Free-Form Gaze Passwords from Cameras Embedded in Smart Glasses

Eira Friström, Elias Lius, Niki Ulmanen, Paavo Hietala, Pauliina Kärkkäinen, Tommi Mäkinen, Stephan Sigg, and Rainhard Dieter Findling
{firstname.lastname}@aalto.fi
Ambient Intelligence Group, Department of Communications and Networking, Aalto University
Espoo, Finland

ABSTRACT

Contemporary personal mobile devices support a variety of authentication approaches, featuring different levels of security and usability. With cameras embedded in smart glasses, seamless, hands-free mobile authentication based on gaze is possible. Gaze authentication relies on knowledge as a secret, and gaze passwords are composed from a series of gaze points or gaze gestures. This paper investigates the concept of free-form mobile gaze passwords. Instead of relying on gaze gestures or points, free-form gaze gestures exploit the trajectory of the gaze over time. We collect and investigate a set of 29 different free-form gaze passwords from 19 subjects. In addition, the practical security of the approach is investigated in a study with 6 attackers observing eye movements during password input to subsequently perform spoofing. Our investigation indicates that most free-form gaze passwords can be expressed as a set of common geometrical shapes. Further, our free-form gaze authentication yields a true positive rate of 81% and a false positive rate with other gaze passwords of 12%, while targeted observation and spoofing is successful in 17.5% of all cases. Our usability study reveals that further work on the usability of gaze input is required as subjects reported that they felt uncomfortable creating and performing free-form passwords.

CCS CONCEPTS

• **Security and privacy → Graphical / visual passwords**; • **Human-centered computing** → *Mobile computing*; *Mobile devices.*

KEYWORDS

authentication, free-form, gaze password, matching, smart glasses

ACM Reference Format:
Eira Friström, Elias Lius, Niki Ulmanen, Paavo Hietala, Pauliina Kärkkäinen, Tommi Mäkinen, Stephan Sigg, and Rainhard Dieter Findling. 2019. Free-Form Gaze Passwords from Cameras Embedded in Smart Glasses. In *17th International Conference on Advances in Mobile Computing & Multimedia (MoMM '19), December 2–4, 2019, Munich, Germany.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3365921.3365928

MoMM '19, December 2–4, 2019, Munich, Germany

ACM ISBN 978-1-4503-7178-0/19/12…$15.00
https://doi.org/10.1145/3365921.3365928

1 INTRODUCTION

Many modern mobile devices feature biometrics based authentication, such as fingerprint, face, or gait authentication [8]. However, knowledge remains the dominant form of authentication with mobile devices, such as using PIN, password, and unlock pattern [15]. Recently, also image-based approaches have been proposed [1, 21]. Key advantages of knowledge-based passwords are their technical simplicity and the ease of altering the secret should an adversary become aware of it. Especially the latter is arguably difficult with biometrics.

With modern mobile devices new forms of authentication become possible [9, 16]. Among those devices are smart glasses with cameras built into the frame as well as processing and networking capabilities [7, 13, 24]. The combination of those features allows for mobile gaze-based authentication with smart glasses. Gaze authentication promises various advantages over other authentication approaches. It does not require direct physical interaction and is hands-free. Gaze authentication usually utilizes gaze passwords from either fixate gaze points (position and order of points are the authentication secret [3, 6, 11, 22, 25]), or from gaze gestures (type and order of gestures are the authentication secret [6, 10]).

In this paper, we investigate free-form gaze passwords, which are not restricted to gaze points or gestures. In contrast to previous work on gaze passwords, new matching metrics are required. Further, it has not yet been investigated which free-form gaze passwords users choose if there are no restrictions from gaze points or gestures. However, previous research indicates that users tend to choose easy passwords [2]. The research questions addressed, and our contributions to those are:

How well can free-form mobile gaze passwords be distinguished? To address this we a) propose a methodology to match free-form gaze passwords with dynamic time warping, and b) collect a dataset of 29 unique free-form gaze passwords with a total of 454 samples, from 19 different subjects.

How successful are targeted observation and spoofing attacks on free-form mobile gaze password? To address this, we collect 166 attacks on 15 passwords from a total of 6 different attackers, which at first observe the password input multiple times, then try to spoof the password they have seen. From this we evaluate how successful targeted observation and spoofing attacks on free-form passwords are.

What is the perceived usability of free-form mobile gaze passwords? To address this, we perform a user study to asses the users' perspective on free-form gaze passwords for authentication.

Table 1: Overview of previous work on gaze passwords. No studies have addressed free-form gaze passwords yet.

Related work	Gaze points/ gestures	Approach	Results
EyePassword, Kumar et al. [22]	Gaze points	Gaze-based typing	Gaze password input can achieve similar accuracy as keyboard password input. Error rates: 3-4% (Gaze+dwell), 15% (Gaze+trigger). Users feel more comfortable using gaze passwords instead of a keyboard in public.
EyePIN, De Luca et al. [6]	Gaze points & gestures	Predefined patterns for numbers & gaze-based typing	Eye gaze input for the PIN prevents majority of observation attacks. 9.5% error rate for eye gestures, 23.8% for gaze + dwell and 20.6% for gaze + trigger. Eye gesture input is ~4 times slower to use than gaze points.
Cued Gaze Points (CGP), Forget et al. [11]	Gaze points	5 gaze points to choose from	CGP T-51: successful logins for ≤ 3 tries, error rate 7%, T-31: successful logins for ≤ 3 tries, 21% error rate. In theory the success rate of attacks (even with eye recordings) would be low.
Gaze points, Bulling et al. [3]	Gaze points	Background picture to help to select gaze passwords	Saliciency masking is more secure for selecting gaze points than traditional gaze point methods. 1.3% of password points fell to the saliciency region, when saliciency mask was present, otherwise 34.5%.
GazeTouchPIN, Khamis et al. [20]	Gestures	Two-phase selection with both touch and gaze	GazeTouchPIN is more secure than touch-based systems against both iterative and side attacks. No statistically significant method for error rate. Successful iterative attack, 4.2% success rate. Successful side attack, 17% success rate.
Moving gaze points, Rajanna and Hammond [25]	Gaze points	Selected 3 from 12 defined shapes & follow their movement	Gaze-based authentication from screen with gaze. Template matching algorithm is reported to have 95% accuracy, decision tree algorithm to have 90.2% accuracy.
Closed-eye gaze gestures, Findling et al. [10]	Gestures	Closed-eye gaze gestures with optical flow extraction	Extend existing gaze gesture alphabets by utilizing closed-eye gaze gestures. Achieve 82.8-91.6% detection and 92.9-99.2% recognition of gaze gestures.

