 4.1 and analysis the experimental results in Section

4.1. Experimental Setup

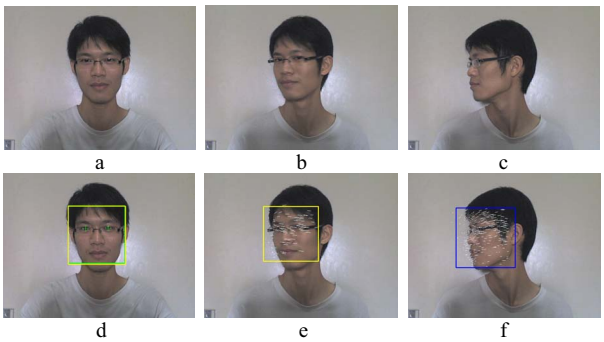


Figure 6. One sample of the "real face sequences"
a. b. c. Three frames of a "real face sequences" sample;
d. Frontal face is detected; e. Tracking the detected face; f. Profile is detected.

Figure 7. Five subcategories of "spoofing sequences"
a. The photo used for spoofing test; b. Translation; c. Swing; d. Bent; e. Bent and swing, a photographic mask; f. g. and h. Shuffle.

We conduct our experiment on 2 groups of sample data. For the first group, the "real face sequences", we collect 100 samples from 4 people. Each sample contain a entire procedure of turning face from frontal to profile, in the duration of 1 second to 3 seconds. Figure 6 shows one of these samples.

For the second group, the "spoofing sequences", we divide it into five subcategories, each of which has 25 samples, respecting a different kind of spoof. The first subcategory is translation. We translate portraits in front of the camera horizontally and vertically. The second subcategory is swing. Photos are swinging in order to simulate someone is trying to mislead the anti-spoofing system that there is a real face rotating. The third subcategory is bending, in which photos are bent in order to generating some three-dimension properties. Combining the bending and swinging is the fourth subcategory, on the purpose of imitating the case that someone is wearing a photographic mask. The last subcategory is shuffling. Someone may want to cheat the system by stacking two images. The first one is a frontal face image and the second one is a profile. Quickly removing the frontal one and exposing the profile one in front of the camera, the trickster tries to pass the frontal face and profile detectors. These five subcategories are shown in Figure 7.

4.2. Experimental Results

As it has been shown in Table 1, all of the testing cases pass the frontal face detection. 99 cases of the "real face sequences" pass the tracking procedure and profile detection while one fails in tracking due to the too fast rotation of head, which will give rise to inform the user to restart the anti-spoofing detection. Most of the cases in "spoofing sequences" cannot pass the tracking module, especially those cases of bent and swing as well as shuffle. Because most of these motions can easily generate high variance of the optical flow and is rejected by the tracking module. Even though 20 cases pass the tracking module, they still cannot pass the profile detection. On average, 99% of the real face cases can get authorization while 100% of the spoofing cases are rejected by the anti-spoofing system, which proves our anti-spoofing system is reliable.

TABLE 1. TESTING RESULTS

		Frontal face detected	Tracking	Profile detected
"Real face sequences"		100	99	99
"Spoofing sequences"	Translation	25	11	0
	Swing	25	5	0
	Bent	25	4	0
	Bent & swing	25	0	0
	Shuffle	25	0	0

5. Conclusions

In this paper, we illustrate an anti-spoofing mechanism for an access control system constructed by a RFID subsystem and a face recognition function in order to enhance the security level. This mechanism utilizes the three-dimension attribute of human face by detecting the frontal faces and profiles. The experimental results show that this anti-spoofing technique is reliable. In future, we

will improve the accuracy of the system by estimating the angle of the head rotation, instead of only detecting frontal face and profile.

Acknowledgements

This work is supported by the Fundamental Research Funds for the Central Universities 2009ZZ0050 and a 985 project, South China University of Technology.

References

[1] Hossain M.M., Prybutok V.R., "Consumer Acceptance of RFID Technology:An Exploratory Study", IEEE Transactions on Engineering Management, Vol 55, Issue 2, pp. 316 – 328, May 2008.

