Influences of Human Cognition and Visual Behavior on Password Strength during Picture Password Composition

Christina Katsini[1,2], Christos Fidas[3], George E. Raptis[1,2], Marios Belk[4,5], George Samaras[5], Nikolaos Avouris[2]

[1]Human Opsis, Patras, Greece, [2]HCI Group, University of Patras, Greece, [3]Department of Cultural Heritage Management and New Technologies, University of Patras, Greece, [4]Cognitive UX GmbH, Heidelberg, Germany, [5]Department of Computer Science, University of Cyprus, Nicosia, Cyprus
katsinic@upnet.gr, fidas@upatras.gr, raptisg@upnet.gr, belk@cognitiveux.de, cssamara@cs.ucy.ac.cy, avouris@upatras.gr

ABSTRACT

Visual attention, search, processing and comprehension are important cognitive tasks during a graphical password composition activity. Aiming to shed light on whether individual differences on visual behavior affect the strength of the created passwords, we conducted an eye-tracking study (N=36) and adopted an accredited cognitive style theory to interpret the results. The analysis revealed that users with different cognitive styles followed different patterns of visual behavior which affected the strength of the created passwords. Motivated, by the results of the first study, we introduced adaptive characteristics to the user authentication mechanism, aiming to assist specific cognitive style user groups to create more secure passwords, and conducted a second study with a new sample (N=40) to test the adaptive characteristics. Results strengthen our assumptions that adaptive mechanisms based on users' differences in cognitive and visual behavior uncover a new perspective for improving the password's strength within graphical user authentication realms.

Author Keywords

Usable Security; Graphical User Authentication; Cued-Recall Authentication; Picture Passwords; Eye-tracking; Visual Behavior; Cognitive Styles; Field Dependence-Independence.

ACM Classification Keywords

K.6.5 [Management of Computing and Information Systems]: Security and protection---Authentication; H.5.2 [Information interfaces and presentation]: User Interfaces---Graphical user interfaces.

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3173661

INTRODUCTION

Graphical User Authentication (GUA) schemes are constantly gaining market share as they scaffold natural human-computer interaction and adapt easier to nowadays mobile and immersive user interaction realms [11,20,64]. Examples of commercially deployed GUA schemes are the Android Pattern Unlock and the Windows 8™ Picture Gesture Authentication (PGA). GUA schemes lie under two main categories: recognition-based and recall-based.

In recognition-based schemes, the users memorize a set of images during registration which they must distinguish among a set of decoy images during login. Examples of such mechanisms are Passfaces [9], Dejavu [17] and VIP [2]. Despite that recognition-based passwords seem easy to remember; their drawback lies in that a large image pool is required in order to achieve a sufficiently high entropy [25].

In recall-based schemes, the users are required to memorize and reproduce a graphical password. A notable example of such scheme is DAS [27], where the users draw a shape on a grid. These schemes are quick and convenient to use, but users often make mistakes in remembering the order and the precise location, when redrawing their secret [23,27]. Cues were introduced to help users reproduce their passwords more accurately, without them having a direct role in the password. Most often, images play the role of the cue. PassPoints [60], Cued Click Points (CCP) [14], and PGA are examples of such schemes. In PassPoints the users are required to select five points on a provided image. To log-in, they must repeat the sequence of the points in the correct order within a system-defined tolerance. In CCP, the users are presented with a number of images in sequence and are required to select a point on each image. To log-in, each image is displayed after selecting the correct point at the previous one. In PGA, the users are required to draw three gestures on an image they selected. To log-in, they must reproduce the three gestures within a system-defined tolerance.

Despite the research efforts in the GUA field, studies have revealed that people make predictable choices when using graphical passwords [40,49,55], introducing vulnerabilities to systems and services. Since password composition and login in GUA encompass visual information processing and

considering that socio-cognitive theories have been used to explain users' behavior in visual tasks [18,46,61], they could be used to shed light on how people make their password choices. A cognitive theory interrelated with the visual behavior is the Field Dependence-Independence (FD-I) theory [61], which suggests that individuals have different approaches in retrieving, recalling, processing, and storing graphical information. FD-I theory characterizes individuals as either field dependent (FD) or field independent (FI). FDs tend to follow a more holistic approach to process visual information and have difficulties in identifying details in complex visual scenes [61], while FIs tend to follow a more analytical approach to process visual information, pay attention to details, and easily separate simple structures from the surrounding visual context [61].

Considering that the strength of the chosen password is determined during password composition, in this paper we adopt an FD-I perspective and investigate how users react to stimuli, through analyzing their visual behavior, aiming to understand how they decide on the graphical passwords they create. This will allow us to draw conclusions on the effects of cognitive styles on the strength of the created passwords, understand whether and how this is associated with the users' visual behavior, and investigate whether this knowledge could be used to design adaptive mechanisms that could enable users to make stronger passwords.

Based on our motivation, we report two contributions. First, we provide an exploratory study to identify whether there are effects of cognitive styles on the strength of the user-created recall-based passwords and whether these are correlated to the users' visual behavior during password creation. Second, we introduce a new feature to the GUA scheme based on the results revealed in the first study and report on the comparison of the strength of the created passwords of the two studies.

RELATED WORK

Several studies have investigated the effects of user choices on the strength of the created graphical passwords. User choices can be affected by human factors, such as gender and cultural background [36], technological factors, such as device type [11], GUA scheme characteristics, such as grid size [8,34], design space [50], etc.

Two crucial parameters that influence the strength of the password are the gesture(s) drawn and the background image(s) used. Regarding gestures, Alt et al. [1] showed that most passwords consist of two or three strokes, with top-to-bottom or left-to-right direction being the two most common. Similar findings were revealed by Zhao et al. [67], who showed that taps and lines are the most popular gestures. Regarding image type and context, research has revealed that the users prefer images showing people [1,67], scenery [1], and comic [1], while coherent images fit better as graphical images compared to jumbled ones [4]. In addition, people's choices are affected by the human characteristic of facial images such as race, age, and gender [16], and the colors and the category of images [37]. Images have attention points where people draw gestures [1,18,55,66,67], which can be revealed through saliency and proximity filters [59]. These have been used effectively for offline password attacks [55], revealing that people's choices are related to the image's saliency points. Therefore, image complexity (i.e., number of attention points in an image) [12,21,59], and tolerance or accuracy rate [11,59] affect password strength and memorability (the less complex the image, the more predictable the created password is; the more the tolerance, the more easy for attackers to guess the created password). Several attempts to identify attention points of images through eye-tracking have been made, and eye-tracking has been used to increase the strength of the graphical passwords [10,34].

From a human cognitive perspective, Belk et al. investigated the effects of cognitive processing styles [6], and abilities [7] towards users' login performance and memorability of textual and graphical passwords. Their research revealed that the FI users outperformed the FD users during login in terms of time. Users with enhanced working memory and processing speed outperformed users with limited processing abilities during login tasks. In Katsini et al. [29] work, a preliminary analysis revealed that FD users created less strong passwords compared to FI users when using a recognition-based GUA scheme.

Regarding elementary cognitive processes, Chiasson et al. [13] reported that people could remember more easily graphical over text-based passwords, a finding that was also supported by Meng et al. [35]. Everitt et al. [22] found that people who accessed four different infrequent graphical passwords each week had greater failure rates than those accessing a single infrequent password. Stobert and Biddle [52] showed that cued-recall was better than free-recall and that recognition-based graphical passwords were more memorable than recall-based passwords. Huestegge and Pimenidis [26] found increased login times when memory load increased and longer retention intervals yielded an increase of search times and login failures when using a face-based GUA scheme.

