Picture Passwords in Mixed Reality: Implementation and Evaluation

George Hadjidemetriou
Department of Computer Science,
University of Cyprus, 1678 Nicosia, Cyprus
ghadji12@cs.ucy.ac.cy

Marios Belk
School of Sciences, University of Central Lancashire, Cyprus Campus, 7080 Larnaka, Cyprus, mbelk1@uclan.ac.uk

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

Andreas Pitsillides
Department of Computer Science,
University of Cyprus, 1678 Nicosia, Cyprus
andreas.pitsillides@ucy.ac.cy

ABSTRACT

We present *HoloPass*, a mixed reality application for the HoloLens wearable device, which allows users to perform user authentication tasks through gesture-based interaction. In particular, this paper reports the implementation of picture passwords for mixed reality environments, and highlights the development procedure, lessons learned from common design and development issues, and how they were addressed. It further reports a between-subjects study (N=30) which compared usability, security, and likeability aspects of picture passwords in mixed reality *vs.* traditional desktop contexts aiming to investigate and reason on the viability of picture passwords as an alternative user authentication approach for mixed reality. This work can be of value for enhancing and driving future implementations of picture passwords in mixed reality since initial results are promising towards following such a research line.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3313076

KEYWORDS

Knowledge-based User Authentication; Picture Passwords; Mixed Reality; Implementation; Feasibility Study.

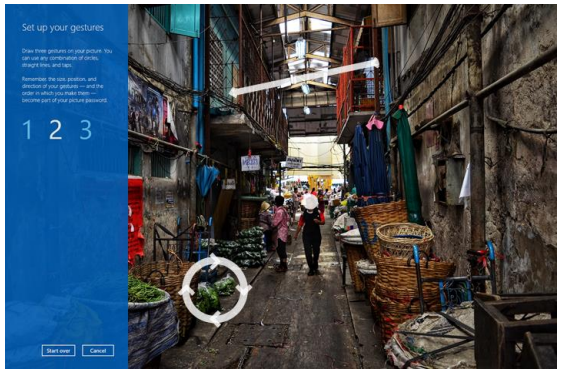

Figure 1: Example of Microsoft Windows 10 Picture Gesture Authentication on a traditional desktop computer.

Figure 2: User interacting with HoloPass that resembles PGA in mixed reality.

1 INTRODUCTION

Mixed reality technologies embrace hand gesture-based interaction modalities which can be leveraged by picture passwords, as they require users to draw secret gestures on a background image. However up to date, user authentication tasks in popular mixed reality technologies, such as Microsoft HoloLens, solely deploy text passwords which is known to depreciate usability, since hand gesture-based text input in a virtual keyboard is a difficult and time demanding task [21, 22].

Picture passwords have been introduced as alternative user authentication schemes for providing a fluid login experience on desktop computers and tablets, however, little attention has been given so far to investigate such schemes in mixed reality contexts. A widely deployed picture password is Microsoft Windows 10 Picture Gesture Authentication (PGA) (**Figure 1**) [1, 12]. PGA is an instance of background draw-a-secret schemes - BDAS [2] (see [3] on a review on popular picture password schemes, *e.g.*, BDAS [2], DAS [4], PassPoints [5]).

Recent works on user authentication have explored alternative schemes in mixed and virtual reality contexts, including [6] that investigated three different authentication mechanisms in virtual reality such as 3D patterns, 2D sliding patterns and pin-based authentication; [7] that discussed users' personal views on sharing QR codes between a physical display and an HMD to authenticate applications; [8] that adapted two traditional authentication schemes (pin- and pattern-based) in virtual reality; [9] that introduced two pin-based mechanisms on Google Glass; and [10] that introduced a biometric system to analyze the bone conduction of sound through the user's skull on Google Glass to identify and authenticate the user.

