On the Accuracy of Eye Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords

Argyris Constantinides
University of Cyprus & CiTARD Services Ltd.,
Nicosia, Cyprus
aconst12@cs.ucy.ac.cy

Marios Belk
University of Central Lancashire, CY Campus & University of Cyprus
Nicosia, Cyprus
mbelk1@uclan.ac.uk

Christos Fidas
University of Patras
Rio, Patras, Greece
fidas@upatras.gr

Andreas Pitsillides
University of Cyprus
Nicosia, Cyprus
cspitsil@cs.ucy.ac.cy

ABSTRACT

Graphical passwords leverage the picture superiority effect to enhance memorability, and reflect today's haptic users' interaction realms. Images related to users' past sociocultural experiences (*e.g.*, retrospective) enable the creation of memorable and secure passwords, while randomly system-assigned images (*e.g.*, generic) lead to easy-to-predict hotspot regions within graphical password schemes. What remains rather unexplored is whether the image type could be inferred during the password creation. In this work, we present a between-subjects user study in which 37 participants completed a recall-based graphical password creation task with retrospective and generic images, while we were capturing their visual behavior. We found that the image type can be inferred within a few seconds in real-time. User adaptive mechanisms might benefit from our work's findings, by providing users early feedback whether they are moving towards the creation of a weak graphical password.

CCS CONCEPTS

• **Human-centered computing** → Human computer interaction → HCI theory, concepts and models

KEYWORDS

Graphical Passwords, Sociocultural Experiences, Visual Behavior.

ACM Reference format:

Argyris Constantinides, Marios Belk, Christos Fidas, Andreas Pitsillides. 2019. On the Accuracy of Eye-Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords. *In Proceedings of 27th Conference on User Modeling, Adaptation and Personalization, Larnaca, Cyprus, June 9–12, 2019 (UMAP '19), 5 pages.* https://doi.org/10.1145/3320435.3320474

UMAP '19, June 9–12, 2019, Larnaca, Cyprus

ACM ISBN 978-1-4503-6021-0/19/06…$15.00
https://doi.org/10.1145/3320435.3320474

1 INTRODUCTION

Intelligent user authentication schemes are moving in the center of attention lately [1-4] since it is known that non-agile user authentication approaches fail to assist users with the creation of secure and memorable passwords. Focusing on graphical user authentication (GUA) schemes, which require users to select images (or parts thereof) as their secret password, state-of-the-art research has provided evidence that the image content used during graphical password creation impacts the security and memorability of the potential user-selected password.

Various GUA schemes follow either a predefined approach for the image content used during password creation [2, 5] or allow end-users to provide it [6, 7]. Such approaches introduce limitations; When image content is delivered randomly, the memorability of the graphical password is limited since users cannot easily connect prior experiences in their episodic memory with the depicted generic content [8, 9]. When users are allowed to upload image content, security and privacy considerations arise since users tend to create easily guessable passwords [9] and could violate the privacy of people depicted in the uploaded images [10]. Recent works [4, 11] revealed that image content related to users' past sociocultural experiences (retrospective approach) assists users with the creation of more memorable and secure graphical passwords, which opened new perspectives for leveraging on users' episodic memories in the design of adaptive GUA schemes that aim to deliver personalized image content during password creation.

Despite the large research efforts on the approaches used for the delivery of image content within GUA schemes, users tend to select easily predictable graphical passwords. This can be attributed to the existence of hotspots (areas of interest on an image that attract users to select them), therefore, several works focused on alleviating the hotspots issue, mainly by limiting the available choices during password creation [2, 5, 15]. What remains rather unexplored is whether we could predict in real-time if during graphical password creation users are processing either generic image content, which could lead them in making hotspots selections, or retrospective image content which could lead them in making selections based on their prior sociocultural experiences and episodic memories while avoiding hotspots selections. Considering that hotspots selections influence negatively the strength of the graphical passwords, such

predictions are of major importance and could provide early feedback to users whether they are moving towards the creation of an insecure graphical password.

A good indicator of estimating the type of image content a user is processing during graphical password creation is her visual behavior with respect to the hotspots regions of the image. Hence, this work aims to investigate whether the type of image content could be predicted in real-time using eye-tracking data. We envision that such knowledge will assist GUA scheme designers with the design of assistive and/or adaptive mechanisms within GUA schemes, as well as assist end-users with the creation of more secure and memorable passwords.