Based on the related work, we infer that from a human cognition perspective: (a) existing research focuses rather on the login task per se, and not on the password composition; and (b) there is no research work which investigates whether users' individual cognitive characteristics are reflected in their visual behavior during graphical password composition, and whether they have an impact on security aspects of recall-based graphical passwords. Given the importance of visual information processing in GUAs, we argue that investigating the effect of users' cognitive styles on passwords' strength and visual behavior within graphical password composition activities, can provide important insights about the value of considering individual cognitive differences as a design factor, in both design- and run-time, aiming to uncover a new perspective for improving the security within graphical user authentication realms.

EXPLORATORY STUDY

We designed a controlled experiment in which the participants were asked to use a web-based picture passwords mechanism similar to PGA. In PGA, the users select their own image as their password background image cue; thus, they can use images of varying complexity. Considering that image complexity is known to affect both the password strength [59] and the gesture combinations [1,40,41,55], we intentionally decided to provide two images of different complexity (in terms of number of attention points) and examine whether cognitive and visual behavior differences during password composition affect the strength of the created passwords.

Hypotheses

We formed the following null hypotheses:

H0$_1$. There is no significant difference on the strength of the created graphical passwords between field-dependent (FD) and field-independent (FI) individuals across background images of varying complexity;

H0$_2$. There is no correlation between the strength of the created graphical passwords and the visual behavior of field-dependent (FD) and field-independent (FI) individuals across background images of varying complexity.

Participants

A total of 36 individuals (16 females) participated in the study. Their age ranged between 22 and 38 years (m = 31.7; sd = 6.1). Thirteen participants were undergraduate students; nineteen participants were postgraduate students; four participants were professionals. Participants did not have any vision problems or wore glasses. The recruitment took place by communicating the research via posting flyers on bulletin boards at various places on campus, and directly contacting acquaintances of the research team. To increase internal validity of the study, we recruited participants that had no prior experience and had never heard of PGA.

Study Instruments

Recall-based Graphical Authentication Mechanism

We used a web-based picture passwords mechanism, shown in Figure 1,which resembles the workflow and appearance of PGA [28]. This is a cued-recall graphical authentication scheme, used for creating gesture-based passwords using a background image as a cue. There are three types of permitted gestures: *taps*, *lines* and *circles*. Free line gestures, are converted to one of the three recognized gestures. To store the gestures the mechanism creates a grid on the image by dividing the longest dimension of the image into 100 segments and then dividing the shortest dimension by the same scale. The gestures are then stored based on their position on the grid, with their coordinates corresponding to segments rather than to pixels. The following information is stored for each type of gesture: for taps the coordinates of a point, for lines the coordinates of the starting and the ending point, and for circles the coordinates of the center, the radius and the direction.

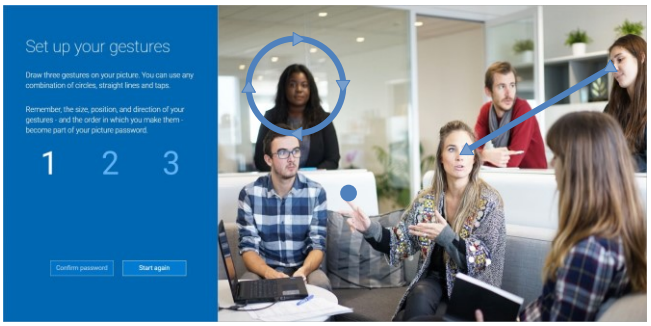


Figure 1: The recall-based GUA scheme used in our study resembled Windows 8™ Picture Gesture Authentication. The users could create their password by making three of the following types of gestures: taps, lines, and circles.

During enrolment, the screen is divided in two parts as shown in Figure 1. On the left, instructions for creating a password are provided. In addition, there are three numbers (1, 2 and 3) which provide feedback on the currently active gesture (the corresponding number is highlighted). At the bottom, there is a "Start again" button, which allows the user to restart the enrolment, and a "Confirm password" button, which is activated once all three gestures have been recorded. The background image, on which the user creates the password, by drawing three gestures, is located on the right side of the screen. On releasing each gesture, the shape of the gesture is displayed temporarily on the corresponding location, to inform the user that the gesture has been recorded. To confirm the gestures and create the graphical password the users must reproduce the three gestures. The comparison of the two passwords shows some tolerance in terms of coordinates (36 segments around the selected segment are accepted). No tolerance is shown in type, ordering and directionality of the gestures. If any of these does not match, then the password will not be created.

During login, the user is provided with the same screen. The image is loaded and the number 1 is highlighted. The mechanism allows the user to reproduce all three gestures and then compares the reproduced password with the stored one. Login succeeds if a) the gestures (type, ordering, and directionality) match with the stored ones and b) the distance between the reproduced and the stored gestures is within the tolerance interval.

To control image complexity, we calculated the saliency map and the entropy of several images, and we decided to use the following two: a simple image which consists of a main attention point and shows a flying jet (entropy =.453) and a complex image which consists of several attention points and shows a workplace (entropy = .983). The images are representative of the two most popular image categories, based on research which revealed that people tend to select images which show people [1,21] and images which show a scenery and/or a single object [21,66] as background images for passwords. Both the images we selected and their saliency maps, as produced by the saliency filters provided by [42], are depicted in Figure 2.

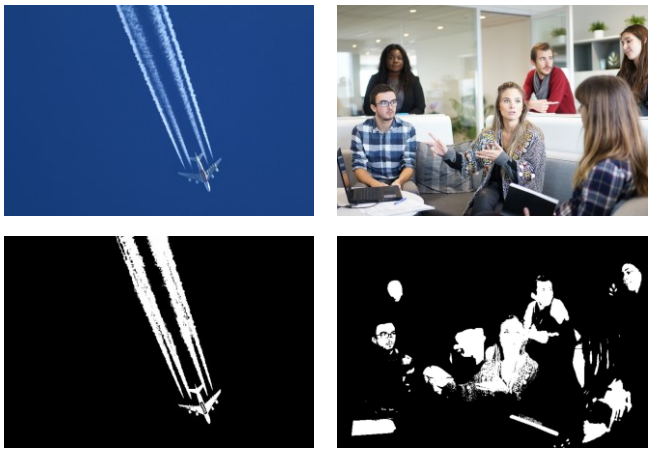


Figure 2: Images of different complexity used in the study, a simple image showing a jet (left), and a complex image showing a workplace (right). At the bottom, the saliency maps of the images are depicted.

Cognitive Style Classification Test

To classify the participants as either FD or FI we used the *Group Embedded Figures Test* (GEFT) [39], which is the original classification FD-I tool. GEFT is a credible and validated time-administered "paper and pencil" instrument [31], which measures the ability of an individual to identify a simple figure within a complex background. Individuals are asked to identify and outline a given simple pattern in a visually complex context within a given amount of time. The test is divided in three sections. The first section is used for practice. The correct answers of the next two sections are summed to provide a raw score, ranging between 0 and 18. Individuals are classified as FD or FI by using a cut-off score.

In our study, the participants' scores were normally distributed and ranged between 3 and 18 (m=11.27, sd=3.51, p=.085). Our sample's mean GEFT score is comparable to the national mean of 11.4 in Witkin et al. [39]. The cut-off score was determined to be 12, as it has been widely used in the literature [3,24,45], meaning that the participants who scored from 0 to 11 were classified as FD, and those who scored from 12 to 18 as FI. 17 participants were classified as FD, and 19 as FI.

Equipment

The study was conducted using a Samsung Galaxy Tab S2 tablet computer with a 9.7" monitor at a screen resolution of 2048x1536 pixels (*i.e.*, 4:3). To capture the eye movements, we used the Tobii Pro Glasses 2, which captures data at 50Hz. Fixations were extracted using a customized velocity threshold identification (I-VT) algorithm [32], based on the I-VT algorithm provided by Tobii.

Metrics

Password Strength Metric

To measure the created graphical passwords' strength, we adopted password guessability, a widely used metric for measuring password strength [66,67]. We used a brute-force approach based on the attention points of each background image, as discussed in [48,66]. Our brute-force algorithm started from the segments covering the attention points, next checked the neighboring segments, and finally checked the rest of the image segments. The password strength was measured in number of guesses required to crack each password.

