# Biometric authentication based on eye movements by using scan-path comparison algorithms

Carlos-Alberto Quintana-Nevárez[1], Francisco López-Orozco[1], Rogelio Florencia-Juárez[1]
[1] *LabTEC[2], División Multidisciplinaria de la UACJ en Ciudad Universitaria, Cd. Juárez, Chihuahua, México.*

**Abstract**—This paper presents an approach for an authentication method of people by using their eye movements. Our method is based on a simple scan-path comparison. People's eye movements were recorded by using an eye tracker when they were drawing a personal identification number (PIN) on a screen numeric pad. Data was analyzed using the *Eyenalysis* algorithm to measure the similarity of scan-paths by calculating and normalizing the distance in pixels for each point in the scan-paths. In the results of a first experiment and analysis we got an average acceptance rate of 80% and a low false acceptance rate under 25%. In a second experiment a previous training for each participant was done, and we got best results with trained people. However, we are continuing with this research in order to make a new study where variables like fixation time and distance from the equipment are also considered.

**Index Terms**—algorithms, authentication, biometrics, eye movement.

## 1 Introduction

At present, information security is a very important issue when talking about digital devices. We have a constant concern that our information is not violated. That is why techniques were developed to authenticate that a person is, in fact, who he claims to be.
These mechanisms fall into three categories: something you know (eg. passwords, PIN, patterns), something you have (eg. magnetic cards, chips, keys) and something you are (eg. body parts, voice, iris pattern.).

Belonging to last category, biometric authentication systems were born [1] which are divided into several categories such as fingerprint recognition [2], facial recognition [3], voice recognition [4] and iris recognition [5], which have already been violated.
The case of the fingerprint [6], that was violated using a mold of the victims fingerprint or the case of iris [7], violated by decoding the binary that was saved in the database and reconstructing the iris in base on that binary codes. This are the most trustworthy and secure biometric authentication methods existing, and they are examples on why we are faced with the need to create a new method of biometric authentication that is less vulnerable than the previous ones. This is why the idea of authentication through eye movements via the eye tracker is presented here.

Due to the fact that privacy is an issue that can not be ignored, especially when we talk about the information we store in our mobile devices, it is necessary to develop and improve the existing authentication methods, or in addition, create one new, since these are proven to be vulnerable, as in the case of Android unlock pattern [8] and Numeric PIN on any mobile device with camera and microphone [9]. In view of this need is why it was decided to create this new method based on eye movements, which, through an *eye tracker* will recognize the movements of a person against a stimulus which could be a static image, a pad or a simple text, then to match it with a register previously recorded in a database. A general background of biometric authentication and people recognition based on eye movements methods are presented. A theoretical framework will be presented on previous works in the area of *Eye Movement*, such as those developed by Hermens [10], where it explains how social stimuli affect people's attention to visualize an object.
Halverson [11] discusses how to clean the systematic error given by eye tracking devices when analyzing the data they provide.
In our work, we propose a prototype of an algorithm for the authentication of users based on eye movements with comparison of ocular movement patterns, as proposed by Mathot and Cristino [12]. This algorithm measures the Euclidean distance of each of the points in a scan-path, makes a summation and normalizes it by dividing it by the number of elements in the scan-path. This distance is represented in pixels, and shows the difference between two scan-paths. Two experiments were made where we capture the eye movements of 10 participants on a numeric pad on the screen with the numbers sorted between 0 and 9. Participants were asked to create a numeric password of 4 or 6 digits-length as an identification key. Several captures with the eye tracker were made. Then they were analyzed to find a relation between each of the captures of the participants.

