Findling, Rainhard; Quddus, Tahmid; Sigg, Stephan

Hide my Gaze with EOG!: Towards Closed-Eye Gaze Gesture Passwords that Resist Observation-Attacks with Electrooculography in Smart Glasses

Published in:
17th International Conference on Advances in Mobile Computing & Multimedia (MoMM2019)

DOI:
10.1145/3365921.3365922

Published: 01/12/2019

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Findling, R., Quddus, T., & Sigg, S. (2019). Hide my Gaze with EOG!: Towards Closed-Eye Gaze Gesture Passwords that Resist Observation-Attacks with Electrooculography in Smart Glasses. In *17th International Conference on Advances in Mobile Computing & Multimedia (MoMM2019)* (pp. 107–116). ACM. https://doi.org/10.1145/3365921.3365922

Hide my Gaze with EOG!

Towards Closed-Eye Gaze Gesture Passwords that Resist Observation-Attacks with Electrooculography in Smart Glasses

Rainhard Dieter Findling, Tahmid Quddus, Stephan Sigg
[firstname.lastname]@aalto.fi
Ambient Intelligence Group, Department of Communications and Networking, Aalto University
Espoo, Finland

ABSTRACT

Smart glasses allow for gaze gesture passwords as a hands-free form of mobile authentication. However, pupil movements for password input are easily observed by attackers, who thereby can derive the password. In this paper we investigate closed-eye gaze gesture passwords with EOG sensors in smart glasses. We propose an approach to detect and recognize closed-eye gaze gestures, together with a 7 and 9 character gaze gesture alphabet. Our evaluation indicates good gaze gesture detection rates. However, recognition is challenging specifically for vertical eye movements with 71.2%-86.5% accuracy and better results for opened than closed eyes. We further find that closed-eye gaze gesture passwords are difficult to attack from observations with 0% success rate in our evaluation, while attacks on open eye passwords succeed with 61%. This indicates that closed-eye gaze gesture passwords protect the authentication secret significantly better than their open eye counterparts.

CCS CONCEPTS

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

KEYWORDS

Authentication, closed-eye, EOG sensors, hands-free, gaze gestures, mobile, password, smart glasses

ACM Reference Format:
Rainhard Dieter Findling, Tahmid Quddus, Stephan Sigg. 2018. Hide my Gaze with EOG!: Towards Closed-Eye Gaze Gesture Passwords that Resist Observation-Attacks with Electrooculography in Smart Glasses. In *MoMM '19: MoMM '19: 17th International Conference on Advances in Mobile Computing & Multimedia, December 02–04, 2019, Munich, Germany.* ACM, New York, NY, USA, 10 pages. https://doi.org/-----

1 INTRODUCTION

Modern mobile devices have access to diverse types of private data [30], which is why access to them is often protected with different types of authentication [31]. Compared to classic computers, mobile devices feature more frequent but shorter user interaction sessions [17, 18] in a broader range of situations. Further, classic mobile device authentication, like PIN, password, or unlock pattern, are vulnerable to diverse attacks from shoulder surfing [28] over smudge attacks [2] to thermal attacks [1]. This, and the different nature of mentioned situations, make users benefit from having a multitude of authentication approaches available that are appropriate for diverse everyday situations (cf. [12, 13]). The overall authentication should be unobtrusive, provide different choices in a flexible way, and ideally automatically combine different authentication data sources [16, 19].

Smart glasses allow for such additional forms of authentication: eye-facing cameras built into the glasses frames, which observe pupil movements [24], can be utilized for gaze password input and authentication. A key issue with pupil based gaze passwords are observation-based attacks: pupil movements can easily be observed by attackers watching the user's eyes during authentication [8]. One option to avoid pupils being visible to attackers is to close eyelids when performing gaze passwords. The underlying assumption is that eye movements are more difficult to observe with closed eyelids than with pupils being visible. However, this also renders pupil based gaze extraction unusable. So far, only one recent approach has considered closed-eye gaze altogether [14]. Their approach utilizes eye-facing cameras built into smart glasses and extracts closed-eye gaze gestures with optical flow from movements observed on the eyelids. However, their work focuses only on user input and does not consider potential application in mobile authentication and corresponding security aspects.

Closed-eye gaze extraction with cameras, as in [14], bears the disadvantage that eye movements have to be extracted from optical recordings of closed eyelids, which in turn might be impacted by illumination of the eyelids, and in general seems difficult from a technical perspective. Hence, being able to use other data sources for sensing closed-eye gaze gestures would be beneficial. Electrooculography (EOG) sensors are one such option that can be built into smart glasses frames. In contrast to cameras, EOG sensors require skin contact. Bulling et al. [7] have investigated EOG-based gaze extraction with EOG goggles. However, their approach utilizes sensor positions unavailable with regular glasses frames, e.g. above and below the eye, which would require the frame to be extended towards the form factor of goggles. With regular glasses, positions

MoMM '19, December 02–04, 2019, Munich, Germany

ACM ISBN —–…$15.00
https://doi.org/-----

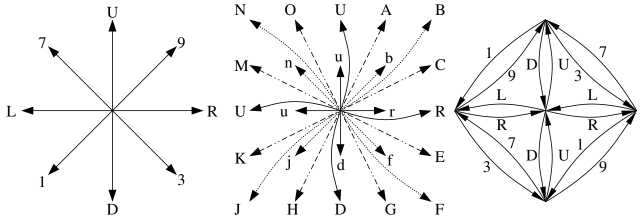


Figure 1: Gaze gestures in related work: horizontal, vertical, and diagonal gestures without [8] and with [7] considering the size of the gesture (left and center), as well as with defined start and/or end point [23] (right).

available for sensors that require skin contact are those where the frame naturally touches the skin, such as on the nose and behind the ears.