2 RELATED WORK

Multiple studies on gaze authentication have been conducted [3, 6, 11, 20, 22, 25] (Tab. 1). Gaze passwords in general are perceived as being useful for mobile authentication in situations where security seems essential [20]. However, comparing security and usability aspects of the corresponding approaches is difficult due to different definitions of failed password input and the absence or presence of training for individual users [11].

Existing studies on gaze passwords mostly rely on camera based gaze detection, and are in general limited to the use of certain password shapes [6, 11], or use digits from an alphabet which are chosen via gaze [20, 22]. Outside camera based gaze detection, recent work [10] has examined the possibility of including closed-eye movement as an extension to detecting pupil movement from open eyes using a predefined set of gaze gestures. In a similar manner, sensing gaze gestures with electroculography (EOG) has been explored in [4, 5], again using a predefined set of gaze gestures. So far, free-form gaze passwords for mobile authentication have not been considered. One concept related to the idea of free-form gaze passwords is graphical passwords which utilize background images as help for the user. In those, passwords are performed by users looking at points in an image in a certain order [3].

Concerns towards knowledge-based mobile authentication approaches, like PIN and pattern, come from both the theoretical password space (TPS), the actual password space (APS), as well as from the vulnerability to shoulder surfing [26]. A 4-digit PIN, as the most frequently used mobile authentication approach, has an TPS of 13.3 bit. In contrast, gaze passwords have been assessed to have a bigger TPS, e.g. 25.3 bit with saliciency masked pictures [3], and 29.9 bit for cued 5-point gaze passwords [11]. However, the APS has been shown to be smaller than the TPS. This results from the prominent use of easy passwords, which reside in a subspace of the TPS, and which therefore are easier to guess. Forget et al. [11] point out that not all users seem to be able to come up with secure passwords. This argument is confirmed by a study by Bulling et al. [3], where parts of pictures are assessed to be areas of high popularity for gaze points, and hence get masked by saliciency masks when creating a gaze password. This resulted in participants choosing different areas and in turn in more entropy. The increased APS is less prone to gaze point based dictionary attacks. A key takeaway is that when no saliciency masks were used, 34.5% of the user chosen gaze points fell within assessed areas of high popularity. In a similar study, Thorpe and Oorschot [27] found hot spots in images for gaze passwords. Such hot spots decrease the APS over the TPS and make the corresponding passwords vulnerable to brute force and dictionary-aided attacks.

Other concerns towards gaze passwords originate in the required time to perform authentication. In [11], participants selected points on a sequence of 5 pictures with their gaze to perform a gaze password. The mean duration required for this was 53.5 s for small and 36.7 s for large tolerance squares. In a related study, Heikkilä et al. [14] suggested to provide visual feedback while performing a gaze password to decrease the input duration. In addition to the slow input time of the password, Forget et al. [11] question whether it is practical to adapt gaze passwords to real life applications due to possible errors during password input. In a setting of two different gaze input areas (31×31 and 51×51 pixel boxes), a significant difference for increased errors was found present. The smaller area was noted to be harder to confirm as a password point with one's gaze. However, as was noted in a different study by Khamis et al. [20], a learning curve has been present for some types of gaze passwords.

3 APPROACH

We utilize smart glasses with eye-facing cameras for mobile free-form gaze password authentication. The cameras are embedded in the glasses frames, with which pupil movement is monitored, from which then the gaze direction is derived.

Our approach consists of an enrollment and an authentication part (Fig. 1). Processing of gaze passwords is similar for enrollment and authentication. At first, passwords are sensed using the eye-facing cameras in the smart glasses. The gaze direction is derived from pupil movements. Those raw gaze passwords are timeseries

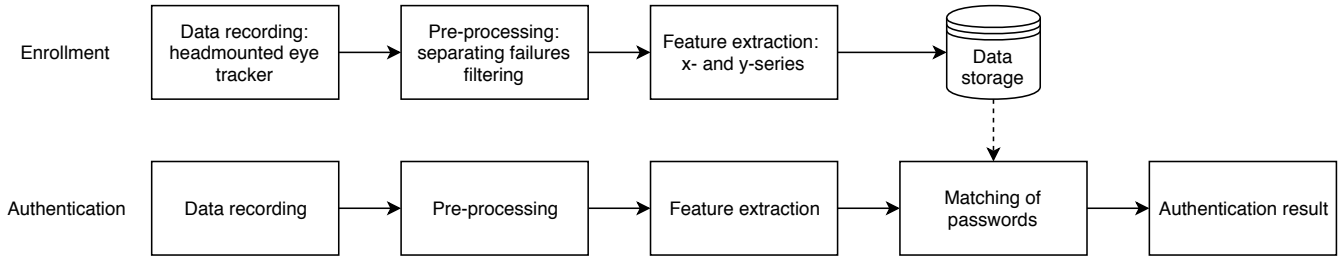


Figure 1: Overview of our approach from a processing perspective. Users at first enroll with their chosen free-form gaze password and later on authenticate by performing the same password again, which is matched with the enrollment samples.

in the form of horizontal and vertical eye movements over time. In the processing, we filter and normalize those timeseries. As a result, each gaze password sample that we consider during enrollment and authentication consists of a pair of processed horizontal and vertical timeseries of eye movements.