• *Quintana-Nevárez is a undergraduate student of the Software Engineering programme at UACJ.*
*E-mail: al131608@alumnos.uacj.mx .*

## 2 Previous works

Several works and studies related to this subject have been proposed. These works propose different methods to achieve the authentication or identification of people based on *eye tracking*. For example the work proposed by Komogortsev uses complex characteristics of ocular behavior to identify a person [13]. Other of their reported works uses geometric characteristics of the eye shape to perform an identification [14]. In collaboration with Holland, they analyzed the influence of the environment and the stimuli given at the time of authentication [15]. They also conducted an experiment on eye tracking in a common tablet to authenticate a person using only a webcam [16]. At the International Conference on Applied Cryptography and Network Security, Liu proposed a method for smartphone authentication that consisted of displaying 4 objects on the mobile phone screen and randomly spreading them to be followed by the eye movement of the participants [17]. Here, a simple linear regression algorithm was proposed as a method to identify people.
In [18], *ImagePass* is proposed and tested as a graphical authentication system based on pattern recognition. It makes a comparison of vision patterns of the system, with identified patterns in other studies. In [19], the possibility of creating a secure and usable authentication system via eye tracking for smartphone technology was also analyzed. This proposal is called *EyeVeri*, where the mobile front camera and pattern tie algorithms are used to identify if a person is who he claims to be presenting to users different kinds of stimuli.

Security is a really important factor in contemporary systems since that some of existing authentication methods are vulnerable. For example, fingerprint method has been violated several years ago [6]. Antti Sten, Antti Kaseva and Teemupekka Virtanen, from the Department of Telecommunications, Software and Multimedia at the University of Helsinki, explain that "Typically, a human finger contains a lot of fat that leaves a mark that is not visible where it touches, therefore, it generally leaves a clear mark also on the scanner. This stain can be made visible in many ways and even a mere breath can show the impression very clearly. The scheme is to use this stain, breathe the scanner and make it. The scanner thinks that there is a live finger pressed against its pad. A variation of this idea is to use a finger-like substance that has a flat surface and press it against the pad leaving the fat stain below it" [6]. Although the modern scanners, also make finger recognition to know if it is a living finger, even so it is easy to circumvent this protection, as it was already mentioned. One of the techniques used in [6] is to create a finger based on a mold and gelatin, having these same conductivity as a human finger.

The recognition of iris was also violated in recent times as explained in [7], where a method was proposed to reconstruct an iris based on the binary information that is saved when registering it in the system. Other authentication methods such as the numeric PIN, and the unlock pattern for Android, were breached using techniques based on the microphone and camera for the PIN [9], and an attack where the grease left by the fingers was used to Identify the unlock pattern for Android [8].

That is why it is intended to develop this project. The principal objective is to find if authentication via *Eye Tracking* is more robust or less vulnerable than those mentioned above.

## 3 Proposed method

In this research, an own software program displaying a numeric on-screen pad (Figure 1) was developed. Users are supposed to draw a numerical password with their eyes on the numeric pad while eye movements are captured by an eye tracker and a comparison of the captured scan-paths is also performed.

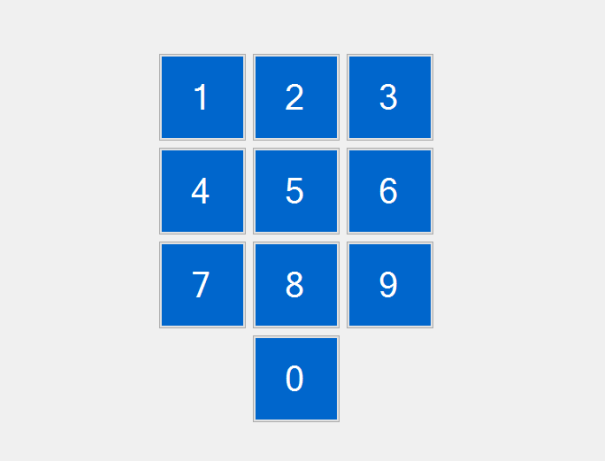



Fig. 1. On-screen numeric pad used during the experiment.

For comparison purpose, various pattern recognition and similarity measures where used, but we will talk about the one that allowed interesting results in our experiments: The *Eyenalysis* algorithm proposed by Mathot & Cristino [12].

The method followed is described in the next algorithm. It shows the process performed to capture data that will be analyzed after the experimental phase.