Visual Behavior Metrics

Our visual behavior metrics are: fixation duration, number of fixations, number of fixated segments and fixation distance, as they are related to FD-I cognitive style and visual decision making tasks [45]. Fixations are one of the basic eye-movements [19], and they occur while individuals' eyes are kept aligned with the target for a certain duration, allowing for the visual scene details to be processed. The *fixation duration* metric is the total duration of fixations of an individual within an area of interest (AOI), considering visits and revisits to the AOI. The *number of fixations* metric is the total number of fixations of an individual within each AOI, considering visits and revisits to the AOI. The *number of fixated segments* metric is the total number of unique fixations on each segment of the GUA scheme without considering revisits. In our study, each segment of the image is an AOI. The *fixation distance* metric is the Euclidean distance between two fixation points mapped on the background image.

Procedure

Each participant visited our lab at a previously agreed date and time. The study was conducted in a quiet room in our lab. The procedure involved the following steps: first, the participant was introduced to the task and familiarized with the eye-tracking equipment. Participants wearing glasses wore the eye-tracking glasses on top of their glasses. The eye-tracking calibration process, as described in [56], followed. Next, the participants were asked to use the tablet and create their graphical password, by creating a username in the first step and then by drawing three gestures using their hand, which they had to reproduce to confirm the created password. As discussed earlier, users were provided with two images of different complexity. After creating the first password, the facilitator changed the background image and asked the participant to refresh the web-page and follow the same process to create a second password. To avoid order effects, we counterbalanced the sequence of the background images; thus, 18 participants used the simple image first, while the other 18 participants used the complex image first. After creating the password, the participants were distracted for about 20 minutes with completing the GEFT test. Next, they were asked to use the login details they had created for both images to log-in and answer a short questionnaire on demographics. We included this step to ensure users did not create the passwords randomly. Finally, an informal discussion on how the participants created their graphical passwords took place. Prior to the study, the participants were informed that the collected data during the session would be stored anonymously and would be used only for research purposes by the research group, and they provided their consent. To avoid bias effects, no details regarding the research objective were provided to the study participants.

Results

To investigate **H0$_1$**, we ran a mixed ANOVA test, with the FD-I cognitive style (FD or FI) and the image complexity (simple or complex) as the independent variables, and the number of guesses needed to crack the password as the dependent variable. The test met all the mixed ANOVA assumptions. The analysis revealed a significant interaction between the effects of the FD-I cognitive style and the image complexity on the strength of the created passwords, $F = 4.183$, $p = .041$, $\eta^2 = .166$. Pairwise comparisons, with p-values Bonferroni-adjusted and 95% confidence intervals, revealed that 120 thousand fewer guesses were required to crack the passwords of the FIs when using the simple background image compared to the FDs when using the simple background image ($p = .042$). For the FDs, no significant differences were revealed between the passwords created using the two images. For the FIs, 138 thousand more guesses were required to crack the passwords created using the complex background image compared to those created using the simple background image ($p = .028$).

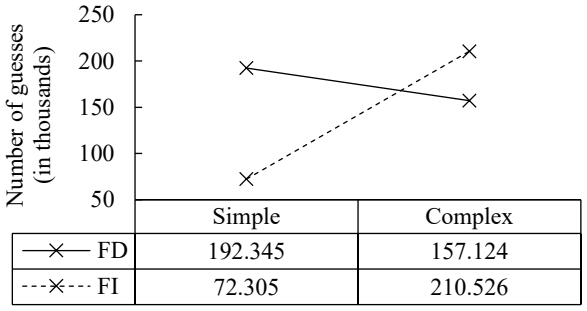


Figure 3: The impact of the cognitive style on the password strength is affected by the complexity of the background image. FIs created stronger passwords when using a complex background image, while FDs created stronger passwords when using a simple background image.

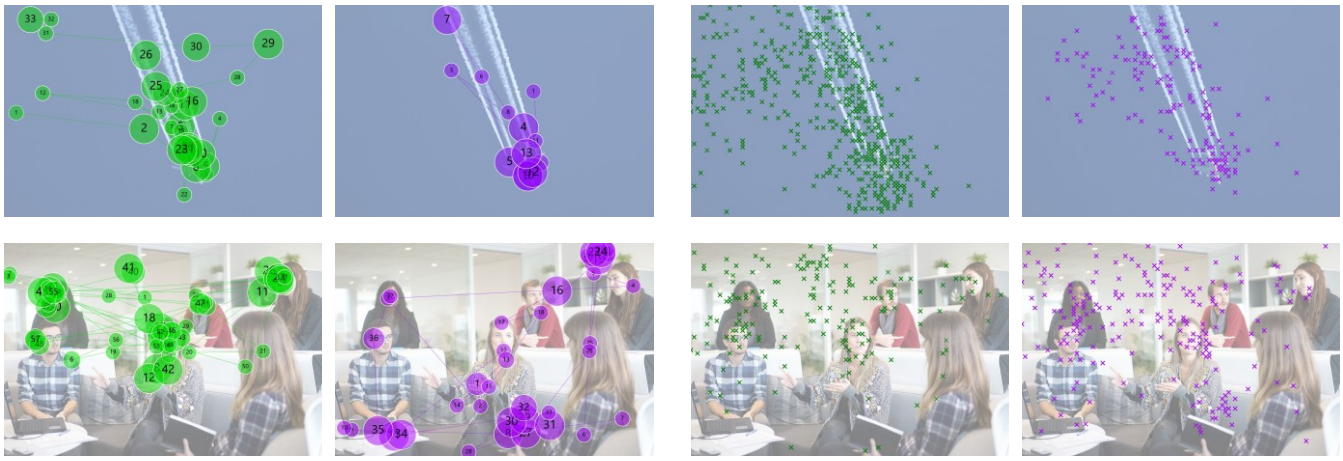
To assess the relationship between the security of the created passwords and the visual behavior (**H0$_2$**) we ran a Pearson correlation test. Preliminary analyses showed that the relationship is linear with both variables being normally distributed, as assessed by Shapiro-Wilk's test ($p > .05$), and there were no outliers. The analysis revealed a strong correlation between the strength of the created passwords (in terms of number of guesses needed to crack) and the number of fixated segments ($r = .618$, $p = .041$), and a small correlation between the passwords' strength and the fixation duration ($r = .296$, $p = .044$). To investigate the influence of the FD-I cognitive style and the image complexity on the correlation between the visual behavior metrics and the password strength, we ran a series of partial Pearson correlations. The analysis revealed a medium correlation between the number of fixated segments and the password strength, when considering the FD-I cognitive style as a control factor ($r = .323$, $p = .043$). When considering both the FD-I cognitive style and the image complexity as the control factors, a medium correlation between the passwords' strength and the number of fixated segments ($r = .306$, $p = .044$), and between the passwords strength and the fixation duration ($r = .319$, $p = .035$) was revealed. The results are summarized in Table 1.

	Fixated segments	Number of fixations	Fixation duration	Fixation distance
				No control factor
Password strength	r = .618 p = .041	r = .235 p = .116	r = .296 p = .044	r = .239 p = .109
				Controlling for FD-I cognitive style
Password strength	r = .323 p = .043	r = .207 p = .173	r = .268 p = .075	r = .214 p = .157
				Controlling for FD-I cognitive style and image complexity
Password strength	r = .306 p = .044	r = .225 p = .141	r = .319 p = .035	r = .003 p = .985

Table 1: Pearson correlation analysis between the security of the graphical passwords and the visual behavior metrics.

To further investigate the visual behavior of the study participants and understand whether there is an interaction between the FD-I cognitive style and the image complexity on the visual behavior metrics, we ran a mixed MANOVA test. The independent variables were the cognitive style (FD or FI) and the image complexity (simple and complex). The dependent variables of the test were the combined visual behavior metrics (number of fixations, number of fixated segments, fixation duration, and fixation distance). Residual analysis revealed that all the MANOVA assumptions were met (the dependent variables' data that was not normally distributed was transformed according to the approach proposed by [53]).