Users enroll by performing their free-form gaze password multiple times, of which the processing result is stored for usage during authentication. After enrollment, users can authenticate by performing their gaze password, which is compared to the previously stored enrollment samples, and which yields a binary authentication decision (accept/reject).

3.1 Sample Processing

During preprocessing, we apply filtering and normalization to gaze passwords. At first, we normalize both horizontal and vertical timeseries to be within [0, 1] (Eq. 1).

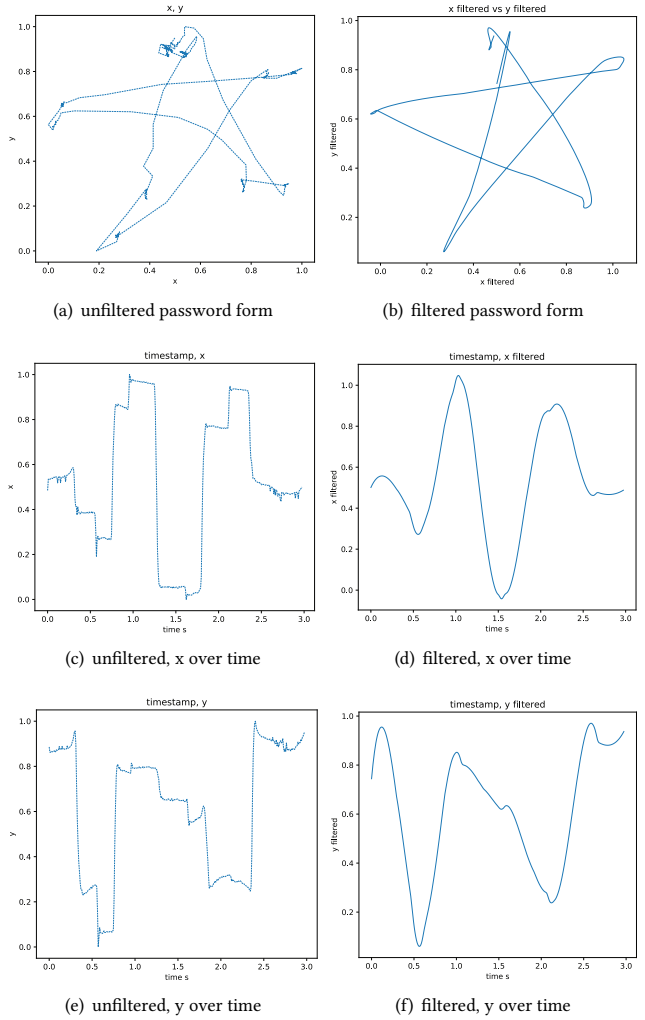
$$V_n' = \frac{V_n - min(V)}{max(V) - min(V)} \tag{1}$$

Next, we employ a Saviztky-Golay filter (SG-filter) [12] to remove high frequency noise. We utilize an SG-filter over a running mean or median filter, since it preserves minima and maxima better. The filter is configured to use a sliding window of 0.36 s and a 3rd degree polynomial for function approximation within the window (Fig. 2).

3.2 Enrollment and Authentication

Enrollment requires that the free-form gaze password is repeated at least three times. The samples are processed, then stored for reference during matching.

During authentication, the processed gaze password is matched to the previously stored enrollment passwords. Since our goal is to utilize free-form passwords without explicit gaze points or gestures, we do not rely on matching methods exploited in the literature for gaze authentication. Instead, the timeseries of samples is matched via dynamic time warping (DTW) [19] with L^2-norm as internal path error metric. We utilize DTW over other timeseries based similarity metrics, like cross correlation, due to its ability to dynamically stretch and compress the series to be compared. This allows for changes in the speed in which gaze passwords are performed. DTW thereby yields a distance d that expresses similarity, where smaller distance corresponds to higher similarity. Authentication is successful if d is lower than a predefined reference threshold T (Eq. 2).



(a) unfiltered password form (b) filtered password form

(c) unfiltered, x over time (d) filtered, x over time

(e) unfiltered, y over time (f) filtered, y over time

Figure 2: Raw data in x any y dimension (left), x data over time (center), y data over time (right), for both raw data (upper row) and filtered data (lower row). The noise removal from filtering is clearly visible.

$$\text{auth} = \begin{cases} \text{accept} & \text{if } d \leq T \\ \text{reject} & \text{otherwise} \end{cases} \tag{2}$$

4 EVALUATION DATA

In this section, we discuss our evaluation data, including the recording hardware, recording setup, as well as type and amount of data recorded for our subsequent evaluation. For quantifying both success rates for matching and attacking passwords with observation and spoofing, we need two types of data: users performing their free-form gaze passwords, as well as attackers observing the pupil movements during password input and subsequently trying to reproduce the observed password to spoof the authentication. Data for our user study, which is highlighted in Sec. 5.3, was also gathered at password recording time.

4.1 Recording Hardware

To record free-form gaze passwords, we utilize a first generation Pupil eyetracker from PupilLabs [17]. The device features an eye-facing camera for pupil monitoring and gaze direction derivation. The camera is operating in the infrared (IR) spectrum and has an accompanying IR LED next to it for IR illumination. The eye-facing camera of the eye tracker can be used with different resolutions and sampling rates. In our setup, we utilized the right eye-facing camera with a 320×256 resolution with 120 Hz sampling rate for free-form gaze gesture recording. From data gathered with the eye tracker, gaze direction is extracted via the PupilLabs software, which internally uses the dark pupil detection approach [18] on the IR image data from the hardware.