In this work we investigate smart glasses authentication with closed-eye gaze gesture passwords that are sensed with EOG sensors embedded in the glasses frames. Our approach utilizes closed-eye gaze gestures adapted from related work (cf. [7, 14, 23]) but employs them for authentication. EOG sensors are embedded in the glasses frames in the bridge and the nose pads, so that they naturally touch the user's skin, just as regular glasses would. While those restricted sensor positions impair the EOG sensing capabilities over previous work, such as [7], we deem those restriction important to not impair usability in daily usage by extending the frame beyond regular glasses. The central hypotheses of this paper are a) closed-eye gaze passwords with EOG sensors embedded in smart glasses frames are feasible without extending the glasses frame form beyond regular glasses, and b) closed-eye gaze gesture passwords are more difficult to observe by attackers than their open-eye counterparts. Summarizing, the contributions of this paper are:

- We propose a methodology to extract closed-eye gaze gestures from EOG sensors embedded in smart glasses. We only utilize sensor positions around the nose where the frame naturally touches the skin.
- We propose a 7 and 9 character gaze gesture alphabet and protocol for the chosen EOG sensor positions.
- We evaluate our approach for detection and recognition rates as well as success of observation-based attacks of closed- and open-eyes gaze gestures, with 15 subjects and 81 gaze gesture passwords, containing a total of 380 gaze gestures, as well as 18 attackers and 36 observation-based attacks.

2 RELATED WORK

In this section we review relevant previous work on both gaze gestures as well as on authentication based on them, with an overview of approaches and key attributes in Tab. 1 and gaze gesture examples in Fig. 1.

2.1 Gaze Gestures

There has been numerous prior work on open-eye gaze gestures [15]. EyeWrite [35] uses gaze gesture input for text composition. The concept is based on EdgeWrite [34], in which each character is replaced by a gesture. The alphabet therefore contains 26+10 gestures for numeric characters and further gestures for punctuation and text control. The approach is designed to work with a stationary Tobii ET-1750 eye tracker in the form factor of a computer monitor. A set of 12 gaze gestures is used in [23]. Each gaze gesture in their alphabet consists of left, right, up, down, and optional diagonal movements. They evaluate their approach with a PC setup, and compare it to dwell-based gaze input in subsequent work [21]. The duration of L, triangle, line, rectangle, and circle based gaze gestures is investigated in [15]. The paper compares the duration it takes to perform gaze gestures on an empty space with no background to using a helping structure in the form of the intended shape as background. Their results indicate that performing gaze gestures with a blank background without any helping structure is quicker to perform. In [11], an alphabet of 8 gaze gestures is used. Each gesture is an unidirectional stroke into a certain direction (left, right, up, down, and the four diagonals in between). The authors utilize a setup with a computer monitor and a camera with attached infrared light to perform pupil tracking and extract gaze gestures. The same alphabet is used in [10] for gaze gesture input to mobile devices.

All those approaches have in common that they rely on optical pupil tracking, hence on opened eyes, for gaze gesture extraction. While cameras can be built into smart glasses frames [24], pupils are not visible with closed eyes, which prevents those approaches from being applied to closed-eye gaze gestures. Recently, in [14] a different path was investigated: the extraction of closed-eye movements from eye-facing cameras embedded in smart glasses frames. Instead of tracking pupils, optical flow is utilized to extract the direction of gestures from closed eyelids. Four different alphabets with 5-9 possible gestures were tried, where each gesture is either a big or small, uni- or bidirectional stroke into a certain direction (left, right, up, down), or a squint (similar to blinking eyes while eyes stay closed). In contrast, our work differs by focusing on passwords over user input only, as well as in using EOG sensors instead of cameras as data source.

EOG recognition has been utilized for gaze gestures in prior work. As it does not rely on pupil tracking it seems to be a viable option for extracting closed-eye gaze gestures, but has not been investigated yet. Related work on EOG-based gaze gestures with open eyes [5] uses an alphabet related to the one in [11], consisting of 8 gestures (left, right, up, down, and four diagonals). In subsequent work they expand user input to also have small and big eye movements in left, right, up, and down direction [7]. By combining two movements they thereby encode a total of 16 different characters for user input.

When considering smart glasses, EOG sensors bring a significant drawback. In contrast to optical sensors, EOG sensors need to touch the skin, which limits possible sensor positions with regular glasses frames to around the nose and close to the ears (similar to, for example, the J!NS MƎME device [22]). Those locations cause sensors to be positioned horizontally to each other, but not vertically. While this allows for horizontal eye movement sensing, vertical eye movement sensing is more difficult, as it naturally would benefit from sensors above and below the eye, similar to the goggles utilized in [6]. However, adding sensors above and below the eyes would make the device significantly more cumbersome due to increased size and weight, and would change the frame form factor from glasses to goggles.

