An Empirical Study of Picture Password Composition on Smartwatches

Marios Belk[1,2], Christos Fidas[3], Eleni Katsi[2], Argyris Constantinides[2,4], Andreas Pitsillides[2]

[1]Cognitive UX GmbH, Heidelberg, Germany
belk@cognitiveux.de
[2]Department of Computer Science, University of Cyprus, Nicosia, Cyprus
ekatsi03@cs.ucy.ac.cy, andreas.pitsillides@cs.ucy.ac.cy
[3]Department of Electrical and Computer Engineering, University of Patras, Patras, Greece
fidas@upatras.gr
[4]Cognitive UX LTD, Nicosia, Cyprus
argyris@cognitiveux.com

Abstract. Recent research works suggest that human cognitive differences affect security and usability of picture passwords within a variety of interaction contexts, such as conventional desktops, smartphones, and extended reality. However, the interplay of human cognition towards users' interaction behavior and security of picture passwords on smartwatch devices has not been investigated so far. In this paper, we report on such a research attempt that embraced a between-subjects in-lab user study (n=50) in which users were classified according to their cognitive processing characteristics (*i.e.*, Field Dependence-Independence cognitive differences), and further composed a picture password on a smartwatch device. Analysis of results reveal that already known effects of human cognition towards interaction behavior and security of picture passwords within conventional interaction contexts, do not necessarily replicate when these are deployed on smartwatch devices. Findings point towards the need to design for diversity and device-aware picture password schemes.

Keywords: Graphical Authentication, Human Cognition, Efficiency, Security.

1 Introduction

Research on smartwatch user authentication has become a complex endeavor, since it entails a variety of factors that affect human behavior, security and user experience [1-5]. Smartwatch-based user authentication is primarily achieved with Personal Identification Numbers (PIN) and Pattern Lock [1, 6]. User authentication methods on smartwatch devices can be grouped in two broad categories.

Knowledge-based user authentication approaches include CirclePin [6], which asks users to enter a PIN through a 10-item color index using the smartwatch crown; Draw-a-Pin [7], which authenticates users by drawing the PIN on the touchscreen; 2GesturePIN [8], which requires from users to conduct two gestures through the smartwatch

rotating bezel or crown; TapMeIn [9], that allows users to tap a secret and memorable melody on the screen; and Personal Identification Chord [10], a chorded keypad that allows users to enter various tap-based inputs. Studies have also investigated the effectiveness of user authentication methods on smartwatch devices [1, 11].

Biometric-based user authentication approaches have been proposed that leverage on device-specific signals (*e.g.*, accelerometer, physiological, heart rate, etc.), including MotionAuth [12], which authenticates users by analyzing their gestures (raising/lowering hand, rotation, circle) utilizing a smartwatch; iAuth [13], which continuously authenticates users by exploiting built-in device sensors; and SoundCraft [14] that authenticates users based on non-vocal hand acoustics.

In this paper, we focus on knowledge-based user authentication schemes and in particular on *picture passwords* [15], which require from users to select regions on a background image that acts as a cue. Picture password authentication already represents an alternative knowledge-based user authentication scheme in conventional interaction contexts (*e.g.*, desktops, smartphones, etc.) [15] and used daily by millions of users [16]. However, picture passwords have not been deployed and investigated within smartwatch-based interaction contexts, despite the fact that they can leverage on the picture superiority effect, suggesting that individuals are effective in recalling visual information [15, 17], and they can be easily adapted for touch interaction [5].

Picture password systems require from users to perceive, represent and recall visual information that is processed on a cognitive level, and researchers have studied the effects of human cognitive differences in information processing on various aspects of user authentication [5, 18-21, 35], which are described next.

2 Related Work and Research Motivation

Field Dependence-Independence (FD-I) is considered an accredited theory [22-25], which indicates the users' abilities to extract relevant information in visual scenes. *Field Dependent (FD)* individuals obtain experiences through an integral approach and their perception can be easily affected by the environment. They are not attentive to detail, tend to handle problems in a holistic way and they are not efficient and effective in extracting relevant information from a complex whole [5, 26]. *Field Independent (FI)* individuals can obtain experiences through analysis and their perception is not easily affected by the context. FI users are effective in disembedding information from a complex whole, they prefer to handle it in an analytical way and are able to distinguish pertinent visual information embedded in an image [5, 26].

