Poster: Real-Time Continuous Iris Recognition for Authentication Using an Eye Tracker

Kenrick Mock
University of Alaska Anchorage
3211 Providence Dr.
Anchorage, AK 99508, USA
1-907-786-1956
kjmock@uaa.alaska.edu

Bogdan Hoanca
University of Alaska Anchorage
3211 Providence Dr.
Anchorage, AK 99508, USA
1-907-786-4140
bhoanca@uaa.alaska.edu

Justin Weaver
University of Alaska Anchorage
Anchorage, AK 99508, USA
piranther@gmail.com

Mikal Milton
University of Alaska Anchorage
Anchorage, AK 99508, USA
mmilton1@alaska.edu

ABSTRACT

The majority of today's authentication systems, including password and fingerprint scanners, are based on one-time, static authentication methods. A continuous, real-time authentication system opens up the possibility for greater security, but such a system must be unobtrusive and secure. In this work we studied whether a commercial eye tracker can be used for unobtrusive, continuous, real-time user authentication via iris recognition. In a user study, all 37 participants could be authenticated with 11% equal error rate (EER). For 14 of the 37 users, iris occlusion was sufficiently small to authenticate with 9% EER. When classified using a k-nearest neighbors algorithm and only the right iris, the same data set allowed 100% accuracy for k = 3. Although these error rates are too high for standalone use, iris recognition via an eye tracker might enable real-time continuous authentication when combined with other more reliable authentication means (e.g., a password). As eye trackers become widely available their capabilities for multiple factor, continuous authentication will become compelling.

Categories and Subject Descriptors

D.4.6 Security and Protection, Authentication; K.4.2 Social Issues, Abuse and crime involving computers; K.6.5 Security and Protection, Authentication (D.4.6, K.4.2): Authentication;

General Terms

Security

Keywords

Eye Tracking, Iris Recognition, Authentication

1. INTRODUCTION

There is considerable interest in biometrics-based authentication because of several compelling advantages. Biometrics can provide sufficient information entropy for good security. In particular, human iris patterns are unique even for identical twins [1]. Because biometric traits are part of the user's body, they are not typically lost or forgotten, although they can be stolen or duplicated [2]. Finally, biometrics, particularly those that are related to subconscious physical functions of the human body may even have the ability to support continuous authentication [3]. This is because such biometrics can be sampled automatically and unobtrusively by the authentication system, as they do not require a deliberate action on behalf of the user.

Recent advances in the capabilities of commercial remote eye tracking devices and decreases in their cost may lead to their use for user-friendly, secure, continuous biometric authentication. If they become widely available, it would be natural to attempt to use eye trackers for authentication purposes. Eye trackers could support multi-factor biometrics, combining iris recognition with the biometrics of eye gaze movement, and possibly even with the traditional password [4]. By using a combination of biometrics, such as gaze tracking and iris recognition, eye trackers may be able to prevent the fake iris attack [2].

2. EYE TRACKING FOR USER AUTHENTICATION

Continuous authentication via iris recognition using eye trackers is a topic at the intersection of three fields that have had relatively little overlap.

Continuous authentication is a relatively new concept. Keystroke dynamics, first proposed by Spillane [5], was the first technique that could be used for continuous authentication [6]. More recently, research on continuous authentication is based on multiple biometric factors in addition to keyboard dynamics, including: mouse dynamics [7], ECG data [3], posture and chair dynamics [8], face recognition [9] and even garment recognition [10]. All of these techniques have relatively large error rates. A survey of keyboard dynamics found that even the best machine learning algorithms could only achieve around 9% equal error rates [11]. As such, they are not candidates for standalone authentication but are intended for use in combination with a more accurate and established means of authentication [12].

