On Sociocultural-Centered Graphical Passwords: An Initial Framework

Argyris Constantinides
Department of Computer Science
University of Cyprus
1678 Nicosia, Cyprus &
CiTARD Services Ltd.
2064 Nicosia, Cyprus
aconst12@cs.ucy.ac.cy

Marios Belk
Cognitive UX GmbH
69253 Heidelberg, Germany &
Department of Computer Science
University of Cyprus
1678 Nicosia, Cyprus
belk@cognitiveux.de

Christos Fidas
Department of Cultural Heritage
Management and New
Technologies
University of Patras
26504 Rio, Greece
fidas@upatras.gr

George Samaras
Department of Computer Science
University of Cyprus
1678 Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

MobileHCI '18 Adjunct, September 3–6, 2018, Barcelona, Spain
© 2018 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-5941-2/18/09.
https://doi.org/10.1145/3236112.3236150

Abstract

Graphical user authentication schemes typically require users to draw a secret on a background image or select images on a grid. Although it is known that various image-related attributes affect security and memorability of generated passwords, current state-of-the-art approaches deliver image-content either randomly or based on the end-users' selections. Motivated by sociocultural theories which underpin that the meaning of an image varies across different people depending on their sociocultural background and experiences, in this paper we elaborate on a multi-layer image-content delivery approach which is supported by an initial framework that targets to deliver background images tailored to the unique sociocultural experiences of users. By doing so, we aim to trigger the users' sociocultural episodic memories, and ultimately help the creation of more secure and memorable passwords. Initial experimental results related to the value of this approach are also presented.

Author Keywords

User Authentication; Graphical Passwords; Sociocultural Context; Episodic Memory; Security; Memorability.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Figure 1: *Generic image* depicting planet Mars. Such content is completely unfamiliar and not meaningful to most individuals on planet Earth.

Figure 2: *Personal image* depicting a particular user with her family members at a coffee shop. Such content is highly related to the individual, highly meaningful, and highly related to her privacy.

Introduction

With the advent of mobile and immersive interaction environments, graphical user authentication (GUA) schemes are increasingly being embraced by practitioners and researchers as they leverage on novel interaction techniques [1, 2], *e.g.*, drawing secret patterns through gestures in a mixed reality environment. Two important quality dimensions of an effective GUA scheme commonly relate to its *security against adversary attacks*, and *usability* in terms of *users' memorability of selected passwords* [3-6].

Despite the research efforts in GUA, studies have shown that people make predictable choices when creating graphical passwords [7, 8, 26]. An important design factor that has a strong influence on both the security and memorability of graphical passwords is the underlying image(s) used [6-9]. Prior works have investigated the use of either *generic (random) images* (Figure 1, *i.e.*, landscapes, abstract images, etc.) or *personal images* (Figure 2, *i.e.*, family members, friends, objects highly meaningful and private to the users) and reported their effects on GUA security and usability.

When using *generic images*, results have shown that users tend to choose predictable points (hotspots) as part of their passwords [6, 8], and that unfamiliarity with the content of the image leads to low memorability [9, 10]. On the other hand, using *personal images* that have strong connection to the users increases memorability as users leverage on their episodic memory (*i.e.*, the part of long-term memory that involves the recollection of personal experiences in events and certain situations) [9, 10], however these raise security issues since selections on such images are easily guessable [7], as well as privacy issues since personal images are revealed during login [16].

In this paper we elaborate on a novel image-content delivery approach in GUA schemes, and accordingly propose an initial conceptual framework in which the image content can be represented at a particular level of user familiarity. Such a framework could be used to effectively deliver image content related to the users' sociocultural experiences aiming to trigger deeper processing through familiarity during graphical password composition. We hypothesize that delivering image content related to one's unique sociocultural experiences can provide benefits on two levels: *i)* decrease predictability of passwords since the selection of points will be based on the users' familiarity with the image content, and not through the selection of predictable hotspots [6]; and *ii)* information processed at a deeper and more meaningful way may lead to the creation of strong memory connections, and hence increase graphical password memorability [17].

Related Work

Several studies have investigated the effects of the image(s) used in graphical password schemes with respect to the security strength and memorability of the created password. Two widely used types of images in prior GUA works are images that depict either *generic (Figure 1)* or *personal (Figure 2) content*.