From a human cognition perspective, prior research has shown FD-I effects on *picture password exploration and composition time* [18, 5], and *password selections* [19] within conventional interaction contexts, *i.e.*, desktops, smartphones, extended reality. For example, the work in [18, 5] revealed that FD users spend more time to explore and compose a picture password on desktop and mixed reality devices compared to FI users. The work in [19, 35] showed that FD users make stronger password selections than FI users during picture password composition on desktop computers.

In this context, we further examine whether such effects continue to hold when picture passwords are deployed on smartwatch devices. Hence, the contribution of this paper is two-fold: *a)* we deploy picture password schemes on smartwatch devices, which is the first attempt so far to the best of our knowledge, and we study users' interaction behavior and security under the light of an accredited human cognition theory (*i.e.*, Witkin's Field Dependence-Independence [22]); and *b)* we provide initial empirical evidence on the effects of human cognition towards users' interaction behavior and security of smartwatch-based picture passwords.

3 Method of Study

3.1 Null Hypotheses

***H*$_{01}$.** There are no interaction effects between FD-I users and password selections towards picture password composition efficiency on smartwatch devices.

***H*$_{02}$.** There are no significant differences between FD-I users towards picture password security on smartwatch devices.

3.2 Research Instruments

Picture Password System. A cued-recall-based graphical authentication system (**Figure 1**) was designed and developed, following guidelines of Microsoft Windows 10^{TM} Picture Gesture Authentication [29] in which users create selections on a background image that acts as a cue. For representing the users' selections, the system creates a 4x4 grid on the image, and consequently, stores the corresponding segment that was selected. Users are asked to make five click-based selections (repeated selections are allowed) in a specific order aiming to achieve a comparable theoretical key space of PIN-based authentication on the picture password. Specifically, a six-digit PIN yields 10^6 combinations, with a theoretical entropy of $log_2(10^6)$=19.93 bits, while a five-click-based selection on a 4x4 image grid yields 16^5 combinations, with a theoretical entropy of $log_2(16^5)$=20 bits.

Smartwatch Device. The picture password system was deployed on a Fitbit Versa smartwatch (https://www.fitbit.com), which has a 1.34'' and 300x300 pixels display.

Picture Password Image. We intentionally chose an image that would include Points of Interests (PoI – regions on an image that attract the users' attention) across four quadrants, and including widely applied image semantics (*i.e.*, scenery [33]). **Figure 1** illustrates the picture password and background image used in the study, and its corresponding saliency map that indicates the Points of Interests.

Cognitive Factor Elicitation. We used Witkin's Group Embedded Figures Test (GEFT) [30], which is an accredited and widely applied paper-and-pencil test [5, 18, 19, 26, 27]. The test measures the user's ability to find common geometric shapes in a larger design. Depending on the users' responses, scores range between 0-18. Using a widely applied cut-off score [5, 18, 19, 26], users that identify less than 12 items are classified as FD, and users that identify 12 items and more are classified as FI.

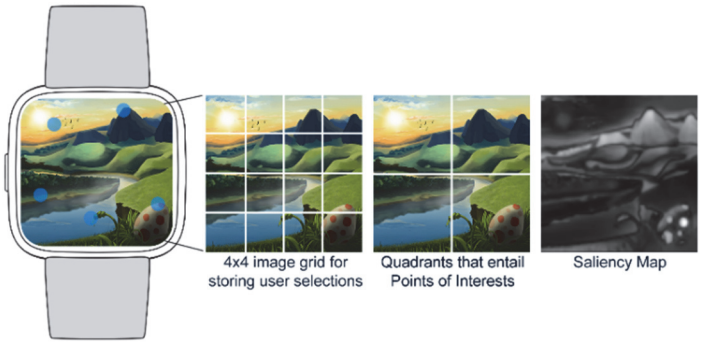

Fig. 1. Picture password and background image used in the study, and its corresponding saliency map that indicates the Points of Interests.