The second field, iris recognition, has had a much longer history. Discriminating between individuals based on differences in iris patterns was first proposed in 1936, but the procedure was patented only in 1987. Dr. John Daugman played a key role in developing an algorithm for iris recognition, resulting in a patent in 1994. The IrisCodes algorithm he developed is still widely used today for iris recognition. Iris recognition is fairly mature, and it is among the strongest biometric authentication technologies with false positive rates around a few in a billion [1].

CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA.
ACM 978-1-4503-1651-4/12/10.

Thirdly, eye tracking technologies were first developed in the 1970's, but only became mainstream around the year 2000 [13].

Although iris recognition using an eye tracker may seem as a natural extension of the camera functionality in the device, the feasibility of such a use has not been demonstrated yet. This is due to several practical limitations of eye trackers as iris recognition devices. Not surprisingly, eye trackers are optimized for eye tracking, and the iris images they acquire are not well suited for iris recognition. Specifically, eye trackers have a relatively wide field of view to allow continued tracking even when the user moves his or her head. This leads to iris images that are small and provide lower resolution than iris images from an iris scanner, in which the iris fills most of the field of view. Moreover, the eye tracker must be able to handle fast motions, blinks, and other actions that reduce image quality.

Despite these challenges in acquiring quality iris data, using an eye tracker for iris recognition is less intrusive for the user than using an iris recognition camera, and, as shown below, it works.

3. METHODOLOGY

The device we used is an EyeTech TM3 eye tracker [14]. The eye tracker camera can capture images with 960x1280 pixel resolution, but for efficiency, it only returns the image area around the eyes, a 420x1280 pixels box where the iris radius is 40-60 pixels, depending on the user's anatomy and distance from the eye tracker. A sample image is included in Figure 1. Most, but not all eye tracking manufacturers make available the eye image, but all use infrared cameras which capture similar images.

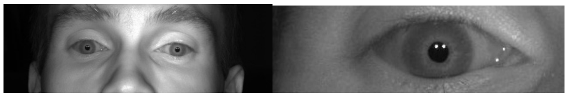

Figure 1. Eye tracker image showing two glint spots in each eye a) entire image b) magnified iris image.

The eye tracker uses two infrared LEDs operating at an 880 nm wavelength to generate two bright-point reflections (glint spots) on the surface of the eye. The eye tracker returns several parameters along with the eye image: pupil position and diameter, as well as glint positions (two glint points per eye).

We used existing software for iris recognition [15]. The original software, intended for high-resolution images with 160-300 pixels for the iris diameter, took 15-30 minutes per iris. Using the 2-4x lower resolution images from the eye tracker achieves a speedup of about 4-16x. A further source of speedup is from the way we locate the iris and pupil using the glint spots. Finally, instead of accurately detecting the iris boundary, we used an iris annulus of fixed width, which requires minimal image processing, but includes the distinctive zigzag collarette region of the iris [16]. The source code is otherwise unmodified. Overall, these changes allowed us to reduce the processing time to about 2 seconds per sample, which allows near real-time iris recognition.

The iris comparison is based on Daugman's algorithm [1]. To compare two irises, the algorithm computes iris templates, masking out areas that do not contain valid iris data (glare, eyelids, eyelashes etc.) and then performs a bitwise comparison of the unmasked template regions, calculating the Hamming distance. A distance of 0 indicates a perfect match, while a distance of 0.5 indicates a totally random matching of bits. A distance of 1 corresponds to one iris being a negative image of the other. To decide whether two irises match, we use a threshold distance: samples with distance below threshold are deemed from the same user, while samples with distances exceeding the threshold are assumed to be from different users.

There are three parameters to be determined in the iris recognition model: the Hamming threshold and the angular and radial sampling rates for the iris image. For example, a 20x60 iris is the result of using 20 samples in the radial dimension and 60 samples around the contour (in the angular dimension). To determine the parameters, we ran the iris recognition software on samples from a database of user iris images [17], with data from 64 users (three samples per user, both eyes) in 768x576x24 color PNG files. We only used the iris information from the red channel in the color images [18]. We also used the database to confirm that the low resolution of the eye tracker was not a major impediment.