4.2 Free-Form Gaze Password Data

For choosing and performing passwords, participants were instructed to choose their own free-form gaze password such that it would be difficult to guess and reproduce by attackers. No further instructions or restrictions towards password choice were given. All recordings were done indoors with normal ceiling-mounted room lightning installed in the office room. During password input, users were sitting at a table with the laptop to which the eye tracker was connected to. The laptop screen did not show any reference points, but the geometry of the screen itself was used as reference for participants. After recording a password sample, it is automatically checked for validity and discarded if invalid. A sample is valid when horizontal and vertical pupil movements are not constant zero and horizontal and vertical ranges do not exceed the width and height of the calibrated area. This is done due to hardware issues we experienced during recording in which the device was unable to locate the pupil of the participant.

The resulting free-form gaze password dataset we recorded consists of 29 distinct passwords of a total of 19 participants. Each participant performed each of their self chosen passwords 5-27 times (mean 15.1, std 6.4) in one session each, which results in a total of 454 password samples. Passwords in our database have a duration between 1.96 s and 11.76 s, with a mean duration of 4.64 s (std 1.68 s). Each of the password samples is represented as a pair of raw horizontal and vertical gaze direction time series during password input.

4.3 Observation-Spoofing Attack Data

While recording free-form gaze passwords, the recording of 15 passwords was used to also prepare data for an observation based attack scenario. The attack scenario is other people (the attackers) observing the pupil movements while users perform gaze passwords, and later on trying to reproduce the observed gaze passwords to spoof the authentication. For this scenario, 15 users performing their gaze passwords were filmed from the other side of the table they were sitting at, which resulted in a 1 m distance (Fig. 3). The device used for recording attack data was an off-the-shelf high end smartphone: a OnePuls 6, with a camera with 1080p resolution and 30 Hz video frame rate. We deem it realistic for attackers to use video recording of gaze password input, as smartphone cameras are widespread and relatively unsuspicious when used. It might further aid attackers in their attacks to be able to re-watch password input. While recording of eye movements from close distance during password input has a high change to be detected, we argue that this also captures the capabilities of more powerful attackers. Those might employ more higher quality cameras from larger distance, in which video based attacks would be more difficult to detect.

Figure 3: The attackers' perspective: snapshot of a video recording of a user performing their gaze password, filmed from the opposite side of the table the user is sitting at.

Six participants of our study were selected to also act as attackers. Each of them attacked each of the 15 passwords, for which they watched the videos multiple times. They were allowed to use tools like a notebook to aid their observation, which some attackers chose to do. After the observation, the attackers tried to recreate the gaze password they observed as input to the eyetracker, 5 times per password and attacker. This results in a total of 166 attacks, which we utilize as our observation-spoofing attack dataset.

Table 2: Overview of data gathered for our evaluation, including both gaze password input and observation-spoofing attacks.

Free-form gaze password users	Passwords	Total samples
19	29	454
Free-form gaze password attackers	Passwords attacked	Total attacks
6	15	166

Summarizing, our evaluation data set contains a total of 454 free-form gaze password samples from a 29 unique passwords and 19 unique users, as well as a total of 166 observation-spoofing attacks on 15 passwords, performed by 6 attackers (Tab. 2).

5 EVALUATION AND RESULTS

We first highlight patterns we found in the passwords users chose. We then evaluate how successful samples of passwords in our dataset can be recognized to be from the same password, and how well they can be distinguished to be from different passwords. Finally, we show the success rates of attacking gaze passwords with observation and spoofing.

5.1 Encountered Password Shapes

Analyzing the passwords in our evaluation dataset revealed certain patterns in users' gaze password choices. This is in-line with prior research which shows that users tend to choose simple PINs and passwords [2], unlock patterns and graphical passwords [28]. While it decreases the entropy of the search space if attackers get to know the form of the password, it still is important to note that the passwords are not fully defined by the shapes they approximate. The chosen form names do not capture details such as different start and end points, size of movements, direction of movement, and so forth.

Forms that we encountered in the passwords include: left arrow, down arrow, triangle with an additional line, rectangle, rectangle with 2 diagonal lines, half circle, circle with 2 additional horizontal and vertical lines, circle with a middle line, combination of a half-circle with a triangle, circle with a plus symbol, hourglass, hourglass (crooked), 4-dot infinity symbol, 4-dot infinity symbol (crooked), 4-dot infinity symbol with an additional line, partial 4-dot infinity symbol, wave, sawtooth, star (two different forms, one serves as basis for Fig. 2), the letter E, the letter S (crooked), the letter P, the letter W (mirrored). Only 5 free-from gaze passwords seem to not be at least partially describable with commonly known geometrical forms. While we observed those patterns to exist in our evaluation data, we are specifically interested in how difficult it is for attackers to perform an observe-spoofing attack and leave further analysis of pattern in gaze password choices as well as the resulting entropy and guessability of passwords to future work.

5.2 Recognition of Free-Form Gaze Passwords

With our gathered free-form gaze password dataset we simulate enrollment and authentication for each user. For enrollment, we consider in between 6-27 samples the user performed of their self chosen password. We process those samples according to our approach and form a mean template. This template represents the mean of the user-chosen free-form password and contains the mean of horizontal and vertical positions over all samples considered, for each point in time. We use this mean template to detect and remove outlier samples. For this, we first calculate the difference between the 10% and the 90% quantiles $q_{diff} = q_{90} - q_{10}$ over all samples. Outliers are defined outside $q_i \pm (1.5 \cdot q_{diff})$, where q_i is an individual value in one password sample. Values found outside this area are considered outliers and removed. The remaining samples are considered to be the enrollment samples of the user.