2 RELATED WORK

Numerous studies revealed that various images are susceptible to hotspots [12, 13], thus leading to the creation of easily predictable passwords [14]. Several works focused on preventing users from making poor password selections, mainly by limiting the available choices during password creation. Chiasson et al. [15] proposed a scheme in which users' choices are limited to one click-point per image for a total of five images. In their subsequent work [5], they used a viewport that highlights a random small area of the image to persuade users selecting passwords that are less likely to include salient regions. Using saliency maps, Bulling et al. [2] proposed to hide potential hotspots from being part of the users' passwords. Thorpe et al. [16] used the "presentation effect", which gradually reveals the underlying image, to influence users' choices during password creation. Likewise, Katsini et al. [17] used a fade-out effect that starts from the highest saliency mask level and gradually reveals the background image based on users' cognitive styles.

Prior research introduced eye-tracking metrics across diverse domains such as gaze-based authentication schemes [2, 18, 19], biometrics authentication [20, 21], security quantification based on users' visual behavior on the image(s) [22], inference of FD-I cognitive style from visual search and visual decision-making tasks [23], and elicitation of individual cognitive differences during graphical password creation [1]. However, to the best of authors' knowledge, no research attempts have been made to predict in real-time whether users are processing retrospective-based image content in GUA schemes using eye-tracking data.

3 USER STUDY

3.1 Research Question

RQ: Is it feasible to use eye-tracking data to predict the type of image content used (generic *vs.* retrospective) during graphical password creation? If so, what are the most predictive features?

3.2 Study Instruments and Metrics

Graphical User Authentication Scheme. We implemented a Web-based picture password mechanism (**Figure 1**), similar to Windows 10™ PGA [7]. This is a cued-recall GUA scheme, in which users can create gesture-based passwords on a background image that acts as a cue. Three types of gestures are allowed: taps, lines and circles. The image is divided in a grid containing 100 segments on the longest side and scaled accordingly on the shortest side. The mechanism allows for a tolerance distance (36 segments around each selected segment are acceptable), but there is no tolerance regarding the ordering, type and directionality of the gestures.

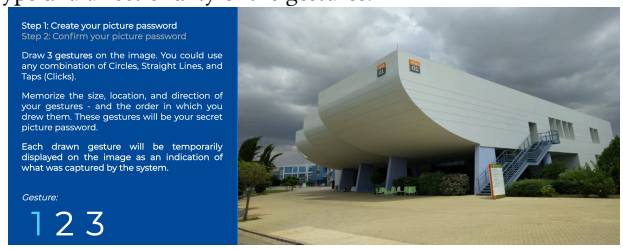

Figure 1: The recall-based PGA scheme used in our study. Users could create a graphical password by drawing three gestures; any combination of taps, lines, and circles.

Image Types. We chose two specific image sets (**Figure 2**): *i) retrospective images*: images highly related to the participants' daily life context, *e.g.*, sceneries of a University campus such as lab rooms, cafeteria, etc.; and *ii) generic images*: images illustrating generic content unfamiliar to the users, *e.g.*, with generic sceneries and people. The selection of images was based on existing research that has shown that users tend to select images illustrating people [24, 36] and scenery [24, 25]. Considering that image complexity and number of hotspots affects the password strength [17, 26], we chose images of similar complexity using saliency maps [27] and entropy estimators [28].

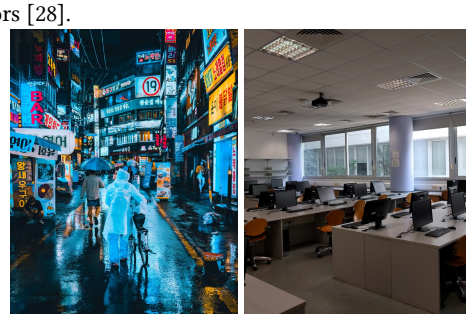

Figure 2: A generic image depicting a generic scenery with people (left), and a retrospective image depicting a lab room at the participants' university (right).

Apparatus. The study was conducted using an All-in-One HP personal computer with a 24" monitor at a screen resolution of 1920x1080 pixels. To capture the eye metrics, we used the Gazepoint GP3 video-based eye tracker [29]. No equipment was attached to the participants.