The interaction effect between the FD-I cognitive style and the image complexity on the combined visual behavior metrics was not statistically significant, $F = .408$, $p = .632$, Wilks' $\Lambda = .956$, partial $\eta^2 = .144$. However, there was a statistically significant main effect on the combined visual behavior metrics for the FD-I cognitive style ($F = 2.158$, $p = .048$, Wilks' $\Lambda = .801$, partial $\eta^2 = .397$), and the image complexity ($F = 3.828$, $p = .021$, Wilks' $\Lambda = .603$, partial $\eta^2 = .460$). Regarding the main effects of FD-I cognitive style on the visual behavior metrics, there was a statistically significant main effect for the number of fixated segments ($F = 5.358$, $p = .031$, partial $\eta^2 = .203$), the number of fixations ($F = 5.859$, $p = .025$, partial $\eta^2 = .218$), fixation duration ($F = 4.694$, $p = .042$, partial $\eta^2 = .183$), but not for fixation distance ($F = 2.149$, $p = .158$, partial $\eta^2 = .093$). All p-values are Bonferroni-adjusted. FDs produced 22.085 (95% CI, -.384 to 44.553, $p = .041$) more fixations than FIs on the simple background image. FDs fixated for 11.442 (95% CI, 3.559 to 17.194, $p = .037$) more seconds on the simple background image than the FIs. FDs fixated on 26.910 (95% CI, -1.725 to 55.545, $p = .043$) more segments in the simple background image than FIs. No main effects of the image complexity for any of the visual behavior metrics were revealed.



(a) (b)

Figure 4: (a) Gaze plots of a typical FD (left) and a typical FI (right) participant for the simple (top) and the complex (bottom) background image. (b) Fixation scatter plots of FDs (left) and FIs (right) for the simple (top) and the complex (bottom) image.

Interpretation of Results

FDs created stronger passwords than FIs when using the simple background image. Observing their visual behavior allowed us to draw conclusions about their approach during password composition. Despite that the saliency points of the image drew FDs' attention, they created their passwords not directly on the saliency points, but instead they used them as a reference for creating their passwords. They followed a holistic search approach, as shown in the gaze plot of a typical FD in Figure 4. They did not pay attention to details (e.g., wings, turbines), but used their creative thinking to draw their passwords, aiming to make them less predictable.

> *"The airplane is the center of the picture, so that's where all the others draw their passwords. I avoided drawing on it, but I drew my password around it"* ~ P02

> *"I split the image in the middle and created a graphical password around the jet, having the airframe as my starting point. I believe I created a symmetrical password, which I can easily remember"* ~ P14

We should note that none of the participants was aware of how the password strength is measured, but the FDs inherently assumed that it is related to the saliency point because, as they said, most people would draw their gestures on the airplane. On the other hand, FIs selected passwords following image shapes. The airplane drew their attention, as shown in the gaze plot of a typical FI in Figure 4, and they focused on identifying the shapes that could possibly be used to form their password. Their choices were based on extracting simple shapes. Circling the airplane, drawing lines on the wings, and taping the turbines are typical examples of passwords created by the FIs.

> *"I think I created a strong password, since I focused on the almost hidden details of the wings"* ~ P08

> *"I drew short gestures forming some of the letters of the brand, which was visible at the airframe"* ~ P19

On complex image, FIs created stronger passwords than FDs. FDs scanned the complex image around the saliency points and they focused on hands and gestures which reflected the interaction among the people. Given that FDs are more attentive to social cues than FIs [62], this could reflect their inherent need to communicate. Examples of gestures used by FDs are connecting lines between faces or lines following the gaze of the people in the image.

> *"I used lines to connect the gaze of two people"* ~ P11

> *"I tried to create a more complex password by drawing lines that cross the image and connect people"* ~ P20

On the other hand, FI individuals scanned the image starting by the faces. Then, their attention shifted to shapes and objects which, again, they used to accurately draw gestures. Circling objects, or creating lines on objects were common gestures used by the FIs.

> *"I like books, so I circled the book and then I noticed a pen, so I drew a line on the pen"* ~ P01

> *"I used certain characteristics of the people to create my passwords, e.g. eyes"* ~ P09

Finally, FIs created stronger passwords when using the complex image compared to when using the simple one. Given that the complex image included more saliency points, they were able to scan the image and use their analytical skills to detect simple shapes, which they used to draw their gestures. The saliency points of the simple image were limited; thus, they could not exploit their skills and draw unique gestures. Their abilities were confined by the poor, in terms of visual content, image. To conclude, results of the first study revealed that both the cognitive style and the complexity of the image affected the visual behavior of the participants. This is evident in the gaze and the scatter plots of Figure 4, which reveal that in both images FDs followed a more holistic visual exploration approach, while the FIs focused on shapes.

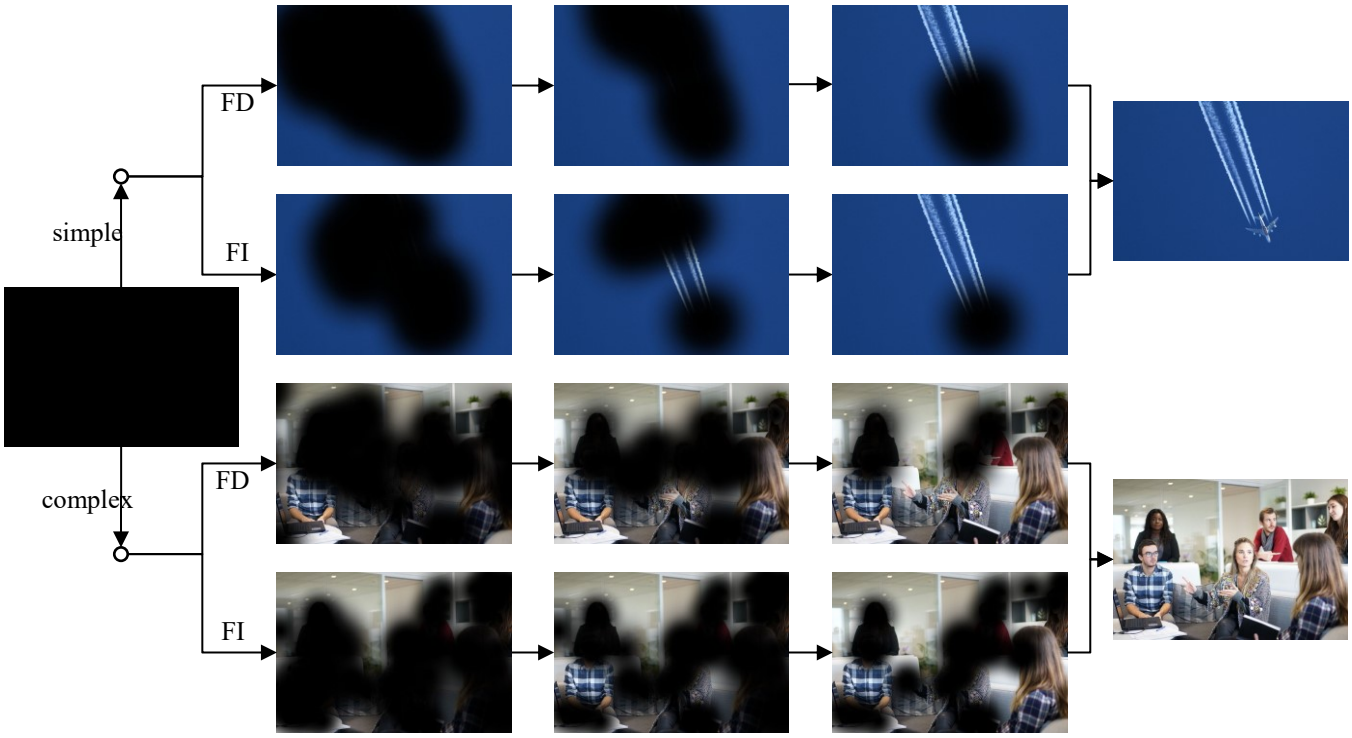


Figure 5: The image is totally covered at the beginning, and then the successive saliency levels based on the eye-tracking data of each cognitive group fade-out within 20 seconds.