The aforementioned schemes and current password or pin-based schemes seem not be adequate in such contexts since research has shown that text input in a virtual keyboard hinders usability [21, 22]. Hence, we believe that background draw-a-secret schemes in mixed reality is a research line that is worth investigation. In this paper, we report on the first implementation of a picture password scheme for mixed reality environments, and highlight the development procedure and lessons learned. We further report on a user study which compared usability, security, and likeability aspects of picture passwords in mixed reality *vs.* desktop contexts to investigate the viability of picture passwords as an alternative user authentication approach for mixed reality.

2 IMPLEMENTATION OF PICTURE PASSWORDS FOR MIXED REALITY

HoloPass is a mixed reality application that utilizes the Microsoft HoloLens device to allow users to directly interact with picture-based holograms in order to perform user authentication tasks. The current prototype was developed in Unity 3D, using C# and Microsoft's Mixed Reality Toolkit for HoloLens, and follows implementation guidelines of Microsoft Windows 10 PGA [12] in which users draw three secret gestures (*dots*, *lines*, *circles*) on a background image that acts as a cue (**Figure 1**). HoloPass implements the following user authentication tasks: *i)* picture password creation; *ii)* user login; and *iii)* picture password reset. In each task, the screen is split in two sides (**Figure 2**). The left side illustrates instructions about the task and status of activity, and the right side illustrates the background image on which users indicate their password by drawing three secret gestures. The high-level architecture of HoloPass is depicted in **Figure 3**.

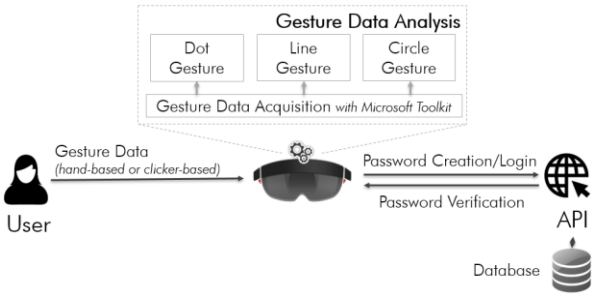

Figure 3: HoloPass high-level architecture. Users perform gestures to draw secret patterns on the background image (dot, line, circle) which are processed and stored for verification in the system's database.

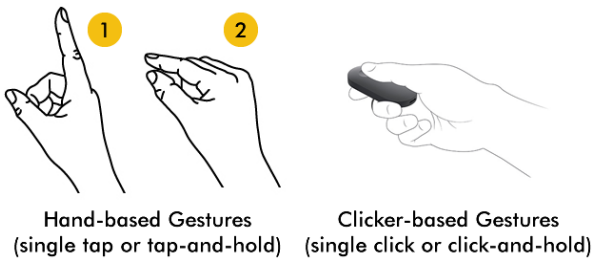

Figure 4: User input through hand gestures (left) or using the HoloLens clicker (right)

Gesture Data Analysis Module. Three gestures were implemented, *i.e.*, *dot*, *line*, *circle* which can be achieved through *hand-based gestures* or *clicker-based gestures* (**Figure 4**). For implementing hand-based gestures, we used Microsoft Toolkit's *Manipulation events* which allow full control over the position of the hand in each frame, and whether the user is performing a tap or hold gesture. For implementing clicker-based gestures, we used Microsoft Toolkit's *Navigation events* which returns the magnitude of the user's interaction using the clicker with a normalized range [-1, 1] which is translated into a global position using Unity's built-in functions (*e.g.*, *OnNavigationStarted*, *OnNavigationUpdated*, *OnNavigationCompleted*). Based on initial user feedback with early prototypes of the system, users rated the clicker as more usable than hand gestures, since the clicker does not interfere with the user's field of view during interaction and requires less hand movements for capturing a gesture.

The *dot gesture* was implemented by capturing the users' tap (either through hand or click) at the position where they focus. The *line gesture* was implemented by capturing the start and end position of the line. To start drawing a line, users first tap-and-hold on the starting position (this way we can initiate the line gesture and differentiate it from the dot gesture), and then move their hand or clicker to the end position. When the desired end position is reached, users release their finger or clicker to register the line gesture. Finally, to initiate the *circle gesture* and differentiate it from the dot and line gestures, we implemented a double-tap-and-hold mechanic using coroutines and timers. When users double tap and hold the second tap, they can control the circle radius by moving their hand to the left or right with the center of the circle being the users' gaze position.