Eye Metrics. Following common practices, we selected *fixation count* and *fixation duration* as suggested in [30]. Since the determinant factor relates to hotspots, we take into consideration the fixation count and fixation duration on the

hotspots regions of the image. For each of these basic measures, we included computed features, as discussed in [31]. For fixation count, we calculated the total number of fixations and the fixation rate, while for fixation duration we calculated the sum, mean, max, and std. deviation.

3.3 Classification Setup

We treated the prediction of the image content type as a classification task using the discussed eye metrics. Based on Toker's et al. [32], we divided the activity time in time-slots of 1 second, which start with the user's first engagement with the password creation task and last until the mean time required to complete the task. We posit that users' visual behavior with respect to hotspots could be captured from the beginning of the password creation task until the time-slot in which the first gesture has been created. In each time-slot, the image content type was classified either as generic or retrospective for the combination of the aforementioned eye metrics, and an accuracy rate was calculated. We also compared the classification results with those of the baseline model (*i.e.*, type of image content is classified in each time-slot according to a Dummy classifier that makes predictions based on the most frequent class value).

Since classifications are done in increasing time-slots within the password creation task, there are cases where users complete the task in less than the mean time. To ensure that the results are not biased, these users are removed from the dataset at those time-slots, given that some metrics are correlated with time (*e.g.*, fixation duration). Moreover, the baseline, which is based on the Dummy classifier, is re-calculated in each time-slot.

3.4 Sampling and Procedure

Participants. A total of 37 individuals (13 females) participated in the study, ranging in age between 20-32 years old (m=24, sd=3.1). Participants were split evenly into two groups, and the image type was randomly varied across all users. To increase the internal validity of the study, we recruited participants that had no prior experience with PGA-like mechanisms, and had spent the last three years at the University campus, assuming they would have had experiences within the University's context.

Experimental Design and Procedure. All participants performed the task in a quiet lab room with only the researcher present. To avoid any bias effects, no details regarding the research objective were revealed to the participants. The study involved the following steps: first, participants were informed that the collected data would be stored anonymously and would be used only for research purposes, and they signed a consent form. Then, they completed a questionnaire on demographics and the eye-calibration process followed. Next, they familiarized themselves with the process of drawing gestures. Half of the participants received a selection of nine retrospective images, and the other half a selection of nine generic images. Participants were then requested to create a user account in order to access an online service. First, they created a username and then they selected one image out of the nine available images, on which they drew three gestures using a mouse. To confirm their password, they were requested to reproduce the initial three gestures.

3.5 Analysis of Results

To investigate our ***RQ*** we used *Python scikit-learn module* (*https://scikit-learn.org*). In order to avoid overfitting, we used a 10-fold cross-validation. We tested various classifiers (Logistic Regression, k-Nearest Neighbors, Naïve Bayes, and Support Vector Machines) to predict the correctly classified instances, with Logistic Regression (LR) providing the best accuracy. Results (**Figure 3**) revealed that the highest accuracy (*i.e.*, 83%) of the classifier was achieved at the 5th second. We should note that the mean time-slot for the creation of the first gesture was the 5th and the 7th second for the generic image group and the retrospective image group respectively. Considering that a user's data might be removed at any given time-slot, given that she had finished with the creation of her first gesture, we did not consider the eye metrics after the 8th second as the sample becomes very small. Nonetheless, there was an upward trend for the accuracy of LR for the combined features after the 3rd second.

The observed high prediction accuracies at an early stage are of major importance for the current work, considering that the aim is to identify the image type at early stages of graphical password creation. Such knowledge will enable the delivery of assistive and/or adaptive mechanisms within GUA schemes, which could provide early feedback to users whether they are moving towards the creation of an insecure graphical password, even before they finalize their selections, and could influence them towards creating more secure and memorable passwords. Moving towards this direction, the LR classifier achieved maximum accuracy (*i.e.*, 83%) at the 5th time-slot and performed better than the baseline across all time-slots. **Table 1** summarizes the model evaluation metrics.