Table 1: Overview of gestures and alphabets in previous work on open-eyed gaze gesture user input and authentication.

Gaze gest. user input	Modality	Gesture alphabet	Gesture duration	Error rate	Attack success rate	Remarks
Drewes and Schmidt [11]	Optical, stationary	RLUD1379	0.6 s	–	–	Gestures consist of one stroke. Use IR lights and IR cameras.
Drewes et al. [10]	Optical, mobile	RLUD1379	<0.9 s	–	–	Mobile devices in a stationary setup. Fix head and use of external camera for eye tracking.
Wobbrock et al. [35]	Optical, stationary	Full alphanumeric	–	–	–	EyeWrite: EdgeWrite [34] with gaze. Gestures consists of multiple connected strokes.
Bulling et al. [5, 6]	EOG, mobile	RLUD1379	0.4-1.0 s	5%-14%	–	Mobile EOG googles. Gestures consist of one stroke, simpler gesture alphabet.
Bulling et al. [7]	EOG, mobile	LlRrUuDd-NnJjFfBb	–	23.9% FNR, 29.5% FPR	–	Mobile EOG googles. Gestures consist of one stroke, more complex alphabet.
Istance et al. [23]	Optical, stationary	TBLRCN	0.5-0.9 s	–	–	Gaze input to PC gaming. Gestures start and stop in center and consist of either 2 or 3 strokes.
Findling et al. [14]	Optical, mobile	LRUDS to LlRrUuDdS	–	8.4-17.2% detection, 8.1-0.3% recognition	–	Extend gaze gesture alphabets with closed-eye gaze gestures. Evaluate 4 gaze gesture protocols.
Gaze gest. auth.	**Modality**	**Gesture alphabet**	**Auth. duration**	**Error rate**	**Attack success rate**	**Remarks**
De Luca et al. [9]	Optical, stationary	Numeric 0-9	54 s	9.5%	–	EyePIN: numeric gestures from EdgeWrite [34] with gaze. Gestures consist of multiple connected strokes.
De Luca et al. [8]	Optical, stationary	RLUD1379	12.5 s	–	55% (3 tries)	EyePassShapes: PassShapes [33] with gaze. Gestures consist of one stroke.
Hossain et al. [20]	EOG, stationary	LRUD1379+blink	–	–	–	5 point EOG sensor setup. Gestures consist of one stroke.
Khamis et al. [25]	Optical, mobile	Left-right	3.1 s	23%-42%	19%-44%	GazeTouchPass: concatenate touch screen characters (numeric 0-9) with left-right gaze gesture characters.
Khamis et al. [26]	Optical, mobile	Left-right	10.8 s	–	4.2%-16.7%	GazeTouchPIN: combine touch screen list row selection with left-right gaze gesture for columns selection in a Nx2 character grid.

2.2 Authentication with Gaze Gestures

The first gaze gesture based authentication was proposed by De Luca et al. with EyePIN [9], in which users enter a numeric PIN with gaze gestures. The underlying alphabet is based on EdgeWrite [34], in which each numeric character is represented by a gesture drawn with a pen. EyePIN utilizes only numeric characters of this alphabet and replaces the pen with gaze for gesture input. It has been designed to work with a stationary monitor and eye tracking setup and uses the commercial ERICA eye tracker in its evaluation. To begin and end recording of a gaze gesture, users press a button on the keyboard. The evaluation compares input based on dwell (fixate point for given time), look-and-shoot (fixate point and press a key), and gaze gestures, and find gestures to be slowest (mean 54 s) with the smallest error rate (9.5%).

In subsequent work, De Luca et al. combine the gaze aspects of EyePIN with the gesture aspects of PassShapes [33] to EyePassShapes [8]. PassShapes is a graphical password scheme with an alphabet of 8 directions: left, right, up, down, (LRUD), and the four diagonals in between, labeled clockwise by the corresponding numbers on a keypad (1379). PassShapes is designed to work with a (touch)screen and a pen. A password thereby consists of a series of gestures, which are separated by pen-up events. EyePassShapes utilizes the same alphabet as PassShapes, and similarly to EyePIN, replaces PIN with gaze gestures. Like EyePIN, EyePassShapes is designed for a stationary monitor and eye tracking setup, and users press a keyboard button to begin and end gaze recording. They comparatively evaluate PIN, EyePIN, PassShapes, and EyePassShapes authentication. Their findings indicate that EyePassShapes is quicker (12.5 s) than EyePIN, but slower than PIN or PassShapes, and that the attackability with 3 input tries from attackers beforehand observing users' eyes during authentication (55%) is lower than with PIN or PassShapes, but higher than with EyePIN.

