SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Enhancing Image-Emoji Graphical Password Multi-Factor Authentication by Utilizing Single Touch and Multi-Touch Gesture

Nuur Alifah Roslan[1,*], Noris Mohd Norowi[1], Nursyabila Zabidi[2], Ramlan Mahmod[3], Auzi Asfarian[4]

[1] Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[2] Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja, B86400 Batu Pahat, Johor, Malaysia
[3] Universiti Politeknik Mara Malaysia, Taman Shamelin Perkasa, 56100 Kuala Lumpur, Malaysia
[4] Institut Pertanian Bogor, Kabupaten Bogor, Jawa Barat 16680, Indonesia

Keywords:

Graphical password; authentication; mobile gestures; emoji authentication

ABSTRACT

Smartphones have evolved into a basic human requirement. PINs, passwords, swipes and other methods are used to authenticate users on mobile devices. However, existing authentication systems are vulnerable to modern security vulnerabilities. As the number of touch devices increases, gesture-based authentication becomes increasingly crucial. The distinctness of a gesture in a touch base mobile device is investigated in this research. Analysis reveals that a specific user has distinct finger gestures. An experimental study demonstrates that an individual's index finger and thumbs improve finger accuracy in a gesture-based authentication. The purpose of this article is to investigate the influence of single and multi-touch on the production of graphical passwords, specifically using images and emoji and based on a two-factor authentication mechanism. Our finding proves the efficiency increasing up, where it took an average of 37 seconds to register their credentials when using the multi-touch gesture approach compare 47.93 seconds on average for single-touch approach. As for the effectiveness, which referring the trial attempts determined that multi-touch gestures are more successful than single touch gestures, with a 78% success.

1. Introduction

Human-Computer Interaction and Security is a growing field of study that combines human interaction skills and computer security. Smartphones users are increasing rapidly, in 2017users are approximately 3.6 billion worldwide and the smartphone users will be 9.6 billion till 2020 approximately [1]. In our rapid technology with the expansion of smartphones and mobile network, all essential information is hold on in mobile devices. Therefore, there is a need to protect and secured the personal data by authenticate the user.

Smartphone authentication [2], which includes PIN-based passcodes, pattern-based passcodes, fingerprints and facial recognition, is a general used approach for tackling this problem. However, for convenience and memorability, most users choose weak and simple passcodes [3].

* *Corresponding author.*
E-mail address: nuuralifah@upm.edu.my

https://doi.org/10.37934/araset.XX.X.184193

Text passwords are frequently composed of ASCII characters. A password's likelihood of being cracked will increase if it is too simple. A too-complicated password, though, is hard to remember. As a result, the text-based password is not advised because it is challenging for reputable users to remember [4]. Individuals have a higher probability to remember visuals than texts.

Referring to Biddle, Chiasson and Van Oorschot [5], images incorporate a depiction of the sensory properties perceived by the users, making them easier to remember then, the uses of images as a password became an option to the text-based password and known as a Graphical password. The graphical password can be used in many ways approach such as a drag-and-drop gestures or a long press gesture. Our previous research by Zabidi, Norowi and Rahmat [6], use the drag-and drop gestures for users to authenticate the graphical password. Long press gestures are unnatural in terms of movement. The issue with drag and drop motion has been addressed using touch dynamics (single touch or multi-touch). Single and multiple touch capabilities are what set apart mobile phones with touch screens. The creation of graphical passwords can be simple by using various movements.

This study's primary goal is to investigate how single-touch and multitouch can improve graphical passwords. The main contribution of this paper is giving a clear result of the best setting of usability for SecureEmoji Graphical Password. Reminders of the papers include a previous work section, the procedure setting, measurement criteria, result and discussion and last but not least is the conclusion.

2. Previous Work

2.1 User Authentication

The user relies on built-in security features like PINs, swipes, passwords, patterns, etc. to prevent unauthorized access because all smartphones have different authentication parameters. Although popular, some features have certain drawbacks. Therefore, a Two Factor Authentication (2FA) provide an additional security layer known as "multi factor authentication" that requires something that the individual possesses solely on them in addition to a password and login. For instance, a piece of information that only they should be aware of or have readily available, such as a physical token [7].

