A Study on Gaze-Controlled PIN Input with Biometric Data Analysis

Virginio Cantoni
Department of Electrical, Computer and Biomedical Engineering, University of Pavia
Via A. Ferrata 5 – 27100 – Pavia – Italy
virginio.cantoni@unipv.it

Tomas Lacovara
Department of Electrical, Computer and Biomedical Engineering, University of Pavia
Via A. Ferrata 5 – 27100 – Pavia – Italy
tomas.lacovara01@universitadipavia.it

Marco Porta
Department of Electrical, Computer and Biomedical Engineering, University of Pavia
Via A. Ferrata 5 – 27100 – Pavia – Italy
marco.porta@unipv.it

Haochen Wang
Department of Electrical, Computer and Biomedical Engineering, University of Pavia
Via A. Ferrata 5 – 27100 – Pavia – Italy
haochen.wang01@universitadipavia.it

ABSTRACT

Common methods for checking a user's identity (e.g., passwords) do not consider personal elements characterizing a subject. In this paper, we present a study on the exploitation of eye information for biometric purposes. Data is acquired when the user enters a PIN (Personal Identification Number) through the gaze, by means of an on-screen virtual numeric keypad. Both identification (i.e., the recognition of a subject in a group) and verification (i.e., the confirmation of an individual's claimed identity) are considered. Using machine learning algorithms, we performed two kinds of analysis, one for the entire PIN sequence and one for each key (i.e., digit) in the series. Overall, the achieved results can be considered satisfying in the context of "soft biometrics", which does not require very high success rates and is meant to be used along with other identification or verification techniques—in our case, the PIN itself—as an additional security level.

CCS CONCEPTS

• **Security and privacy** → **Biometrics** • *Security and privacy* → *Multi-factor authentication* • *Human-centered computing* → *Interaction paradigms* • *Human-centered computing* → *Interaction devices*

CompSysTech'18, September 13–14, 2018, Ruse, Bulgaria

ACM ISBN 978-1-4503-6425-6/18/09…$15.00
https://doi.org/10.1145/3274005.3274029

KEYWORDS

Eye tracking, gaze communication, soft biometrics

ACM Reference format:

V. Cantoni, T. Lacovara, M. Porta, H. Wang. 2018. A Study on Gaze-Controlled PIN Input with Biometric Data Analysis. In *Proceedings of CompSysTech 2018: 19th International Conference on Computer Systems and Technologies, September 13–14, 2018, Ruse, Bulgaria*, 5 pages.
https://doi.org/10.1145/3274005.3274029

1 INTRODUCTION

Biometrics means measuring human characteristics to distinguish individuals or groups of individuals. In particular, biometric traits can be both physiological (like fingerprints and iris) or behavioral (like eye movements) [1]. Indeed, human beings develop unique behaviors depending on their social, cultural, and psychological experiences [2].

Many studies on behavioral biometrics have been carried out to date, as this kind of "soft biometrics" can be a useful additional security measure, to be combined with traditional solutions (such as PIN or password).

Eye-related biometric features are typically physiological, like those involving iris, conjunctival vasculature, and periocular area [3]. However, behavioral gaze-based biometrics has received increasing attention in recent years [4]. In this paper, we consider the use of a conventional authentication method—typing a PIN—with the enhancement of gaze biometric data. The PIN is entered by means of an eye tracker through a virtual keypad displayed on a screen. The idea is that gaze data can be exploited to additionally check the identity of the user. For example, the PIN may have been stolen: by detecting that the way the PIN is entered is different from what expected, the system may require a further verification (e.g., by also asking the user to enter a password).

The experiments implemented to test the system consisted in entering randomly generated six-digit PINs. The obtained eye data was then analyzed for both the whole PIN sequence and for each digit in the succession. Machine learning algorithms were exploited to implement the identification and verification processes.

2 RELATED WORK

The use of eye trackers in identification and verification tasks dates back to more than a decade ago, when Kasprowski and Ober [5] proposed the use of eye movements for biometrics.

In this section, representative studies are subdivided into five groups, according to the considered features, namely *PIN/password*, *fixation/scan paths*, *eye velocity*, *pupil size*, and *oculomotor characteristics*.