Effects of Generic Images towards Security and Memorability

From the security perspective, Thorpe et al. [8] showed that various generic images are susceptible to hotspotting (areas of interest), thus, leading to more predictable choices in the selected graphical passwords.

Similar findings were reported by van Oorschot et al. [7], who presented existence of hotspots for several generic content images, some to a greater extent than others. The fact that users tend to choose hotspots as part of their graphical passwords raises security concerns, since such choices are prone to automated attacks [11].

In this context, various research attempts focused on alleviating the hotspot issue, primarily by limiting users' choices during password composition. Chiasson et al. [12] proposed Cued Click-Points (CCP), in which users select one click-point on each image for a sequence of 5 images. Evaluation results revealed greater security and improved memorability compared to other cued-recall schemes. In a subsequent research scheme, coined Persuasive Cued Click-Points (PCCP) [13], in which a random small area of the image is highlighted through a viewport during password creation, users are asked to select their click-point from within the viewport area. Results of the usability study showed reduced hotspot selections from users without sacrificing the usability of the scheme. In another approach, Bulling et al. [6] proposed to filter out potential hotspots in the image with the use of saliency maps, thus, preventing users from selecting them as part of their passwords. Results showed that the use of saliency masks increased the security of the selected passwords.

From the memorability perspective, generic content decreases memorability since users cannot easily connect prior experiences (in their episodic memory) with the depicted content. In particular, Renaud [9] conducted a study to compare the efficiency of three types of images; doodles, generic pictures of random everyday objects, and personal pictures provided by users showing that the generic pictures were the least memorable because of the lack of strong connection between users and the pictures. Similar findings were reported by Tullis and Tedesco [10], in which generic pictures (*i.e.*, random stock pictures) were less memorable compared to personal pictures.

Effects of Personal Images towards Security and Memorability

From the security point of view, Tullis and Tedesco [10] revealed that the use of personal images leads to the creation of passwords that are easily guessable from people that are familiar with the user. Furthermore, the use of familiar images, *i.e.*, containing family members or friends, increases the likelihood of certain regions in the image to be selected as part of the password [6]. Another issue with the use of personal images in GUA schemes is data privacy. The fact that users do not actually understand security features, or experience difficulties in using them properly [15], may lead to sharing personal photos that violate the privacy of others depicted in the photo [16].

With respect to memorability of personal images, studies in [10] revealed that users exhibited better memorability performance for personal pictures over random stock pictures. The finding was consistent even after a few months had elapsed between the studies, and even after introducing very similar distractor images. A study conducted with the same participants after six years from their password creation [14] revealed that 12 out of 13 participants could authenticate successfully. The possible reason for personal images being more memorable is the familiarity of users with the depicted image content.

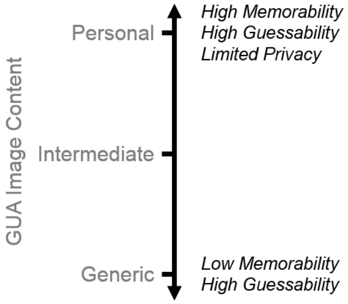

Figure 3: GUA image content related to one's familiarity. *Personal images* tend to be highly memorable, but highly predictable; *generic images* tend to be less memorable and highly predictable. *Intermediate images* may provide a promising balance on guessability and memorability.

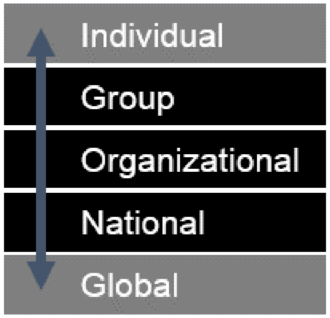

Figure 4: Levels of familiarity. The image content can fit into any level, depending on the user's familiarity and past sociocultural experiences with the depicted image content.

Research Motivation & Approach

The aforementioned works provide evidence that delivering images at the two extremes of being too generic *vs.* personal to the user raises security and memorability issues (Figure 3). Inspired by the concept of exploiting the users' familiarity and prior experience related to the image content, we suggest that a promising direction towards selecting the most appropriate image (that is neither too generic nor too personal) is by leveraging on the sociocultural activities and experiences of users (*e.g.*, *"going to a coffee shop in my neighborhood"*). Such activities incorporate the semantics of both *generic* and *personal* content, since they are relevant with a subset of the entire population (generic, but relevant to certain users), and exploit users' familiarity with the activity without raising any privacy concerns (personal, but without explicitly revealing private information).