[2] Weinstein R., "RFID: a technical overview and its application to the enterprise", IT Professional, Vol 7, Issue 3, pp. 27 – 33,May-June 2005

[3] Landt J., "The history of RFID", Potentials IEEE,Vol 24, Issue 4, pp. 8–11,Oct.-Nov. 2005

[4] Rieback M.R., Crispo B., Tanenbaum A.S., "The Evolution of RFID Security", Pervasive Computing, Vol 5, No.1, pp.62 – 69, Jan 2006.

[5] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using kernel direct discriminant analysis algorithms," IEEE Trans. Neural Netw., vol. 14, no. 1, pp. 117–126, Jan. 2003.

[6] H. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "MPCA: Multilinear principal component analysis of tensor objects," IEEE Trans. Neural Netw., vol. 19, no. 1, pp. 18–39, Jan. 2008.

[7] Biometric Systems Technology, Design and Performance Evaluation, J. Wayman, A. Jain, D. Maltoni, and D. Maio, eds. Springer, 2005.

[8] T. Choudhury, B. Clarkson, T. Jebara, and A. Pentland. Multimodal Person Recognition using Unconstrained Audio and Video. In 2nd AVBPA, Washington D.C., 22–23 March 1999. 1, 2

[9] L. Sun, G. Pan, and Z. Wu, "Blinking-based live face detection using conditional random fields," International Conference on Biometrics, Aug. 2007, Lecture Notes in Computer Science, vol. 4261, 2007, pp. 252-260.

[10] H.K. Jee, S.U. Jung, and J.H. Yoo, "Liveness detection for embedded face recognition system," International Journal of Biomedical Sciences, vol. 1, no. 4, 2006, pp. 235–238.

[11] K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating liveness by face images and the structure tensor," Fourth IEEE Workshop on Automatic Identification Advanced Technologies, Oct. 2005, pp. 75-80.

[12] G. Chetty and M. Wagner. Liveness Verification in Audio-Video Speaker Authentication. In 10th Australian Int. Conference on Speech Science and Technology, p. 358–363, Sydney, Australia, December 8-10, 2004. 2

[13] M. I. Faraj and J. Bigun. Audio visual person authentication using lip-motion from orientation maps. Pattern Recognition Letters, 28(11): 1368–1382, 2007. 2, 3

[14] M. I. Faraj and J. Bigun. Lip biometrics for digit recognition. In Int. Conference on Computer Analysis of Images and Patterns, volume 4673 of LNCS, p. 360–366, 2007. 1, 2

[15] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of Fourier spectra. In Biometric Technology for Human Identification, p. 296–303. SPIE Volume: 5404, August 2004. 2

[16] P. Viola and M. J. Jones, "Robust Real-Time Face Detection," Int'l J. Computer Vision, vol. 57, no. 2, pp. 137-154, 2004.

[17] B. Lucas, and T. Kanade. "An iterative image registration technique with an application to stereo vision"[C]. In: Hayes PJ, ed. Proc. of the 7th Int'l Joint Conf. on Artificial Intelligence. Vancouver: Morgan Kaufmann Publishers, 1981, pp.674-679.

[18] C. Tomasi, and T. Kanade. "Detection and tracking of point features"[R]. Pittsburgh, Carnegie Mellon University, CMU CS-91-132, 1991.

[19] J. B. Shi, and C. Tomasi. "Good features to track"[C]. Proc. IEEE Comput. Soc. Conf. Comput. Vision and Pattern Recogn., 1994, pp.593-600.

[20] D. J. FLEET and A. D. JEPSON, "Computation of Component Image Velocity from Local Phase Information," Int. Journal of Computer Vision, vol. 5, no. 1, pp. 77-104, 1990.

[21] J. L. Barron and D. J. Fleet, "Performance of Optical Flow Techniques," Int. Journal on Computer Vision, vol.12, no.1, pp. 43-77, 1994.

[22] T. Gautama and M. M. V. Hulle, "A Phase-Based Approach to the Estimation of the Optical Flow Field Using Spatial Filtering," IEEE TRANS ON NEURAL NETWORKS, Vol. 13,No. 5, pp. 1127-1136, SEPTEMBER 2002

[23] T. Amiaza, E. Lubetzkyb and N. Kiryatia, "Coarse to over-fine optical flow estimation," Pattern Recognition, vol.40, no.9, pp. 2496-2503, 2007.