*Experiment starts*
*Computer starts calibration process*
**if** $UserStaresAtFixationCross \leftarrow true$ **then**
  $numericPad \leftarrow true$
  *user draws his pin with eyes*
  *experiment ends*
**else**
  $numericPad \leftarrow false$
  *waiting for user*
**end if**

## 4 Experiment

### 4.1 First experiment

Ten users where asked to create a 4-to-6 digit PIN (e.g. 2704) and follow it with their eyes. Subsequently, the numeric pad appears as shown in Figure 1 and the participant must draw the numeric PIN with the eyes.

For the purpose of this experiment, a previous calibration was done in order to obtain the best possible results in the data capture. This calibration step was done by the

calibration software developed by the eye tracker manufacturer. In the computer screen shown in Figure 2 t can be seen the image of the calibration software.

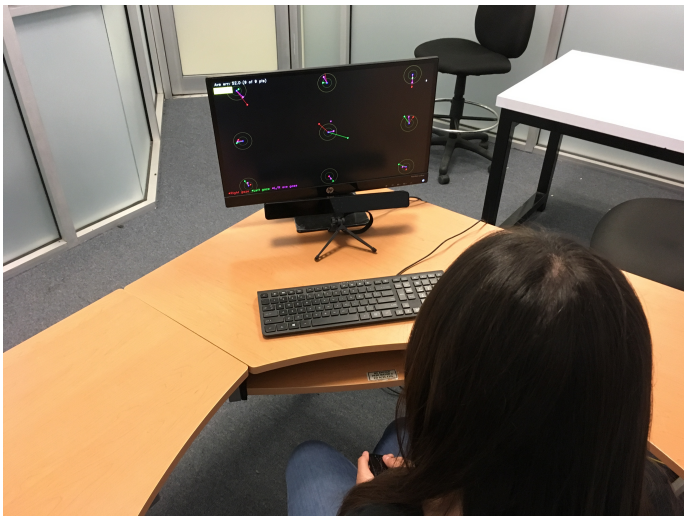


Fig. 2. Eye tracker calibration process.

Error given by the calibration step is an average of the error of all the nine points displayed on the calibration screen. Subsequently, the numeric pad appears as shown in Figure 1 and the participant must draw the numeric PIN with the eyes.

### 4.2 Second experiment

For the second experiment, 3 users where asked to do the same process as the previous experiment, with the difference that in this time, the first user had no training at all. Second participant had experience with eye tracking because of participations in previous experiments. The third participant had extensive training on eye tracking with previous experiments and a process where he was asked to read and visualize images focusing on specifics parts of them.

## 5 Data Analysis

In both of the experiments, a total of 4 scan-paths were captured from each participant after a training were 5 scan-paths for participant was captured. The last 4 scan-paths were used as data to be compared in the data analysis section. Data was analyzed with the *Eyenalysis* algorithm [12]. This algorithm was selected because we find in literature that it has many applications in the scan-paths comparison fields and we can make an adaption to our work.

### 5.1 First experiment

#### 5.1.1 Eyenalisis

*Eyenalysis* algorithm was proposed by Mathot & Cristino [12]. There they find the similarity between two scan-paths by finding the Euclidean distance point by point in the scan-path, with the following formula:

$$d(p,q) = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2}$$

where $p$ and $q$ are points in the scan-path. After that, they find the normalized form of all the points, dividing this number by the maximum number of points from the two scan-paths:

$$D(S,T) = \frac{\sum_{i=1}^{n} d_S^i + \sum_{j=1}^{n} d_T^j}{\max(n_S, n_T)}$$

where $S$ and $T$ are scan-paths to be compared and $d$ is the distance calculated beforehand for each point in the scan-path.

This method gives good results based on a distance calculated in pixels. The minor is the distance, the more similar the scan-path is to the other one, the authors of this algorithm say that around 100 px is considered a good measure of similarity.

For the intruder acceptance rate, we ask a participant to make the same password than the other participant, just telling him to imitate the password in the correct numeric order, but never tell him how much time he should last in each number.

In Figure 3 we can see how we got a better sight on how the acceptance rate for a intruder, was much more low than the person trying to authenticate himself.