3.3 Sampling and Procedure

A total of 50 individuals participated in the user study with ages ranging between 21 to 44 years old (*m*=32; *sd*=5.7). All individuals participated voluntarily and could opt-out from the study at any time. All participants were familiar with using smartwatches and PIN-based authentication. No participant was familiar with picture passwords. Based on the users' GEFT scores, 21 participants were classified as FD and 29 participants as FI (GEFT scores: *m*=12.34; *sd*= 4.26; *min*=2; *max*=18).

We adopted the University's human research protocol that considers users' privacy, confidentiality and anonymity. Participants were invited and visited the researchers' laboratory at a time convenient for the participants. The user study was conducted with one individual at a time. Participants were informed about the study, and were asked to read, accept and sign a consent form to participate. Once participants accepted and signed the consent form, the GEFT test was administered aiming to highlight the participants' cognitive characteristics (*i.e.*, classify them as FD *vs.* FI). Participants were then instructed to wear the smartwatch on the hand they usually wear one and familiarized themselves with the picture password system on the smartwatch. Aiming to increase ecological validity of the study, we asked participants to compose a picture password that would be used to access individual data on the smartwatch.

3.4 Data Metrics

The following data were measured: *i) visual exploration and overall password composition time:* visual exploration time includes the time as soon as the user is shown with the task until the user makes the first password selection, and overall password composition time further includes the time until the user successfully completes the password composition task; and *ii) picture password strength:* we adopted a widely used metric for picture password strength [16, 31] by calculating *password guessability*, which is the number of guesses required to crack the users' passwords. Following prior approaches that consider Points of Interests (PoI) [16, 19, 31, 32], we used a PoI-assisted brute-force attack model [16] starting from segments covering the PoIs, then checking the neighboring segments, and finally checking the rest segments.

4 Analysis of Results and Main Findings

4.1 Interaction Effects between FD-I Users and Password Selections towards Picture Password Composition Efficiency on Smartwatch Devices (H_{01})

To investigate H_{01}, we ran a two-way mixed analysis of variance (ANOVA) with the FD-I group (FD *vs.* FI) and users' password selections (five consecutive selections) as the independent variables, and the time to make each password selection as the dependent variable. There was a statistically significant interaction between the FD-I group and users' password selections on the overall time to compose the picture password, $F(1, 48)=7.11$, $p<.01$, *partial* $\eta^2=.129$. **Figure 2** depicts the time to make each of the five password selections.

Given the interaction effect, we further examined simple main effects for each password selection. Data are mean ± standard error, unless otherwise stated. The analysis revealed that visual exploration time, *i.e.*, from start until making the first password selection between the two groups, was statistically significant (FD: 3.14 ± .34 sec *vs.* FI: 2.21 ± .29 sec) with a mean difference of .927 seconds, $F(1, 48)=4.161$, $p=.047$, *partial* $\eta^2=.08$. For the remaining four password selections (selections 2-5), there were no significant differences between the FD and FI group ($p>.05$).

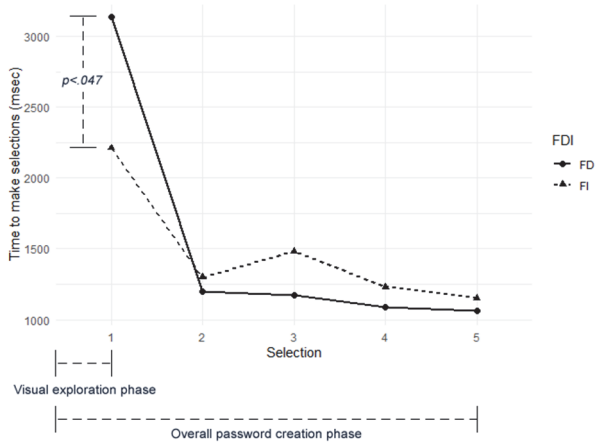

Fig. 2. Time to make password selections. Results reveal significant differences between FD-I users in exploration time (*i.e.*, from start until making the first password selection), whereas in the remaining four password selections (selections 2-5), there are no significant differences.

Main Finding related to H_{01}. FD users spent significantly more time exploring the image prior making their first selection (visual exploration phase). This can be explained by the fact that FD users (having more trained the global information processing stream) [22-25], spent more time exploring the visual cue since they follow a more holistic and exploratory approach during visual search compared to FI users, who typically focus on specific focal points of an image during interaction.