For the first category, Maeder et al. [6] proposed an authentication system in which the user had to look at six predefined points within a 3x3 grid. Kumar et al. [7] presented a system in which the keys of a virtual keyboard could be selected with a keypress on the physical keyboard or via dwell time. Dunphy et al. [8] proposed *Passfaces*, where faces were used instead of digits. Cymek et al. [9] studied the possibility of using smooth pursuit to enter passwords. Unlike our study, all these works considered only the sequence of observation points, without any analysis of eye features.

For the general class of methods based on fixation and scan path analysis, Silver and Biggs [10] compared keystroke biometrics to eye tracking biometrics. Holland and Komogortsev [11] tested the possibility of using reading scans to identify users. Galdi et al. [12] analyzed the fixations on different areas of face images. In an extension of this study, Cantoni et al. [13] associated weights to arcs connecting face areas. George and Routray [14] used several fixation and saccade features to identify users.

As regards eye velocity, Bednarik et al. [15] were pioneers in using eye speed and acceleration as biometric traits. Kinnunen et al. [16] described eye movements by transforming velocity into a normalized histogram over the travelled eye angles. Rigas et al. [17], using a jumping point as a stimulus, used the Wald-Wolfowitz test to determine the distribution of features like saccadic velocity. Juhola et al. [18] considered a jumping point in a black bar as a stimulus to measure saccadic movements for identification with a high (400 Hz) and low (30 Hz) frequency eye tracker. Starting from this experiment, Zhang et al. [19] performed a similar investigation using only a low sampling rate device. Srivastava et al. [20] proposed a method based on eye velocity, eye position and eye difference, using a jumping point as a stimulus.

Pupil size was exploited in the already cited work by Bednarik et al. [15]. Nugrahaningsih and Porta [21] used a simple black cross at the center of a white screen as a stimulus. Eberz et al. [22] presented a study where testers took part in three experiments with different kinds of instructions.

For the last category—oculomotor features—Kasprowski and Ober [5] considered the eye movements of testers following a jumping point. Komogortsev et al. [23] transformed saccadic movements into Oculomotor Plant Characteristics (OPC). Komogortsev et al. [24] also studied the possibility of employing a multimodal biometric approach involving OPC, complex eye movements, and the iris structure.

3 EXPERIMENTS

Our dataset was built involving 45 volunteer testers (9 females and 36 males), 33 of whom took part in the experiment in at least two sessions out of three, and 23 participated in all three sessions. Most participants (39) were under-30 students. All testers reported normal or corrected to normal vision.

The experiment consisted in entering six-digit PINs using the on-screen keypad shown in Fig. 1.

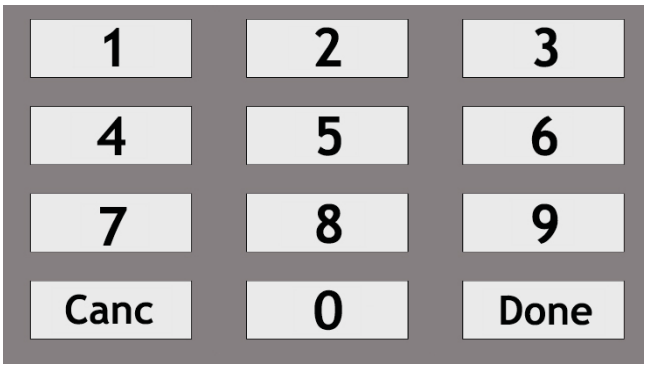

Figure 1: Keypad used in the experiments

To reduce possible precision problems, the screen was divided into 12 adjacent rectangles (the area surrounding each button was considered as part of the button itself). At each session, participants had to enter four 6-digit PINs, randomly generated at each run.

In the experiment interface, implemented in C#, a key "press" occurred by looking at a key for two seconds (after which an acoustic signal was also played). This dwell time is a good compromise between comfortable use (especially by users with no prior experience in gaze input) and efficiency. The PIN had to be confirmed by pressing the "Done" key, while the "Canc" key was used to delete the last digit entered in case of errors.

Remembering the PIN was a potential issue for testers: they could have spent some time to memorize their PINs, or could have used written notes.

However, the first solution was time consuming and some testers could have had more difficulties than others in remembering PINs. The second option was not problem-free either, as it would have required testers to constantly move their head, leading to low-quality gaze data. We therefore decided to dictate the PINs to testers during the experiments. With this approach, testers could constantly keep their gaze on the screen, and only 3% of PINs were entered incorrectly.