Based on Table 1 categorization, it can be concluded that knowledge-based authentication is something a user knows such as password or PIN. On the other hand, possession-based or token-based authentication is something a user has. For example, a certificate or card. While biometric-based authentication is some- thing a user is, such as iris scan, fingerprint and face recognition [6].

Table 1
The categorization of user authentication [6]

Category	Definition	Example
Knowledge-based	Something a user knows	Password, PIN
Possession-based	Something a user has	Certificate, Card
Biometric-based	Something a user is (Physical or Behavioural)	Fingerprint, Iris Scan, Face

These classifications lead to the conclusion that knowledge-based authentication uses a password or PIN that the user is aware of. On the other hand, a user has a possession using possession-based or token-based authentication. a card or certificate, as an illustration. While a user must be anything for biometric-based identification such as fingerprint, iris scan and face recognition.

The biometrics-based can be measure physiology and behaviour. Physical features are measured using fingerprint, face, iris, retina and hand scan data. Behaviour is measured via keystrokes, speech

and signature scans. Human traits are measured using fingerprint, face, iris, retina and hand scan data [8].

Our research will be focusing on the Knowledge-based domain. Through several studies, we addressed the issues of usability and security in using password and PIN as user authentication method. When it comes to memorizing many strings with no shared meanings, humans find it challenging. Then, they will choose a less secure passwords by linking them to common objects in order to make them easier to remember [6]. Implementing the authentication using smartphones, they are highly potential for a shoulder surfing where hackers can access to security codes through different ant-social engineering [1].

Additionally, passwords are easily crack able in an adversary scenario, i.e., phone charging assaults make it possible to record the screen while the phone is charging [9,10]. Android unlock pattern are based on the original 3x3 Android graphical unlock pattern [11]. Numerous researchers have proposed attacks on these patterns and many have calculated the amount of unlock patterns that users have access [12,13]. For instance, the smudge attack [14-16],which recovers the pattern by using the remaining oil on the touch screen to guess the Android graphical password and the accelerometer-based side channel attack [17].

2.2 Graphical Password

Graphical passwords are an alternative to text-based passwords. The existing graphical password systems. They can be categorised to three categories; recall-based graphical password, cue-based recall graphical password and recognition-based graphical password [11]. Draw A Secret (DAS) presented in 1999 using the recalled-based password [18]. The recall-based password method must enter their prior password settings again to complete the authentication. Users generate passwords by drawing images on a 2D grid and then redraw them when they log in. Then it is improved by adding a background password image behind the grid word by Dunphy and Yan [19].

The cue-based recall graphic password system made it easier to remember passwords by using graphical prompts. The PassPoints system, which has its roots in Blonder's patent [19], serves as the primary illustration. Users of PassPoints [21], a graphical password system, can request five distinct click points on photos after viewing them. To log in, users must click the same five buttons in the same order. Users find it challenging to click precisely on the right pixels each time they log in, so an area of tolerance will be set up around each point and any clicks within that tolerance area will be allowed.

A graphical password recognition-based generated from a grid of different photographs, the users choose pictures in order. A commercial graphical password system called PassFaces [11] authenticates users by seeing faces in a grid. Each user is given a group of three faces to use as their login password and when they log in, a display of nine faces appears. Additionally, the user must select a face that is a portion of the password that was given to them. The user must choose the right face from the three arrays and the interfering faces are always the same to increase security.

Referring to our previous prototype authentication system, we were developed a SecureImageEmoji [6] (Figure 1). This prototype application will generate a graphical password with a multi-factor authentication which is image and emoji selection. There will be a grid of six of an image to be selected from the user as the In the first round of authentication, users need to create a graphical password by choosing an image from the six images provided. The process followed by choosing four selected emojis to the image selected before. The selected emoji is personal choose by the user make the SecureImageEmoji easy to remember for the authentication.