For processing gestures, we calculate a transparent grid of the image containing 100 segments on the longest side, and then dividing the shortest side by the same scale. This approach allows storing the gestures based on their segment position on the grid rather than pixel coordinates.

Alternative Implementation of Gestures. An alternative implementation of gestures was based using Microsoft's *Custom Vision AI*, an online machine learning service, that enables building, deploying and improving custom image classifiers. For detecting hand gestures, when a user performs a tap-and-hold to form a line or a circle, the application draws on a sprite, the positions of the user's hand in each frame. The sprite is then sent to the Custom Vision AI API to classify the user's hand gesture. However, this method needs further investigation, since it requires continuous connection to the API, and training to create credible models to limit misclassifications.

3 EVALUATION STUDY

The following research question was examined: *Are PGAs a good alternative and viable authentication solutions for mixed reality contexts?* For doing so, we designed an in-lab study in which participants used a picture password similar to PGA. Specifically, we investigated usability aspects of PGA in mixed reality in terms of task execution and likeability, and security in terms of guessing attacks. In addition, we have compared these metrics with a traditional desktop version of PGA in order to compare whether the technology shift affects the factors under investigation.

Figure 5: Background image used as a cue for the picture password.

3.1 Null Hypotheses

H_{01}. There is no significant difference in the time needed to create a picture password between users that utilize a mixed reality device *vs.* a desktop computer;

H_{02}. There is no significant difference in strength of user-generated picture passwords between users that utilize a mixed reality device *vs.* a desktop computer;

H_{03}. There is no general preference of users towards picture- or text-based passwords, considering main effects and interactions with respect to device used (mixed reality *vs.* desktop).

3.2 Sampling and Procedure

A total of 30 participants were recruited (10 females), in the age range of 22 to 40 (m=31.7; sd=6.1). No participant was familiar with picture passwords and all had no or limited prior experience with mixed reality devices. Following a between-subjects design, we formed two groups; half of the participants interacted with the picture password in HoloLens (*Mixed Reality Group*), and the other half with a traditional desktop-based PGA (*Desktop Group*). Considering that image complexity affects password strength [17] and gesture combinations [18, 19], we provided the same image (**Figure 5**) to keep image complexity the same across users.

The study involved the following steps: *i)* participants were informed that the collected data would be stored anonymously for research purposes, and they signed a consent form; *ii)* they were familiarized with the picture password, HoloLens and clicker-based gestures; *iii)* participants then created a picture password to unlock a real service in order to increase ecological validity; *iv)* they were asked to log in to ensure that the passwords were not created at random; and finally *v)* they interacted with a text password deployed through a (virtual) keyboard and were further asked to choose their preferred authentication type (picture *vs.* text password).

3.3 Data Metrics

We measured the following data for each group: *i)* time required to create the picture password; *ii)* guessability of user-generated picture passwords which represents the number of guesses required to crack a password (following common brute-force attack approaches [1, 20]); and *iii)* likeability through semi-structured interviews and questionnaires.

3.4 Analysis of Results and Main Findings

In the analysis that follows, data are mean ± standard error. There were no significant outliers. **Table 1** summarizes the creation times and guessability. **Figure 6** depicts user preference.

Differences in Picture Password Creation Time. To investigate H_{01}, we ran an independent-samples t-test, with the user group (mixed reality *vs.* desktop) as the independent variable, and the time to create the picture password as the dependent variable. The analysis revealed that password creation times between the two groups were not significant (Mixed Reality: 16.69 sec *vs.* Desktop: 12.88 sec) with a mean difference of 3.81 ± 3.02 seconds (95% CI, -1.39 to 10.01), $t(27)$=1.261, p=.218.