COMPARATIVE STUDY

Considering the correlation between the visual behavior and the strength of the created passwords revealed in the exploratory study, we used the eye-tracking data of the FD and the FI individuals to create an assistive GUA mechanism based on saliency mask. Then, we conducted a user study to investigate the effects of this mechanism on the strength of the created passwords, and compare the mechanism with the initial one, from a cognitive and image complexity perspective.

Hypothesis

H0$_3$. There is no significant difference on the strength of the passwords created with and without the saliency masks of FD and FI individuals across background images of varying complexity.

Participants

Following the recruitment process described in the exploratory study, we recruited 40 individuals (17 females) for the second study. Their age ranged between 18 and 37 years (m = 32.1; sd = 5.8). 11 participants were undergraduate students; 15 participants were postgraduate students; 14 participants were professionals. Participants did not have any vision problems or wore glasses. The participants had no experience with and had never heard of cued-recall GUA schemes (e.g., PGA). Based on the users' GEFT scores, 22 participants were classified as FD, and 18 participants as FI (mean score = 12.15; sd = 5.68; min = 1; max = 18; cut-off score = 12). The scores of the participants were normally distributed according to the Shapiro-Wilk's test (p=.102).

Study Instruments

We used the same instruments as the ones described in the exploratory study. We added the saliency mask feature in the web-based picture passwords mechanism. Instead of using computational methods to create the saliency mask, such as in [10], we used the visual behavior of the FD and the FI users of our first study (i.e. the segments that each group fixated). Thus, we created one saliency mask based on the visual behavior of the FDs and one based on the visual behavior of the FIs, for each image. Instead of completely hiding the saliency points of the images, we were inspired by the "drawing the curtain" used by Thorpe et al. [54] where the image is first covered with a curtain (i.e. white foreground) and then the curtain is drawn from either right-to-left or left-to-right, gradually revealing the image beneath, and used a gaussian distribution algorithm to create saliency layers. Then, we created a fade-out effect starting from the highest saliency mask level (total black foreground) and ending to showing the image without any saliency mask applied. Following common practice [54], 20 seconds were required in total to display the image without any saliency mask. In Figure 5, we show screenshots of the saliency layers for the timestamps 0, 5, 10, 15, and 20 seconds. We added a start button, which the users had to click when ready to view the image. We used this approach to ensure that the user would focus on the image and would gain full advantage of the saliency mask mechanism. We used the GEFT test to elicit the cognitive style of the participants and the same tablet device and eye-tracking equipment as in the first study.

Procedure

The procedure we followed in the comparative study is similar to the procedure of the exploratory study. Each participant visited our lab at a previously agreed date and time. The study was conducted in a quiet room in our lab. The procedure involved the following steps: first, the participants undertook GEFT; their score was calculated, and they were classified either as FD or FI. Based on the classified cognitive style group, the facilitator adjusted the cognitive-dependent saliency-mask mechanism accordingly for the participant. Next, the participants wore the eye-tracking glasses and the calibration process [56] followed. Then, the users created a graphical password using a tablet device, on the two background images of varying complexity used in the exploratory study, along with the corresponding saliency mask for each one. After creating the first password, the facilitator changed the background image and asked the participant to refresh the web-page and follow the same process to create a second password. To avoid order effects, we counterbalanced the sequence of the background images. After creating the password, the participants were distracted for about 20 minutes with an activity similar to GEFT. Next, they used the created passwords for both images to log-in and answer a short questionnaire on demographics. Finally, an informal discussion on how the users created their graphical password took place. Prior to the study, participants were informed that the collected data during the session would be stored anonymously and would be used only for research purposes by the research group, and they provided their consent. No details regarding the research objective were provided.

Results

To investigate **H0$_3$**, we performed a mixed ANOVA, with the FD-I cognitive style (FD or FI), the image complexity (simple or complex), and the saliency mechanism (no-saliency or with-saliency) as the independent variables and the number of guesses needed to crack the password as the dependent variable. The test met all the assumptions (the data that was not normally distributed was transformed according to the approach proposed by [53]). The analysis revealed that there was no statistically significant three-way interaction between the password strength, the cognitive style, and the saliency mechanism, $F = 1.419$, $p = .239$, $\eta^2 = .028$. Focusing on the effect of the saliency mask mechanism, the analysis revealed that the individuals who created their graphical passwords using the saliency mask mechanism created stronger passwords than the individuals who used the original mechanism, $F = 12.342$, $p = .002$, $\eta^2 = .198$, accepted at a Bonferroni-adjusted alpha-level of .025. Focusing on the cognitive style, both FDs and FIs who used the saliency mask drawn stronger passwords on the complex background image than the FDs and FIs who used the original tool (FD: $F = 7.204$, $p = .010$, $\eta^2 = .126$; FI: $F = 3.596$, $p = .023$; $\eta^2 = .098$). Significant differences were also revealed for the passwords drawn on the simple background image by FIs ($F = 3.794$, $p = .021$; $\eta^2 = .101$), but not for FDs. The results are depicted in Figure 6.

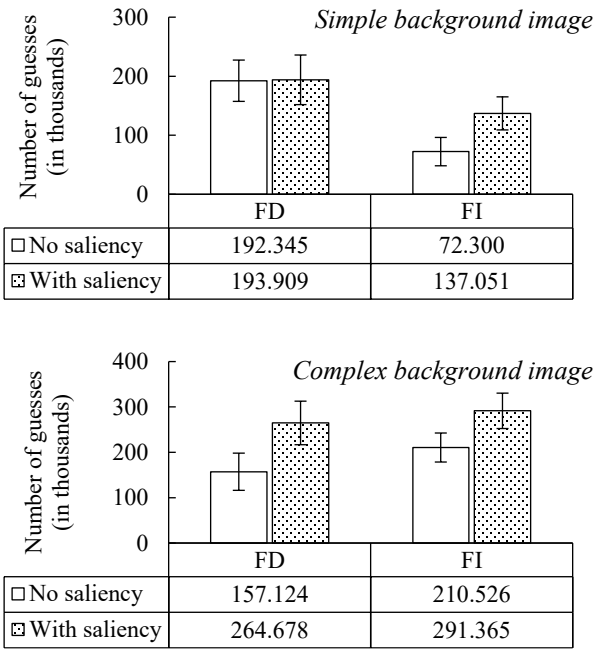


Figure 6: Saliency-mask mechanism helped both FD and FI individuals to create stronger passwords when having simple or complex background images (CI error bars are displayed).

Interpretation of Results

Regarding the simple image, the FDs were not affected by our mechanism, as their passwords were already strong. Similarly, to the case of the simple image of the exploratory study, they used the saliency points as reference points for drawing their gestures. On the other hand, FIs created stronger passwords compared to those created by the FIs in the exploratory study. Compared to the exploratory study, FIs extended the active drawing area of their gestures and used more combinations (e.g., they created passwords including all three gestures more often). As a result, they created stronger passwords than the passwords created by FIs when the saliency mask mechanism was not active (exploratory study). Despite that the strength of the passwords created by the FIs increased, they were still less strong when compared to those created by the FDs, as FIs focused again on the main parts of the airplane (i.e. primary point of interest), such as the airframe and the wings.