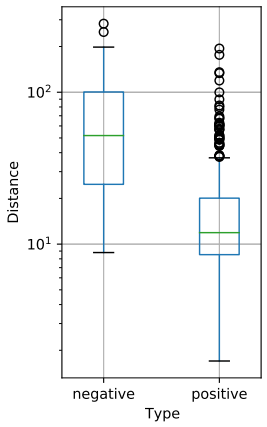


Figure 4: Distribution of distances for positive and negative comparison samples, over all users and free-form gaze passwords.

After enrollment, we simulate authentication. We present both the remaining samples of the user-chosen password, which correspond to comparisons that should match (positive comparison), as well as all samples of all other passwords for authentication, which correspond to comparisons that should not match (negative comparison). Over all comparisons for enrollment and authentication, we see a tendency of positive comparison distances to be smaller than negative comparison distances (Fig. 4). The optimal distance threshold for the authentication decision minimizes the false mismatch rate, which is the rate of legitimate passwords being falsely rejected during authentication, and the false match rate, which is the rate of non-legitimate passwords being falsely accepted during authentication. For our free-form gaze password dataset, the optimal distance threshold varied among users from 2 to 37 (mean 21.7, std 9.1). Calibrating the threshold to individual users would require both matching and non-matching data. For this reason, we consider it to be unrealistic and instead derive a suitable fixed threshold from our dataset, which is applicable to all users. In our setup we define a threshold of 20 (we refrained from taking 21.7, which would have been the optimal choice in our case, and yielded slightly improved results, in order to model the performance in a potential real-world application of the approach, where the optimal choice can only be approximated due to continuous data). Authentication decisions based on this threshold result in a mean false acceptance rate of

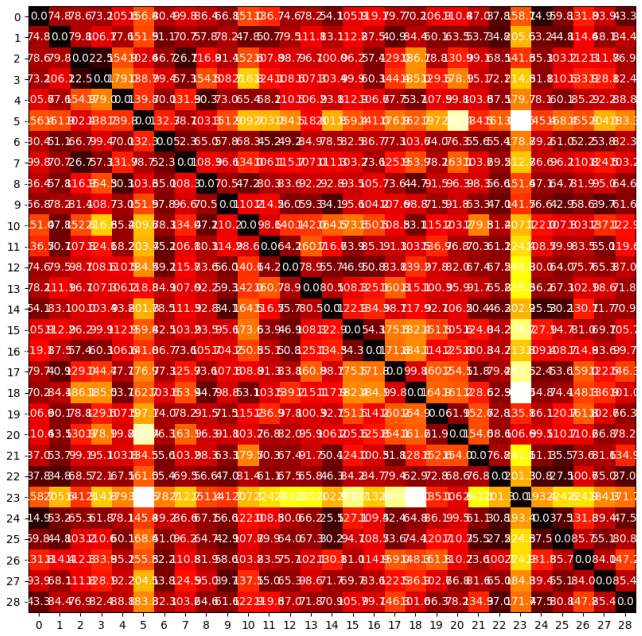


Figure 5: Heatmap of distances between mean templates.

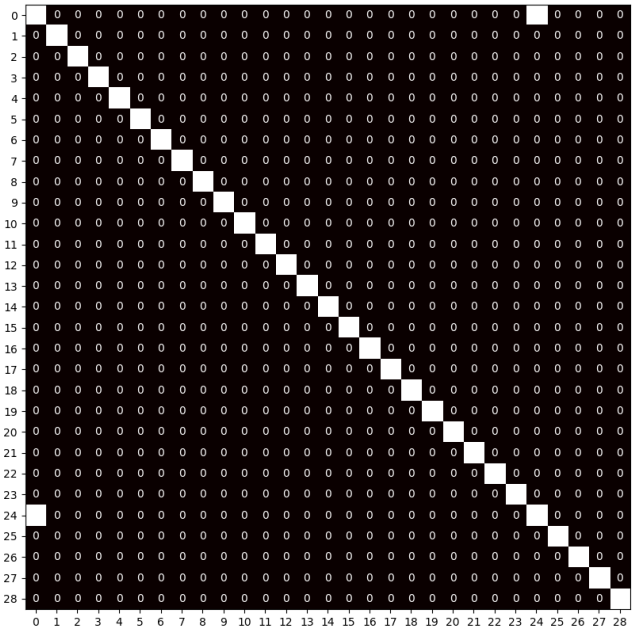
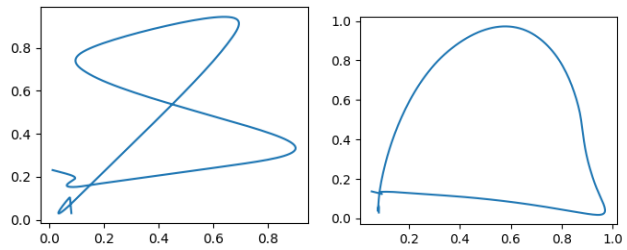


Figure 6: Two mean templates are assessed to be same when directly applying the derived authentication threshold to the templates.

12% (std 2%), a mean false rejection rate of 19% (std 3%), and a corresponding mean equal error rate (EER) of 16% (std 2%), over all users in our free-form gaze password dataset.

We also investigate how different the mean templates used during enrollment are to each other. We do this as we already observed that the chosen free-form passwords can at least partially be expressed as geometrical forms. Comparing the mean template allows for assessing how similar the form of the average passwords are without considering individual noisy samples. The heatmap of distances between mean templates over all passwords shows mostly high distance values, while for only a few samples the pairwise distance is low (Fig. 5). Distances are in the range [15, 321], with 50% being within [70, 129]. Applying our decision threshold of 20 to those distances reveals that two mean templates are assessed as identical (Fig. 6), which are the half-circle and the hourglass (crooked) passwords (Fig. 7).