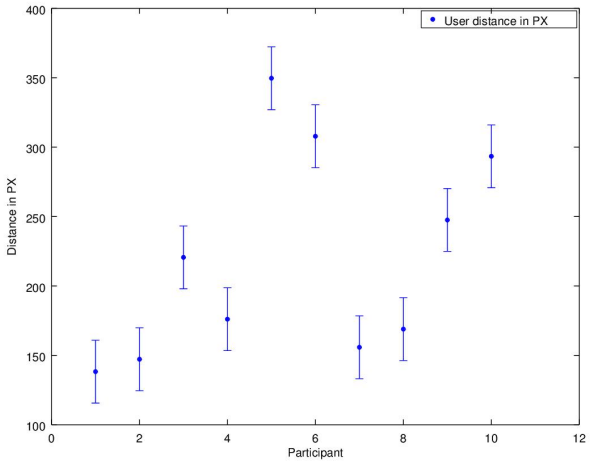



Fig. 3. Plot of acceptance on Eyenalysis algorithm, and considering an intruder trying to vulnerate the user password.

This algorithm give a good way to make an approach for authentication based on eye movement. From the 10 participants of the experiment, 8 were accepted giving us a 80% of acceptance based in the criteria proposed by the author of the algorithm where he says 100 px is considered a good similarity measure, and we add 200 more px to give the users a threshold to commit errors.

### 5.2 Second experiment

A second experiment was run, where 5 participants were recruited and asked to follow the method described before of drawing a numeric PIN with their eyes. The difference in this experiment is that distance is normalized according to *Eyenalysis* algorithm [12]. Here and due the fact that we had participants with different levels of training. For example first participant had no idea of what eye tracking was as we can see his performance in Figure 4 where he obtained a 0% of acceptance based on the previous criteria.

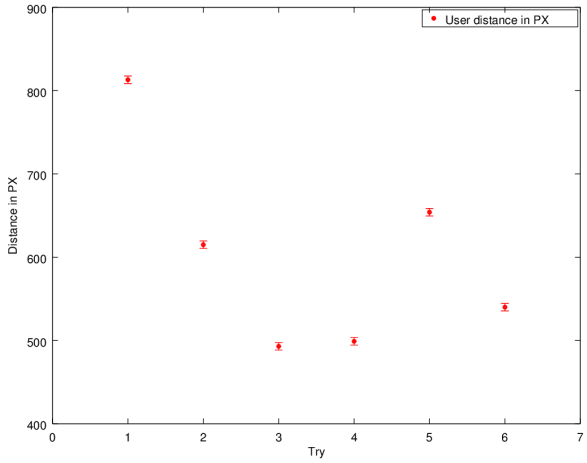



Fig. 4. Results of participant #1.

The second participant, was trained before by being recruited for the first experiment, so he has a little experience on eye tracking and the purposed method. With this participant we obtain the results in Figure 5 obtaining a 16.66% of acceptance.

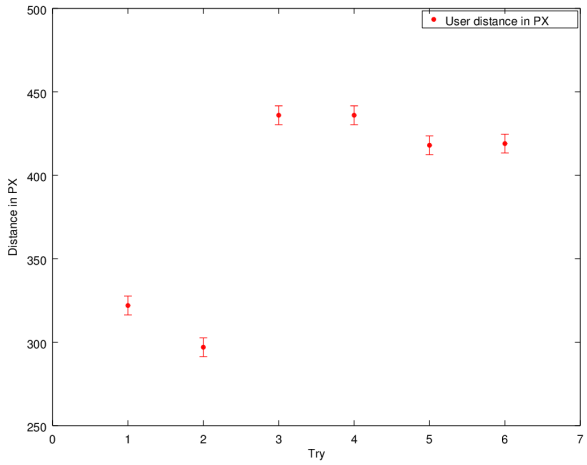



Fig. 5. Results of participant #2.

The last participant in this experiment, had a lot of experience by working with eye tracker technology than the other ones. This participant, was invited for the last experiment. He also contributed in another experiments involving eye tracking and he read articles about eye tracking before. Results with this participant are shown in Figure 6 with a 83.33% of acceptance.