3.1 Procedure

Testers performed the experiment on a full HD (1920x1080 pixels) 24" screen. The interface practically occupied all the display (1920x1074 pixels), and the size of each key was 485x175 pixels. The distance between user and screen, as well as the height of the chair testers were sitting on, were not fixed, to allow a more natural and comfortable interaction through proper adjustments. However, testers were explicitly asked to keep their heads as still as possible during the experiments. Before the actual trial, testers could interact with a tutorial version of the keypad.

As an eye tracker, we used the *Eye Tribe*, one of the cheapest devices that was on the market until the end of 2016. The gaze sampling rate was 30 Hz. Other features characterizing the device are: average accuracy 0.5°, spatial resolution 0.1° (RMS), operating range 45 cm – 75 cm, tracking area 40 cm × 30 cm at a distance of 65 cm.

3.2 Features

The basic features used to characterize testers pertain to six categories, namely *Fixations*, *Pupil Size*, *Lost Gaze Samples*, *Saccades*, *User Behavior*, and *Physiological*.

Features for Fixations (all fixations made during the interaction with the virtual keypad) were (for a given time span):

- *a1*. number of fixations
- *a2*. average fixation duration
- *a3*. standard deviation of fixation duration

Features for Pupil Size were (for a given time span):

- *b1*. average diameter of left pupil
- *b2*. average diameter of right pupil
- *b3*. standard deviation of left pupil diameter
- *b4*. standard deviation of right pupil diameter
- *b5*. differences between the maximum and minimum diameters of left pupil
- *b6*. differences between the maximum and minimum diameters of right pupil
- *b7*. normalized (0-1 range) average diameter of left pupil
- *b8*. normalized (0-1 range) average diameter of right pupil
- *b9*. ratio between the average diameters of left and right pupils

Features related to Lost Gaze Samples, i.e., samples not correctly detected by the eye tracker, were (for a given time span):

- *c1*. total number of lost samples
- *c2*. percentage of lost samples
- *c3*. average length of a "block" of consecutive lost samples
- *c4*. standard deviation of the length of a block of consecutive lost samples

These features imply that data acquisition occurs always in the same conditions (e.g., environment, eye tracker position, etc.) and with the same eye tracker.

Features for Saccades (all saccades made during the interaction with the virtual keypad) were (for a given time span):

- *d1*. number of saccades
- *d2*. average distance (in pixels) covered by saccades
- *d3*. standard deviation of the distance covered by saccades

User Behavior features were the following (all coordinates are referred to the eye tracking camera's coordinate system):

- *e1*. average angle formed by the segment connecting pupils' centers and the *X* axis (in a sense, this feature provides the average horizontal inclination of the user's face)
- *e2*. difference between the maximum and minimum values of the head position (midpoint between the pupils' centers) on the *X* axis
- *e3*. differences between the maximum and minimum values of the head position on the *Y* axis
- *e4*. standard deviation of the head position on the *X* axis
- *e5*. standard deviation of the head position on the *Y* axis
- *e6*. st. deviation of the position of the left pupil on the *X* axis
- *e7*. st. deviation of the position of the right pupil on the *X* axis
- *e8*. st. deviation of the position of the left pupil on the *Y* axis
- *e9*. st. deviation of the position of the right pupil on the *Y* axis

Lastly, only one Physiological feature was considered, namely:

- *f1*. average distance between pupils

We also used additional specific features depending on the two kinds of analysis we carried out: one based on the *whole PIN sequence* and the other focused on the *single key/button*.

For the whole PIN analysis, we used three features, namely:

- *g1*. total time required to enter the PIN
- *g2*. average "reaction time" (difference between the time a tester took to enter the PIN and the minimum time necessary, divided by the PIN length)
- *g3*. sequence length (where a "sequence" is a chronologically ordered list of keys, and a key is part of the sequence if at least one gaze sample falls in the key button area)

Lastly, for the single button analysis, we used the following ten features:

