UNIVERSITI PUTRA MALAYSIA

GRID-BASED MULTI-TOUCH GESTURE TO ENHANCE TWO-FACTOR AUTHENTICATION GRAPHICAL PASSWORD FOR MOBILE PHONES

NUR SYABILA BINTI ZABIDI

FSKTM 2021 4

GRID-BASED MULTI-TOUCH GESTURE TO ENHANCE TWO-FACTOR AUTHENTICATION GRAPHICAL PASSWORD FOR MOBILE PHONES

By

NUR SYABILA BINTI ZABIDI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

February 2021

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

GRID-BASED MULTI-TOUCH GESTURE TO ENHANCE TWO-FACTOR AUTHENTICATION GRAPHICAL PASSWORD FOR MOBILE PHONES

By

NUR SYABILA BINTI ZABIDI

February 2021

Chairman : Noris binti Mohd Norowi, PhD
Faculty : Computer Science and Information Technology

This research focuses on the graphical password authentication, which combines image and emojis by implementing the use of multi-touch gesture that could provide an alternative to a textual password. The assumption of emojis is easier to remember and more secure has motivated the researchers to enhance existing graphical password authentication scheme. Nevertheless, several usability problems have been identified: (i) There is usually a lack of efficient methods in single-factor authentication to execute both usable and secure characteristics; (ii) The current approaches in graphical password authentication rarely combine image and emojis. The methodology used was the User-Centered Design approach, where the process starts with the understanding of needs, design, prototyping and assessment via a usability test. In this research, there are three fundamental studies, which included the preliminary study, the study of effects on grid-based two-factor authentication method and the study of single touch and multi-touch gestures for the application of graphical password authentication. The preliminary study examined user attitudes towards the usability and security of single-factor and two-factor methods for authentication in the context of graphical password application. The grid-based two-factor authentication study introduces recognition-based graphical methods that use emojis to resist several common threats to security without sacrificing the usability of the graphical password. Grid-based scheme enhanced the effectiveness of the graphical password with the success rate of 79%. The outcome of the single touch and multi-touch gesture study on graphical password authentication application has shown that the multi-touch gesture enhanced the user experience. The study on multi-touch gesture showed positive results, including increased success rates, and reduced completion times had been positively affected. This study provides the results that can be used to determine the technique of authentication that users prefer based on data collected during the preliminary study. This study also contributes to improved graphical password authentication, which can solve problems

identified in studies, the picture superiority effect (P.S.E) in images and emojis. Furthermore, this research examines the impact of click and multi-touch gestures on the authentication of the graphical password. The results could be helpful for researchers or mobile developers interested in building a system that will advantage the research on picture and emojis using a graphical password authentication scheme. In future work, a comprehensive guideline for the development and verification of images and emojis, including a long-term assessment of these practices, should be included. The security of the prototype must also be examined closely and how attackers can take advantage of the emergence of hotspots. Overall, this study has introduced recognition-based graphical password methods that use emojis to resist several common threats to security without sacrificing the usability of the graphical password.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

GERAKAN BERBILANG SENTUHAN BERASASKAN GRID UNTUK MENAMBAH BAIK PENGESAHAN KATA LALUAN GRAFIK DUA FAKTOR UNTUK TELEFON BIMBIT

Oleh

NUR SYABILA BINTI ZABIDI

Februari 2021

Pengerusi : Noris binti Mohd Norowi, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Penyelidikan ini memfokuskan pada pengesahan kata laluan grafik, yang menggabungkan gambar dan emoji dengan menerapkan penggunaan isyarat multi-sentuh yang dapat memberikan alternatif kepada kata laluan teks. Anggapan emoji lebih mudah diingat dan lebih selamat telah mendorong para penyelidik untuk meningkatkan skema pengesahan kata laluan grafik yang ada. Walaupun begitu, beberapa masalah kebolehgunaan telah dikenalpasti: (i) Biasanya terdapat kekurangan kaedah yang cekap dalam pengesahan faktor tunggal untuk melaksanakan ciri yang boleh digunakan dan selamat; (ii) Pendekatan semasa dalam pengesahan kata laluan grafik jarang menggabungkan imej dan emoji. Metodologi yang digunakan adalah pendekatan Reka Bentuk Berpusat Pengguna, di mana prosesnya dimulai dengan pemahaman tentang keperluan, reka bentuk, prototaip dan penilaian melalui ujian kebolehgunaan. Dalam penyelidikan ini, terdapat tiga kajian asas, yang merangkumi kajian awal, kajian kesan terhadap kaedah pengesahan dua faktor berasaskan grid dan kajian isyarat sentuhan tunggal dan berbilang sentuhan untuk aplikasi pengesahan kata laluan grafik. Kajian awal mengkaji sikap pengguna terhadap kebolehgunaan dan keselamatan kaedah faktor tunggal dan dua faktor untuk pengesahan dalam konteks aplikasi kata laluan grafik. Kajian pengesahan dua faktor berasaskan grid memperkenalkan kaedah grafik berasaskan pengiktirafan yang menggunakan emoji untuk menentang beberapa ancaman umum terhadap keselamatan tanpa mengorbankan kegunaan kata laluan grafik. Skema berasaskan grid meningkatkan keberkesanan kata laluan grafik dengan kadar kejayaan 79%. Hasil kajian gerakan satu sentuhan dan multi-sentuhan pada aplikasi pengesahan kata laluan grafik telah menunjukkan bahawa isyarat multi-sentuhan meningkatkan pengalaman pengguna. Kajian mengenai gerakan multi-sentuhan menunjukkan hasil positif, termasuk peningkatan kadar kejayaan, dan penurunan masa penyelesaian telah dipengaruhi secara positif. Kajian ini memberikan hasil yang

dapat digunakan untuk menentukan teknik pengesahan yang disukai pengguna berdasarkan data yang dikumpulkan semasa kajian awal. Kajian ini juga menyumbang kepada peningkatan pengesahan kata laluan grafik, yang dapat menyelesaikan masalah yang dikenal pasti dalam kajian, kesan keunggulan gambar (P.S.E) dalam gambar dan emoji. Selanjutnya, penyelidikan ini mengkaji kesan isyarat klik dan berbilang sentuhan terhadap pengesahan kata laluan grafik. Keselamatan prototaip juga harus diperiksa dengan teliti dan bagaimana penyerang dapat memanfaatkan kemunculan titik panas. Secara keseluruhan, kajian ini telah memperkenalkan kaedah kata laluan grafik berasaskan pengiktirafan yang menggunakan emoji untuk menentang beberapa ancaman umum terhadap keselamatan tanpa mengorbankan kegunaan kata laluan grafik.

ACKNOWLEDGEMENTS

First and foremost, praises and thanks to Allah, for his showers of blessings throughout my research journey to complete my study successfully.

I would like to express my deep and sincere gratitude to my research supervisor, Dr Noris Binti Mohd Norowi, for providing invaluable guidance, knowledge and advice throughout this journey. Her dedication, sincerity, vision, has deeply motivated me. My sincere gratitude also presented to my supervisory committee member, Prof Dr. Rahmita Wirza O.K. Rahmat, who has been very helpful throughout this journey.

I would also like to thanks my parents for unconditionally loving and supporting me for everything that I pursue. For my husband and children, you are a great supporter above all. I thank my uni mates, labmates, and everyone who has helped me to achieve this. Special thanks to Teo and Sue for wonderful comments and a great help.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Noris binti Mohd Norowi, PhD
Senior Lecturer
Faculty of Science Computer and Information Technology
Universiti Putra Malaysia
(Chairman)

Rahmita Wirza bt O. K. Rahmat, PhD
Professor
Faculty of Science Computer and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 June 2021

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF EQUATIONS

CHAPTER 1

INTRODUCTION

1.1 Introduction

Human-Computer Interaction and Security is also known as in the sector of computer science as Usable Security, mixing Human-Computer Interaction (HCI) and Computer Security. It is vital because simply put, "A chain is only as strong as its weakest link." This chain is referred to the human in where to achieve high security in human-computer interaction; human should play the leading role (Eloff and Eloff 2002).