Regarding the complex image, both FDs and FIs created stronger passwords compared to those of the complex image of the exploratory study. FDs faced difficulties with processing visual complex scenes, and our mechanism allowed them to process more visual information because it was displayed gradually to them within 20 seconds. Hence, they had more time to conceptualize the context of the image and spot simple objects (e.g., notebook, pot), which they used to draw their gestures on. Likewise, our saliency mask mechanism helped FIs to identify various objects in the scene (e.g., pot on the self, ceiling lights), which were not among the primary attention points. Due to their skill to conceptualize details fast, they used such items to form their graphical password.

DISCUSSION AND IMPLICATIONS

The results of the exploratory study suggest that human cognitive factors and image complexity affect the graphical passwords' strength when using a recall-based GUA scheme. FD and FI individuals have unique characteristics that influence the approach they follow to create a graphical password, which is reflected on their visual behavior. The results of the comparative study suggest that personalized assistive mechanisms, bootstrapped on the unique cognitive characteristics of the users, can be used to improve the strength of the drawn passwords. Simple mechanisms, such as saliency masks, can draw FDs' and FIs' attention to image areas which are less likely to be used based on their visual behavior patterns, and thus help them create less predictable passwords. The findings of both studies are summarized in Table 2.

	No-saliency mask mechanism
Password Strength	FDs created stronger passwords than FIs when using a simple background image. FIs who used a complex background image created stronger passwords than FIs who used a simple background image to draw their gestures.
Visual Behavior	The more image segments a user fixated on, and the longer fixations he/she had, the stronger password he/she created. FDs produced more and longer fixations, fixated on more image segments, and had greater fixation distances than FIs
	Saliency mask mechanism
Password Strength	The passwords created when the saliency mask was active were stronger than the passwords created with the original scheme. Both FDs and FIs created stronger passwords when using the saliency mask mechanism, than the original GUA mechanism.

Table 2: Summarized findings regarding password security and users' visual behavior.

The contribution of the paper entails two important aspects; *theory* and *application*. Regarding theory, our exploratory study provides evidence that the individual cognitive characteristics influence users' choices when creating graphical passwords which are related to their visual behavior. Socio-cognitive theories, like FD-I, can be considered as applicable analysis frameworks in understanding and interpreting users' interactions and approaches in visual decision-making tasks, such as graphical password composition.

Regarding *application*, the analysis and discussion of results underpinned the value of considering cognitive styles as a human design factor and image complexity as a technology factor, in both design and run time, to avoid providing GUAs that unintentionally compromise the strength of the password created by people who share common cognitive characteristics. For example, FIs created less strong passwords than FDs when using a low complexity image. Considering that cognitive styles rarely change through lifespan [58], and that image complexity can be assessed through saliency filters [42], studies like the reported ones could drive the design of personalized GUAs that adapt to individual cognitive styles. Simple mechanisms (e.g., saliency masks) can be elaborated to help users of different cognitive styles improve their password's strength when using images of varying complexity.

Therefore, there is a need to transform the interdependencies between human and GUA design factors into formal representations modeling users' individual characteristics, and accordingly provide adaptive and personalized GUA schemes. Based on the Belk's et al. model [5], we propose a human factor-based formalization framework (Figure 7), which conceptually consists of two main modules; the *user modeling* module that is responsible for eliciting and storing the user's overall context of use during interaction (human and technology specific), and the *adaptation* module that is responsible to map human factors with GUA design factors aiming to deliver the most optimized GUA scheme to each user.

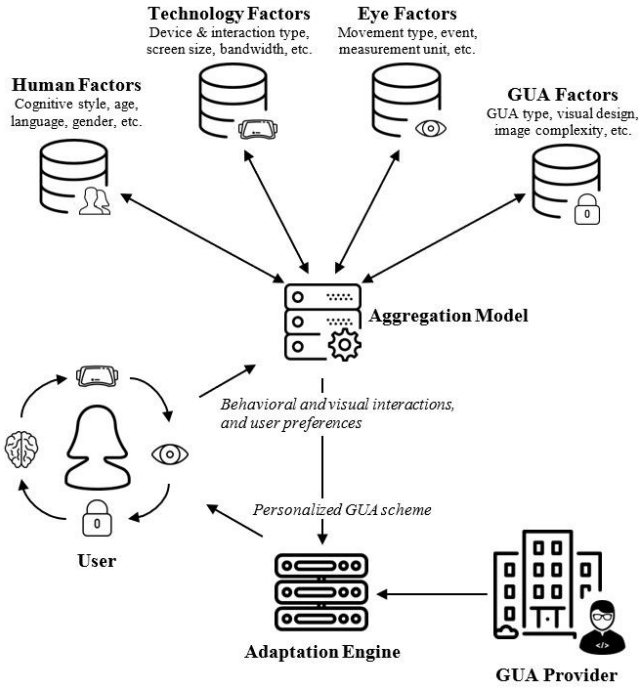


Figure 7: Conceptual design of an extensible framework specialized in delivering personalized GUA schemes

The main results of this study could be transformed into specific context-based recommendation rules, and be further applied in a procedure for recommending a specific GUA scheme and image complexity by considering the users' cognitive processing styles. Similarly with structure-based adaptive policies [51], cognitive-based adaptive policies could be considered for helping users who share common cognitive characteristics to create stronger graphical passwords. These would automatically evolve over time by taking advantage of the common behavioral patterns of the FDs and the FIs. For example, when several FDs have used specific points of images or gestures to create their password or have viewed specific areas of the images, future FDs would not be allowed to use them to create their passwords.

A challenging part of our proposed framework is the elicitation of *human cognition* and *image complexity* factors. Images can be either provided by the GUA scheme or the user can select them. Images selected by the users can be assessed by automatic processes, such as saliency detectors [42,65], entropy estimators [63], and content-based image retrieval techniques [57], to evaluate their complexity. The dataset provided by the GUA scheme could also be assessed by humans to provide a more natural identification of the attention points, for example, by using eye-tracking.

For the elicitation of human cognitive factors in run-time, the method proposed by Raptis et al. [44] could be used, as it is based on an eye-tracking multifactorial model. To evaluate the efficiency of our eye-tracking data, we performed a preliminary small-scale classification experiment following this method aiming to provide proof of concept results. We followed a 10-fold classification approach, mainly due to our small sample size for both background image complexity levels, and tested several classifiers towards the percentage of the correctly classified instances, using Weka software [20]. Logistic Regression classifier worked best for both simple and complex images, as it classified correctly 75% and 70% of the users respectively. Considering that FD-I cognitive style can be inferred in the early stages of the graphical password composition task [30] and that we move towards immersive technologies (e.g., virtual or mixed reality) which are based on natural interactions where visual search and exploration are primary processes, it is important to stress out that inferring human cognitive styles while performing a GUA authentication task in run-time is realistic.

LIMITATIONS

While we took great efforts to maintain our studies' validity, some design aspects of our experimental in-lab studies and the designed assistive feature for the GUA scheme introduce limitations. First, in our study we selected two specific background images, a simple and a complex to control the factors of the study and compare the user selection and visual behavior metrics. There is evidence that the context of the image may affect the user choice [59], nonetheless we have selected two representative images of the most widely used image categories (images including people [1,21] and images including a scenery and a single object [21,66]). Expanding our research to use more images would increase the validity of our study. Given that we conducted a controlled in-lab eye-tracking study the user behavior may have been influenced, although no such comment was received from the participants. Moreover, the sample size was rather small, but the performed statistical tests met all the required assumptions.

The classification of study participants as either FD or FI, was based on the GEFT score, and considering that the GEFT test highlights cognitive differences along a continuum scale, the use of a cut-off score may not classify correctly individuals that fall in between the two end points [15,33]. However, it is important to stress that the frequencies of users' GEFT scores in our sample are similar to general public GEFT scores [31,38,43,47]. The eye-tracking data we used to create our saliency masks was based on a relatively small dataset. Considering, though, that the visual behavior is associated with the cognitive style [45], we are confident that the derived saliency masks did not affect the efficiency of the assistive GUA scheme.