- *h1*. difference between the time stamps of the last and first gaze samples detected inside the button
- *h2*. difference between the time the tester took to press the button and the minimum time necessary (i.e., two seconds in our experiments)
- *h3*. difference between the time stamps of the first gaze sample on the button and the first sample on the previous button
- *h4*. difference between the value of the previous feature (*h3*) and the minimum time necessary for a single button activation (i.e., two seconds)
- *h5*. subdividing the button area into a 2x2 uniform grid, the area (1-4) with more gaze samples (e.g., '2' if area 2 was observed more than the other three areas)
- *h6*. subdividing the button area into a 3x3 uniform grid, the

area (1-9) with more gaze samples (e.g., '6' if area 6 was observed more than the other eight areas)

h7. average position on the *X* axis of gaze samples inside the button (normalized so that the center of the button is 0.5)

h8. standard deviation of gaze position on the *X* axis inside the button

h9. average (normalized) gaze position on the *Y* axis inside the button

h10. standard deviation of gaze position on the *Y* axis inside a button

4 ANALYSIS AND RESULTS

For the study, we used four classifiers, namely Naïve Bayes (NB), Random Forest (RF), Neural Network (NN), and AdaBoost (AB). The 70%-30% (i.e., 70% for training and 30% for testing) random sampling method was employed, with ten times repetition.

The analysis was carried out considering both all features presented in Section 3 and with a selection of those features ranked using the gain ratio method.

4.1 Identification

4.1.1 Whole PIN Analysis. Table 1 shows the results obtained with all features.

Table 1: Identification - Whole PIN, all features

Method	CA	Sensitivity	Specificity	AUC
NB	0.4838	0.5040	0.9840	0.9913
RF	0.7810	0.7704	0.9931	0.999
NN	0.8181	0.8146	0.9943	0.9963
AB	0.6057	0.5964	0.9876	0.9113

CA is the Classification Accuracy. *Sensitivity* is given by *TP*/(*TP*+*FN*), where *TP* is the number of True Positives and *FN* is the number of False Negatives. *Specificity* is calculated as *TN*/(*TN*+*FP*), where *TN* is the number of True Negatives and *FP* is the number of False Positives. *AUC* indicates the Area Under the ROC (Receiver Operating Characteristic) Curve. While AUC is the integral of sensitivity and specificity over all classification thresholds, CA is the best overall accuracy.

With reference to the features described in Section 3, the best 20 ranked features were: *f1*, *b9*, *b1*, *e1*, *b2*, *e2*, *c4*, *b4*, *c1*, *d1*, *c2*, *b5*, *a3*, *e3*, *b3*, *b6*, *c3*, *a1*, *a2*, and *e7*.

Table 2 shows the results obtained with the selected features.

Table 2: Identification - Whole PIN, selected features

Method	CA	Sensitivity	Specificity	AUC
NB	0.5724	0.5999	0.9867	0.9949
RF	0.7533	0.7404	0.9922	0.9988
NN	0.7733	0.7679	0.9929	0.9933
AB	0.5848	0.5828	0.9870	0.9013

4.1.2 Single Button Analysis. Table 3 shows the results obtained with all features. With reference to the features presented in Section 3, the best 20 ranked features were: *f1*, *e1*, *b2*, *b1*, *b9*, *c4*, *c3*, *c2*, *c1*, *h6*, *d1*, *a1*, *g1*, *g2*, *b4*, *b6*, *h9*, *e6*, *e7*, and *e4*. Table 4 shows the results obtained with selected features.

Table 3: Identification - Single button, all features

Method	CA	Sensitivity	Specificity	AUC
NB	0.5441	0.5658	0.9858	0.9919
RF	0.8869	0.8845	0.9964	0.9995
NN	0.8889	0.8853	0.9965	0.9989
AB	0.8105	0.8102	0.9940	0.9764

Table 4: Identification - Single button, selected features

Method	CA	Sensitivity	Specificity	AUC
NB	0.6485	0.6623	0.9890	0.9958
RF	0.8866	0.8850	0.9964	0.9995
NN	0.8894	0.8868	0.9965	0.9988
AB	0.8278	0.8273	0.9946	0.9799

4.2 Verification

For verification, a two-class classification was implemented. For each tester to be verified, all his or her instances in the dataset were turned into "legitimate" instances, while the other testers' instances became "impostor" instances.

To balance the dataset, a random subset of impostor instances was extracted, so that their number was equal to the number of legitimate instances. The resulting dataset was then evaluated using the same methods described for identification, and the process was repeated ten times. The entire procedure was performed for each tester, to produce average results.

4.2.1 Whole PIN Analysis. Tables 5 and 6 show, respectively, the results obtained with all and selected features. *FRR* is the False Rejection Rate, calculated as *FN*/(*FN*+*TP*), while *FAR* is the False Acceptance Rate, given by *FP*/(*FP*+*TN*).