With the growth of smartphones and mobile network, all critical data is stored in mobile devices. There are security vulnerabilities in the existing infrastructure (Horne 2014). In that case, the personal data in smartphones must be protected and secured. This is referred to as authentication. User authentication is generally a method for checking a user's identity. It can be classified according to knowledge-based (password/PIN), possession-based (certificate/card) and biometric-based (finger/iris scan/face) (Srivastava and Sudhish 2016). Figure 1.1 illustrates the different method of user authentication (Mahadi et al. 2018). Authentication derives from Single Factor Authentication (SFA) to Two-Factor Authentication (2FA). SFA contains only one criterion for authenticating the subject (Ometov et al. 2018). An alternative passcode other than PIN is needed when generating a password to improve the security of 2FA (Kemshall 2011).

With the knowledge-based password, one of the challenges is memorability. Memorability is the principal source of password confusion (Adams and Sasse 1999). Passwords can be said as the almost universal encryption system despite rating bad in terms of memorability (Renaud and De Angeli 2004). A text password is commonly made up of ASCII characters. If a password is too easy, it will boost the risk of being hacked. However, it is difficult to remember passwords that are too complex. Due to this, the text-based password is not suggested, because it is hard to legitimate users and difficult to remember (Andriotis et al. 2013); (Rathanavel 2017); (Alsaiari et al. 2016a).

Consequently, the use of passwords is replaced progressively by alternative techniques such as card use, tokens or biometrics, which do not require much memory. While it solves the memorability issues, biometric authentication also faces security and usability problems. For example, Derawi found that the biometric technique presents technical difficulties such as predictive lighting and volatile specimen collection environments (Derawi 2011). Klíma et al. also believe that biometric authentication, such as finger or retinal scanning, cannot

be achieved for a variety of applications in certain medical circumstances (Klíma, Sporka, and Franc 2008). In fingerprints, one of the main components of human identity is a technical aspect to capture the design of the skin ridge present on the fingertips. For such biometric control systems that require fingerprint scanning as a mandating method of the identity and authorization method, adermatoglyphia or merely the lack of fingerprints due to a medical cause reflects taxing circumstances (Sarfraz 2019). A biometric device gives an automated person authentication based on certain features of the user. The retinal biometric method is both unique and reliable for all other biometrics. The retina is healthy and secure and unforgeable since it sits behind the eye (B. Mazumdar 2018).

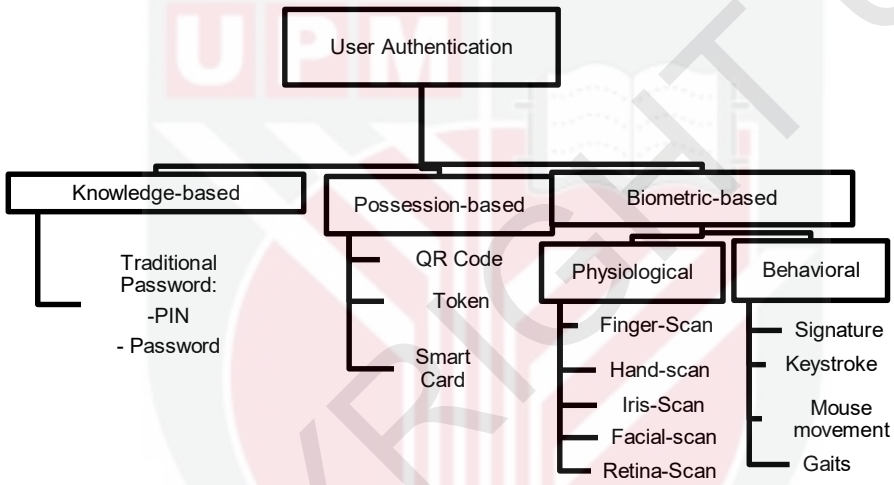

Figure 1.1 : Taxonomy of User Authentication Methods (Mahadi et al. 2018)

Password has several problems and primarily stems from memory limitations. The concept of memorability can be described as making it easy to remember a particular scheme to allow the casual user to log back into the scheme (Harrison, Flood, and Duce 2014). The memory of a picture is a feature defined by the capacity of human beings to recall things they witnessed (Akagunduz, Bors, and Evans 2020). However, recent literature on picture processing describes it as an underlying attribute which can be accomplished independently of the observer. During authentication, the user must be ready to memorize several strings of characters and users tend to forget their passwords (Wiedenbeck, Waters, Birget, et al. 2005a). This can be the user has multiple accounts where different credentials and passwords are required, which exacerbates the password problems further. Biddle et al. claim that users are able to store a variety of photos based upon recognition or another name as cognometric or searchmetric schemes. Then users will recognize their password pictures from decoys (Biddle, Chiasson, and Oorschot 2009).

Graphical password uses images as a password to provide an option to the text-based password (Kumar Jena 2013). Images are easier to be remembered as they include a display of the sensory characteristics experienced by the users (Biddle et al. 2009). The solution that has been investigated in this research is the Picture Superiority Effect (PSE). The Picture Superiority Effect (PSE) is the well-known experimental finding in retrospective memory testing which enables individuals who are exposed to stimuli in image format to perform explicit retrospective memory tests better than those who are exposed to the same stimuli in word format (Ma 2016). In other words, individuals perform better memorability in images than texts. The result of the image dominance indicates that with the photo to-do list users recall completing more tasks. This PSE effect is a clear hypothesis with several simple studies, which indicate that images are better remembered and reminisced than texts (Nelson et al. 1978)(Madigan 1974)(Brady et al. 2008)(Glaser 1992). By their pioneering studies on cognition, learning and memory, Craik and Lockhart made a breakthrough(Craik and Lockhart 1972). They put forth a retrieval theory that dictated if the data is retained in the long-term memory and not how long it was kept in fast memory, through the inadequacy of the knowledge processing process. Furthermore, they found that knowledge such as images provided to the learner, consistent with cognitive constructs already established in the brain, typically has the potential of being more fully interpreted and retained in both short and long-term memory.

The usability of an interface is determined by how simple it is to use. Usability is the degree to which an object or service may be used to achieve a specific purpose by a specific person in a specific environment with satisfaction, efficiency, and effectiveness (Bevan, Carter, and Harker 2015). Usability and security go hand in hand, and the two are inextricably linked. Security protocols ensure that the authentication mechanism's complexity correlates to the criticality of the data being accessed. Security protocols ensure that the authentication mechanism's complexity correlates to the criticality of the data being accessed (Mihajlov, Josimovski, and Jerman-Blazič 2011). While the technological aspects of information management are focused on password protection, the human aspects demand those various aspects of the operation be addressed. The user's efficiency was calculated in terms of how long it took them to perform a task, including register time and login time. The efficiency of the method was calculated by the percentage of tasks performed, and user satisfaction was determined by a questionnaire. Since mobile devices are personal items used by individuals with unique social and cultural norms within an external context determined by their environment, user experience is extremely important (Sun and May 2013).

As high-resolution touch screens emerged on mobile devices, researchers have started investigating how gesture can be applied to the graphical password. Free-form gestures can provide authentication for smartphone users in a potentially fast and secure way (Cheon et al. 2020). One influential direction of study based on gestures containing one or more finger movements required several finger-strokes to overlap briefly. This study also explored ideal

algorithms to understand gesture and usability and memorability of gesture in graphical passwords after intervals of one hour, one day and one week relative to text passwords(Liu, Clark, and Lindqvist 2017)(Yang et al. 2016). Authors claim that gestures reach usability standards comparable to or beyond text passwords, with mean creation times of 69 seconds, recall rates of 89.6% and recall times of 16.49 seconds were indistinguishable from text password results.