Table 1: Password creation times and guessability per user group.

	Creation time (sec)	*Guessability (billion)*
Mixed Reality	16.69 (10.5)	306 (7)
Desktop	12.88 (4.96)	310 (1.1)

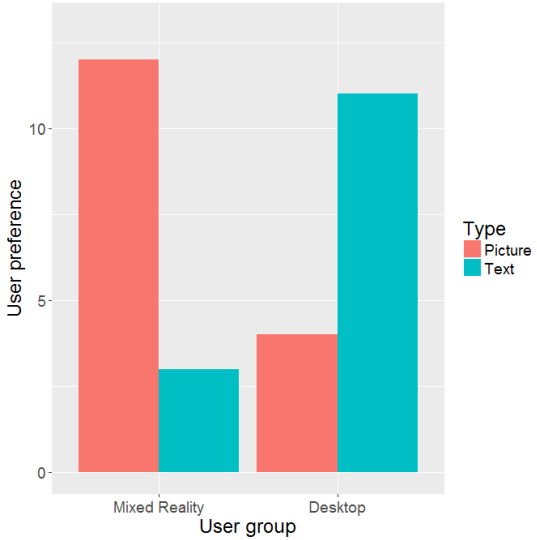

Figure 6: User authentication preference per user group.

ACKNOWLEDGMENTS

This research has been partially supported by EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums). We thank all participants for their time and valuable comments provided during the study.

Differences in Picture Password Strength. To investigate H_{02} and contextualize the usability results, we have further run an independent-samples t-test to investigate whether the two user groups generated different password strengths. Results revealed no significant differences with a mean difference of 4.69 ± 3 billion guesses (95% CI, -1.08 to 1.47), $t(27)=-1.562$, $p=.130$. In particular, user-chosen picture passwords of the Mixed Reality Group required 306 billion guesses to crack, and those of the Desktop Group required 310 billion guesses to crack.

User Preference related to Authentication Type. To investigate H_{03}, we conducted a chi-square test for association between device type and preference towards authentication type (picture *vs.* text passwords). All expected cell frequencies were greater than five. There was a statistically significant association between device type and authentication type preference, $\chi^2(1)=8.571$, $p=.003$. Participants that interacted within mixed reality significantly chose the picture password as their preferred authentication method ($p<.001$). Participants interacting on the desktop computer significantly preferred traditional text passwords ($p<.001$) which can be explained due to familiarity. **Figure 7** summarizes some representative user comments received at the end of the study.

To this end, results revealed that the differences in password creation times and number of guesses required to crack the passwords were not significantly different between the two user groups. Considering that participants had no prior experience with mixed reality devices, such a result is promising towards further investigating picture passwords for mixed reality since picture password interactions are not depreciated when deployed in such contexts. In addition, qualitative feedback received at the end of the study revealed a strong positive preference of users towards using picture passwords when these are deployed in mixed reality.

4 CONCLUSIONS AND FUTURE WORK

This paper presented the implementation and initial evaluation of a picture password scheme for mixed reality. Such an attempt, to the best of our knowledge, is the first of its kind aiming to investigate whether picture passwords are suitable within such contexts. While results based on initial in-lab evaluation studies are promising, further studies are required to evaluate picture passwords in real-life mixed reality contexts to get further insights on security and memorability aspects, and user acceptance.

Given that mixed reality has already entered the market and end-users will continue to use such devices to authenticate themselves, it becomes evident that the current widely deployed text password paradigm might soon become obsolete. Hence, we believe that approaches like picture passwords provide an alternative solution to current state-of-the-art research in mixed reality and have the potential to be adopted within nowadays ubiquitous computation realms.