In particular, we elaborate on the multi-level model of culture proposed in [18], in which culture (*i.e.*, behaviors, attitudes and experiences) can be represented at various levels, originating from the global towards the individual level, getting through the intermediate sociocultural levels (*i.e.*, national, organizational, group) and vice versa.

Motivated by existing works which indicate that the meaning of an image varies across different people depending on their sociocultural background and experiences [19], we posit that the semantics of image content can be represented as an entry into the multi-level cultural model from [18], based on someone's familiarity and experiences with the depicted content (Figure 4). For example, an image depicting a person at a place related to their everyday life or sociocultural experiences (*i.e.*, meet friends at a coffee shop), can be considered to fit into the *individual* level for that particular person. A similar image depicting the same place without any individual being part of the image, can be considered to fit into the *group* level, given that the individual has previous experiences at that place (*e.g.*, had visited that coffee shop in the past with friends or family). At the *organizational* level we could consider an image depicting the coffee break area in the office an individual works, while at the *national* level we could consider an image that depicts a coffee shop which is relevant to one's own culture. Last, at the *global* level we could consider an image depicting a coffee shop not directly relevant to one's own culture.

Conceptual Design of the Framework

Based on the suggested image-content delivery approach, we propose a framework for delivering images tailored to the unique sociocultural experiences of users (Figure 5) aiming to trigger users' sociocultural episodic memories, and ultimately help the creation of more secure and memorable passwords. The framework consists of: *i)* the individual context model; and *ii)* the adaptive image engine.

Individual Context Model

This module is responsible for modeling human factors (*e.g.*, lingual), cultural factors (*e.g.*, familiarity of someone's experiences with the content of an image), and GUA pictorial factors (*e.g.*, image semantics, visual complexity). Implicit contextual gathering techniques (*e.g.*, based on context-aware frameworks such as AWARE [23]) and explicit user information gathering techniques (*e.g.*, during user enrolment) are used for the generation and maintenance of appropriate user models which reflect their sociocultural activities.

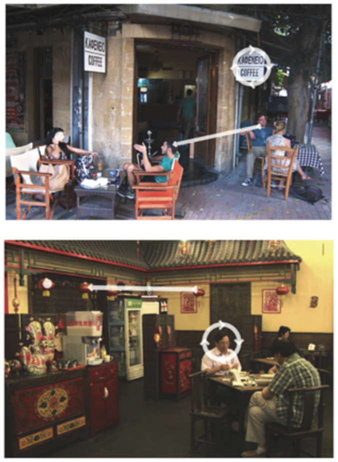

Figure 6: Culture-intensive image (top) illustrating people in a Greek coffee shop/ restaurant *vs.* **culture-neutral image (down)** illustrating people in a Chinese restaurant [22]. We refer to *culture-intensive images* as images that are relevant to the study participants' own culture (*i.e.*, Greek), and to *culture-neutral images* as images that are not relevant to the study participants' own culture (*i.e.*, China).

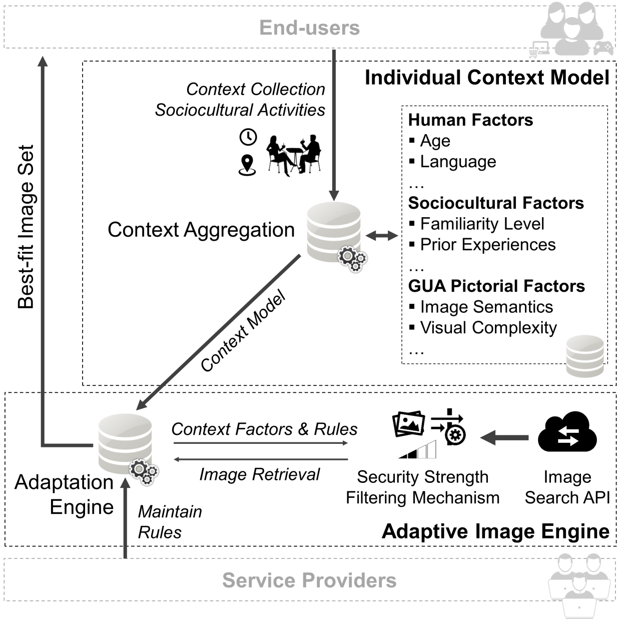

Figure 5: Conceptual design of the GUA framework.