4.2.2 Single Button Analysis. Tables 7 and 8 show, respectively, the results obtained with all and selected features.

5 CONCLUSIONS

In this paper, we have explored the possibility of exploiting information about the way a PIN (Personal Identification Number) is entered through an eye-controlled input system for soft biometric purposes.

Gathered data have been analyzed considering both the whole PIN (a sort of a "coarse grained" analysis) and the single digit button (a "fine grained" analysis) with four classifiers. A 30 Hz low-cost eye tracker has been employed. Tested with a 70%-30% random sampling method, the system exhibits good performances in both identification and verification.

Table 5: Verification - Whole PIN, all features

Method	CA	AUC	Sens.	Spec.	FRR	FAR
NB	0.8363	0.9263	0.8656	0.8005	0.1343	0.1994
NN	0.8309	0.8921	0.8954	0.7686	0.1045	0.2313
AB	0.8072	0.8448	0.8479	0.7737	0.1520	0.2262
RF	0.8419	0.9348	0.8863	0.8027	0.1136	0.1972

Table 6: Verification - Whole PIN, selected features

Method	CA	AUC	Sens.	Spec.	FRR	FAR
NB	0.8774	0.9589	0.9154	0.8371	0.0846	0.1628
NN	0.8747	0.9324	0.9429	0.8075	0.0570	0.1924
AB	0.8372	0.8804	0.8573	0.8212	0.1426	0.1787
RF	0.8743	0.9670	0.9204	0.8323	0.0795	0.1676

Table 7: Verification - Single button, all features

Method	CA	AUC	Sens.	Spec.	FRR	FAR
NB	0.8811	0.9498	0.8906	0.8718	0.1093	0.1281
NN	0.8740	0.9306	0.9106	0.8377	0.0893	0.1622
AB	0.9409	0.9798	0.9535	0.9283	0.0464	0.0716
RF	0.9420	0.9837	0.9499	0.9340	0.0500	0.0659

Table 8: Verification - Single button, selected features

Method	CA	AUC	Sens.	Spec.	FRR	FAR
NB	0.9050	0.9648	0.9175	0.8927	0.0824	0.1072
NN	0.9018	0.9488	0.9285	0.8751	0.0714	0.1248
AB	0.9452	0.9815	0.9544	0.9364	0.0455	0.0635
RF	0.9486	0.9881	0.9588	0.9385	0.0411	0.0614

Button analysis provides a slightly better performance than the whole PIN analysis (around +5% in CA). Using selected features leads to a small gain in terms of accuracy and to a reduction of computational time. The Neural Network and Random Forest classifiers generally produce better results than Naïve Bayes. AdaBoost shows a less constant behavior, sometimes performing like Neural Network and Random Forest, and sometimes performing more poorly.

In this work, we studied gaze-based biometrics almost "in the wild"—unlike most past works in this field, we did not impose any constraints on the user. It is important to stress that, although we used a machine learning approach and compared different classifiers, we were more interested in assessing the feasibility of the solution than in tuning specific models. The proposed biometric method can be used in every situation where PINs or passwords are employed, such as ATMs or the access to PCs. Obviously, the secret PIN is the main authentication method, while the gaze-based soft biometrics is a security enhancement.

Future experiments will validate the results obtained in this work involving more testers and more sessions. More realistic interactions and scenarios should be studied too, also addressing "learning effects", which may change users' behavior while interacting with the system over time. For example, features *g1*, *g2*, and *g3* are probably dependent on the user's "skills", which are likely to improve with experience. Moreover, in future experiments we will try to exclude features related to lost gaze samples, as they may depend on both experimental settings (e.g., eye tracker position) and on the specific device employed. More sophisticated eye tracking devices will be also considered, characterized by higher sampling frequencies and precision.

REFERENCES

[1] S. Mitra, B. Wen, and M. Gofman. 2017. Overview of Biometric Authentication. In Biometrics in a data driven World: Trends, Technologies, and Challenges, CRC Press.

[2] K. Saeed. 2017. New Directions in Behavioral Biometrics. CRC Press.

[3] A. Rattani and R. Derakhshani. 2017. Ocular biometrics in the visible spectrum: A survey. *Image and Vision Computing*, No. 59, 1-16.

[4] A. Darwish and M. Pasquier. 2013. Biometric Identification Using the Dynamic Features of the Eyes. In *Proceedings of 2013 IEEE 6th International Conference on Biometrics: Theory, Applications and Systems* (BTAS'13).