The IRB-approved user study involved 37 users. The eye tracker was connected to a 13" laptop computer. Participants wearing glasses were requested to remove them, to eliminate glare. The experimenter used a secondary monitor to view live video from the camera to ensure that the eye tracker was focused on the participant's eyes. Participants were asked to search for images via a Google Images search. Once the user begun searching, the experimenter would start the recording of iris images. The program recorded two runs, each of 25 valid sample images of the participants' eyes (rejecting as invalid those samples where the eye was fully closed or the iris could not be located). Some of the valid samples included an iris image but had up to 80% of the iris occluded (e.g. for a blink in progress). Each run took 60-90 seconds.

4. EXPERIMENTS, RESULTS, AND DISCUSSION – USER STUDY OF IRIS RECOGNITION

The participant's irises were sampled at a resolution of 20x60 (radial and angular sampling rates), and the images from the eye tracker had iris diameters close to 100 pixels. For each run, the software located the 5 samples with the smallest total Hamming distance (minimum sum of the distances from each sample to all of the other 24). These 5 samples form the core of the run and are treated as reference images for the iris.

In the best-of-batch authentication approach we collected the closest 5 samples from a user's batch of samples for comparison to a core. This approach makes the process more robust to errors in individual samples. For this scenario, the equal error rate (EER) is when the acceptance rate equals the error rate and is 11% for a threshold of 0.235. Figure 2 graphs the true positive vs. the false positive rate.

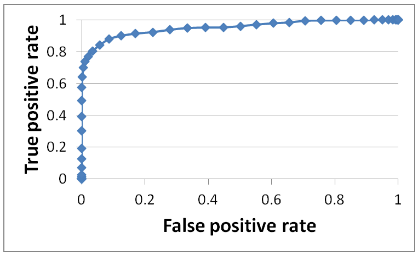

Figure 2. True Positive vs. False Positive Rate

If we require iris occlusion to be below a certain level (30%) then only 14 out of the 37 users in the study meet this criteria. For these users the best performance is an EER of 9%.

We also used a k-nearest neighbors (KNN) machine learning algorithm to compare a core iris sample against the core samples for all users. A test core should match only the core of the same eye taken from different samples. For k=3 and using only the right eyes, the accuracy of the classification is 100%. The realistic metric of the Manhattan distance is able to classify correctly 96.4% of the cores, for k=3.

Table 1. Accuracy of KNN for core-level classification for open eyes.

Metric	knn1	knn3	knn5	knn7	knn9
Left eye	85.7%	82.1%	85.7%	78.6%	67.9%
Right eye	96.4%	100.0%	92.9%	92.9%	82.1%
Manhattan	92.9%	96.4%	92.9%	92.9%	92.9%

5. CONCLUSION

Results from a user study show that a commercial eye tracker can be used with good performance for user authentication via iris recognition. Eye trackers have resolution 2-5x lower than that of dedicated iris recognition systems, and users may move freely while using the eye tracker, which raises considerable challenges in gathering quality iris images.

In a live user study, we were able to discriminate among users with 11% equal error rate. For 14 of the 37 users in the study the iris occlusion was small enough for all samples to allow 9% EER. While consistent with other continuous authentication schemes [11], this error rate is much too high to be used as the sole authentication means, but could be useful when combined with other more accurate techniques. Eye trackers can also be used for user identification. Under the best scenario, selecting only samples of open eyes, and comparing core-to-core may allow classification accuracy close to 100%. Further work will need to consider the effects of lighting conditions, user fatigue (and its effects on iris occlusion), and other long-term factors.

Ultimately, when eye trackers become widely available as user interface devices, they might offer the additional benefit of real-time, continuous user authentication, perhaps replacing traditional passwords or as multifactor authentication systems that combine passwords and eye biometrics. While it is unlikely that the authentication capabilities of eye trackers will lead to their widespread deployment, if eye trackers are already available for other applications, their capabilities for real-time continuous authentication should not be overlooked.