We found that the most effective metric was the sum of fixation duration on hotspots at the mean time-slots (5th and 7th second for the creation of the first gesture) across groups. This can be attributed to the visual behavior differences occurred due to the image content (generic *vs.* retrospective). Users from the generic image group might have exhibited longer fixations on hotspots possibly due to the fact that they could not easily connect prior experiences in their episodic memory with the depicted generic content [8, 9], therefore, they focused on the easy-to-remember hotspots. However, users from the retrospective image group might have spent more time fixating

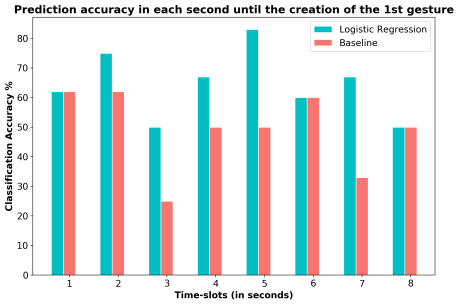

Figure 3: Classification accuracy across time-slots.

Time in seconds	Precision (weighted average)	Recall (weighted average)	AUC	Most Predictive Metrics (Higher to Lower Importance of Coefficients)
1	39%	62%	50%	fix. dur. -0.20; rate 0.23; sum -0.20
2	85%	75%	80%	fix. dur. std -0.43; max -0.42; count 0.34
3	83%	50%	67%	fix. dur. max -0.44; fix. count; 0.43; fix. dur. sum -0.40
4	80%	67%	67%	fix. dur. 0.61; sum -0.61; fix. count 0.35
5	88%	83%	83%	fix. dur. sum -0.80; fix. dur. -0.47; fix. count 0.37
6	36%	60%	50%	fix. dur. sum -0.78; fix. count 0.29; fix. count rate 0.29
7	83%	67%	75%	fix. dur. sum -0.38; fix. count -0.13; fix. dur. max -0.13
8	25%	50%	50%	fix. count -0.46; fix. dur. max 0.26; fix. count -0.19

Table 1: Model evaluation metrics along with the most predictive features at each time-slot.

on non-hotspots possibly due to the fact that the retrospective content triggered users' episodic memories [34], therefore, they focused on regions related to their prior experiences and memories while avoiding long fixations on hotspots.

We further conducted a per-second analysis of the total number of fixations and the fixations on hotspots for each group (**Figure 4**). The analysis revealed that while the two groups exhibited a similar number of fixations overall, however, the generic group exhibited higher number of fixations on hotspots throughout the session. Also, users of the generic group exhibited more and longer fixations on hotspots *vs.* non-hotspots compared to the retrospective group, as depicted in **Figure 5** (left) and **Figure 5** (right) respectively.

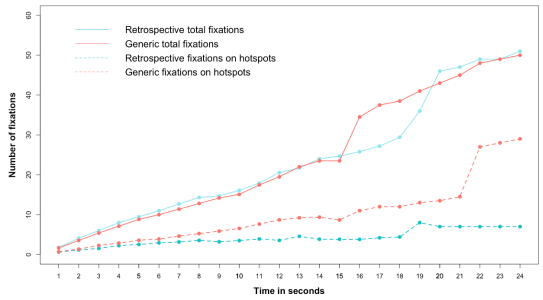

Figure 4: Number of fixations (total and on hotspots) throughout the password creation phase.

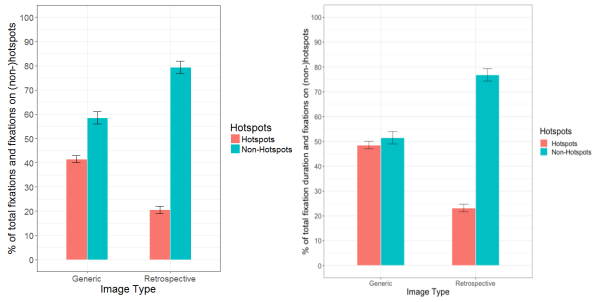

Figure 5. Percentage of total fixation count (left) and fixation duration (right) on hotspots *vs.* non-hotspots.

4 DISCUSSION AND IMPLICATIONS

We investigated the feasibility of building a classifier that predicts the type of the image content a user is processing, after collecting a few seconds of eye-tracking data during graphical password creation. Our classifier (based on Logistic Regression) outperformed the baseline dummy classifier across all time-slots.