This finding is in line with prior studies on investigating FD-I effects on password composition time in desktop computers and mixed reality [18, 5]. Hence, existing

effects continue to exist when picture passwords are deployed on smartwatch devices. Another interpretation can be based on the fact that FI users might be more efficient in adapting to contextual and field changes (desktop *vs.* smartwatches) than FD users, who need more time to adapt to new interaction design paradigms, further supporting previous findings in the field [5, 18, 26-28]. Furthermore, this study is also in line with previous cognitive studies in a different context [34], which revealed that the holistic and analytic behaviors of FD and FI users are respectively amplified when interacting with mixed reality environments compared to conventional desktops.

4.2 Differences between FD-I Users towards Picture Password Security Aspects on Smartwatch Devices (H_{02})

We ran a Welch t-test to determine whether the two user groups (FD *vs.* FI) generated different password strengths in terms of password guessability, due to the assumption of homogeneity of variances being violated, as assessed by Levene's test for equality of variances (p=.044). Results revealed significant differences with a mean difference of 169K guesses (95% CI, -317K to -20K), t(47.633)=-2.289, p=.027. In particular, user-chosen picture passwords of the FD group required 278K guesses to crack, while those of the FI group required 447K guesses to crack. **Figure 3** illustrates the percentage of passwords cracked indicating that FI users exhibited lower percentage of passwords cracked than FD users. The percentage of picture passwords cracked reached 100% for both groups within 2^{20} guesses, which is the picture password key space. Also, a spike occurred after 2^{18} attempts.

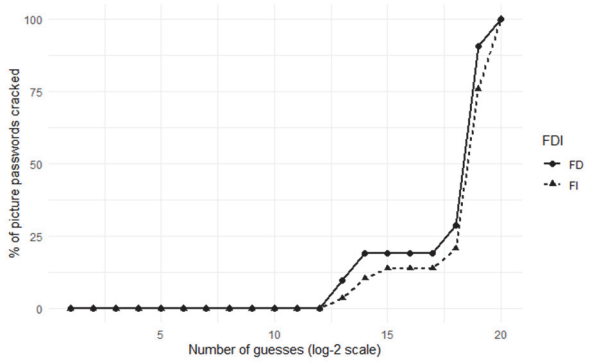

Fig. 3. Percentage of picture passwords cracked, as assessed by the PoI-assisted attack model [16]. FI users exhibited lower percentage of picture passwords cracked than FD users.

We further conducted an analysis on the user password segment selections of the picture password. **Figure 4** illustrates an intensity map of the frequencies of user password selections on the background image of the picture password system among FD-I groups. Each column illustrates the layout of the image grid, with each cell representing a segment in which a user password selection is made. Cell colors indicate the frequency at which each segment was selected as the first, second, third, fourth or fifth selection (darker colors indicate higher frequencies).

We ran a chi-square goodness-of-fit test to determine whether the selected segments are evenly distributed across the entire image grid for both user groups. For doing so, we further split the image in four even quadrants and calculated the frequencies of user password selections of each quadrant. In the FD group, the number of selected segments are statistically significantly different among the quadrants ($\chi^2(3)=13.133$, $p=.004$). In the FI group, the number of selected segments are not statistically significantly different among the quadrants ($\chi^2(3)=1.78$, $p=.61$).

Finally, we analyzed the participants' selections with regards to PoI segments. We ran an independent-samples t-test, with the FD-I group as the independent variable, and the proportion of selections falling into PoI segments as the dependent variable. There was homogeneity of variances, as assessed by Levene's test for equality of variances ($p=.07$). There were no significant outliers in the data, as assessed by inspection of boxplots, and data were normally distributed, as assessed by Shapiro-Wilk's test ($p>.05$). The analysis revealed that FD users had a higher proportion of selections that fall into PoI segments (73.33% ± 21.29%) than FI users (60.68% ± 18.11%), a statistically significant difference of 12.64% ± 5.58% (95% CI, 1.4 to 23.87), $t(48)=2.263$, $p=.033$.