6. ACKNOWLEDGEMENTS

We wish to thank the UAA University Honors College and College of Arts & Sciences for funding part of this research.

7. REFERENCES

[1] Daugman, J. (n.d.). How Iris Recognition Works. Retrieved April 14, 2010, from http://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf

[2] Thalheim, L., Krissler, J. and Zielger, P.-M. (2002). Body check: biometric access protection devices and their programs put to the test, translated by Robert Smith, c't Magazine 11(2002): 114, no longer available online, but cited in Technology Assessment, Using Biometrics for Border Security (GAO-03-174).

[3] Biel, L.; Pettersson, O.; Philipson, L.; Wide, P.; (2001). ECG analysis: a new approach in human identification. Instrumentation and Measurement, IEEE Transactions on , vol.50, no.3, pp.808-812, Jun 2001.

[4] Hoanca, B., & Mock, K. J. (2006). Secure graphical password system for high traffic public areas. Eye Tracking Research and Applications (p. 35). San Diego: ACM.

[5] Spillane, R. (1975). Keyboard apparatus for personal identification. IBM Technical Disclosure Bulletin, 17, 3346.

[6] Denning, D., Neumann, P., & Parker, D.B. (1987). Social aspects of computer security. In Proceedings of the 10th National Computer Security Conference.

[7] Jorgensen, Z. & Yu, T. (2011). `On Mouse Dynamics as a Behavioral Biometric for Authentication. Proceedings of the Sixth ACM Symposium on Information, Computer, and Communications Security.

[8] Slivovsky, L. & Tan, H. (2000). A real-time static posture classification system. Proceedings of the Ninth International Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, American Society of Mechanical Engineers Dynamic Systems and Control Division, Vol. 69-2, S. S. Nair (Ed.), (p. 1049-1056), Orlando, FL.

[9] Bledsoe, W. (1964). The model method in facial recognition. Technical report PRI 15, Panoramic Research, Inc., Palo Alto, CA.

[10] Dantcheva, A. & Dugelay, J. L. (2011). Frontal-to-side face re-identification based on hair, skin and clothes patches. 2011 8th IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS). Klagenfurt, Germany.

[11] Killourhy, K. & Maxion, R. (2009). Comparing Anomaly-Detection Algorithms for Keystroke Dynamics." In International Conference on Dependable Systems & Networks (DSN-09), (p. 125-134), Estoril, Lisbon, Portugal, July 2009. IEEE Computer Society Press, Los Alamitos, CA.

[12] Xiao, Q. (2005). Security issues in biometric authentication, Information Assurance Workshop, IAW 2005 (p. 8-13).

[13] Duchowski, A. (2002). A Breadth-First Survey of Eye-Tracking Applications. Behavior Research Methods Instruments and Computers, 34, 4, (p. 455-470).

[14] TM3 - EyeTech Digital Systems. (n.d.). Retrieved from EyeTech Digital Systems-Eye Tracking Technology Solutions: http://www.eyetechds.com/research/tm3-qc

[15] Masek, L. (2003). Iris Recognition. Retrieved from http://www.csse.uwa.edu.au/~pk/studentprojects/libor/

[16] He, X. & Shi, P. (2005). An Efficient Iris Segmentation Method for Recognition. Third International Conference on Advances in Pattern Recognition. Bath, UK.

[17] Dobeš, M., & Machala, L. (n.d.). Retrieved 4/30/2012 from Iris Database: http://phoenix.inf.upol.cz/iris/

[18] Dobeš M., Machala L., Tichavský P., Pospíšil J. (2004). Human Eye Iris Recognition Using the Mutual Information. Optik Journal for Light and Electron Optics, 115(9), p.399-405, Elsevier, ISSN 0030-4026.