(a) Hourglass (crooked) (b) Half-circle

Figure 7: Mean templates for the "hourglass (crooked)" and the "half-circle" passwords, which are assessed as being the same.

5.3 Observation-Spoofing Attacks

We evaluate the success of targeted observation-spoofing attacks with data from our attack dataset. For all 166 attack samples over all passwords, 29 pass authentication (mean 17.5%, median 0%). However, attack success rates strongly vary with the chosen password. We assume that this results from certain passwords being performed in a quasi-standardized way by users, which makes reproducing them as an attacker significantly easier than reproducing other passwords. For example, on the one hand, the attack success rate the 4-dot infinity symbol password was 100% (over all attackers). This particular sample was performed in a particular slow peace by the corresponding user, which might increase the chance for correct observation by attackers. On the other hand, for the majority of 9 of the 15 attacked passwords, not a single attack of any attacker passes authentication.

From this we conclude that it seems to be easy for attackers to observe eye movement, which aligns with previous findings [6], and that subsequently is also is easy to reproduce at least some password shapes correctly. However, for the majority of passwords, observing and reproducing the observed password was unsuccessful.

6 USER STUDY

After collecting data of free-form gaze passwords for users and attackers, participants were given a questionnaire with 10 questions and 5-point Likert-scale answers (Tab. 3). A total of 17 completed questionnaires were returned of which the answers (Fig. 8) form the

Table 3: The questionnaire presented to participants who acted as both users and attackers, with mean and std over their Likert-scale answers.

Nr	Question + Answers	mean	std
Q1	How confident do you feel in reproducing the imaginary gaze password with your eye movement? Answers from (1) very unconfident to (5) very confident.	3.24	1.25
Q2	How secure do you consider the gaze password method to be in comparison to hand-written passwords? Answers from (1) very much less secure to (5) very much more secure.	2.88	1.27
Q3	How physically comfortable do you feel creating a password with your eye movement? Answers from (1) very uncomfortable to (5) very comfortable.	2.18	0.81
Q4	How practical do you find gaze passwords compared to inputting a password by writing a keyword, inputting a series of digits or drawing a pattern? Answers from (1) very much less practical to (5) very much more practical.	2.35	0.93
Q5	How would you think a grid in the background of the password's input space (computer screen or a white wall, for example) would change the easiness of defining a new gaze password? Answers from (1) very much more difficult to (5) very much easier.	4.47	0.51
Q6	How much would you say your password is free-form and/or based on a well-known 2D geometrical form (a square, triangle etc.) ? Answers from (1) purely geometrical form to (5) purely free-form.	2.18	0.95
Q7	How much would you say your password is free-form and/or based on a well-known symbol (the infinity symbol, a cross etc.) ? Answers from (1) purely a symbol to (5) purely free from.	2.41	1.46
Q8	How difficult would you think it would be for others to guess the form of your password without having seen it? Answers from (1) very much more difficult to (5) not difficult at all.	2.35	1.17
Q9	How difficult would you think it is for others to reproduce your password once they have seen the form of your password but do not have the password drawn down or it is not accessible? Answers from (1) very much more difficult to (5) not difficult at all.	3.76	1.15
Q10	How difficult would you think it is for others to imitate your password if they have seen only your eye movements when inputting the password and not the password itself? Answers from (1) very much more difficult to (5) not difficult at all.	1.94	0.83

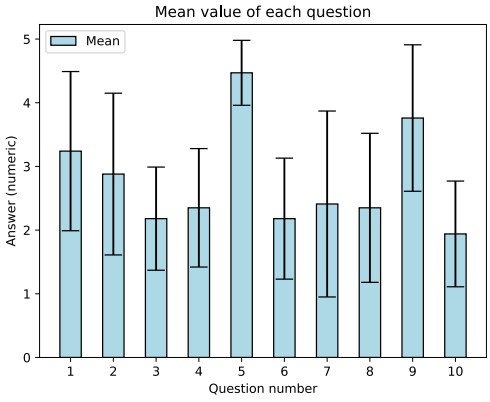


Figure 8: User study result as mean and standard deviation (depicted as error bars) over the Likert-scale answers of the questionnaire

basis of our analysis. Participants were 20-28 years old (mean 23.4, std 2.1), and a majority of them were University students. None had previously used gaze passwords.

Participants felt neutral about being able to reproduce their passwords (Q1). In terms of usability, participants felt uncomfortable performing their passwords (Q3) and they did not consider gaze passwords practical, compared to other forms of knowledge-based authentication (Q4). Participants further mostly agreed on a reference grid being helpful for performing the gaze password (Q5). Concerning form and components of the chosen gaze passwords, answers indicate that participants chose free-form gaze passwords that do incorporate or are based on well-known 2D geometrical forms and symbols (Q6 and Q7). Participants were neutral about overall security of free-form gaze passwords (Q2). In more detail, participants indicated that they think it would be difficult for attackers to guess the form of their chosen password without observing it during password input (Q8). They further also indicated that they think it would be difficult to imitate a password after just having observed it from users' eye movements during password input (Q10). However, participants also indicated that it might not be difficult for attackers to reproduce their passwords once they know the password form itself (Q9). Subsequently, we highlight important findings from the answers to four of the given questions in more detail.

Q1: *How confident do you feel in reproducing the imaginary gaze password with your eye movement?* The mean answer of 3.24 (std 1.25) indicates that participants felt neither unconfident or confident in reproducing their own password. Some participants remarked that it was difficult for them to determine the speed, starting point, and ending points when performing their password. As it was the first time use of gaze passwords for all participants, we assume that if users were to become accustomed to gaze passwords as well as to their own password in particular, it might be that they would feel more confident in reproducing it over time [20].