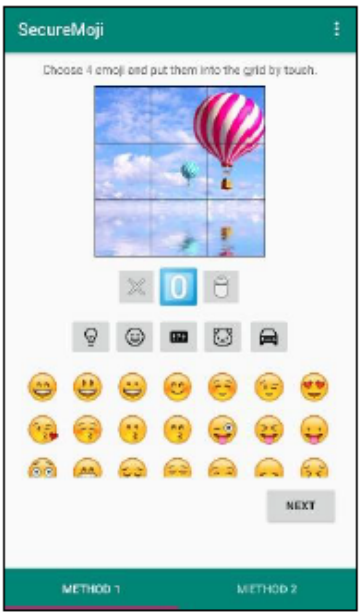

Fig. 1. SecureImageEmoji
(single touch & multi-touch)

2.3 Smartphones and Mobile Touch Screen Technology

Due to the high degree of versatility and user-friendliness of touch screen technology, it has been repurposed as input technology for smartphones. Today's industry is controlled by touch screen technology, which provides additional functionality, improved energy usage and increased storage capacity. As a result, it has become critical to safeguard the sensitive information contained on touchscreens on mobile phones. After a few minutes of inactivity, a phone automatically locks up and the user must enter a PIN number or screen pattern to unlock the device and renew access.

Gestures are vital elements for human communication. A gesture is any bodily movement in a visual environment that a digital interface can detect and respond to without the use of a traditional pointing tool such as a mouse or stylus. The term "touch dynamics" refers to the monitoring and quantification of human rhythms on electronic devices such as digital tablets, smartphones and touch screen panels [22]. Touch dynamics on a mobile phone are characterized as single touch, multi-touch and touch movement [23].

A single touch is an input that begins with a touch-down and ends with a click, with no action in between (Figure 2). Multi-touch is used to keep an entry of two or more simultaneous unique touchdown activities at different touch screen places (i.e., two fingertips pushing the contact screen at the same time) with or without a step before a touch-up event has been initiated (Figure 3).

Fig. 2. Single touch illustration

Fig. 3. Multi touch illustration

3. Task Procedure

3.1 Participant

The conducted experiment involved 15 participants (9 males, 6 females) participated, in the range of age from 21 to 30 (*m* = 1.6; *sd* =13.4). A sample size range for CHI papers ranging from 1 to 916,000, with 12 being the most prevalent sample size [24]. Participants had prior smartphone interaction experience. Users' involvement was entirely voluntary and all users agreed to have their interactions with the prototype documented.

3.2 Procedure

Users can complete their password choosing in this upgraded prototyped application by using a single or two-finger multi-touch gesture. The overall configuration is consistent with past user research. The image pool, in particular, comprises of six photographs (organised in two-by-three grids) with the same theme (scenery images) such as hot air balloons, gardens and historical sites. All of the photographs chosen have the same pixel size of 400 by 400. During the initial round of authentication, users must construct a graphical password by selecting an image from a set of six. The process is then repeated by single-touching or multi-touching four selected emojis to the previously picked image.

A welcome page, registration page and login page were included in a single touch and multi-touch prototype. First, on the welcome page, there are login and registration buttons, as well as two menus (login and register). The system then shows 2x3 grid images for participants to choose from, with only one image required. The registration process is continuously implemented by displaying a 3x3 grid-based image with the previously picked image as the background. It should be noted that there are two techniques to be shown here: method 1 for single touch and method 2 for multi-touch. The single touch method will be covered first. Participants must place four emojis on the appropriate grid. The single touch approach gives an area for locating selected emojis, where the emojis will show on the equipped area and users may further locate the emojis by clicking on the desired grid as shown in Figure 4.