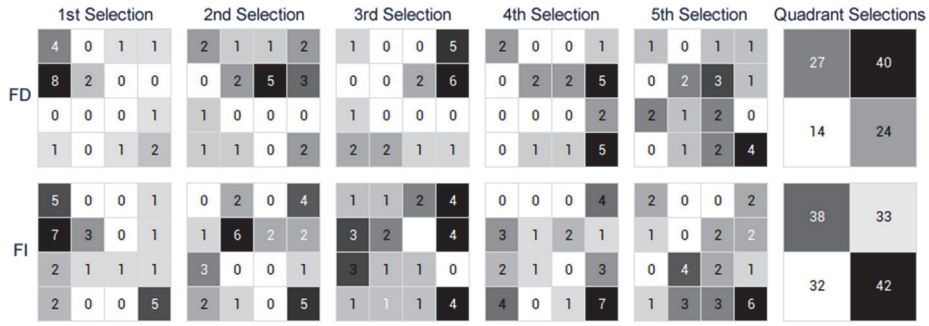

Fig. 4. Frequencies of user selections on the image of the picture password system. User choices of FI users are more evenly distributed across the entire grid, compared to FD users.

Main Finding related to H_{02}. FI users created significantly stronger picture passwords than FD users. The PoI-assisted brute-force attack required 278K guesses to crack FD passwords, and 447K guesses to crack FI passwords. The intensity map of user selections further revealed that user choices of the FI user group were more evenly distributed across the entire grid, compared to the FD group. Given that user password selections of the FI group entailed more randomness, this can explain the improved security strength compared to the FD group. In addition, FD users had a higher proportion of selections that fall into PoI segments compared to the FI users.

Prior research has shown that FD users create stronger passwords than FI users [19] when composing picture passwords on conventional desktop devices since FI users typically tend to select Points of Interests (PoIs – regions that attract the users' attention and are prone to brute-force attacks) due to their inherent ability to focus on the details. In contrary, in this study we found an opposite main effect, which can be explained by the limited screen size and visual field that might have affected the users' selections

towards certain regions that would not take place when the background image would have been deployed on a conventional desktop computer with a larger visual field and clearer attention points. Finally, findings also indicate that users in general tend to make password selections that are based on generic PoI segments, which is in line to recent research [32, 36] that revealed similar observations in desktop interaction contexts.

5 Conclusions and Future Work

In this paper we investigate whether deploying picture passwords on smartwatch devices embraces similar effects of human cognition towards users' interaction behavior and picture password security, as shown in previous studies in conventional interaction contexts [18, 5, 19]. For doing so, we adopted an accredited human cognition theory (Witkin's Field Dependence-Independence) and conducted a between-subjects in-lab user study (n=50) in which participants composed a picture password that was deployed on a smartwatch device.

With regards to Points of Interests (PoI) selections and password composition time, results reveal consistent effects with previous studies, *i.e.*, FD users spend more visual exploration and password composition time than FI users [18, 5], and users tend to make selections based on generic PoI regions [32, 36]. On the counter side, results reveal opposite main effects with regards to picture password strength compared to the literature [19]. Specifically, in contexts where the visual field of interaction is larger (*i.e.*, desktop, mixed reality), FD users create stronger and more random passwords compared to FI users due to their holistic approach in visual information processing. However, when the interaction is held on smaller screen sizes such as smartwatch devices, an opposite effect is revealed given that small areas for visual exploration do not allow full deployment of holistic-type information processing streams and decision-making during picture password selection.

Limitations of the study are related to the fact that only one picture was used for composing the passwords with a specific complexity. Nevertheless, the picture was intentionally chosen based on its complexity, which included widely applied image semantics and points of interest (*i.e.*, scenery and real-life objects [33]). Furthermore, the study was run in a controlled in-lab setting, which might have affected the behavior of users. Nonetheless, we aimed to increase ecological validity by applying the picture password composition task in a real task-based scenario in which users created a picture password for accessing individual data on the smartwatch.