Considering that the image content impacts the security and memorability of the user-chosen passwords [4, 8, 11, 12, 13], the classifier could be used in the design of real-time assistive and/or adaptive mechanisms within GUA schemes, or in combination with adaptive policies [33, 35] to provide appropriate mechanisms for password creation and/or login. For example, users could get early feedback about the image content used for their password creation and the mechanism could suggest users to upload again or recommend them a different set of images in an iterative way until it detects that users will potentially create a strong and memorable graphical password by considering their visual behavior with respect to the hotspots regions of the image. Such knowledge is important since more and longer fixations on hotspots increase the likelihood that users will potentially choose them as part of their passwords.

Limitations. Despite our efforts to keep the validity of the study, some design aspects of the experiment introduce limitations. First, we used specific background images in order to control the factors of the study (generic *vs.* retrospective). Although users' choices may be affected by the content and complexity of the image [24, 26], we provided images of the most widely used image categories (depicting scenery [24] and people [24, 36]) and of similar complexity. Expansion of our research will consider a greater variety of image categories in order to increase the validity of the study. Moreover, considering that we conducted a controlled in-lab eye-tracking study, the users' selections might have been influenced, however, no such comment was received from our participants at the informal discussions that followed the task completion.

5 CONCLUSIONS

In this work we have shown that users' visual behavior can be predictive of the type of image content they are processing at an early stage of graphical password creation task. Identifying the users' intentions with respect to hotspots at the initial stages of password creation could be used to introduce assistive mechanisms to help users with the creation of more secure and memorable passwords. Initial results are encouraging for further investigating various experimental designs for improving the accuracy of real-time classifiers within GUA schemes.

ACKNOWLEDGMENTS

This paper was partially supported by the project SERUMS, funded by the EU Horizon 2020 Framework Programme (826278), and the projects SUCCESS and MEMENTO, funded by the EU Active and Assisted Living Programme (AAL-2016-089, AAL-2016-069).

REFERENCES

[1] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Eye Gaze-driven Prediction of Cognitive Differences during Graphical Password Composition. In *23rd International Conference on Intelligent User Interfaces (IUI '18)*. ACM, New York, NY, USA, 147-152.

[2] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM Press, New York, NY, USA, 3011-3020.

[3] Marios Belk, Andreas Pamboris, Christos Fidas, Christina Katsini, Nikolaos Avouris, and George Samaras. 2017. Sweet-spotting security and usability for intelligent graphical authentication mechanisms. In *Proceedings of the International Conference on Web Intelligence (WI '17)*. ACM, New York, NY, USA, 252-259.

[4] Argyris Constantinides, Marios Belk, Christos Fidas, and George Samaras. 2018. On Cultural-centered Graphical Passwords: Leveraging on Users' Cultural Experiences for Improving Password Memorability. In *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization (UMAP '18)*. ACM, New York, NY, USA, 245-249.

[5] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. 2008. Influencing users towards better passwords: persuasive cued click-points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1 (BCS-HCI '08)*, Vol. 1. British Computer Society, Swinton, UK, UK, 121-130.

[6] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: design and longitudinal evaluation of a graphical password system. *International journal of human-computer studies 63*, 1-2 (July 2005), 102-127.

[7] Jeffrey Jay Johnson, Steve Seixeiro, Zachary Pace, Giles van der Bogert, Sean Gilmour, Levi Siebens, Kenneth Tubbs. 2014. Picture Gesture Authentication. Retrieved from https://www.google.com/patents/US8910253

[8] Karen Renaud. 2009. On user involvement in production of images used in visual authentication. *Journal of Visual Languages and Computing* 20, 1, 1-15.

[9] Thomas S. Tullis and Donna P. Tedesco. 2005. Using personal photos as pictorial passwords. In *CHI '05 Extended Abstracts on Human Factors in Computing Systems (CHI EA '05)*. ACM, New York, NY, USA, 1841-1844.

[10] Shane Ahern, Dean Eckles, Nathaniel S. Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. In P*roceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, New York, NY, USA, 357-366.

[11] Argyris Constantinides, Christos Fidas, Marios Belk, and George Samaras. 2018. On sociocultural-centered graphical passwords: an initial framework. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI '18)*. ACM, New York, NY, USA, 277-284.

[12] Paul C. van Oorschot and Julie Thorpe. 2011. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security* 19, 4 (December 2011), 669-702.