GazeTouchPass [25] and GazeTouchPIN [26] both combine gaze with touch for authentication on handheld mobile devices. Both extract eye movements with the camera built into the mobile device which is facing the user. GazeTouchPass utilizes both numeric characters (0-9, entered via an onscreen keyboard) and characters from gaze (looking left or right). A password thereby is a serial combination of numeric and gaze characters. In contrast, GazeTouchPIn incorporates both touchscreen and gaze input to select one character for a password. In a Nx2 grid, touch selects the desired of N rows, which contains two characters. Gaze then selects either the right or left character (by looking either right or left). A password is thereby a series of characters where each character was composed by both touch and gaze. GazeTouchPass reports an average authentication duration of 3.1 s for a four-character password, 58%-77% error free authentication attempts, and attackers' success from previously observing users during authentication to be 19%-44%, depending on the attack details. In comparison, GazeTouchPIN reports an average authentication duration of 10.8 s with attack success rates of 4.2%-16.7%, depending on the type of attack.

Previous work on EOG-based gaze gesture authentication is sparse. Hossain et al. [20] propose to use EOG for eye movement based authentication. While their gaze gesture alphabet of 9 characters is named differently, it contains the same gaze gestures as the LRUD1379 alphabet of [8], plus eye blinking as an additional character. Their setup uses a stationary BIOPAC MP36 system with 5 wet electrodes around the right eye (atop, below, right of it), left of the left eye, and an ground electrode on the middle of the forehead. While wet electrodes are not applicable with smart glasses and in daily usage, an interesting aspect of their research is that they are able to detect eye blinking by a corresponding zero crossing in

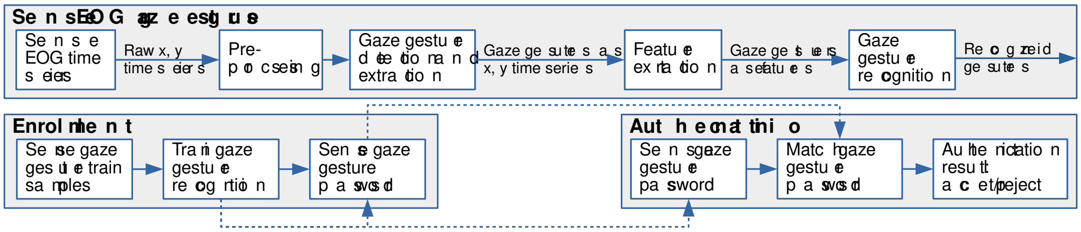

Sense EOG gaze gestures
Sense EOG time series
Raw x, y time series
Pre-processing
Gaze gesture detection and extraction
Gaze gestures as x, y time series
Feature extraction
Gaze gestures as features
Gaze gesture recognition
Recognized gestures
Enrollment
Sense gaze gesture train samples
Train gaze gesture recognition
Sense gaze gesture password
Authentication
Sense gaze gesture password
Match gaze gesture password
Authentication result accept/reject

Figure 2: Overview of processing in our approach to recognize EOG-based closed-eye gaze gestures passwords.

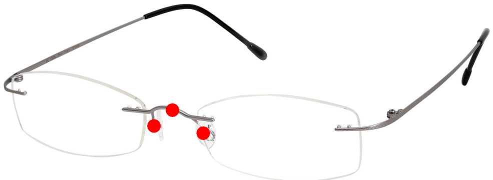


Figure 3: EOG sensor positions with our approach, on the nose pads and the bridge of the frame of the glasses (red).

horizontal and vertical voltage, and that they can differentiate between voluntary blinks (stronger movement) and unintended blinks (weaker movement). For detecting eye movements they perform peak detection and combine information in horizontal and vertical peaks to determine the corresponding direction. While their research outlines the technical aspects, it does not evaluate detection and authentication rates or attackability of their approach.

Summarizing, there is numerous work on gaze gestures from optical sources that utilizes pupil tracking for gaze direction extraction. Some approaches have been employed in authentication and have been evaluated on mobile devices [8]. However, closed-eye gaze gestures have only been investigated once so far [14] for user input, not for authentication. Gaze gesture user input based on EOG sensing has been investigated with goggles [7] that go beyond the frame form factor of regular glasses. EOG gaze gesture authentication has been proposed in [20], but in a non-mobile setup, using wet electrodes, and has not yet been evaluated for authentication or attack success rates. On the intersection of those prior approaches there is room for further work, which combines mobile authentication in smart glasses with closed-eye gaze gestures and EOG-based sensing.

3 APPROACH

Our approach to EOG-based closed-eye gaze gesture passwords with smart glasses consists of two major parts: enrollment and authentication (Fig. 2). Internally, both utilize a processing chain to sense, detect, and extract gaze gestures. In this section we describe the processing details of the corresponding steps as well as the gaze gesture alphabet and protocol utilized in our approach.

3.1 Gaze Gesture Sensing and Preprocessing

For sensing EOG with glasses in an unobtrusive way, sensors can only be embedded in the frame where the glasses naturally touch the user's skin. Those positions are around the nose (nose pads and bridge) as well as behind the ears (bows). For our approach, we utilize the bridge as well as the left and right nose pad of the frame as sensor positions (Fig. 3). This alignment allows for sensing horizontal eye movements well, as the corresponding muscle voltage is clearly visible from sensor positions next to the eyes. However, vertical eye movements are more difficult to sense, as the vertical difference between the left and right sensors to the central sensor is small, and the muscles corresponding to vertical eye movements are not directly located under or next to those sensor positions.