Acknowledgements. This research has been partially supported by the EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums), the Research and Innovation Foundation (Project DiversePass: COMPLEMENTARY/0916/0182), and the European project TRUSTID - Intelligent and Continuous Online Student Identity Management for Improving Security and Trust in European Higher Education Institutions (Grant Agreement No: 2020-1-EL01-KA226-HE-094869), which is funded by the European Commission within the Erasmus+ 2020 Programme and the Greek State Scholarships Foundation I.K.Y.

References

1. Nguyen, T., Memon, N. (2017). Smartwatches Locking Methods: A Comparative Study. WAY 2017 Workshop at the Symposium on Usable Privacy and Security, USENIX
2. Harbach, M., De Luca, A., Egelman, S. (2016). The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. ACM CHI 2016, ACM Press, 4806-4817
3. Aviv, A., Gibson, K., Mossop, E., Blaze, M., Smith, J. (2010). Smudge Attacks on Smartphone Touch Screens. USENIX Conference on Offensive Technologies (WOOT 2010), USENIX Association, 1-7
4. von Zezschwitz, E., De Luca, A., Janssen, P., Hussmann, H. (2015). Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. ACM Conference on Human Factors in Computing Systems (CHI 2015), ACM Press, 2339-2342
5. Belk M., Fidas C., Germanakos P., Samaras G. (2017). The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective. Computers in Human Behavior, 184-200
6. Guerar, M., Verderame, L., Merlo, A., Palmieri, F., Migliardi, M., Vallerini, L. (2020). CirclePIN: A Novel Authentication Mechanism for Smartwatches to Prevent Unauthorized Access to IoT Devices. ACM Transactions on Cyber-Physical Systems, 4(3), article 34
7. Nguyen, T., Sae-Bae, N., Memon, N. (2017). DRAW-A-PIN: Authentication using Finger-drawn Pin on Touch Devices. Computers and Security, 66, 115-128
8. Guerar, M., Verderame, L., Migliardi, M. Merlo, A. (2019). 2GesturePIN: Securing PIN-Based Authentication on Smartwatches. IEEE Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE, 327-333
9. Nguyen, T., Memon, N. (2018). Tap-based User Authentication for Smartwatches. Computers and Security, 78, 174-186
10. Oakley, I., Huh, J.H., Cho, J., Cho, G., Islam, R., Kim, H. (2018). The Personal Identification Chord: A Four Button Authentication System for Smartwatches. Asia Conference on Computer and Communications Security (ASIACCS 2018), ACM Press, 75-87
11. Zhao, Y., Qiu, Z., Yang, Y., Li, W., Fan, M. (2017). An Empirical Study of Touch-based Authentication Methods on Smartwatches. ACM Symposium on Wearable Computers (ISWC 2017), ACM Press, 122-125
12. Yang, J., Li, Y., Xie, M. (2015). MotionAuth: Motion-based Authentication for wrist worn smart devices. IEEE Conference on Pervasive Computing and Communication Workshops (PerCom Workshops 2015), IEEE, 550-555
13. Lee, W., Lee, R. (2016). Implicit Sensor-based Authentication of Smartphone Users with Smartwatch. ACM Conference on Hardware and Architectural Support for Security and Privacy (HASP 2016), ACM Press, article 9, 1-8
14. Han, T., Hasan, K., Nakamura, K., Gomez, R., Irani, P. (2017). SoundCraft: Enabling Spatial Interactions on Smartwatches using Hand Generated Acoustics. ACM Symposium on User Interface Software and Technology (UIST 2017), ACM Press, 579-591
15. Biddle, R., Chiasson, S., van Oorschot, P. (2012). Graphical passwords: Learning from the First Twelve Years. ACM Computing Surveys, 44(4), 41
16. Zhao, Z., Ahn, G.J., Seo, J.J. Hu, H. (2013). On the Security of Picture Gesture Authentication. USENIX Security Symposium (USENIX Security 2013), USENIX, 383-398
17. Paivio, A. Csapo, K. (1973). Picture Superiority in Free Recall: Imagery or Dual Coding?. Cognitive psychology, 5(2), 176-206
18. Fidas, C., Belk, M., Hadjidemetriou, G., Pitsillides, A. (2019). Influences of Mixed Reality and Human Cognition on Picture Passwords: An Eye Tracking Study. IFIP TC13 Conference on Human-Computer Interaction (INTERACT 2019), Springer-Verlag, 304-313