For these reasons, other alternatives are certainly needed, and one of the methods that can be applied is the use of gesture in graphical password. This research concentrates on the feasibility of using gesture in a graphical password as an alternative for smartphones' lock mechanism. Thus, this research also limits input to the small areas screen of typical phone lock systems. The use of gestures has many benefits: i) The theoretical number of possible gestures is enormous (Sherman et al. 2014); ii) Input of a gesture may require less visual attention than input based on buttons or goals selection (Pirhonen, Brewster, and Holguin 2002); iii) It is especially useful for mobile or wearable devices, for which users can work on or operate on small screens and execute other dominant activities(Nguyen and Memon 2018)(Oulasvirta et al. 2005).

In conclusion, this research uses image, emojis and gesture in a graphical password as a feasible solution to a traditional text password in order to improve the memorability of passwords and promote users to exercise secure authentication techniques.

1.2 Problem Statement

The first and most critical issue is the password issue. A few difficulties became apparent when using text password. Passwords present a significant usability challenge for end users, who are required to generate safe, unique passwords for each account, recall each of those passwords for an extended period of time, and remember which password goes with which account for different accounts. These security criteria put demands on users' memory, time, and attention that are beyond human competence, leading them to produce passwords that are unforgettable but easily guessed by attackers.

Graphical passwords are presented as an optional password method to text-based passwords. Dhanake proposed pairing text with pictures or colours in order to generate passwords for authentication session (Dhanake et al. 2014). De Angeli et al. pointed out that little attention was drawn to usability. They also mentioned people's ability to acknowledge previously recognized pictures. (De Angeli et al. 2005). The above issues have led to the exploration of the graphical password scheme. The primary issue of this research is to analyse the usability and security of the suggested scheme so that the weaknesses and disadvantages of graphical password verification are minimized.

Graphical authentication is a promising alternative to replace the traditional alphanumeric password way of authentication. The primary reason is that the human intellect is able to more closely remember graphical or visual items than texts, and even psychological research support these assumptions (Grady et al. 1998). In addition, technological advances are shifting forward with touch-based appliances like portable phones, tablets and even touchscreens.

This research will, therefore carry out a measurable measurement consisting of usability and security metrics to provide fundamental details and evaluation of the suggested scheme. This research seeks to enhance the usability and security of the implementation for graphical password authentication by examining the effects of images and emojis further.

The following are the problem statement summarized for this study:

a) Existing graphical password authentication is generally distinguished by the method of password memorization as recall, recognition, and cued-recall schemes. Additional aspects, such as the cognitive mechanisms and spatial arrangement, also affect usability and security. This issue was not widely studied. In terms of usability problems, the mental model problem is the most associated problem that can be explored in usability issues (Stobert and Biddle 2014). While completing the required authenticating tasks, users found themselves misled based on a lack of awareness where they were in the sequence of events. Another way to look at the problem is to consider the security issues. Predictable patterns and hotspots limit the effective password space of the scheme and create a vulnerability to dictionary attack.

b) The current gesture approaches in graphical password mostly limited to single touch gesture, while multi-touch behaviours have not been studied intensively. The problem associated with typed password is that passwords entered by typing on a virtual touch-based keypad are vulnerable to a "smudge attack," in which the passwords can be learned from the smudges left behind by the user's finger. Furthermore, shoulder-surfing attack, in which an attacker obtains a user's password by direct observation in a close contact condition, makes password authentication vulnerable. It is well-known that gesture password comes with a risk of security and memorability issues. It is discovered that in the absence of instructions, half of users will produce a single finger gesture and the other half will create multi-finger gestures, and that signatures and simple shapes are the gestures that people recall best. The use of multi-touch gestures is intended to complement single-touch gestures by providing users with a wider range of gesture passwords.

c) Multiple passwords are highly difficult to remember. Since users repeat the same password for several devices or expose other passwords when they attempt to log in, security is compromised. Users would now recall several passwords rather than just one. Users are required to select (and reuse) basic passwords that are convenient for attackers to guess as a result of the high memory load. In this fact, there has been little research into the problems associated with multiple passwords.

1.3 Research Question

All of these pertinent unresolved issues relating to the graphical password authentication has led to the following research questions to be addressed in this study:

1. What effective approach that requires both usable and secure graphical password authentication scheme?
2. What effective spatial arrangement that can be utilized to design the graphical password authentication scheme?
3. What effective gesture that can be applied to the graphical password authentication scheme?

1.4 Research Objectives

Based on the above, the objectives of the study are as follows:

1. To design and develop a two-factor, image and emoji-based graphical password authentication system for mobile phones.
2. To design a multi-touch gesture for increasing the efficiency of graphical password authentication in mobile phones.
3. To evaluate the efficiency and user experience of the designed image and emoji-based graphical password authentication system.

1.5 Contribution

This thesis attempted to solve password problems in graphical password authentication, especially in spatial arrangement and gestures, and to suggest solutions to these problems while ensuring usability. The following contributions to the field of user authentication and usable security are described in detail in the thesis:

i. Three user studies had been conducted with participants in IT background in Universiti Putra Malaysia particularly undergraduates and postgraduates of Faculty of Computer Science and Information Technology. Participants were chosen to understand the preferences of authentication approach, spatial arrangement and gestures. It gives interesting results that led the researcher proposing different approach solutions for different spatial arrangement and gestures as needs and ways to motivate users in each approach vary.

ii. In terms of usability of the prototypes, the single factor version has become substantially less usable than the two-factor authentication versions, which undermines the general belief that improved security contributes to reduced usability. It can be concluded that the contribution of integrating two-factor authentication has increase the usability of the graphical password authentication. A visible grid was used to divide the image into distinct parts. In terms of efficiency, applying a grid-based graphical password reduced average register and login times, directly increasing the graphical password's efficiency. In terms of effectiveness, the grid-based system improved the graphical password's effectiveness as well.

iii. Multi-touching adds the security as it increases the difficulties for attackers to guess and pick hotspots compared to single-touching, as the combination of the emojis and their two locations on the screen need to be correctly aligned.

Recent proposals for alternative types of passwords, especially grid-based multi-touch gesture graphical passwords, have sparked the first intention of this study. Instead of using a keyboard to type a text password, the user multi-touches on specific points on an image in such schemes. This graphical password is designed to take advantage of the human ability to recognize and retrieve images more quickly than textual data. This study provides the results that can be used to determine the technique of authentication that users prefer based on data collected during the preliminary study. This study also contributes to improved graphical password authentication, which can solve problems identified in studies, the picture superiority effect (P.S.E) in images and emojis. Furthermore, this research examines the impact of click and multi-touch gestures on the authentication of the graphical password. The results could be helpful for researchers or mobile developers interested in building a system that will advantage the research on picture and emojis using a graphical password authentication scheme. The results of these studies imply that the user experience and usability of the system can be improved.

1.6 Chapter Organization

The thesis consisted of 7 chapters in general. The thesis starts with Chapter 1, introducing and documenting the research. Research problems highlight the problems associated with user authentication and image and emoji interaction on a graphical password authentication scheme. The research objectives have been created to respond to the study issues. In order to attain the study objectives, the significance of the research is then stated.

Chapter 2 examines the literature which focuses on past studies on the authentication scheme of the graphical password. The literature review delivers knowledge of the authentication scheme for graphical passwords, user authentication and the interaction of images and emojis.

Chapter 3 describes the research methodology used in this research. Research methodology design, analytical framework, experimental methods, study methodologies, data collection techniques, and data analysis for this research are listed in the study method.

Chapter 4 provides the relative assessments of authentication of users using four existing graphical methods and their perception of usability and security problems, and their efficiency as a method of image and emoji-based authentication.

SecureImageEmoji system is described in Chapter 5 as the original design and execution of the new technique. The focus of this section is on the evaluation of the prototype, with a specific focus on defining the usability and security of login authentication.