Finally, the approach used to crack the created passwords could not be applied to PGA, given that it only allows for 5 wrong password guesses before a character-based password is required. In addition, the guessing algorithm we used was very simple, but the aim of our study was not to create and test another cracking algorithm, but instead use this as a valid approach for measuring and comparing the strength of a given set of passwords. Despite the limitations, we expect that similar effects will be replicated in the contexts of different GUA schemes, contributing to the study's external validity. Similar findings, on FDs' and FIs' visual behavior, are expected to be found in studies which embrace eye-tracking analysis on visual decision-making tasks.

CONCLUSION

In this paper, we first reported the results of an eye-tracking study aiming to investigate the effects of FD-I cognitive style on the created passwords' strength using a cued recall GUA scheme and explain the results considering the visual behavior. Significant differences were revealed between the created passwords' strength of FDs and FIs, and on the visual behavior of FDs and FIs which were strongly correlated with the passwords' strength. Hence, this paper provides evidence that users with different cognitive style follow different strategies when creating graphical passwords on images of varying complexity and their visual behavior suggests whether their choices will lead to strong passwords.

Triggered by the results of the first study, we designed an assistive mechanism based on the visual behavior of the FDs and the FIs, which we used as saliency mask on the same background images, and conducted a comparative study. Results reveal that the approach we suggested improved the created passwords' strength, reinforcing our assumption that adaptive mechanisms based on the cognitive styles, can provide a feasible solution for creating stronger passwords. Therefore, this work provides evidence that the cognitive styles of the users can be used to provide personalized experiences. The results of our study are summarized in Table 2.

We are encouraged by the results of our work that using cognitive styles for designing personalized assistive features for GUA mechanisms is worth further exploration, and we are eager to design and evaluate more cognitive style-based features to better support the users when creating graphical passwords. Apart from password creation, we intend to investigate the effects of cognitive styles in login, and design and test different adaptive policies. Considering the shift towards immersive technologies and the increasing role of the eye in such environments, there is room for expanding our research in this context.

REFERENCES

1. Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '15*, 316–322. https://doi.org/10.1145/2785830.2785882
2. A. De Angeli, M. Coutts, L. Coventry, G.I. Johnson, D. Cameron, and M.H. Fischer. 2002. VIP: A visual approach to user authentication. In *Proceedings of the Workshop on Advanced Visual Interfaces AVI*, 316–323. https://doi.org/10.1145/1556262.1556312
3. Charoula Angeli, Nicos Valanides, and Paul Kirschner. 2009. Field dependence–independence and instructional-design effects on learners' performance with a computer-modeling tool. *Computers in Human Behavior* 25, 6: 1355–1366. https://doi.org/10.1016/j.chb.2009.05.010
4. Ulku Arslan Aydin, Cengiz Acarturk, and Kursat Cagiltay. 2013. The Role of Visual Coherence in Graphical Passwords. In *Proceedings of the Annual Meeting of the Cognitive Science Society*.
5. Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2015. Do human cognitive differences in information processing affect preference and performance of CAPTCHA? *International Journal of Human-Computer Studies* 84: 1–18. https://doi.org/10.1016/j.ijhcs.2015.07.002
6. 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*. https://doi.org/10.1016/j.chb.2017.06.042
7. Marios Belk, Panagiotis Germanakos, Christos Fidas, and George Samaras. 2013. Studying the effect of human cognition on user authentication tasks. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 102–113. https://doi.org/10.1007/978-3-642-38844-6_9
8. 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*, 252–259. https://doi.org/10.1145/3106426.3106488
9. Sacha Brostoff and M Angela Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *People and Computers XIV — Usability or Else!* Springer London, London, 405–424. https://doi.org/10.1007/978-1-4471-0515-2_27
10. 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 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*, 3011. https://doi.org/10.1145/2207676.2208712
11. Hsin-Yi Chiang and Sonia Chiasson. 2013. Improving user authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*, 251. https://doi.org/10.1145/2493190.2493213
12. Sonia Chiasson, Robert Biddle, and P. C. van Oorschot. 2007. A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07*, 1. https://doi.org/10.1145/1280680.1280682
13. Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. 2009. User interface design affects security: Patterns in click-based graphical passwords. *International Journal of Information Security* 8, 6: 387–398. https://doi.org/10.1007/s10207-009-0080-7
14. Sonia Chiasson, Pc Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *Computer Security–ESORICS ...*, 359–374. https://doi.org/10.1007/978-3-540-74835-9_24
15. Edward E. Cureton. 1957. The upper and lower twenty-seven per cent rule. *Psychometrika* 22, 3: 293–296. https://doi.org/10.1007/BF02289130
16. Darren Davis, Fabian Monrose, and Michael K Reiter. 2004. On User Choice in Graphical Password Schemes. In *In 13th USENIX Security Symposium*.
17. Rachna Dhamija and Adrian Perrig. 2000. Deja Vu-A User Study: Using Images for Authentication. In *USENIX Security Symposium*, 4.
18. Ahmet Emir Dirik, Nasir Memon, and Jean-Camille Birget. 2007. Modeling user choice in the PassPoints graphical password scheme. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07*, 20. https://doi.org/10.1145/1280680.1280684
19. Andrew Duchowski. 2007. Eye tracking methodology: Theory and practice. *Eye Tracking Methodology: Theory and Practice*: 1–328. https://doi.org/10.1007/978-1-84628-609-4
20. Paul Dunphy, Andreas P. Heiner, and N. Asokan. 2010. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1. https://doi.org/10.1145/1837110.1837114
21. 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*, 36. https://doi.org/10.1145/1315245.1315252

22. Katherine M. Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. 2009. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, 889. https://doi.org/10.1145/1518701.1518837
23. Joseph Goldberg, Jennifer Hagman, and Vibha Sazawal. 2002. Doodling our way to better authentication. In *CHI '02 extended abstracts on Human factors in computing systems - CHI '02*, 868. https://doi.org/10.1145/506443.506639
24. Jon-Chao Hong, Ming-Yueh Hwang, Ker-Ping Tam, Yi-Hsuan Lai, and Li-Chun Liu. 2012. Effects of cognitive style on digital jigsaw puzzle performance: A GridWare analysis. *Computers in Human Behavior* 28, 3: 920–928. https://doi.org/10.1016/j.chb.2011.12.012
25. Wei Hu, Xiaoping Wu, and Guoheng Wei. 2010. The Security Analysis of Graphical Passwords. In *2010 International Conference on Communications and Intelligence Information Security*, 200–203. https://doi.org/10.1109/ICCIIS.2010.35
26. L. Huestegge and L. Pimenidis. 2014. Visual Search in Authentication Systems Based on Memorized Faces: Effects of Memory Load and Retention Interval. *International Journal of Human-Computer Interaction* 30, 7: 604–611. https://doi.org/10.1080/10447318.2014.907464
27. Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K Reiter, and Aviel D Rubin. 1999. The Design and Analysis of Graphical Passwords. *Proceedings of the 8th USENIX Security Symposium 8*, 1. https://doi.org/10.1109/ICCIIS.2010.35
28. Jeffrey Jay Johnson, Steve Seixeiro, Zachary Pace, Giles van der Bogert, Sean Gilmour, Levi Siebens, and Kenneth Tubbs. 2014. Picture Gesture Authentication. Retrieved from https://www.google.com/patents/US8910253
29. Christina Katsini, Christos Fidas, Marios Belk, Nikolaos Avouris, and George Samaras. 2017. Influences of Users' Cognitive Strategies on Graphical Password Composition. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '17*, 2698–2705. https://doi.org/10.1145/3027063.3053217
30. 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 *Proceeding of the 23rd International Conference on Intelligent User Interfaces - IUI '18*. https://doi.org/10.1145/3172944.3172996
31. Mohammad Khatib and Rasoul Mohammad Hosseinpur. 2011. On the Validity of the Group Embedded Figure Test (GEFT). *Journal of Language Teaching and Research* 2, 3: 640–648. https://doi.org/10.4304/jltr.2.3.640-648
32. Oleg V Komogortsev, Denise V Gobert, Sampath Jayarathna, Do Hyong Koh, and Sandeep M Gowda. 2010. Standardization of Automated Analyses of Oculomotor Fixation and Saccadic Behaviors. *IEEE Transactions on Biomedical Engineering* 57, 11: 2635–2645. https://doi.org/10.1109/TBME.2010.2057429
33. Min Liu and W Michael Reed. 1995. The relationship between the learning strategies and learning styles in a hypermedia environment. *Computers in Human Behavior* 10, 4: 419–434.
34. Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes! In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 1. https://doi.org/10.1145/1572532.1572542
35. Weizhi Meng, Wenjuan Li, Lijun Jiang, and Liying Meng. 2016. On Multiple Password Interference of Touch Screen Patterns and Text Passwords. In *Chi '16*, 4818–4822. https://doi.org/10.1145/2858036.2858547
36. Martin Mihajlov and Borka Jerman-Blažič. 2011. On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers* 23, 6: 582–593. https://doi.org/10.1016/j.intcom.2011.09.001
37. Martin Mihajlov, Borka Jerman-Blažič, and Anita Ciunova Shuleska. 2016. Why That Picture? Discovering Password Properties in Recognition-Based Graphical Authentication. *International Journal of Human–Computer Interaction* 32, 12: 975–988. https://doi.org/10.1080/10447318.2016.1220103
38. Efi A. Nisiforou, Eleni Michailidou, and Andrew Laghos. 2014. Using Eye Tracking to Understand the Impact of Cognitive Abilities on Search Tasks. . 46–57. https://doi.org/10.1007/978-3-319-07509-9_5
39. Philip K Oltman, Evelyn Raskin, and Herman A Witkin. 1971. *Group embedded figures test*. Consulting Psychologists Press Palo Alto, CA.
40. P. C. Van Oorschot and Julie Thorpe. 2011. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security* 19, 4: 699–702. https://doi.org/10.3233/JCS-2010-0411
41. Zachary Pace. 2011. Signing in with a picture password. Retrieved from https://blogs.msdn.microsoft.com/b8/2011/12/16/signi