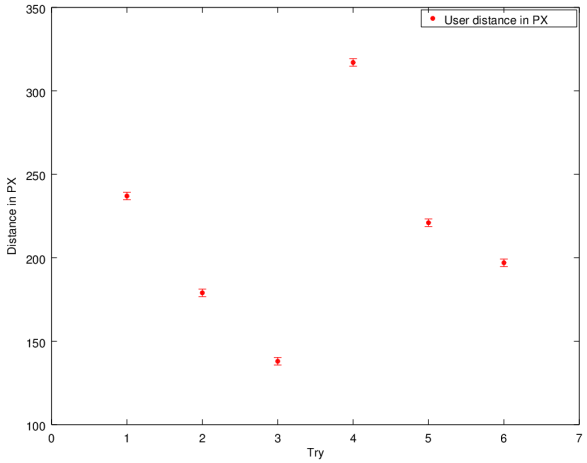



Fig. 6. Results of participant #3.

We can notice that participant with more training perform a better acceptance in both algorithms and with a less error rate, while the participant with not much training performs a good average. Finally, the participant with no training at all, obtained worst results.

## 6 Results & Discussion

In the experimentation process, we find that both methods gave good results, but they do not have a direct point of comparison because the *Eyenalysis* algorithm represents the normalized distance between all the points in a scan-path, while the linear correlation, represent the accuracy rate of a scan-path compared to another comparing point by point in the $x$ axis and then in the $y$ axis leaving no way to make a real comparison. They are different metrics to account similarity.

In the case of the linear correlation, we can say that results are affected by the calibration step and light conditions. Here, the false acceptance rate is measured by comparing the scan-path of the real user with the scan-path of other user.

On other hand, the intruder distance on the *Eyenalysis* method is measured by testing with a different person, and let know him the password of the real user, and then he tries to follow his scanpth.

Results are shown in Figure 5 where we can see that the distance in pixels for the real user is much less from the intruder, so we can deduce that a user will have a threshold to commit errors.

But if we consider that threshold, the best distance reached by the intruders will be much higher than the worst distance

reached by the real user, making this way of authentication have a considerable rate of security.

For the second experiment, a modification to the *Eyenalysis* [12] algorithm was made.
This modification consist on dividing the distance given in pixels by 10, normalizing more the obtained results. This simple modification lead to a way to compare the results in both algorithms as is shown in Figure 4, 5 and 6, where we can see how the training plays an important role in our method.

## 7 Conclusion & future work

In conclusion, *Eyenalysis* [12] algorithm give a good accuracy of security and an almost null accuracy of false positive results as we are trying to reach to ensure that the proposed method can be more secure than the other biometric methods (e.g. fingerprint or iris recognition).

In the case of *Simple Linear Regression* [17], we got good results, but not as as in the case of *Eyenalysis* [12] algorithm. However, *Eyenalysis* is more computationally complex and slower than the *Simple Linear correlation (SLR)* [17].

In future work, we are planning to taking into account more variables like fixation time and a specific fixations set of each eye trying to find a relation between the time of fixations and the level of security. And to improve the algorithm performance with simple algorithms. It is important to evaluate our algorithm method in different experimental conditions in order to assure that is accurate to every kind of situation.

## References


[1] J. Wayman, A. Jain, D. Maltoni, and D. Maio, *An Introduction to Biometric Authentication Systems*, pp. 1–20. London: Springer London, 2005.

[2] T. van der Putte and J. Keuning, *Biometrical Fingerprint Recognition: Don't get your Fingers Burned*, pp. 289–303. Boston, MA: Springer US, 2000.

[3] W. Zhao, R. Chellappa, and A. Krishnaswamy, "Discriminant analysis of principal components for face recognition," in *Proceedings Third IEEE International Conference on Automatic Face and Gesture Recognition*, pp. 336–341, Apr 1998.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 4–20, Jan 2004.

[5] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, pp. 1348–1363, Sep 1997.