Once a series of gaze gestures is obtained, we filter the corresponding horizontal and vertical EOG voltage time series for noise reduction. For this we employ a Saviztky-Golay filter (SG-filter) [27], as it preserves the signal form better than running mean or median filters, which would tend to more strongly smooth minima and maxima. In our approach we utilize a filter with a window length of 0.3 s and a degree of 1.

3.2 Closed-Eye Gaze Gesture Protocol

For our EOG-based closed-eye gaze gesture passwords we utilize a gaze gesture alphabet and protocol adapted from prior work (cf. [7, 8, 14, 23]). At first, we considered an unrestricted series of gaze gestures for our passwords, similar to [7, 8]. However, in preliminary evaluations we identified EOG-based sensing of closed-eye gaze gestures in vertical direction to be difficult, especially towards and around the upper part of the field of vision. Multiple participants showed trembling eyelids when moving their eyes towards the upper boundary of their field of vision. This resulted in larger EOG voltage overlayed with significant noise, for which filtering and smoothing seemed to be unable to recover usable information for subsequent processing. While vertical components in gaze gestures outside the upper part of the field of vision still seemed difficult to sense and recognize correctly with our sensor setup, we deem having both horizontal and vertical components important and expect to be able to recover at least parts of the information for further processing. For this reason we still include horizontal, vertical, and diagonal gaze gestures, similar to [14, 23], but leave out gaze gestures towards the upper boundary of the field of vision.

Our gaze alphabet thereby includes a total of 9 gaze gestures in the lrud1379s variant (Fig. 4). Four horizontal and vertical and four diagonal gaze gestures, as in [8, 14, 23]: left (l), right (r), up (u), down (d), left-down (1), right-down (3), left-up (7), and right-up (9), as well as a squint/flick gesture (s) as in [14]. In our evaluation we also utilize a lr1379s variant, which is a subset of the 9 character version

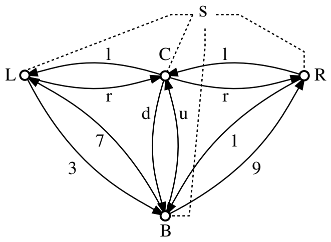


Figure 4: Graphical depiction of gaze gestures in our closed-eye gaze gesture passwords, including horizontal (l, r), vertical (u, d), diagonal (1, 3, 7, 9), and a squint/flick (s) gesture.

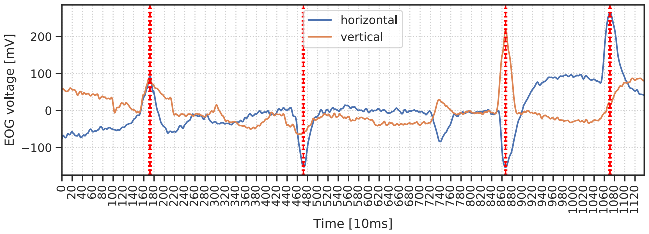
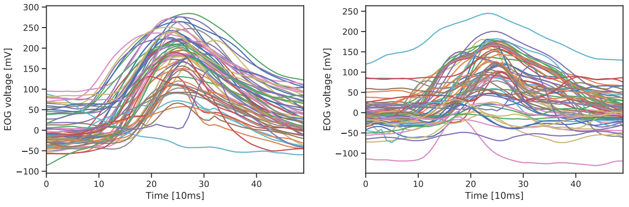


Figure 5: Filtered EOG time series for a "r17r" closed-eye gaze gesture password. Detected peaks are marked in red.



(a) horizontal

(b) vertical

Figure 6: Multiple samples of a left (r) EOG-based closed-eye gaze gesture, in horizontal and vertical direction.

and leaves out the u and d gestures. Gaze passwords always start in the center of users’ vision, but can end after any gaze gesture in any position. When users are prompted for a gaze password, once they close their eyes, subsequent movements of the closed eyelids are recognized as closed-eye gaze gestures.

3.3 Gaze Gesture and Feature Extraction

For gaze gesture detection and extraction we utilize a simple parametric peak detection. We at first sum the absolutes of the filtered horizontal and vertical eye movements in the sample. Then we detect peaks in the signal, so that each peak is the highest value within 0.5 s and has a value of at least 170 mV for both horizontal and vertical axis combined (Fig. 5). We then segment a 0.5 s window around each peak to extract the filtered time series for each detected gaze gesture. Each extracted gaze gesture sample therefore consists of two 0.5 s filtered time series, for the corresponding EOG-sensed eye movement, in horizontal and vertical direction (Fig. 6).

For feature reduction we at first normalize data by centering it to mean=0 and scaling it to std=1. We then employ principal component analysis (PCA), of which we keep only the most important principal components which together explain 95% of the variance in the data. Due to gaze gestures being simple patterns in their respective time series, as well as due to those time series being expected to show a high correlation between their values at time t and $t + 1$, we thereby expect PCA to be effective in feature reduction. The transformation parameters for centering, scaling, as well as PCA are determined from the enrollment data of each individual user, and are applied the same way to data of subsequent authentication attempts.