Q3: *How physically comfortable do you feel creating a password with your eye movement?* The mean of 2.18 (std 0.81) indicates that the majority of participants felt uncomfortable when performing their free-form gaze password. Some participants reported some anxiety and tiredness of the eyes after performing their gaze password multiple times. We noticed that forcing oneself to keep the eyes fully open seems to help in successfully performing the gaze password. This seems to also correspond to the pupil detection mechanism having a higher chance of failure when eyes would not be fully closed. Despite the higher success rate of passwords when

forcing oneself to keep ones eyes full open, it also causes a tiring effect for the eyes, hence for subsequently feeling uncomfortable. A further reason for participants to feel uncomfortable might be that gaze passwords require additional concentration that users are not used to or would feel prepared for in all situations (given that they are not used to gaze passwords altogether). To further assess if users feel comfortable or uncomfortable with free-form gaze passwords, a long-term user study would be required, which would be a viable target for subsequent work.

Q5: *How would you think a grid in the background of the password's input space (computer screen or a white wall, for example) would change the ease of defining a new gaze password?* The mean of 4.47 (std 0.51) shows that the majority of users is convinced that having reference points in the form of a grid would be beneficial for gaze password input. Static, location depend reference grids, like one printed on a wall would thereby not be suitable for smart glasses based mobile gaze password input, as they would not readily be available in each situation and location users would perform their passwords. Also, using other devices, such as laptops for reference grids would be too cumbersome. A potentially viable solution would be that smart glasses display a reference grid for the user once gaze password input is required, e.g. with augmented or virtual reality.

Q6: *How much would you say your password is free-form and/or based on a well-known 2D geometrical form (a square, a triangle etc.)?* The mean of 2.18 (std 0.95) indicates that participants felt that their password shapes were often not truly free-form, but that they instead had geometrical aspects. Comments of participants revealed that they felt it was difficult to come up with something completely free-form, and that round movements are difficult to produce, which concurs with findings of previous research on eye movements [23].

Question 10: *How difficult would you think it is for other to imitate your password if they have seen only your eye movements when inputting the password and not the password itself?* With a mean of 1.94 (std 0.83) the answers point out that participants who acted as both users and attackers consider it difficult to imitate free-form gaze passwords, after they have observed them from other users performing them. This also aligns with the attackability results in our evaluation, which show that only 17.5% of attacks are successful after attackers have observed the user's eye movements during password input.

In summary, important takeaways include that participants felt their passwords were not of free-form, but rather geometrical or follow forms of known symbols. However, even if the passwords were not considered to be of free-form, the participants felt neutral about reproducing their own password, and that it would be difficult for an attacker to imitate the password just by looking at their eye movements.

7 CONCLUSION

We investigated the concept of free-form gaze passwords in as an alternative to fixation-based gaze point or gaze-gesture-based passwords. The most important difference to previous work is that password matching cannot rely on gaze points (points of fixation) or gaze gestures being present in the password. For this reason, we directly match gaze passwords by their gaze direction time series in horizontal and vertical direction with dynamic time warping (DTW). DTW thereby allows users to change the speed in which they perform their password.

In our evaluation we utilized 454 samples of 29 distinct free-form gaze passwords from 19 users. Results indicate that our authentication correctly recognizes passwords with a true positive rate of 81% and a false positive rate of 12%. This indicates– while the results are not error free – that free-from gaze passwords can successfully be matched with time series similarity or distance metrics like DTW. An interesting finding in our dataset was that most free-form gaze passwords can be at least partially described by well known geometrical forms, like circles, rectangles, stars, hourglass, etc. While this indicates that the passwords might not truly be free-form, knowing the form alone is not sufficient to capture all information required to recreate a free-form gaze password. Information that is not contained by the form of the password would be, for example, the start and endpoint of the password, the overall dimension of the password, the size and relation of individual parts to each other, the rotation, etc.

We also evaluated how well free-from gaze passwords could be attacked from observations and subsequent spoofing. For this, we utilized 166 attacks from 6 distinct attackers on 15 of the passwords in our dataset. In those attacks, attackers watch a video of the user performing gaze password authentication, and then try to spoof the authentication by re-performing the password they saw in the video. Based on this data we found attack success rates to largely differ between different passwords. For one password in our dataset the attack success rate was 100%. We assume this is due to reproducing the password in a particularly slow manner, as well as that it is easier for attackers to reproduce certain specific passwords forms than the majority of passwords. For the majority of passwords (9 of 15 in our dataset), not a single attack attempt was successful. The resulting mean and median attack success rates over all passwords and samples in our dataset, after having observed eye movements during authentication, are 17.5% and 0% .

We further performed a user study with a 10-question questionnaire and 5-point Likert-scale answers. Results indicate that users felt neutral about their ability to correctly reproduce their free-form password, but that they did not feel comfortable during performing their password or would consider them practical. They further thought that a grid as reference would be helpful during password input. Such a grid could be shown to smart glasses users e.g. by augmented reality once they are prompted for password input. Results also show that users think their passwords are based on geometrical forms. In terms of security, results indicate that users think neutral about overall free-form gaze password security. Users think that it would be difficult for attackers to guess their password without having observed it during password input, but also that observing the password would make it easy for attackers to spoof the authentication.

Future work could investigate the applicability of different features and further matching metrics for free-form gaze password authentication. An extended user study could investigate the long-term usability, including both memorability of free-form passwords, as well as their applicability in diverse everyday life situations. Future work could furthermore also investigate extended attacks. One

interesting aspect of this would be the success rate of attacks in which attackers only have different types of descriptions of the passwords, but have not observed the password input themselves. Such information could include the name of the geometrical form of the password as well as potential meta-information, such as duration and speed, direction, dimensions, rotation, and so forth.