[13] Julie Thorpe, and Paul C. van Oorschot. 2007. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of the 16th USENIX Security Symposium (SS '07)*. USENIX Association, Berkeley, CA, USA, Article 8, 16 pages.

[14] Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe. 2010. Purely Automated Attacks on PassPoints-Style Graphical Passwords. In *IEEE Transactions on Information Forensics and Security* 5, 3 (September 2010), 393-405.

[15] Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *Proceedings of the 12th European Conference on Research in Computer Security (ESORICS '07)*, Joachim Biskup and Javier Lopez (Eds.). Springer-Verlag, Berlin, Heidelberg, 359-374.

[16] Julie Thorpe, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. 2014. The presentation effect on graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2947-2950.

[17] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Influences of Human Cognition and Visual Behavior on Password Strength during Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Paper 87, 14 pages.

[18] Darrell S. Best and Andrew T. Duchowski. 2016. A Rotary Dial for Gaze-based PIN Entry. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '16)*. ACM, New York, NY, USA, 69–76.

[19] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes!: can you guess my password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7 , 12 pages.

[20] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. 2012. Real-time Continuous Iris Recognition for Authentication Using an Eye Tracker. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, New York, NY, USA, 1007–1009.

[21] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2016. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 1056–1067.

[22] Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Towards gaze-based quantification of the security of graphical authentication schemes. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications (ETRA '18)*. ACM, New York, NY, USA, Article 17, 5 pages.

[23] George E. Raptis, Christina Katsini, Marios Belk, Christos Fidas, George Samaras, and Nikolaos Avouris. 2017. Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. In *Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization (UMAP '17)*. ACM, New York, NY, USA, 164-173.

[24] Paul Dunphy and Jeff Yan. 2007. Do background images improve "draw a secret" graphical passwords?. In *Proceedings of the 14th ACM conference on Computer and communications security (CCS '07)*. ACM, New York, NY, USA, 36-47.

[25] Ziming Zhao, Gail-Joon Ahn, and Hongxin Hu. 2015. Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation. *Journal of ACM Transactions on Information and System Security (TISSEC)* 17, 4, Article 14 (April 2015), 37 pages.

[26] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. Authentication using graphical passwords: effects of tolerance and image choice. In *Proceedings of the 2005 Symposium on Usable privacy and security (SOUPS '05)*. ACM, New York, NY, USA, 1-12.

[27] Federico Perazzi, Philipp Krähenbühl, Yael Pritch, and Alexander Hornung. 2012. Saliency filters: Contrast based filtering for salient region detection. *2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR '12)*. IEEE, Providence, RI, USA, 733-740.

[28] Maurizio Cardaci, Vito Di Gesù, Maria Petrou, and Marco Elio Tabacchi. 2009. A fuzzy approach to the evaluation of image complexity. *Fuzzy Sets and Systems* 160, 10 (May 2009), 1474-1484.

[29] GP3 Eye Tracker. 2018. [Online] Available at: https://www.gazept.com/

[30] George E. Raptis, Christos A. Fidas, and Nikolaos M. Avouris. 2016. Using Eye Tracking to Identify Cognitive Differences: A Brief Literature Review. *In Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI '16)*. ACM, New York, NY, USA, Article 21, 6 pages.

[31] Dereck Toker, Ben Steichen, Matthew Gingerich, Cristina Conati, and Giuseppe Carenini. 2014. Towards facilitating user skill acquisition: identifying untrained visualization users through eye tracking. In *Proceedings of the 19th International Conference on Intelligent User Interfaces (IUI '14)*. ACM, New York, NY, USA, 105-114.

[32] Dereck Toker, Sébastien Lallé, and Cristina Conati. 2017. Pupillometry and Head Distance to the Screen to Predict Skill Acquisition During Information Visualization Tasks. In *Proceedings of the 22nd International Conference on Intelligent User Interfaces (IUI '17)*. ACM, New York, NY, USA, 221-231.

[33] Sean M. Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2017. Diversify to Survive: Making Passwords Stronger with Adaptive Policies. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*: 1–12.

[34] Tulving, E. (1972). Episodic and semantic memory. *Organization of memory*, 1, 381-403.

[35] Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2017. The interplay between humans, technology and user authentication: a cognitive processing perspective, *Computers in Human Behavior*, 76, 184-200.

[36] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-based Authentication Schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM Press, New York, NY, USA, 316-322.