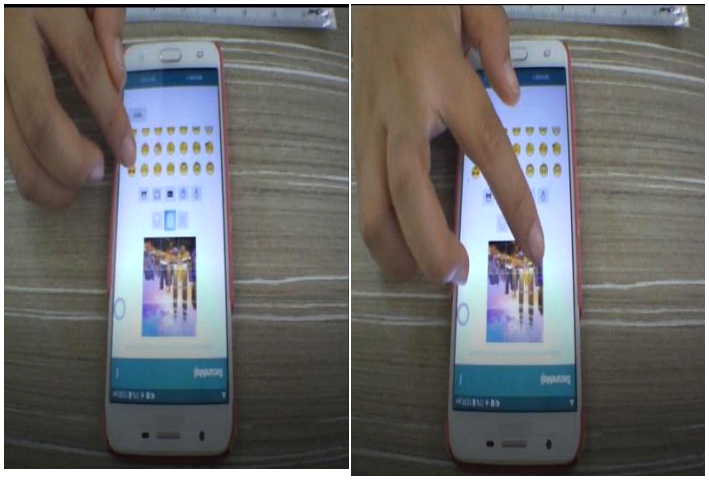

Fig. 4. Single touch method selected emojis presentation

Except for the area where you select emojis, the multi-touch approach has the identical UI as the single touch method. Users must multi-touch one emoji and one chosen grid at the same time. Figure 5 depicts the interface. Because users must multi-touch emojis and the grid at the same time, the multitouch approach does not provide any selected emojis area. The system also informed users of how many emojis remained to be chosen. Users can easily cancel any unwanted emojis by clicking on the "X" button for single emojis or the "dustbin" symbol button for all selected emojis. Users must then confirm their emoji choices by clicking "yes" or "no" to proceed. After checking all of the required details, this interface alerts users that a password has been created and they are returned to the welcome page to log in. If the users correctly clicked all four emojis, they were granted access to the system. If a user enters a password incorrectly, the system warns them.

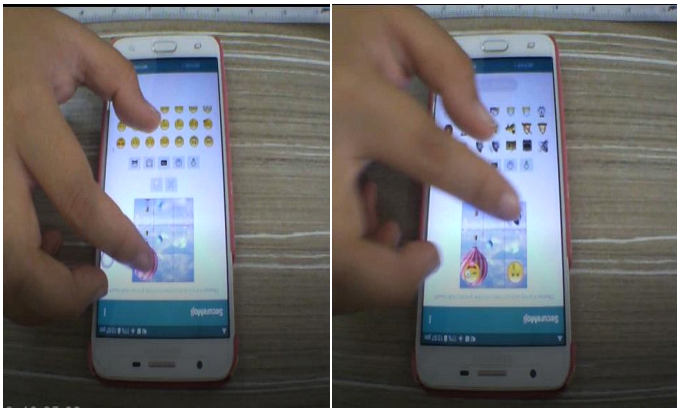

Fig. 5. Multi-touch method selected emojis presentation

3.3 Measurement

This paper will evaluate the efficiency (average registration and login time) and the effectiveness (success rate) between the single touch and multi-touch graphical password as the alternative to the drag and drop approach. In the new standard, efficiency is defined as the resources utilised to achieve a specified goal (i.e. times to complete a specific activity) [26]. This study performed an efficiency evaluation by calculating average registration and login times.

The password's efficiency was determined by the proportion of participants who were able to successfully log into the prototype within a specified time frame [4]. In this study, efficiency is employed to calculate the following:

i. register time
ii. login time.

Meanwhile, the accurate and complete attainment of certain objectives by users is characterised as effectiveness [27]. This study assessed effectiveness by calculating the success rate of the proposed system by assessing the fraction of all successful login attempts across all trials. The effectiveness is measured based on the following equation:

$$Success\ Rate = \frac{Number\ of\ successfull\ login}{Number\ of\ total\ logins} \quad (1)$$

4. Result and Discussion

4.1 Efficiency

As illustrated in Figure 6, employing multi-touch reduces the average register time when constructing a graphical password. Using a single touch gesture method, participants completed the registration task in 47.93 seconds on average. While employing the multi-touch gesture strategy, it took an average of 37 seconds to register their credentials. Multi-touch enables natural and intuitive engagement by providing rapid responses to the emojis displayed, resulting in a shorter password registration time. Because their mini-environment is tightly regulated, using multi-touch gestures keeps participants engaged. According to participant 001, "*multi-touch saves time because it uses two fingers at once*."