"It is much easier to draw my password than using the virtual keyboard." ~ P24

"I liked the variety of gestures and the ease of their creation." ~ P07

"In the beginning it was quite hard because it is my first time but with more practice, I could create a password in no time" ~ P16

"It is a more creative way to create a password and escapes the dullness of the keyboard" ~ P30

"I really like the freedom I have with moving my hand in order to create the gesture" - P01

"I found drawing circles difficult because of the accuracy of the center" - P02

"The most difficult part was finding where to draw the gestures but I believe that adds up to the security of the password" - P15

Figure 7: Users' comments received at the end of the study.

REFERENCES

[1] Zhao, Z., Ahn, G., Seo, J., Hu, H. (2013). On the security of picture gesture authentication. In USENIX Security 2013. USENIX Association, 383-398.

[2] Dunphy, P., & Yan, J. Do background images improve draw a secret graphical passwords? In ACM CCS 2007, ACM press, 36-47.

[3] Biddle, R., Chiasson, S., & van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), 41.

[4] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In USENIX Security Symposium 1999, USENIX Association.

[5] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: effects of tolerance and image choice. In ACM SOUPS 2005, ACM Press, 1-12.

[6] Yu, Z., Liang, H.N., Fleming, C., & Man, K.L. (2016). An exploration of usable authentication mechanisms for virtual reality systems. In IEEE APCCAS 2016, IEEE, 458-460.

[7] Roesner, F., Kohno, T., & Molnar, D. (2014). Security and privacy for augmented reality systems. Commun. ACM 57, 4, 88-96.

[8] George, C., Khamis, M., Zezschwitz, E.V., Burger, M., Schmidt, H., Alt, F., & Hußmann, H. (2017). Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In USEC 2017.

[9] Yadav, D. K., Ionascu, B., Ongole, S. V. K., Roy, A., & Memon, N. (2015). Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on google glass. In Financial Cryptography and Data Security 2015, Springer Verlag.

[10] Schneegaß, S., Oualil, Y., & Bulling, A. (2016). SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In ACM CHI 2016, ACM Press, 1379-1384.

[11] Li, S., Ashok, A., Zhang, Y., Xu, C. Lindqvist, J., & Gruteser, M. (2016). Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In IEEE PerCom 2016, IEEE, 1-9.

[12] Johnson, J.J., Seixeiro, S., Pace, Z., van der Bogert, G., Gilmour, S., Siebens, L., & Tubbs, K. (2014). Picture gesture authentication. Retrieved from https://www.google.com/patents/US8910253

[13] Kassner, M., Patera, W., & Bulling, A. (2014). Pupil: an open source platform for pervasive eye tracking and mobile gaze-based interaction. In ACM UbiComp 2014, ACM Press, 1151-1160.

[14] Salvucci, D.D., & Goldberg, J.H. (2000). Identifying fixations and saccades in eye-tracking protocols. In ACM ETRA 2000, ACM Press, 71-78.

[15] Stuart, S., Galna, B., Lord, S., Rochester, L., & Godfrey, A. (2014). Quantifying saccades while walking: Validity of a novel velocity-based algorithm for mobile eye tracking. In IEEE EMBC 2014.

[16] Krejtz, K., Duchowski, A., Szmidt, T., Krejtz, I., Perilli, F.G., Pires, A., Vilaro, A., & Villalobos, N. (2015). Gaze transition entropy. ACM Transactions on Applied Perception, 13(1), article 4

[17] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: effects of tolerance and image choice. In ACM SOUPS 2005, ACM Press, 1-12.

[18] Alt, F., Schneegass, S., Shirazi, A.S., Hassib, M., & Bulling, A. (2015). Graphical passwords in the wild. In ACM MobileHCI 2015, ACM Press, 316-322.

[19] Van Oorschot, P.C., Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. Journal of Computer Security 19, 4, 699-702.

[20] Zhao, Z., Ahn, G., & Hu, H. (2015). Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. ACM Trans. Inf. Syst. Secur. 17, 4, article 14, 37 pages.

[21] von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In ACM NordiCHI 2014, ACM Press, 461-470.

[22] Findlater, L., Wobbrock, J., & Wigdor, D. (2011). Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces. In ACM CHI 2011, ACM Press, 2453-2462.