19. Katsini, C., Fidas, C., Raptis, G., Belk, M., Samaras, G., Avouris, N. (2018). Influences of Human Cognition and Visual Behavior on Password Security during Picture Password Composition. ACM Human Factors in Computing Systems (CHI 2018), ACM Press, p. 87
20. Ma, Y., Feng, J., Kumin, L., Lazar, J. (2013). Investigating User Behavior for Authentication Methods: A Comparison between Individuals with Down Syndrome and Neurotypical Users. ACM Transactions on Accessible Computing, 4(4), article 15, 27 pages
21. Grindrod, K., Khan, H., Hengartner, U., Ong, S., Logan, A.G., Vogel, D., et al. (2018). Evaluating Authentication Options for Mobile Health Applications in Younger and Older Adults. PLoS ONE 13(1), e0189048
22. Witkin, H., Moore, C., Goodenough, D., Cox, P. (1977). Field-dependent and Field-independent Cognitive Styles and their Educational Implications. Educational Research, 47(1), 1-64
23. Riding, R., Cheema, I. (1991). Cognitive Styles - An Overview and Integration. Educational Psychology, 11(3-4), 193-215
24. Peterson, E., Rayner, S., Armstrong, S. (2009). Researching the Psychology of Cognitive Style and Learning Style: Is There Really a Future? Learning and Individual Differences, 19(4), 518-523
25. Kozhevnikov, M. (2007). Cognitive Styles in the Context of Modern Psychology: Toward an Integrated Framework of Cognitive Style. Psychological Bulletin, 133(3), 464-481
26. Hong, J., Hwang, M., Tam, K., Lai, Y., Liu, L. (2012). Effects of Cognitive Style on Digital Jigsaw Puzzle Performance: A GridWare Analysis. Computers in Human Behavior, 28(3), 920-928
27. Raptis, G.E., Katsini, C., Belk, M., Fidas, C., Samaras, G., Avouris, N. (2017). Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. ACM User Modeling, Adaptation and Personalization (UMAP 2017), 164-173
28. Davis, J. (1991). Educational Implications of Field Dependence-Independence. Field Dependence-Independence: Cognitive Style across the Lifespan, Lawrence Erlbaum, 149-175
29. Johnson, J.J., Seixeiro, S., Pace, Z., van der Bogert, G., Gilmour, S., Siebens, L., Tubbs, K. (2014). Picture Gesture Authentication. https://www.google.com/patents/US8910253
30. Witkin, H. A., Oltman, P., Raskin, E., Karp, S. (1971). A Manual for the Embedded Figures Test. Palo Alto, CA: Consulting Psychologists Press
31. Zhao, Z., Ahn, G., Hu, H. (2015). Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation. ACM Transactions on Information and System Security (TISSEC), 17(4), 1-37
32. Constantinides, A., Fidas, C., Belk, M., Pietron, A., Han, T., Pitsillides, A. (2021). From Hot-spots towards Experience-spots: Leveraging on Users' Sociocultural Experiences to Enhance Security in Cued-recall Graphical Authentication. International Journal of Human-Computer Studies, 149
33. Dunphy, P. Yan, J. (2007). Do Background Images improve "Draw a Secret" Graphical Passwords?. Computer and Communications Security (CCS 2007), ACM Press, 36-47
34. Raptis, G., Fidas, C., Avouris, N. (2018). Effects of Mixed-reality on Players' Behaviour and Immersion in a Cultural Tourism Game: A Cognitive Processing Perspective. International Journal of Human-Computer Studies, 114, 69-79
35. Katsini, C., Fidas, C., Raptis, G., Belk, M., Samaras, G., Avouris, N. (2018). Eye Gaze-driven Prediction of Cognitive Differences during Graphical Password Composition. ACM SIGCHI Intelligent User Interfaces (IUI 2018), ACM Press, 147-152
36. Constantinides, A., Pietron, A., Belk, M., Fidas, C., Han, T., Pitsillides, A. (2020). A Cross-cultural Perspective for Personalizing Picture Passwords. ACM User Modeling Adaptation and Personalization (UMAP 2020), ACM Press, 43-52