ng-in-with-a-picture-password/

42. F. Perazzi, P. Krahenbuhl, Y. Pritch, and A. Hornung. 2012. Saliency filters: Contrast based filtering for salient region detection. In *2012 IEEE Conference on Computer Vision and Pattern Recognition*, 733–740. https://doi.org/10.1109/CVPR.2012.6247743

43. George E. Raptis, Christos A. Fidas, and Nikolaos M. Avouris. 2016. Do Field Dependence-Independence Differences of Game Players Affect Performance and Behaviour in Cultural Heritage Games? In *Proceedings of the 2016 Annual Symposium on Computer-Human Interaction in Play - CHI PLAY '16*, 38–43. https://doi.org/10.1145/2967934.2968107

44. George E. Raptis, Christina Katsini, Marios Belk, Christos Fidas, George Samaras, and Nikos Avouris. 2017. Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. *Springer User Modeling, Adaptation, and Personalization (UMAP 2017)*. https://doi.org/10.1145/3079628.3079690

45. George E Raptis, Christos A Fidas, and Nikolaos M Avouris. 2016. Using Eye Tracking to Identify Cognitive Differences. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics - PCI '16*, 1–6. https://doi.org/10.1145/3003733.3003762

46. R.J. Riding and J. Ashmore. 1980. Verbaliser-Imager Learning Style and Children's Recall of Information Presented in Pictorial versus Written Form. *Educational Studies* 6, 2: 141–145. https://doi.org/10.1080/0305569800060204

47. Kent A. Rittschof. 2010. Field dependence–independence as visuospatial and executive functioning in working memory: implications for instructional systems design and research. *Educational Technology Research and Development* 58, 1: 99–114. https://doi.org/10.1007/s11423-008-9093-6

48. Amir Sadovnik and Tsuhan Chen. 2013. A visual dictionary attack on Picture Passwords. In *2013 IEEE International Conference on Image Processing*, 4447–4451. https://doi.org/10.1109/ICIP.2013.6738916

49. Amirali Salehi-Abari, Julie Thorpe, and P. C. Van Oorschot. 2008. On purely automated attacks and click-based graphical passwords. *Proceedings - Annual Computer Security Applications Conference, ACSAC*: 111–120. https://doi.org/10.1109/ACSAC.2008.18

50. Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. https://doi.org/10.1145/2501604.2501615

51. 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. *e Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*: 1–12. Retrieved from https://www.usenix.org/system/files/conference/soups2017/soups2017-segreti.pdf

52. Elizabeth Stobert and Robert Biddle. 2013. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. https://doi.org/10.1145/2501604.2501619

53. Gary F. Templeton. 2011. A two-step approach for transforming continuous variables to normal: Implications and recommendations for IS research. *Communications of the Association for Information Systems* 28, 1: 41–58.

54. Julie Thorpe, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. 2014. The presentation effect on graphical passwords. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, 2947–2950. https://doi.org/10.1145/2556288.2557212

55. Julie Thorpe and P C Van Oorschot. 2007. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords * 1. *16th USENIX Security Symposium*: 8. Retrieved from http://dl.acm.org/citation.cfm?id=1362903.1362911%5Cnhttp://www.usenix.org/event/sec07/tech/full_papers/thorpe/thorpe_html/

56. Tobii AB. Tobii Pro Glasses Analyzer User's Manual.

57. Xiang-Yang Wang, Yong-Wei Li, Pan-Pan Niu, Hong-Ying Yang, and Dong-Ming Li. 2014. Content-based Image Retrieval using Visual Attention Point Features. *Fundamenta Informaticae* 135: 309–329. https://doi.org/10.3233/FI-2014-1124

58. Seymour Wapner and Jack Demick. 1992. Field Dependence-Independence in Adult Development and Aging. *Field Dependence-independence Bio–psycho-social Factors Across the Life Span*: 245–268.

59. Susan Wiedenbeck, Jim Waters, and Jc Birget. 2005. Authentication using graphical passwords: effects of tolerance and image choice. *Proceedings of the …*: 1–12. https://doi.org/10.1145/1073001.1073002

60. 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: 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010

61. H. A. Witkin, C. A. Moore, D. R. Goodenough, and P.

W. Cox. 1975. Field-Dependent and Field-Independent Cognitive Styles and Their Educational Implications. *ETS Research Bulletin Series* 1975, 2: 1–64. https://doi.org/10.1002/j.2333-8504.1975.tb01065.x

62. Herman A. Witkin and Donald R. Goodenough. 1976. Field Dependence and Interpersonal Behavior. *ETS Research Bulletin Series* 1976, 1: i-78. https://doi.org/10.1002/j.2333-8504.1976.tb01098.x
63. Honghai Yu and Stefan Winkler. 2013. Image complexity and spatial information. In *2013 Fifth International Workshop on Quality of Multimedia Experience (QoMEX)*, 12–17. https://doi.org/10.1109/QoMEX.2013.6603194
64. Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the wild. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*, 261. https://doi.org/10.1145/2493190.2493231
65. Jianming Zhang and Stan Sclaroff. 2013. Saliency detection: A boolean map approach. *Proceedings of the IEEE International Conference on Computer Vision*: 153–160. https://doi.org/10.1109/ICCV.2013.26
66. Ziming Zhao, Gail-Joon Ahn, and Hongxin Hu. 2015. Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation. *ACM Transactions on Information and System Security* 17, 4: 1–37. https://doi.org/10.1145/2701423
67. Ziming Zhao, Gail-joon Ahn, and G F S Technology. 2013. On the Security of Picture Gesture Authentication On the Security of Picture Gesture Authentication. *In Proceedings of SS 2013*: 383–398.