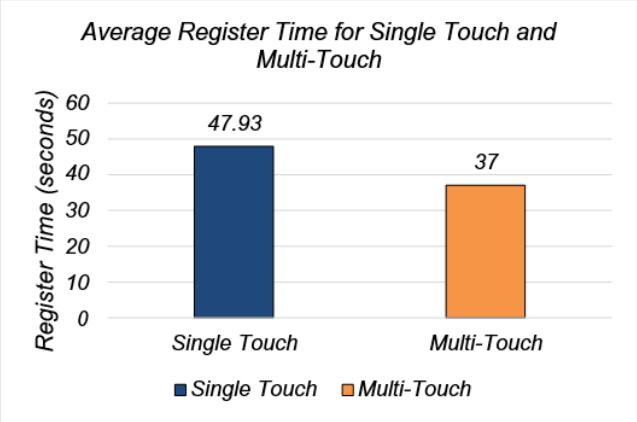

Fig. 6. Average register time for single touch and multi-touch bar chart

During this login phase, participants were required to log in (maximum of three attempts) under the following conditions: a total of three correct authentication attempts represents that the participant successfully completed the login session and a total of three incorrect attempts represents that he/she did not successfully complete the login task session.

When comparing login times for both techniques, it can be concluded that multi-touch gesture is more efficient than single touch gesture due to the average login time for multi-touch, which was 73.97 seconds. The login process takes less time to complete than registering the password since

users have been acquainted with their pictures and emojis; thus, they took less time in verifying themselves. The majority of participants demonstrated that the multi-touch technique could generate and verify passwords quickly.

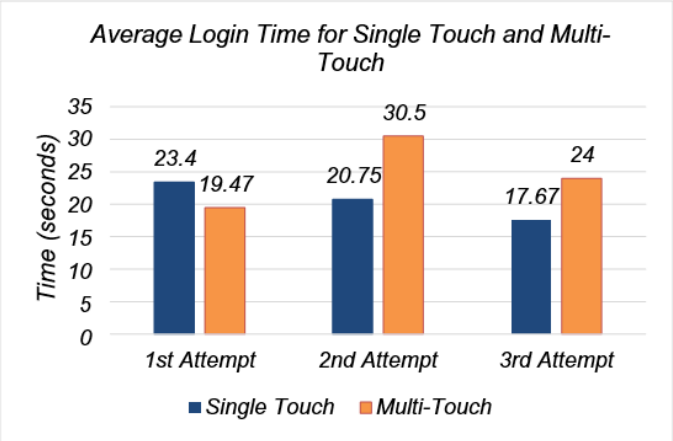

Fig. 7. Average register time for single touch and multi-touch bar chart

4.2 Effectiveness

Effectiveness is defined as the precise and detailed achievement of certain goals [27]. The proportion of successful login attempts in all trials for both single touch and multitouch gesture approaches was assessed to determine overall effectiveness. According to our result, the one touch gesture approach received 23 attempts, with a success percentage of 57%. Several failed efforts (43%) were discovered as a result of individuals either forgetting their chosen image or mistakenly tapping on the wrong emojis. With a 78% success rate, all trial attempts concluded that multi-touch gestures are more successful than single touch gestures. The participants believed that multi-touch motion could help them with password creation and memory. Participants 001 reported that the "multi-touch approach saves time by utilising two fingertips at once." Multi-touch reduces the effort required for users to learn, utilise and recall, making it more intuitive and successful. The purpose of multi-touch interaction is to reduce the effort required by users to understand, use and recall experiences such that they are as natural as feasible given real-world constraints [28].

Besides efficiency and effectiveness, the usability and password space computation can be accountable to measure the SecureImageEmoji security and usability using single and multi-touch approach. There is limitation in this study where it did not utilize any real simulation of attack. One of the future goals is to imitate real-world attacks. Graphical password systems may necessitate more preparation than text password systems since attackers may need to acquire one or more images first. In this study, users can form their password using 867 clickable emojis by single or multi-touching desired emojis on the selected image. In theory, an invader will have 1/867 chances to select the appropriate emojis. However, by integrating multi-touch, attackers should spend more time identifying hotspots. Hotspots are specific areas on an image that most users are more likely to utilise as part of their passwords. Last but not least, implementing the artificial intelligence and consideration of three factors authentication might provide a higher level of security for the future works [29,30].