ACKNOWLEDGMENTS

We appreciate funding in the frame of the ChistEra RadioSense Big Data and process modeling for Smart Industry (BDSI) project.

REFERENCES

[1] Sadiq Almuairfi, 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 (2013), 108–116.

[2] J. Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *IEEE Symposium on Security and Privacy (SP 2012)*. 538–552. https://doi.org/10.1109/SP.2012.49

[3] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3011–3020.

[4] Andreas Bulling, Daniel Roggen, and Gerhard Tröster. 2008. It's in your eyes: towards context-awareness and mobile HCI using wearable EOG goggles. In *Proceedings of the 10th international conference on Ubiquitous computing*. ACM, 84–93.

[5] Andreas Bulling, Daniel Roggen, and Gerhard Tröster. 2009. *Wearable EOG goggles: eye-based interaction in everyday environments*. ACM.

[6] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces*. ACM, 199–202.

[7] Murtaza Dhuliawala, Juyoung Lee, Junichi Shimizu, Andreas Bulling, Kai Kunze, Thad Starner, and Woontack Woo. 2016. Smooth eye movement interaction using EOG glasses. In *Proceedings of the 18th ACM International Conference on Multimodal Interaction*. ACM, 307–311.

[8] Rainhard Dieter Findling, Michael Hölzl, and René Mayrhofer. 2018. Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics. *IEEE Transactions on Mobile Computing (TMC)* 14, 11 (Nov. 2018), 2578–2590. https://doi.org/10.1109/TMC.2018.2812883

[9] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2017. ShakeUnlock: Securely Transfer Authentication States Between Mobile Devices. *IEEE Transactions on Mobile Computing (TMC)* 16, 4 (April 2017), 1163–1175. https://doi.org/10.1109/TMC.2016.2582489

[10] Rainhard Dieter Findling, Le Ngu Nguyen, and Stephan Sigg. 2019. Closed-Eye Gaze Gestures: Detection and Recognition of Closed-Eye Movements with Cameras in Smart Glasses. In *15th International Work-Conference on Artificial Neural Networks (IWANN 2019) (LNCS)*. Springer.

[11] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1107–1110.

[12] José Luis Guiñón, Emma Ortega, José García-Antón, and Valentín Pérez-Herranz. 2007. Moving average and Savitzki-Golay smoothing filters using Mathcad. *Papers ICEE* 2007 (2007).

[13] Michael Haslgrübler, Peter Fritz, Benedikt Gollan, and Alois Ferscha. 2017. Getting through: modality selection in a multi-sensor-actuator industrial IoT environment. In *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, 21.

[14] Henna Heikkilä and Kari-Jouko Räihä. 2009. Speed and accuracy of gaze gestures. *Journal of Eye Movement Research* 3, 2 (2009), 1.

[15] Daniel Hintze, Philipp Hintze, Rainhard Dieter Findling, and René Mayrhofer. 2017. A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics. *Proc. ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 2 (June 2017). https://doi.org/10.1145/3090078

[16] Daniel Hintze, Muhammad Muaaz, Rainhard Dieter Findling, S. Scholz, E. Koch, and René Mayrhofer. 2015. Confidence and Risk Estimation Plugins for Multi-Modal Authentication on Mobile Devices using CORMORANT. In *13th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2015)*. ACM, Brussels, Belgium, 384–388. https://doi.org/10.1145/2837126.2843845

[17] Moritz Kassner, William Patera, and Andreas Bulling. 2014. Pupil: An Open Source Platform for Pervasive Eye Tracking and Mobile Gaze-based Interaction. In *Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1151–1160. https://doi.org/10.1145/2638728.2641695

[18] Moritz Kassner, William Patera, and Andreas Bulling. 2014. Pupil: an open source platform for pervasive eye tracking and mobile gaze-based interaction. In *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct publication*. ACM, 1151–1160.

[19] Eamonn J Keogh and Michael J Pazzani. 2001. Derivative dynamic time warping. In *Proceedings of the 2001 SIAM international conference on data mining*. SIAM, 1–11.

[20] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction*. ACM, 446–450.

[21] Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. 2017. On the Use of Emojis in Mobile Authentication. In *ICT Systems Security and Privacy Protection*, Sabrina De Capitani di Vimercati and Fabio Martinelli (Eds.).

[22] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 13–19.

[23] Michael F Land. 1999. Motion and vision: why animals move their eyes. *Journal of Comparative Physiology A* 185, 4 (1999), 341–352.

[24] Stefan Mitrasinovic, Elvis Camacho, Nirali Trivedi, Julia Logan, Colson Campbell, Robert Zilinyi, Bryan Lieber, Eliza Bruce, Blake Taylor, David Martineau, et al. 2015. Clinical and surgical applications of smart glasses. *Technology and Health Care* 23, 4 (2015), 381–401.

[25] Vijay Rajanna and Tracy Hammond. 2018. Gaze-Assisted User Authentication to Counter Shoulder-surfing Attacks. *arXiv preprint arXiv:1803.07782* (2018).

[26] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proc. of the second symposium on Usable privacy and security (SOUPS '06)*. ACM, New York, NY, USA, 56–66. https://doi.org/10.1145/1143120.1143128

[27] Julie Thorpe and Paul C van Oorschot. 2007. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords.. In *USENIX Security Symposium*, Vol. 8. 1–8.

[28] Paul C. van Oorschot and Julie Thorpe. 2008. On Predictive Models and User-drawn Graphical Passwords. *ACM Trans. Inf. Syst. Secur.* 10, 4, Article 5 (Jan. 2008), 33 pages. https://doi.org/10.1145/1284680.1284685