3.4 Recognition: Enrollment & Authentication

Enrollment consists of two steps: gaze gesture model training and setting of the gaze password. Users at first record multiple samples for each gaze gesture. Those samples are detected and segmented, preprocessed, and their features are extracted. Together with their known labels they form the basis of training a gaze gesture recognition model for this user. This model is able to distinguish gaze gestures of this user and is stored for further usage. Note that model training has to be done only once: the password can be changed later on without changing the model. Users then set their gaze gesture password by recording it. The gestures contained in the password are extracted, recognized by the previously stored model, and its salted hash is stored for comparison during authentication. As we are interested in the extraction and recognition of closed-eye gaze gestures, we declare further details of cryptographic aspects, like choice of salt, hash function, and storage out of scope of our work.

For authentication, users perform their closed-eye gaze gesture password. The contained gaze gestures are detected, extracted, preprocessed, and their features are extracted – with the parametrization as determined during enrollment. The gaze gesture recognition model created during enrollment is then employed to recognize the type of gaze gestures. Finally, for the resulting password, composed from the extracted gaze gestures, the salted hash is computed and compared to the stored password hash to yield an accept/reject authentication decision.

4 EVALUATION

In this section we describe our evaluation setup, including the data recording, the obtained dataset, and the usage of the data in the evaluation procedure. Results and findings are discussed in Sec. 5.

4.1 Recording Device

For our evaluation data recording we utilize J!NS MEME smart glasses [22]. They feature three contact-based, dry EOG electrodes: two on the nose pads and one at the nose bridge of the frame, with an EOG sampling frequency of 100 Hz and 12 bit quantization. All three electrodes touch the skin when wearing the glasses in a normal fashion. The device thereby yields EOG time series in horizontal and vertical direction. However, as the positioning of the left and right electrodes provide for a more robust signal in the horizontal direction, horizontal eye movements are sensed more reliably than vertical eye movements.

Table 2: Our evaluation data for closed and open eyes. For password samples: amount of subjects, amount of password samples and total contained gaze gestures, and the mean and std of password length in characters and duration in s. For attack samples: amount of subjects, passwords attacked, attackers, and amount of attacks.

Eyes	Subjects	Passwords	Gaze gestures	PW length	Dur. [s]
Closed	14	38	177	4.66/0.48	10.8/0.2
Open	15	43	203	4.75/0.45	10.0/0.2

Eyes	Subjects	Passwords	Attackers	Attacks
Closed	18	18	18	18
Open	18	18	18	18

4.2 Evaluation Data

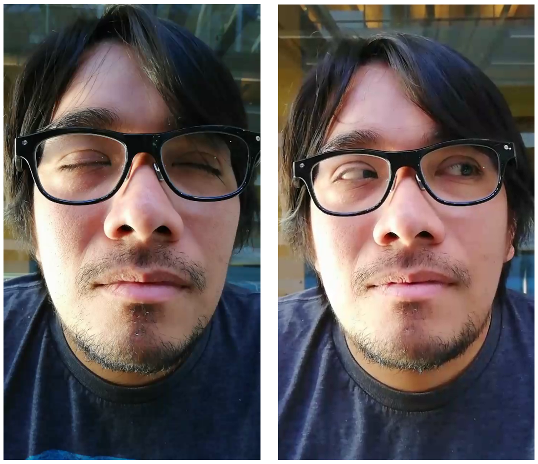
Our evaluation data comprises of two parts. The first part is a set of EOG-based gaze gesture passwords as sensed by the smart glasses, which we use to evaluate the performance of our gaze gesture authentication approach. The second part is a set of videos of users performing gaze gesture password authentication, filmed with an external camera, which we use to quantify the success of observation-based attacks.

4.2.1 Gaze Gesture Password Dataset. The EOG gaze gesture password dataset comprises of 15 subjects. Each subject choses one or two gaze gesture passwords, containing 4-5 gaze gestures each. Password input was recorded 2-5 times per subject and password, both for closed and opened eyes, where subjects did pause for at least 0.5 s between individual eye movements. This results in a total of 81 password samples, containing a total of 380 gaze gestures (Tab. 2). Participants were students and employees of Aalto University with a mean age of 28.5 years (std 5.2).

4.2.2 Observation-Based Attack Dataset. The observation-based attack dataset comprises of a total of 14 password videos from 7 different users, assessed by 18 different attacker participants. Each of the 7 users was filmed twice, one time for closed and one time for opened eyes, while performing one of their gaze gesture passwords. The recording environment was an office space with light sources being ceiling lamps and windows on one side of the room. Eye movements were filmed with the 16 MP video camera embedded in a Huawei P20 LITE, from 1-1.5 m distance to the user's face. The resulting attack videos have 1080p resolution with 30 frames per second (Fig. 7). Attackers utilizing such devices for their attacks is deemed realistic since they are easily available.

Recording from a close distance of 1-1.5 m to the user might raise suspicion; however, users are unable to recognize attackers during the short time of password input since their eyes are closed. Furthermore, recordings in close proximity to the user also simulates stronger attackers, who would utilize more expensive and higher quality cameras from a larger distance.