The enhanced design and execution of *SecureImageEmoji* system are discussed in Chapter 6. The findings of the evaluation on the feasibility of implementing single touch and multi-touch gestures are also presented here.

The results of all studies reported in the thesis are summarized in Chapter 7, which lastly recognizes the weaknesses and constraints of the studies and the potential for future research.

REFERENCES

Abate, Andrea F., Michele Nappi, and Stefano Ricciardi. 2016. "Smartphone Enabled Person Authentication Based on Ear Biometrics and Arm Gesture." Pp. 003719–24 in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.

Adams, Anne, and Martina Angela Sasse. 1999. "Users Are Not the Enemy." *Communications of the ACM* 42(12):40–46.

Akagunduz, Erdem, Adrian G. Bors, and Karla K. Evans. 2020. "Defining Image Memorability Using the Visual Memory Schema." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 42(9):2165–78.

Almuairfi, Sadiq, Prakash Veeraraghavan, and Naveen Chilamkurti. 2013. "A Novel Image-Based Implicit Password Authentication System (IPAS) for Mobile and Non-Mobile Devices." *Mathematical and Computer Modelling* 58(1):108–16.

Alsaiari, Hussain, Maria Papadaki, Paul Dowland, and Steven Furnell. 2016a. "Graphical One-Time Password (GOTPass): A Usability Evaluation." *Information Security Journal: A Global Perspective* 25(1–3):94–108.

Alsaiari, Hussain, Maria Papadaki, Paul Dowland, and Steven Furnell. 2016b. "Graphical One-Time Password (GOTPass): A Usability Evaluation." *Information Security Journal* 25(1–3):94–108.

Anderson, Nancy S., Donald A. Norman, and Stephen W. Draper. 1988. "User Centered System Design: New Perspectives on Human-Computer Interaction." *The American Journal of Psychology* 101(1):148.

Andre, A., and H. Dinata. 2018. "Interaction Design to Enhance UX of University Timetable Plotting System on Mobile Version." *IOP Conference Series: Materials Science and Engineering* 407(1):012174.

Andriotis, Panagiotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. "A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks." P. 1 in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec '13*. New York, New York, USA: ACM Press.

De Angeli, Antonella, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems." *International Journal of Human Computer Studies* 63(1–2):128–52.

Anthony, Lisa, Kathryn A. Stofer, and Annie Luc. 2016. "Characterizing User Gestures on Touch Tables and Touch Walls in a Public Science Center." P. under review in *Proceedings of the International Conference on Interaction Design and Children*.

Arnowitz, Jonathan, Michael Arent, and Nevin Berger. 2007. "Define Prototype Content and Fidelity." Pp. 84–105 in *Effective Prototyping for Software Makers*. Elsevier.

Assal, Hala, Ahsan Imran, and Sonia Chiasson. 2018. "An Exploration of Graphical Password Authentication for Children." *International Journal of Child-Computer Interaction*.

B. Mazumdar, Jarina. 2018. "Retina Based Biometric Authentication System: A Review." *International Journal of Advanced Research in Computer Science* 9(1):711–18.

Belk, Marios, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2017. "The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective." *Computers in Human Behavior* 76:184–200.

Belk, Marios, Andreas Pamboris, Christos Fidas, Christina Katsini, Nikolaos Avouris, and George Samaras. 2017. "Sweet-Spotting Security and Usability for Intelligent Graphical Authentication Mechanisms." *Proceedings of the International Conference on Web Intelligence - WI '17* 252–59.

Ben-asher, Noam, Beer Sheva, T. U. Berlin, Joachim Meyer, and M. Sebastian. 2011. "On the Need for Different Security Methods on Mobile Phones." *MobileHCI 2011* 465–73.

Bevan, Nigel. 2001. "International Standards for HCI and Usability." *International Journal of Human Computer Studies* 55(4):533–52.

Bevan, Nigel, James Carter, and Susan Harker. 2015. "ISO 9241-11 Revised: What Have We Learnt About Usability Since 1998?" Pp. 143–51 in *Human-Computer Interaction*. Vol. 9169, *Lecture Notes in Computer Science*, edited by M. Kurosu. Cham: Springer International Publishing.

Bevan, Nigel, and Miles Macleod. 1994. "Usability Measurement in Context." *Behaviour & Information Technology* 13(1–2):132–45.

Biddle, Robert, Sonia Chiasson, and P. C. Van Oorschot. 2009. "Graphical Passwords : Learning from the First Twelve Years." *Security* V:1–43.

Biddle, Robert, Sonia Chiasson, and P. C. Van Oorschot. 2012. "Graphical Passwords : Learning from the First Twelve Years." *ACM Computing Surveys (CSUR)* 44(4):1–43.

Birmingham, Peter. 2003. *Using Research Instruments*. Routledge.

Bozanta, Aysun, Birgul Kutlu, Nuket Nowlan, and Shervin Shirmohammadi. 2016. "Effects of Serious Games on Perceived Team Cohesiveness in a Multi-User Virtual Environment." *Computers in Human Behavior* 59:380–88.

Brady, Timothy F., Talia Konkle, George A. Alvarez, and Aude Oliva. 2008. "Visual Long-Term Memory Has a Massive Storage Capacity for Object Details." *Proceedings of the National Academy of Sciences* 105(38):14325–29.

Brostoff, Sacha, and M. Angela Sasse. 2000. "Are Passfaces More Usable than Passwords? A Field Trial Investigation." *People and Computers* 1–20.

Brown, Charles E. 2008. *The Essential Guide to Flex 3 (Essential Guide)*. Friends of Ed.

Cain, Ashley A., and Jeremiah D. Still. 2019. "Graphical Authentication Passcode Memorability: Context, Length, and Number." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 63(1):447–51.

Carifio, James, and Rocco Perla. 2008. "Resolving the 50-Year Debate around Using and Misusing Likert Scales." *Medical Education* 42(12):1150–52.

Catani, Michael B., and David W. Biers. 1998. "Usability Evaluation and Prototype Fidelity: Users and Usability Professionals." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 42(19):1331–35.

Chang, Ting Yi, Cheng Jung Tsai, and Jyun Hao Lin. 2012. "A Graphical-Based Password Keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices." *Journal of Systems and Software* 85(5):1157–65.

Cheon, Eunyong, Yonghwan Shin, Jun Ho Huh, Hyoungshick Kim, and Ian Oakley. 2020. "Gesture Authentication for Smartphones: Evaluation of Gesture Password Selection Policies." Pp. 249–67 in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE.

Chiang, Hsin-yi, and Sonia Chiasson. 2013. "Improving User Authentication on Mobile Devices: A Touchscreen Graphical Password." *MobileHCI '13* 251–60.

Chiang, Hsin-Yi, and Sonia Chiasson. 2013. "Improving User Authentication on Mobile Devices." P. 251 in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*. New York, New York, USA: ACM Press.

Chiasson, Sonia, Robert Biddle, and P. C. van Oorschot. 2007. “A Second Look at the Usability of Click-Based Graphical Passwords.” P. 1 in *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS ’07*. New York, New York, USA: ACM Press.

Constantine, S. 2013. “Natural Interaction through Gesture Recognition and Head and Body Tracking.” *HCI Newsletter Issue* (58).

Constantinides, Argyris, Christos Fidas, Marios Belk, and Andreas Pitsillides. 2019a. “‘I Recall This Picture’: Understanding Picture Password Selections Based on Users’ Sociocultural Experiences.” Pp. 408–12 in *IEEE/WIC/ACM International Conference on Web Intelligence on - WI ’19*. New York, New York, USA: ACM Press.

Constantinides, Argyris, Christos Fidas, Marios Belk, and Andreas Pitsillides. 2019b. “On the Personalization of Image Content in Graphical Passwords Based on Users’ Sociocultural Experiences: New Challenges and Opportunities.” *ACM UMAP 2019 Adjunct - Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization* (Apps):199–202.