5. Conclusion

SecureImageEmoji, a single-touch and multi-touch grid-based two-factor authentication application solution for touchscreen mobile devices, is presented in this study. It highlights the utility of multi-touch for user authentication. The system's performance was tested using data from 15 users who used the improved application. The results reveal that the multi-touch gesture outperformed the single touch gesture in terms of efficiency (password registration time) and efficacy (password login time). In terms of user satisfaction, single touch required more mental effort because participants had to tap on one emoji and then tap on one desired grid on the background image; at the same time, multi-touch simplified the process by allowing participants to tap on one emoji and one desired grid at the same time.

Acknowledgement

This research was not funded by any grant.

References

[1] Rehman, Anwar Ur, Muhammad Awais and Munam Ali Shah. "Authentication analysis using input gestures in touch-based mobile devices." In *2017 23rd international conference on automation and computing (ICAC)*, pp. 1-5. IEEE, 2017. https://doi.org/10.23919/IConAC.2017.8082062

[2] La Polla, Mariantonietta, Fabio Martinelli and Daniele Sgandurra. "A survey on security for mobile devices." *IEEE communications surveys & tutorials* 15, no. 1 (2012): 446-471. https://doi.org/10.1109/SURV.2012.013012.00028

[3] Mazurek, Michelle L., Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay and Blase Ur. "Measuring password guessability for an entire university." In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 173-186. 2013. https://doi.org/10.1145/2508859.2516726

[4] Alsaiari, Hussain, Maria Papadaki, Paul Dowland and Steven Furnell. "Graphical one-time password (GOTPass): a usability evaluation." *Information security journal: a global perspective* 25, no. 1-3 (2016): 94-108. https://doi.org/10.1080/19393555.2016.1179374

[5] Biddle, Robert, Sonia Chiasson and Paul C. Van Oorschot. "Graphical passwords: Learning from the first twelve years." *ACM Computing Surveys (CSUR)* 44, no. 4 (2012): 1-41. https://doi.org/10.1145/2333112.2333114

[6] Zabidi, Nur Syabila, Noris Mohd Norowi and R. W. O. Rahmat. "A usability evaluation of image and emojis in graphical password." *Int J Eng Technol* 7, no. 4.31 (2018): 400-407. https://doi.org/10.14419/ijet.v7i4.31.23719

[7] Bonneau, Joseph. "The science of guessing: analyzing an anonymized corpus of 70 million passwords." In *2012 IEEE symposium on security and privacy*, pp. 538-552. IEEE, 2012. https://doi.org/10.1109/SP.2012.49

[8] Zin, Muhamad Zulfikri Md, Raihana Md Saidi, Faridah Sappar and Mohamad Asrol Arshad. "Multi-factor authentication to authorizing access to an application: A conceptual framework." *Journal of Advanced Research in Computing and Applications* 16, no. 1 (2019): 1-9.

[9] Li, Wenjuan, Yu Wang, Jin Li and Yang Xiang. "Toward supervised shape-based behavioral authentication on smartphones." *Journal of Information Security and Applications* 55 (2020): 102591. https://doi.org/10.1016/j.jisa.2020.102591

[10] Meng, Weizhi, Lijun Jiang, Yu Wang, Jin Li, Jun Zhang and Yang Xiang. "JFCGuard: detecting juice filming charging attack via processor usage analysis on smartphones." *Computers & Security* 76 (2018): 252-264. https://doi.org/10.1016/j.cose.2017.11.012

[11] Zhang, Lei, Yajun Guo, Xiaowei Guo and Xiaowei Shao. "Does the layout of the Android unlock pattern affect the security and usability of the password?." *Journal of Information Security and Applications* 62 (2021): 103011. https://doi.org/10.1016/j.jisa.2021.103011

[12] Uellenbeck, Sebastian, Markus Dürmuth, Christopher Wolf and Thorsten Holz. "Quantifying the security of graphical passwords: The case of android unlock patterns." In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 161-172. 2013. https://doi.org/10.1145/2508859.2516700

[13] Kessler, Gary C. "Technology corner: Calculating the number of Android lock patterns: An unfinished study in number theory." *Journal of Digital Forensics, Security and Law* 8, no. 4 (2013): 4. https://doi.org/10.15394/jdfsl.2013.1156