To simulate observation-based attacks, 18 randomly chosen participants of our study were asked to watch two randomly selected videos, each showing one user performing on of their password – one for closed eyes, and one for open eyes. Attackers could watch the video as many times as they liked, and then were asked to derive the gaze gesture password from what they saw in the video. This resulted in a total of 36 observation-based attacks: 18 for closed eyes and 18 for open eyes (Tab. 2). Attacker participants were students and employees of Aalto University with a mean age of 28.5 years (std 5.2), who all also did participate in the first study.



(a) Password input, eyes closed (b) Password input, eyes opened

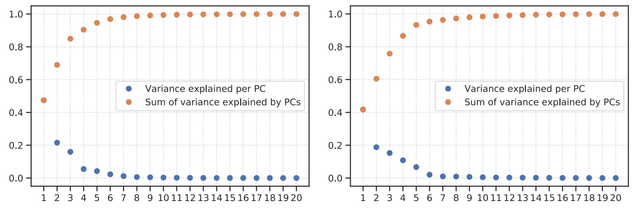
Figure 7: Perspective of a gaze gesture password attack: videos showing users during their gaze gesture password input form the basis of observation-based attacks.

4.3 Evaluation Procedure

In our evaluation we investigate closed and opened eyes for gaze gesture passwords alongside each other and compare their results.

For our authentication evaluation, we at first apply gaze gesture processing as specified in Sec. 3 and report the corresponding detection rate. Based on detected gestures from all passwords, we investigate dimensionality reduction outcomes and highlight the amount of principal components needed to explain 95% variance in the data. To determine a suitable gaze gesture recognition model we rely on double cross validation (CV). We use the first CV loop to train, evaluate, and select a model type and its hyperparameter set from a list of model types and exponential hyperparameter grids, including k-nearest neighbor (KNN), linear discriminant analysis (LDA), classification tree (CT), and a linear (l-SVM) and radial support vector machine (rbf-SVM). The second CV loop utilizes user data to train the corresponding model with the previously determined model type and hyperparameter set, and to determine the corresponding normalization and transformation parameters. The trained model is then tested on gaze password samples from the left out partition. From this CV loop we report the gaze gesture recognition rates of the left out gaze password samples in the form of gesture confusion matrices, as well as the resulting authentication success rates.

In our attack evaluation, to compute the attack success rates, we compare the passwords attackers derived from observing users performing gaze password authentication to the actual password of that user. We count an attack as successful if the attacker correctly derived all contained gaze gestures in their correct order, and as



(a) Closed eyes (b) Open eyes

Figure 8: Amount of variance captured by the first 20 PCs for closed and opened eyes.

Table 3: Amount of principal components required to explain 80%-99% variance of gaze gestures for closed and opened eyes.

Eyes	80%	90%	95%	98%	99%
Closed	3	5	6	7	9
Open	4	5	6	10	13

unsuccessful otherwise. From those results we report gaze gesture attack success rates for closed and opened eyes.

5 RESULTS AND DISCUSSION

5.1 Gaze Gesture Extraction Results

Over all gaze gesture password samples in our evaluation data set, for closed eyes we were able to detect all gaze gestures correctly. For open eyes one "1" gesture was missed, which was below the detection threshold. We believe that those good results are caused by participants pausing at least 0.5 s in between subsequent gaze gestures in their passwords in our data. If this pause is omitted or shortened in evaluation data of future work we expect a higher amount of detection errors.

5.2 Feature Extraction Results

After extracting gaze gestures from our evaluation data, to determine the amount of components required for representing gaze gestures, we normalize all data and apply PCA. With a cumulative sum over principal components in descending order, PCA is able to capture 95% of the variance in all data with just 6 components for both closed and open eye gaze gestures (Fig. 8 and Tab. 3). In the principal component feature space (Fig. 9) especially the s gesture is well distinguished. Other gestures show clustering-like patterns – but they still partially overlap, which will cause errors in subsequent recognition of gaze gesture types.

5.3 Gaze Gesture Recognition Results

When utilizing all 9 gaze gestures of our lrud1379s protocol, the outer CV loop for model tuning and selection indicates a significant confusion of the vertical-only gestures u and d. This is why we also evaluate the 7-character lr1379s version of our protocol, which leaves out the u and d gesture. The best model type for both the lrud1379s and the lr1379s version is a rbf-SVM (Tab. 4). For the lrud1379s version, the optimal hyperparameter set from an exponential grid of base 3 is $C = 3^3, \gamma = 3^{-3}$ for closed and $C = 3^3, \gamma = 3^{-4}$ for opened eyes. For the lr1379s version, the optimal hyperparameter set is $C = 3^3, \gamma = 3^{-3}$ for closed and $C = 3^5, \gamma = 3^{-6}$ for opened eyes. We therefore use those model configurations for subsequent training and recognition of gaze gestures in the second CV loop.