Coolican, H. 1990. “Research Methods and Statistics in Psychology. 1999.”

Corbin, Juliet, and Anselm Strauss. 2014. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage publications.

Craik, Fergus I. M., and Robert S. Lockhart. 1972. “Levels of Processing: A Framework for Memory Research.” *Journal of Verbal Learning and Verbal Behavior* 11(6):671–84.

Davis, Darren, Fabian Monrose, and Michael K. Reiter. 2004a. “On User Choice in Graphical Password Schemes.” *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13* 11.

Davis, Darren, Fabian Monrose, and Michael K. Reiter. 2004b. “On User Choice in Graphical Password Schemes.” P. 11 in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, *SSYM’04*. USA: USENIX Association.

Derawi, Mohammad Omar. 2011. “Biometric Options for Mobile Phone Authentication.” *Biometric Technology Today* 2011(10):5–7.

Dhamija, Rachna, and Adrian Perrig. 2000. “Deja vu: A User Study Using Images for Authentication.” *In Proceedings of the 9th USENIX Security Symposium, Denver, CO: Usenix, 2000.* (102590):45–58.

Dhanake, Sagar A., Umesh M. Korade, MrChetan P. Shitole, Sagar B. Kedar, and V. M. Lomte. 2014. "Authentication Scheme for Session Password Using Matrix Colour and Text." *IOSR Journal of Computer Engineering Ver. II* 16(1):2278–8727.

Dowling, Robyn, Kate Lloyd, and Sandie Suchet-Pearson. 2018. "Qualitative Methods III." *Progress in Human Geography* 42(5):779–88.

Dunphy, Paul. 2012. "Usable, Secure and Deployable Graphical Passwords." (November):189.

Dunphy, Paul, and Jeff Yan. 2007. "Do Background Images Improve 'Draw a Secret' Graphical Passwords?" P. 36 in *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*. New York, New York, USA: ACM Press.

Eloff, M. M., and J. H. P. Eloff. 2002. "Human Computer Interaction: An Information Security Perspectives." Pp. 535–45 in *Security in the Information Society: Visions and Perspectives*, edited by M. A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan. Boston, MA: Springer US.

Ferreira, Juan M., Silvia T. Acuña, Oscar Dieste, Sira Vegas, Adrián Santos, Francy Rodríguez, and Natalia Juristo. 2020. "Impact of Usability Mechanisms: An Experiment on Efficiency, Effectiveness and User Satisfaction." *Information and Software Technology* 117(November 2018):106195.

Foster, John C., Rachael Dutton, Mervyn A. Jack, Stephen Love, Ian A. Nairn, Nathalie Vergeynst, and F. W. M. Stentiford. 2002. "Intelligent Dialogues in Automated Telephone Services." *Interactive Speech Technology: Human Factors Issues In The Application Of Speech Input/Output To Computers: Human Factors Issues In The Application Of Speech Input/Output To Computers* 167.

Galy, Edith, Julie Paxion, and Catherine Berthelon. 2018. "Measuring Mental Workload with the NASA-TLX Needs to Examine Each Dimension Rather than Relying on the Global Score: An Example with Driving." *Ergonomics* 61(4):517–27.

Gao, Qin, Yang Wang, Fei Song, Zhizhong Li, and Xiaolu Dong. 2013. "Mental Workload Measurement for Emergency Operating Procedures in Digital Nuclear Power Plants." *Ergonomics* 56:1070–85.

Glaser, Wilhelm R. 1992. "Picture Naming." *Cognition* 42(1–3):61–105.

Gokhale, Mrs. Aakansha S., and Vijaya S. Waghmare. 2016. "The Shoulder Surfing Resistant Graphical Password Authentication Technique." *Procedia Computer Science* 79:490–98.

Golla, Maximilian, Dennis Detering, and Markus DŸrmut. 2017. “EmojiAuth: Quantifying the Security of Emoji-Based Authentication.” Pp. 1–13 in *Proceedings 2017 Workshop on Usable Security*. Reston, VA: Internet Society.

Gordon, Mitchell L., and Shumin Zhai. 2019. “Touchscreen Haptic Augmentation Effects on Tapping, Drag and Drop, and Path Following.” *Conference on Human Factors in Computing Systems - Proceedings* 1–12.

Grady, Cheryl L., A. R. McIntosh, M. Natasha Rajah, and Fergus I. M. Craik. 1998. “Neural Correlates of the Episodic Encoding of Pictures and Words.” *Proceedings of the National Academy of Sciences* 95(5):2703–8.

Gunson, Nancie, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. “User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking.” *Computers and Security* 30(4):208–20.

Harrison, Rachel, Derek Flood, and David Duce. 2014. “Usability of Mobile Applications : Literature Review and Rationale for a New Usability Model.” *International Journal of Mobile Human Computer Interaction* 6(1):54–70.

Hart, Sandra G. 2006. “NASA-Task Load Index (NASA-TLX); 20 Years Later.” *Proceedings of the Human Factors and Ergonomics Society* 904–8.

Hart, Sandra G., and Lowell E. Staveland. 1988. “Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research.” Pp. 139–83 in *Advances in Psychology*. Vol. 52.

Hartson, Rex, and Pardha Pyla. 2019. “Prototyping.” Pp. 405–32 in *The UX Book*. Elsevier.

Holsti, Ole R. 1969. “Content Analysis for the Social Sciences and Humanities.” *Reading. MA: Addison-Wesley (Content Analysis)*.

Holz, Christian, Senaka Buthpitiya, and Marius Knaust. 2015. “Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts.” *CHI - ACM Conference on Human Factors in Computing Systems* 3011–14.

Horne, Bill. 2014. “Humans in the Loop.” *IEEE Security and Privacy* 12(1):3–4.

Ibrahim, Tahir Musa, Shafi’i Muhammad Abdulhamid, Ala Abdusalam Alarood, Haruna Chiroma, Mohammed Ali Al-garadi, Nadim Rana, Amina Nuhu Muhammad, Adamu Abubakar, Khalid Haruna, and Lubna A. Gabralla. 2019. “Recent Advances in Mobile Touch Screen Security Authentication Methods: A Systematic Literature Review.” *Computers and Security* 85:1–24.

Ingram, Amy, Xiaoyu Wang, and William Ribarsky. 2012. "Towards the Establishment of a Framework for Intuitive Multi-Touch Interaction Design." *Proceedings of the Workshop on Advanced Visual Interfaces AVI* 66–73.

Jermyn, Ian, 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.

Jokela, Timo, Netta Iivari, Juha Matero, and Minna Karukka. 2003. "The Standard of User-Centered Design and the Standard Definition of Usability: Analyzing ISO 13407 against ISO 9241-11." *ACM International Conference Proceeding Series* 46:53–60.

Jonker, Jan, and Bartjan Pennink. 2010. *The Essence of Research Methodology*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Jøsang, Audun, and Mary Anne Patton. 2003. "User Interface Requirements for Authentication of Communication." *In the Proceedings of the Australasian User Interface Conference* 18:75–80.

Joshi, Ankur, Saket Kale, Satish Chandel, and D. Pal. 2015. "Likert Scale: Explored and Explained." *British Journal of Applied Science & Technology* 7(4):396–403.

Jourdan, Pierre, and Eliana Stavrou. 2019. "Towards Designing Advanced Password Cracking Toolkits: Optimizing the Password Cracking Process." *ACM UMAP 2019 Adjunct - Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization* (Apps):203–8.

Katsini, Christina, Christos Fidas, Marios Belk, George Samaras, and Nikolaos Avouris. 2019. "A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication." *International Journal of Human–Computer Interaction* 35(19):1800–1812.

Katsini, Christina, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. "Does Image Grid Visualization Affect Password Strength and Creation Time in Graphical Authentication?" Pp. 1–5 in *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*. New York, NY, USA: ACM.