[6] A. Stén, A. Kaseva, and T. Virtanen, "Fooling fingerprint scanners-biometric vulnerabilities of the precise biometrics 100 sc scanner," in *Proceedings of 4th Australian Information Warfare and IT Security Conference*, vol. 2003, pp. 333–340, 2003.

[7] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "From the iriscode to the iris: A new vulnerability of iris recognition systems," *Black Hat Briefings USA*, 2012.

[8] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens.," *Woot*, vol. 10, pp. 1–7, 2010.

[9] L. Simon and R. Anderson, "Pin skimmer: Inferring pins through the camera and microphone," in *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices*, pp. 67–78, ACM, 2013.

[10] F. Hermens and R. Walker, "Do you look where i look? attention shifts and response preparation following dynamic social cues," *Journal of Eye Movement Research*, vol. 5, no. 5, 2012.

[11] A. J. Hornof and T. Halverson, "Cleaning up systematic error in eye-tracking data by using required fixation locations," *Behavior Research Methods, Instruments, & Computers*, vol. 34, no. 4, pp. 592–604, 2002.

[12] S. Mathôt, F. Cristino, I. D. Gilchrist, and J. Theeuwes, "A simple way to estimate similarity between pairs of eye movement sequences," *Journal of Eye Movement Research*, vol. 5, no. 1, 2012.

[13] O. V. Komogortsev and C. D. Holland, "Biometric authentication via complex oculomotor behavior," in *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, pp. 1–8, IEEE, 2013.

[14] O. V. Komogortsev, A. Karpov, L. R. Price, and C. Aragon, "Biometric authentication via oculomotor plant characteristics," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, pp. 413–420, IEEE, 2012.

[15] C. D. Holland and O. V. Komogortsev, "Biometric verification via complex eye movements: The effects of environment and stimulus," in *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*, pp. 39–46, IEEE, 2012.

[16] C. Holland and O. Komogortsev, "Eye tracking on unmodified common tablets: challenges and solutions," in *Proceedings of the Symposium on Eye Tracking Research and Applications*, pp. 277–280, ACM, 2012.

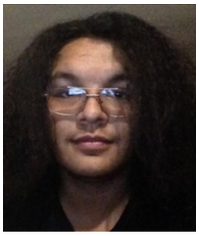
[17] D. Liu, B. Dong, X. Gao, and H. Wang, "Exploiting eye tracking for smartphone authentication," in *International Conference on Applied Cryptography and Network Security*, pp. 457–477, Springer, 2015.

[18] M. Martin, T. Marija, and A. Sime, "Eye tracking recognition-based graphical authentication," in *Application of Information and Communication Technologies (AICT), 2013 7th International Conference on*, pp. 1–5, IEEE, 2013.

[19] C. Song, A. Wang, K. Ren, and W. Xu, "Eyeveri: A secure and usable approach for smartphone user authentication," in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, pp. 1–9, IEEE, 2016.


## Acknowledgments

The first author would like to thank to LabTEC$^2$ to provide the necessary equipment for run the experiments.



**Alberto Quintana-Nevárez** Is a software engineer undergraduate student at UACJ in México, Quintana-Nevárez has participated in projects at LabTEC$^2$. His research focuses on information security, secure app development, social computing and eye movement.

**Francisco López-Orozco** PhD. Since 2015, he is an associate professor in the Software and Computer Systems Engineering undergraduate programs at UACJ. He obtained his PhD from the University of Grenoble, France in 2013. He is a co-founder and permanent member of the Laboratory of Emerging Technologies in Computer Science (LabTEC$^2$) at UACJ. His research focuses on cognitive computational and experimental psychology, human-computer interaction, centered user design.

**Florencia-Juárez** received the PhD degree in Computer Science from Tijuana Institute of Technology, México, in 2016. He received the M.Sc. degree in Computer Science from Madero Institute of Technology, México, in 2010. He is currently Professor of the Software and Computer Systems Engineering, Autonomous University of Ciudad Juárez, México. His research interests are in the areas of natural language processing, natural language interfaces to databases and knowledge representation.