Adaptive Image Engine
This module is responsible for retrieving image content from an online source that is relevant to the image semantics from GUA pictorial factors. After the relevant images are fetched, they pass through a security strength filtering mechanism which filters out image content that does not pass a security threshold adjusted by the Service Provider (*i.e.*, baseline security). The complexity of a fetched image (*e.g.*, in terms of the number of attention points it entails) can be assessed by automatic processes using saliency maps [24] and entropy estimators [25].

The module also decides and delivers the "best-fit" image content to each user, based on the individual context model. Adaptation mechanisms can be applied at different perspectives, based on the underlying factors (*e.g.*, human factors' adaptation, sociocultural factors' adaptation, etc.). We envision simple rule-based mechanisms to be used for deciding which adaptation to be applied. More sophisticated adaptive policies could evolve over time based on collaborative filtering mechanisms, that would suggest image content that has been successfully used by existing users that share similar sociocultural habits and experiences.

Use Case Scenario
Savvas is an accountant who lives and works in Cyprus. On his way to work, he usually makes a stop to grab his daily Freddo Espresso from the coffee shop in his neighborhood. Savvas also enjoys going to the stadium to watch the games of the football club (APOEL FC) he supports. The *Individual Context Model* tracks Savvas' sociocultural activities, along with other context-related data (*e.g.*, location, time), and extracts the semantics of these activities (*i.e.*, Cypriot coffee shop, APOEL FC's football stadium, etc.) to build a context model. The context model is then passed to the *Adaptive Image Engine*, which is responsible to find visually-rich images relevant to the semantics and of certain security strength (set by the service provider). Finally, it delivers a set of images depicting coffee shops in Cyprus close to his location and events related to the football team he supports.

Preliminary Results

We conducted an exploratory study (analyzed and reported in [22]) with the aim to gain initial knowledge regarding security and memorability of the created password when the image content belongs in one of the intermediate sociocultural levels of the framework.

Metrics	Image Type	
	Culture-intensive	*Culture-neutral*
Time to create password (seconds)	50.1 ± 23.79	38.06 ± 9.05
Memorability time (hours)	292.08 ± 27.4	265.4 ± 40.96
Number of guesses (millions)	315.08 ± 12.2	324.53 ± 15.2

Table 1: Summary of initial results. Data are mean ± standard deviation.

Procedure and Image Selection

Participants were asked to create a graphical password in the context of a real-life task (*i.e.*, post on a blogging Web-site) through a Web-based GUA scheme we implemented, similar to Windows$^{\text{TM}}$ Picture Gesture Authentication [20], using any combination of three gestures (taps, circles, lines) on a background image.

We selected two images (Figure 6) that depict a social habit/activity of people falling into the age category of our participants (*i.e.*, people going to a coffee shop). With respect to our participants, the first image we chose fits into the *national level* (*i.e.*, relevant to the participants' culture), while the second image fits into the *global level* (*i.e.*, not relevant to the participants' culture). We recruited participants that had spent the last 5 years in Greek societies; assuming they would have had experience with regional coffee shops' culture, etc. We selected images of similar complexity depicting scenery and people, since users tend to make such selections [21] as part of their password.

Initial Findings

Results (see [22]) indicate interdependencies between users' sociocultural experiences, the time to create a graphical password and memorability (Table 1). Users that created graphical passwords with the *national level* image spent more time to create their password, exhibiting significant higher levels of memorability than users with the *global level* image. Correlation analyses also indicate that the time spent to create the password was positively correlated with memorability, while security analyses showed no significant differences between the two user groups.

Conclusions and Future Work

We proposed an initial framework which is based on an innovative image-content delivery approach that annotates images at various levels of familiarity, based on one's sociocultural experiences with the depicted content. We also presented components of a framework aiming to recommend specific image content tailored to users' sociocultural experiences during password composition. Initial experimental results provide evidence about the added value of considering users' sociocultural experiences as a personalization factor for graphical password schemes. Future work entails further refining the suggested image-content delivery approach by running more user studies aiming to investigate the usability aspects and user acceptance of the proposed framework. Particular focus will be placed on evaluating the accuracy of the selected relevant images and users' workload and experience on providing input selections during password composition.