Keinonen, Turkka. 2008. "User-Centered Design and Fundamental Need." *ACM International Conference Proceeding Series* 358:211–20.

Kemshall, Andy. 2011. "Why Mobile Two-Factor Authentication Makes Sense." *Network Security* 2011(4):9–12.

Khodadadi, Touraj, A. K. M. Muzahidu. Islam, Sabariah Baharun, and Shozo Komaki. 2016. "Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes." *International*

Journal of Electrical and Computer Engineering 6(6):2939–48.

Kjeldskov, Jesper, Mikael B. Skov, and Jan Stage. 2005. "Does Time Heal? A Longitudinal Study of Usability." *Proceedings of the 17th Australia Conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future (OZCHI'05)* 1–10.

Klíma, M., A. J. Sporka, and J. Franc. 2008. "You Are Who You Know : User Authentication by Face Recognition." *Proc. 7th ICDVRAT with ArtAbilitation, Maia, Portugal,* 97–102.

Konoth, Radhesh Krishnan, Victor van der Veen, and Herbert Bos. 2016. "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication." Pp. 405–21 in *International Conference on Financial Cryptography and Data Security*.

Kraus, Lydia, Robert Schmidt, Marcel Walch, Florian Schaub, Christopher Krügelstein, and Sebastian Möller. 2016. "Implications of the Use of Emojis in Mobile Authentication." *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016* 10–11.

Kristensson, Per Ola, Olof Arnell, Annelie Björk, Nils Dahlbäck, Joackim Pennerup, Erik Prytz, Johan Wikman, and Niclas Åström. 2008. "Infotouch: An Explorative Multi-Touch Visualization Interface for Tagged Photo Collections." *ACM International Conference Proceeding Series* 358:491–94.

Kumar Jena, Sanjay. 2013. "Graphical User Authentication." (May).

Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. 2017a. "Analyzing Qualitative Data." Pp. 299–327 in *Research Methods in Human Computer Interaction*. Elsevier.

Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. 2017b. "Statistical Analysis." Pp. 71–104 in *Research Methods in Human Computer Interaction*. Elsevier.

Lewis, James R. 2006. "Usability Testing." Pp. 1275–1316 in *Handbook of Human Factors and Ergonomics*. John Wiley & Sons, Ltd.

Likert, R. 1932. "A Technique for the Measurement of Attitudes." *Archives of Psychology* 22 140:55.

Liu, Can, Gradeigh D. Clark, and Janne Lindqvist. 2017. "Where Usability and Security Go Hand-in-Hand." Pp. 374–86 in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM.

Liu, Chao Liang, Cheng Jung Tsai, Ting Yi Chang, Wang Jui Tsai, and Po Kai Zhong. 2015. "Implementing Multiple Biometric Features for a Recall-Based Graphical Keystroke Dynamics Authentication System on a Smart Phone." *Journal of Network and Computer Applications* 53:128–39.

Liu, Linchuan, and Peter Khooshabeh. 2003. "Paper or Interactive? A Study of Prototyping Techniques for Ubiquitous Computing Environments." Pp. 1030–1031 in *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, *CHI EA '03*. New York, NY, USA: Association for Computing Machinery.

Lopes, Adriana, Natasha Valentim, Bruna Moraes, Renata Zilse, and Tayana Conte. 2018. "Applying User-Centered Techniques to Analyze and Design a Mobile Application." *Journal of Software Engineering Research and Development* 6(1):1–23.

Love, S., R. Dutton, J. C. Foster, and M. A. Jack. 1992. "Towards a Usability Measure for Automated Telephone Services." *PROCEEDINGS-INSTITUTE OF ACOUSTICS* 14:p553--p553.

Love, Stephen. 1997. "Role of Individual Differences in Dialogue Engineering for Automated Telephone Services."

Love, Stephen, R. T. Dutton, John C. Foster, Mervyn A. Jack, and F. W. M. Stentiford. 1994. "Identifying Salient Usability Attributes for Automated Telephone Services." in *Third International Conference on Spoken Language Processing*.

Ma, Yingying. 2016. "Can More Pictures Bring More Readership?: An Examination of the 'Picture Superiority Effect' in the News Consumption Process." *Procedia - Social and Behavioral Sciences* 236(December 2015):34–38.

Madigan, Stephen. 1974. "Representational Storage in Picture Memory." *Bulletin of the Psychonomic Society* 4(6):567–68.

Mahadi, Nurul Afnan, Mohamad Afendee Mohamed, Amirul Ihsan Mohamad, Mokhairi Makhtar, Mohd Fadzil Abdul Kadir, and Mustafa Mamat. 2018. "A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication." *Recent Advances in Cryptography and Network Security* (November 2018).

Marschark, Marc, and Cesare Cornoldi. 1991. "Imagery and Verbal Memory." Pp. 133–82 in *Imagery and Cognition*. New York, NY: Springer US.

Mator, Janine D., William E. Lehman, Wyatt McManus, Sarah Powers, Lauren Tiller, James R. Unverricht, and Jeremiah D. Still. 2020. "Usability: Adoption, Measurement, Value." *Human Factors*.

Mayron, Liam M. 2015. “Biometric Authentication on Mobile Devices.” *2015 IEEE Security & Privacy* 13(3):70–73.

McCoy, J. M., and G. W. Evans. 2005. “Physical Work Environment.” Pp. 219–46 in.

McCreery, Michael P., David B. Vallett, and Cynthia Clark. 2015. “Social Interaction in a Virtual Environment: Examining Socio-Spatial Interactivity and Social Presence Using Behavioral Analytics.” *Computers in Human Behavior* 51(PA):203–6.

Melicher, William, Michelle L. Mazurek, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. “Usability and Security of Text Passwords on Mobile Devices.” *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI ’16* 527–39.

Meng, Weizhi. 2016. “Evaluating the Effect of Multi-Touch Behaviours on Android Unlock Patterns.” *Information and Computer Security* 24(3):277–87.

Meng, Weizhi, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, and Jinguang Han. 2018. “CPMap: Design of Click-Points Map-Based Graphical Password Authentication.” Pp. 18–32 in *ICT Systems Security and Privacy Protection*, edited by L. J. Janczewski and M. Kutyłowski. Cham: Springer International Publishing.

Meng, Weizhi, Wenjuan Li, Lijun Jiang, and Liying Meng. 2016. “On Multiple Password Interference of Touch Screen Patterns and Text Passwords.” Pp. 4818–4822 in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, *CHI ’16*. New York, NY, USA: Association for Computing Machinery.

Meng, Weizhi, Wenjuan Li, Lam For Kwok, and Kim Kwang Raymond Choo. 2017. “Towards Enhancing Click-Draw Based Graphical Passwords Using Multi-Touch Behaviours on Smartphones.” *Computers and Security* 65:213–29.

Meng, Weizhi, Wenjuan Li, Duncan S. Wong, and Jianying Zhou. 2016. “TMGuard: A Touch Movement-Based Security Mechanism for Screen Unlock Patterns on Smartphones.” Pp. 629–47 in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 9696.

Meng, Weizhi, Yu Wang, Duncan S. Wong, Sheng Wen, and Yang Xiang. 2018. “TouchWB: Touch Behavioral User Authentication Based on Web Browsing on Smartphones.” *Journal of Network and Computer Applications* 117(May):1–9.

Meng, Yuxin, Duncan S. Wong, Roman Schlegel, and Lam For Kwok. 2013. "Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7763 LNCS:331–50.

Mihajlov, Martin, and Borka Jerman-Blažič. 2011. "On Designing Usable and Secure Recognition-Based Graphical Authentication Mechanisms." *Interacting with Computers* 23(6):582–93.

Mihajlov, Martin, 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):975–88.

Mihajlov, Martin, Saso Josimovski, and Borka Jerman-Blazič. 2011. "A Conceptual Framework for Evaluating Usable Security in Authentication Mechanisms - Usability Perspectives." *Proceedings - 2011 5th International Conference on Network and System Security, NSS 2011* (December 2014):332–36.