[5] P. Kasprowski and J. Ober. 2004. Eye movements in biometrics. In *Proceedings of 2004 International Workshop on Biometric Authentication*, 248-258.

[6] A. Maeder, C. Fookes, and S. Sridharan. 2004. Gaze Based User Authentication for Personal Computer Applications. In *Proceedings of the 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing*, 727-730.

[7] M. Kumar, T. Garfinkel, D. Boneh, T. Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 13–19.

[8] P. Dunphy, A. Fitch, and P. Olivier. 2008. Gaze-contingent passwords at the ATM. In *Proceedings of the 4th Conference on Communication by Gaze Interaction* (COGAIN), 59-62.

[9] D. H. Cymek, A. C. Venjakob, S. Ruff, O. H.-M. Lutz, S. Hofmann, and M. Roetting 2014. Entering PIN codes by smooth pursuit eye movements. *Journal of Eye Movement Research*, Vol. 7, No. 4, 1-11.

[10] D. L. Silver and A. J. Biggs. 2006. Keystroke and eye-tracking biometrics for user identification. In *Proceedings of the 2006 International Conference on Artificial Intelligence* (ICAI'06), Vol. 2.

[11] C. Holland and O. V. Komogortsev. 2011. Biometric identification via eye movement scanpaths in reading. In Proceedings of 2011 International Joint Conference on Biometrics (IJCB'11), 1-8.

[12] C. Galdi, M. Nappi, D. Riccio, V. Cantoni, and M. Porta. 2013. A new gaze analysis based soft-biometric. In *Proceedings of the 2013 Mexican Conference on Pattern Recognition*, 136-144.

[13] V. Cantoni, C. Galdi, M. Nappi, M. Porta, and D. Riccio. 2015. GANT: gaze analysis technique for human identification. *Pattern Recognition*, Vol. 48, No. 4, 1027-1038.

[14] A. George and A. Routray. 2016. A score level fusion method for eye movement biometrics. *Pattern Recognition Letters*, Vol. 82, Part 2, 207-215.

[15] R. Bednarik, T. Kinnunen, A. Mihaila, and P. Fränti. 2005. Eye-movements as a biometric. In *Proceedings of the 2005 Scandinavian Conference on Image Analysis (SCIA'05)*, 780-789.

[16] T. Kinnunen, F. Sedlak, and R. Bednarik. 2010. Towards task-independent person authentication using eye movement signals. In *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications* (ETRA'10), 187-190.

[17] I. Rigas, G. Economou, and S. Fotopoulos. 2012. Human eye movements as a trait for biometrical identification. In *Proceedings of 5th IEEE International Conference on Biometrics: Theory, Applications and Systems*, 217-222.

[18] M. Juhola, Y. Zhang, and J. Rasku. 2013. Biometric verification of a subject through eye movements. *Comput. Biol. Med.*, Vol. 43, No. 1, 42-50.

[19] Y. Zhang, J. Laurikkala, and M. Juhola. 2014. Biometric verification of a subject with eye movements, with special reference to temporal variability in saccades between a subject's measurements. *Int. J. Biometrics*, Vol. 6, No. 1.

[20] N. Srivastava, U. Agrawal, S. K. Roy, and U. S. Tiwary. 2015. Human identification using linear multiclass SVM and eye movement biometrics. In *Proceedings of the 8th International Conference on Contemporary Computing*, 365-369.

[21] N. Nugrahaningsih and M. Porta. 2014. Pupil Size as a Biometric Trait. In *Proceedings of the 2014 International Workshop on Biometric Authentication* (BIOMET'14), 222-233.

[22] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic. 2015. Preventing lunchtime attacks:fighting insider threats with eye movement biometrics. In *Proceedings of the 2015 Network and Distributed System Security Symposium* (NDSS), 1-13.

[23] O. V. Komogortsev, A. Karpov, L. R. Price, and C. Aragon 2012. Biometric authentication via oculomotor plant characteristics. In *Proceedings of the 5th IAPR International Conference on Biometrics* (ICB'12), 413-420.

[24] O. V. Komogortsev, A. Karpov, C. D. Holland, and H. P. Proença. 2012. Multimodal ocular biometrics approach: a feasibility study. In *Proceedings of IEEE 5th International Conference on Biometrics: Theory, Applications and Systems* (BTAS'12), 209-216.