Acknowledgments

This paper was partially supported by the project ADVisE, within the University of Cyprus' internal-funded projects, and the project SUCCESS, funded by the EU Active and Assisted Living Programme (AAL-2016-089).

References

1. Hsin-Yi Chiang and Sonia Chiasson. 2013. Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13)*. ACM Press, New York, NY, USA, 251-260. DOI:https://doi.org/10.1145/2493190.2493213
2. Emanuel Von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the wild: a

field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13)*. ACM Press, New York, NY, USA, 261-270. DOI:https://doi.org/10.1145/2493190.2493231

3. Robert Biddle, Sonia Chiasson, and Paul C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)* 44, 4, Article 19 (September 2012), 41 pages. DOI:https://doi.org/10.1145/2333112.2333114
4. 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 Press, New York, NY, USA, Paper 87, 14 pages. DOI:https://doi.org/10.1145/3173574.3173661
5. 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, C (November 2017), 184-200. DOI:https://doi.org/10.1016/j.chb.2017.06.042
6. 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. DOI:https://doi.org/10.1145/2207676.2208712
7. 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.
8. 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.
9. Karen Renaud. 2009. On user involvement in production of images used in visual authentication. *Journal of Visual Languages and Computing* 20, 1 (February 2009), 1-15. DOI:https://doi.org/10.1016/j.jvlc.2008.04.001
10. 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 Press, New York, NY, USA, 1841-1844. DOI:https://doi.org/10.1145/1056808.1057036
11. 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. DOI:https://doi.org/10.1109/TIFS.2010.2053706
12. Sonia Chiasson, Paul 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)*. Springer-Verlag, Berlin, Heidelberg, Germany, 359-374.
13. Sonia Chiasson, Alain Forget, Robert Biddle, and Paul 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)*. BCS Learning & Development Ltd., Swindon, UK, 121-130.
14. Thomas S. Tullis, Donna P. Tedesco, and Kate E. McCaffrey. 2011. Can users remember their pictorial passwords six years later. In *CHI'11*

Extended Abstracts on Human Factors in Computing Systems (CHI EA '11). ACM Press, New York, NY, USA, 1789-1794. DOI:https://doi.org/10.1145/1979742.1979945

15. Steven Furnell. 2005. Why users cannot use security. *Computers and Security* 24, 4 (June 2005), 274-279. DOI:https://doi.org/10.1016/j.cose.2005.04.003
16. 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 *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM Press, New York, NY, USA, 357-366. DOI:https://doi.org/10.1145/1240624.1240683
17. Fergus I.M. Craik and Robert S. Lockhart. 1972. Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal Behavior* 11, 6 (December 1972), 671-684. DOI:https://doi.org/10.1016/S0022-5371(72)80001-X
18. Miriam Erez and Efrat Gati. 2004. A Dynamic, Multi-Level Model of Culture: From the Micro Level of the Individual to the Macro Level of a Global Culture. *Applied Psychology: An International Review* 53, 4 (September 2004), 583-598. DOI:http://dx.doi.org/10.1111/j.1464-0597.2004.00190.x
19. Marita Sturken and Lisa Cartwright. 2017. *Practices of Looking: An Introduction to Visual Culture* (3rd. ed.). Oxford University Press, Oxford, UK.
20. Jeffrey Jay Johnson, Steve Seixeiro, Zachary Pace, Giles van der Bogert, Sean Gilmour, Levi Siebens, Ken Tubbs. 2014. Picture gesture authentication. (Feb. 2014). Patent No. 8650636, Filed June 17th., 2011, Issued Feb. 11th., 2014.
21. 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. DOI:https://doi.org/10.1145/2785830.2785882
22. 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 Press, New York, NY, USA, 245-249. DOI:https://doi.org/10.1145/3209219.3209254
23. AWARE Framework. 2018. Open-source Context Instrumentation Framework For Everyone. (May 2014). Retrieved May 16, 2018 from http://www.awareframework.com
24. 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. DOI:https://doi.org/10.1109/CVPR.2012.6247743
25. 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. DOI:https://doi.org/10.1016/j.fss.2008.11.017
26. 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 Press, New York, NY, USA, 252-259. DOI:https://doi.org/10.1145/3106426.3106488