Mohamed, Mona, Joyram Chakraborty, and Sharma Pillutla. 2020. "Effects of Culture on Graphical Password Image Selection and Design." *Journal of Systems and Information Technology* 22(4):73–95.

Nelson, Thomas O., Gene Greene, Brian Ronk, Gary Hatchett, and Valerie Igl. 1978. "Effect of Multiple Images on Associative Learning." *Memory & Cognition* 6(4):337–41.

Nguyen, Toan, and Nasir Memon. 2018. "Tap-Based User Authentication for Smartwatches." *Computers and Security* 78:174–86.

Nicholson, James, Lynne Coventry, and Pam Briggs. 2013. "Age-Related Performance Issues for PIN and Face-Based Authentication Systems." *Conference on Human Factors in Computing Systems - Proceedings* 323–32.

Nickerson, R. S. 1965. "Short-Term Memory For Complex Meaningful Visual Configurations: A Demonstration Of Capacity." *Canadian Journal of Psychology* 19(2):155–60.

Nielsen, Jakob. 1994. *Usability Engineering*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

O'Gorman, L. 2003. "Comparing Passwords, Tokens, and Biometrics for User Authentication." *Proceedings of the IEEE* 91(12):2019–20.

Olson, Judith S., and Wendy A. Kellogg. 2014. *Ways of Knowing in HCI*. edited by J. S. Olson and W. A. Kellogg. New York, NY: Springer New York.

Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. "Multi-Factor Authentication: A Survey." *Cryptography* 2(1):1.

Oulasvirta, Antti, Sakari Tamminen, Virpi Roto, and Jaana Kuorelahti. 2005. "Interaction in 4-Second Bursts." P. 919 in *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*. New York, New York, USA: ACM Press.

Petsas, Thanasis, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. "Two-Factor Authentication: Is the World Ready?" Pp. 1–7 in *Proceedings of the Eighth European Workshop on System Security - EuroSec '15*. New York, New York, USA: ACM Press.

Pirhonen, Antti, Stephen Brewster, and Christopher Holguin. 2002. "Gestural and Audio Metaphors as a Means of Control for Mobile Devices." *Conference on Human Factors in Computing Systems - Proceedings* 4(1):291–98.

Preece, J. Rogers, and Y. Rogers. n.d. "Y. & Sharp, H.(2002)." *Interaction Design: Beyond Human-Computer Interaction*.

Preece, Jenny, Yvonne Rogers, and Helen Sharp. 2015. *Interaction Design: Beyond Human-Computer Interaction (4th Ed)*. Chichester: John Wiley & Sons.

Rajasekar, S., P. Philominathan, and V. Chinnathambi. 2006. "Research Methodology." *Contributions to Management Science* 75–100.

Ramkumar, Anjana, Pieter Jan Stappers, Wiro J. Niessen, Sonja Adebahr, Tanja Schimek-Jasch, Ursula Nestle, and Yu Song. 2017. "Using GOMS and NASA-TLX to Evaluate Human–Computer Interaction Process in Interactive Segmentation." *International Journal of Human-Computer Interaction* 33(2):123–34.

Rathanavel, Veena. 2017. "Graphical Password as an OTP." *International Journal Of Engineering And Computer Science* 6(1):20090–95.

Renaud, Karen, and Antonella De Angeli. 2004. "My Password Is Here! An Investigation into Visuo-Spatial Authentication Mechanisms." *Interacting with Computers* 16(6):1017–41.

Ritter, Daniel, Florian Schaub, Marcel Walch, and Michael Weber. 2013. "MIBA: Multitouch Image-Based Authentication on Smartphones." *CHI '13 Extended Abstracts on Human Factors in Computing Systems* 787–92.

Rogowski, Marcin, Khalid Saeed, Mariusz Rybnik, Marek Tabedzki, and Marcin Adamski. 2013. "User Authentication for Mobile Devices." Pp. 47–58 in *Computer Information Systems and Industrial Management: 12th IFIP*

TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013. Proceedings, edited by K. Saeed, R. Chaki, A. Cortesi, and S. Wierzchoń. Berlin, Heidelberg: Springer Berlin Heidelberg.

Rosenthal, Robert, and R. L. Rosnow. 1991. *Essentials of Behavioral Research: Methods and Data Analysis*. Vol. 2. McGraw-Hill New York.

Rubin, Jeffrey. 1994. *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. 1st ed. USA: John Wiley & Sons, Inc.

Salehi-Abari, Amirali, Julie Thorpe, and P. C. Van Oorschot. 2008. "On Purely Automated Attacks and Click-Based Graphical Passwords." *Proceedings - Annual Computer Security Applications Conference, ACSAC* 111–20.

Sarfraz, Nuraiz. 2019. "Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative." *Cureus* 11(2).

Sauer, Jürgen, Katrin Seibel, and Bruno Rüttinger. 2010. "The Influence of User Expertise and Prototype Fidelity in Usability Tests." *Applied Ergonomics* 41(1):130–40.

Schaub, Florian, Ruben Deyhle, and Michael Weber. 2012. "Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms." in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, *MUM '12*. New York, NY, USA: Association for Computing Machinery.

Schaub, Florian, Marcel Walch, Bastian Könings, and Michael Weber. 2013. "Exploring the Design Space of Graphical Passwords on Smartphones." P. 1 in *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*. New York, New York, USA: ACM Press.

Schmidt, Dominik, Florian Block, and Hans Gellersen. 2009. "A Comparison of Direct and Indirect Multi-Touch Input for Large Surfaces." Pp. 582–94 in *Human-Computer Interaction -- INTERACT 2009*, edited by T. Gross, J. Gulliksen, P. Kotzé, L. Oestreicher, P. Palanque, R. O. Prates, and M. Winckler. Berlin, Heidelberg: Springer Berlin Heidelberg.

Schrum, Mariah L., Michael Johnson, Muyleng Ghuy, and Matthew C. Gombolay. 2020. "Four Years in Review: Statistical Practices of Likert Scales in Human-Robot Interaction Studies."

Sefelin, Reinhard, Manfred Tscheligi, and Verena Giller. 2003. "Paper Prototyping - What Is It Good for? A Comparison of Paper- and Computer-Based Low-Fidelity Prototyping." Pp. 778–779 in *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, *CHI EA '03*. New York, NY, USA: Association for Computing Machinery.

Seitz, Tobias, Florian Mathis, and Heinrich Hussmann. 2017a. “The Bird Is the Word.” Pp. 10–20 in *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI ’17*. New York, New York, USA: ACM Press.

Seitz, Tobias, Florian Mathis, and Heinrich Hussmann. 2017b. “The Bird Is the Word.” Pp. 10–20 in *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI ’17*. Vol. 52. New York, New York, USA: ACM Press.

Shahzad, Muhammad, Alex X. Liu, and Arjmand Samuel. 2013. “Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures - You Can See It but You Can Not Do It.” *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM* 39–50.

Shankar, Vishnu, Karan Singh, and Ajai Kumar. 2016. “IPCT: A Scheme for Mobile Authentication.” *Perspectives in Science* 8:522–24.

Sherman, Michael, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. “User-Generated Free-Form Gestures for Authentication: Security and Memorability.” Pp. 176–89 in *MobiSys 2014 - Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*.

Simeone, Adalberto L., Julian Seifert, Dominik Schmidt, Paul Holleis, Enrico Rukzio, and Hans Gellersen. 2013. “A Cross-Device Drag-and-Drop Technique.” in *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia*, *MUM ’13*. New York, NY, USA: Association for Computing Machinery.

Snyder, Carolyn. 2003. *Paper Prototyping: The Fast and Easy Way to Design and Refine User Interfaces*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

Souppaya, Murugiah, and Karen Scarfone. 2013. “Guidelines for Managing the Security of Mobile Devices in the Enterprise.” *NIST Special Publication 800-124, Revision 1* 1–30.