[14] Aviv, Adam J., Katherine Gibson, Evan Mossop, Matt Blaze and Jonathan M. Smith. "Smudge attacks on smartphone touch screens." In *4th USENIX workshop on offensive technologies (WOOT 10)*. 2010.
[15] Cha, Seunghun, Sungsu Kwag, Hyoungshick Kim and Jun Ho Huh. "Boosting the guessing attack performance on android lock patterns with smudge attacks." In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pp. 313-326. 2017. https://doi.org/10.1145/3052973.3052989
[16] Andriotis, Panagiotis, Theo Tryfonas, George Oikonomou and Can Yildiz. "A pilot study on the security of pattern screen-lock methods and soft side channel attacks." In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pp. 1-6. 2013. https://doi.org/10.1145/2462096.2462098
[17] Aviv, Adam J., Benjamin Sapp, Matt Blaze and Jonathan M. Smith. "Practicality of accelerometer side channels on smartphones." In *Proceedings of the 28th annual computer security applications conference*, pp. 41-50. 2012. https://doi.org/10.1145/2420950.2420957
[18] Jermyn, Ian, Alain Mayer, Fabian Monrose, Michael K. Reiter and Aviel Rubin. "The design and analysis of graphical passwords." In *8th USENIX Security Symposium (USENIX Security 99)*. 1999.
[19] Dunphy, Paul and Jeff Yan. "Do background images improve" draw a secret" graphical passwords?." In *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 36-47. 2007. https://doi.org/10.1145/1315245.1315252
[20] Blonder, Greg E. "Graphical password." U.S. Patent 5,559,961, issued September 24, 1996.
[21] Chiasson, Sonia, Robert Biddle and Paul C. Van Oorschot. "A second look at the usability of click-based graphical passwords." In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pp. 1-12. 2007. https://doi.org/10.1145/1280680.1280682
[22] Teh, Pin Shen, Ning Zhang andrew Beng Jin Teoh and Ke Chen. "Recognizing your touch: Towards strengthening mobile device authentication via touch dynamics integration." In *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia*, pp. 108-116. 2015. https://doi.org/10.1145/2837126.2837127
[23] Meng, Weizhi. "Evaluating the effect of multi-touch behaviours on android unlock patterns." *Information & Computer Security* 24, no. 3 (2016): 277-287. https://doi.org/10.1108/ICS-12-2014-0078
[24] Woodruff, Jonathan and Jason Alexander. "Data transfer: A longitudinal analysis of clipboard and drag-and-drop use in desktop applications." *International Journal of Human-Computer Studies* 132 (2019): 112-120. https://doi.org/10.1016/j.ijhcs.2019.08.005
[25] Cain, Ashley A. and Jeremiah D. Still. "Graphical authentication passcode memorability: Context, length and number." In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 63, no. 1, pp. 447-451. Sage CA: Los Angeles, CA: SAGE Publications, 2019. https://doi.org/10.1177/1071181319631077
[26] Bevan, Nigel, James Carter and Susan Harker. "ISO 9241-11 revised: What have we learnt about usability since 1998?." In *Human-Computer Interaction: Design and Evaluation: 17th International Conference, HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015, Proceedings, Part I 17*, pp. 143-151. Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-20901-2_13
[27] Jourdan, Pierre and Eliana Stavrou. "Towards designing advanced password cracking toolkits: optimizing the password cracking process." In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, pp. 203-208. 2019. https://doi.org/10.1145/3314183.3324967
[28] Ingram, Amy, Xiaoyu Wang and William Ribarsky. "Towards the establishment of a framework for intuitive multi-touch interaction design." In *Proceedings of the International Working Conference on Advanced Visual Interfaces*, pp. 66-73. 2012. https://doi.org/10.1145/2254556.2254571
[29] Aleluya, Earl Ryan M. and Celesamae T. Vicente. "Faceture ID: face and hand gesture multi-factor authentication using deep learning." *Procedia Computer Science* 135 (2018): 147-154. https://doi.org/10.1016/j.procs.2018.08.160
[30] Mihailescu, Marius Iulian and Stefania Loredana Nita. "Three-Factor Authentication Scheme Based on Searchable Encryption and Biometric Fingerprint." In *2020 13th International Conference on Communications (COMM)*, pp. 139-144. IEEE, 2020. https://doi.org/10.1109/COMM48946.2020.9141956