Srivastava, Stuti, and Prem Sewak Sudhish. 2016. “Continuous Multi-Biometric User Authentication Fusion of Face Recognition and Keystoke Dynamics.” Pp. 1–7 in *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*. IEEE.

Standing, Lionel. 1973. “Learning 10,000 Pictures.” *Quarterly Journal of Experimental Psychology (I 973)* 25(I 973):207–22.

Standing, Lionel, Jerry Conezio, and Ralph Norman Haber. 1970. “Perception and Memory for Pictures: Single-Trial Learning of 2500 Visual Stimuli.”

Psychonomic Science 19(2):73–74.

Stemler, Steve. 2000. "An Overview of Content Analysis." *Practical Assessment, Research, and Evaluation* 7(1):17.

Stobert, Elizabeth, and Robert Biddle. 2014. "A Password Manager That Doesn't Remember Passwords." *ACM International Conference Proceeding Series* 15-18-Sept:39–52.

Sun, Hung Min, Shiuan Tung Chen, Jyh Haw Yeh, and Chia Yun Cheng. 2018. "A Shoulder Surfing Resistant Graphical Authentication System." *IEEE Transactions on Dependable and Secure Computing* 15(2):180–93.

Sun, Xu, and Andrew May. 2013. "A Comparison of Field-Based and Lab-Based Experiments to Evaluate User Experience of Personalised Mobile Devices." *Advances in Human-Computer Interaction* 2013:1–9.

Taggart, C. 2016. *New Words for Old: Recycling Our Language for the Modern World*. Michael O'Mara Books, Limited.

Tao, Hai, and Carlisle Adams. 2008. "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords." *International Journal of Network Security* 7(2):273–92.

Teh, Pin Shen, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2015a. "Recognizing Your Touch: Towards Strengthening Mobile Device Authentication via Touch Dynamics Integration." Pp. 108–116 in *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia, MoMM 2015*. New York, NY, USA: Association for Computing Machinery.

Teh, Pin Shen, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2015b. "Recognizing Your Touch." Pp. 108–16 in *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia - MoMM 2015*. New York, New York, USA: ACM Press.

Thorpe, Julie, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. 2014. "The Presentation Effect on Graphical Passwords." *Conference on Human Factors in Computing Systems - Proceedings* 2947–50.

Thorpe, Julie, and P. C. van Oorschot. 2007. "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords." *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07)* 8.

Tilke, Juddk, Krista Ehinger, Frédo Durand, and Antonio Torralba. 2009. "Learning to Predict Where Humans Look." *Proceedings of the IEEE International Conference on Computer Vision* (Iccv):2106–13.

Toledano, Doroteo T., Rubén Fernández Pozo, Álvaro Hernández Trapote, and Luis Hernández Gómez. 2006. "Usability Evaluation of Multi-Modal Biometric Verification Systems." *Interacting with Computers* 18(5):1101–22.

Tullis, T. S. 1990. "High-Fidelity Prototyping throughout the Design Process." P. 266 in *Proceedings of the Human Factors Society 34th Annual Meeting (Santa Monica, CA, Human Factors Society 1990)*.

Uebelbacher, A., A. Sonderegger, and J. Sauer. 2013. "Effects of Perceived Prototype Fidelity in Usability Testing under Different Conditions of Observer Presence." *Interacting with Computers* 25(1):91–101.

Villamor, Craig, Dan Willi, and Luke Wroblewski. 2010. "Touch Gesture Reference Guide." *Touch Gesture Reference Guide* 1–23.

Walliman, Nicholas. 2011. "Research Methods : The Basics."

Wazir, Waqas, Hasan Ali Khattak, Ahmad Almogren, Mudassar Ali Khan, and Ikram Ud Din. 2020. "Doodle-Based Authentication Technique Using Augmented Reality." *IEEE Access* 8:4022–34.

Weir, Catherine S., Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. "User Perceptions of Security, Convenience and Usability for Ebanking Authentication Tokens." *Computers and Security* 28(1–2):47–62.

Weir, Catherine S., Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. "Usable Security: User Preferences for Authentication Methods in EBanking and the Effects of Experience." *Interacting with Computers* 22(3):153–64.

Wiedenbeck, Susan, Jim Waters, and Jc Birget. 2005. "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice." *Proceedings of the 2005 Symposium on Usable Privacy and Security* 1–12.

Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005a. "Authentication Using Graphical Passwords." *Proceedings of the 2005 Symposium on Usable Privacy and Security - SOUPS '05* 1–12.

Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005b. "Authentication Using Graphical Passwords." Pp. 1–12 in *Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05*. New York, New York, USA: ACM Press.

Woodruff, Jonathan, and Jason Alexander. 2019a. "Data Transfer: A Longitudinal Analysis of Clipboard and Drag-and-Drop Use in Desktop Applications." *International Journal of Human-Computer Studies* 132:112–

20.

Woodruff, Jonathan, and Jason Alexander. 2019b. "Data Transfer: A Longitudinal Analysis of Clipboard and Drag-and-Drop Use in Desktop Applications." *International Journal of Human Computer Studies* 132(February):112–20.

Yang, Yulong, Gradeigh D. Clark, Janne Lindqvist, and Antti Oulasvirta. 2016. "Free-Form Gesture Authentication in the Wild." Pp. 3722–35 in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM.

Zabidi, Nur Syabila, Noris Mohd Norowi, and Rahmita Wirza O. K. Rahmat. 2019. "On the Use of Image and Emojis in Graphical Password Application." *International Journal of Innovative Technology and Exploring Engineering* 8(8):379–85.

Zajonc, Robert B. 1965. "Social Facilitation." *Science* 149(3681):269–74.

von Zezschwitz, Emanuel, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. "Making Graphic-Based Authentication Secure against Smudge Attacks." 277.

Zhao, Ziming, Gail-Joon Ahn, and Hongxin Hu. 2015. "Picture Gesture Authentication." *ACM Transactions on Information and System Security* 17(4):1–37.

Zhou, Bing, Jay Lohokare, and Fan Ye. 2018. "EchoPrint : Two-Factor Authentication Using Acoustics and Vision on Smartphones." 321–36.

BIODATA OF STUDENT

Nur Syabila binti Zabidi

Universiti Putra Malaysia (UPM)

Field: Human-Computer Interaction

She is a graduate student for Master of Science in Human-Computer Interaction (HCI) at the Multimedia Department, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. Her research title is "Utilizing Multi-Gesture in Enhancing Two-Factor Authentication Graphical Password Application". Her field of expert is mobile application development and android programming.

LIST OF PUBLICATIONS

Zabidi, Nur Syabila, Noris Mohd Norowi, and Rahmita Wirza O. K. Rahmat. 2019. "On the Use of Image and Emojis in Graphical Password Application." *International Journal of Innovative Technology and Exploring Engineering* 8(8):379–85.

Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. O. (2018). A Survey of User Preferences on Biometric Authentication for Smartphones. *International Journal of Engineering & Technology*, *7*(4.15), 491-495.

Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. O. (2018). A Usability Evaluation of Image and Emojis in Graphical Password. *International Journal of Engineering & Technology*, *7*(4.31), 400-407.

Zabidi, Nur Syabila, Noris Mohd Norowi, and Rahmita Wirza OK Rahmat. "A review on gesture recognition technology in children's interactive storybook." In 2016 4th International Conference on User Science and Engineering (i-USEr), pp. 232-236. IEEE, 2016.

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : _____

TITLE OF THESIS / PROJECT REPORT :

_____

_____

_____

NAME OF STUDENT : _____

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☐	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐	**PATENT**	Embargo from_____ until _____ (date) (date)

Approved by:

_____	_____
(Signature of Student)	(Signature of Chairman of Supervisory Committee)
New IC No/ Passport No.:	Name:
Date :	Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]