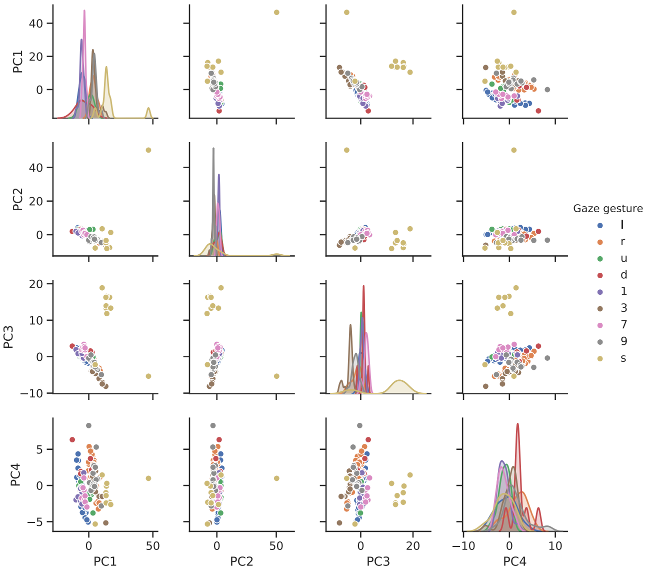
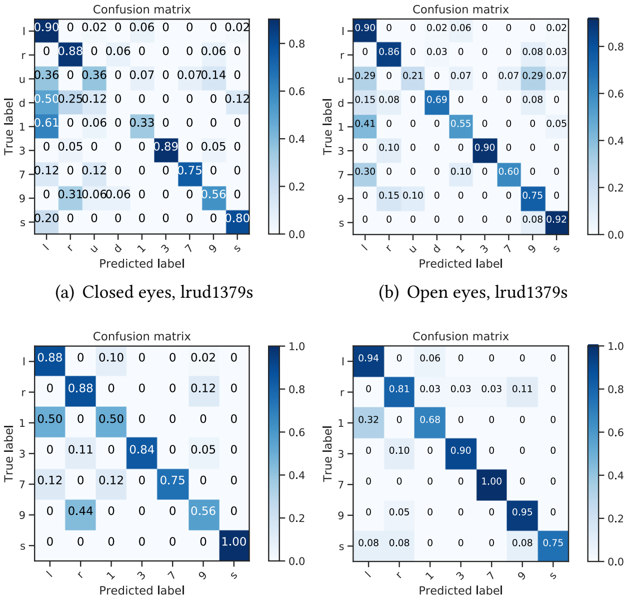


Figure 9: Scatter of closed-eye gaze gesture samples in their first four principal component feature dimensions.

Table 4: Model evaluation results from CV-based gaze gesture recognition. The results depict the accuracy [%] as mean/standard deviation for the best hyperparameter set per model type. The best result for closed and open eyes is emphasized in black.

Eyes	Alphabet	KNN	LDA	CT	l-SVM	rbf-SVM
Closed	lrud1379s	72.3/10.3	56.5/9.1	61.0/17.3	71.8/6.5	**74.5/7.2**
Open	lrud1379s	75.8/8.8	60.6/5.8	59.1/11.4	73.2/7.3	**80.3/9.0**
Closed	lr1379s	76.8/10.1	69.0/12.6	67.1/11.9	76.1/9.6	**80.6/11.5**
Open	lr1379s	82.5/6.8	62.0/10.8	69.0/9.5	81.9/7.4	**88.3/6.2**

With the selected model configurations, the outer CV loop confirms that vertical-only gaze gestures are challenging to be recognized correctly with our EOG sensor setup. With closed eyes, no d gestures are recognized correctly, and the majority of u gestures and 1 gestures are recognized wrongly. The latter is mostly confused with being a l gesture, which has the same horizontal but a different vertical component. With open eyes, only 21% of u gestures are recognized correctly, however 69% of d gestures are recognized correctly. In comparison, utilizing the lr1379s 7-character gaze gesture subset achieves better results. The majority of confusion is in between gaze gestures that have the same horizontal but different vertical components, such as 1 being confused as l (50% and 32% with closed and opened eyes), or 9 as r (44% with closed eyes, but only 8% with opened eyes). The overall gaze gesture recognition



(a) Closed eyes, lrud1379s

(b) Open eyes, lrud1379s

(c) Closed eyes, lr1379s

(d) Open eyes, lr1379s

Figure 10: Gaze gesture confusion for closed and opened eyes from the outer CV evaluation.

rate for the lrud1379s version is 71.2% and 76.3% for closed and opened eyes, while for the lr1379s it is 80.0% and 86.5%.

5.4 Gaze Gesture Authentication Results

With the second CV loop we also evaluate the resulting gaze gesture password authentication success rate. This is the rate for which users can successfully authenticate with their gaze gesture passwords, based on the model trained from their training data. If the detected and recognized gaze gestures in a password sample fully agree in type, amount, and order with the actually contained gaze gestures, the authentication is counted as pass, and as fail otherwise. Due to the gaze gesture confusion encountered during evaluating the gaze gesture recognition, the resulting authentication success rate, hence passing the authentication, is low. With the lrud1379s alphabet, 36.8% (closed eyes) and 28.6% (opened eyes) of legitimate attempts pass authentication, while with the lr1379s subset, 44.7% (closed eyes) and 54.8% (opened eyes) of legitimate attempts pass authentication. While this result is not yet acceptable for employing the corresponding authentication, due to the gaze gesture patterns observed during our evaluation, we believe that future work will be able to achieve better results by investigating the exact sensor position in more detail as well as by employing and fine tuning more sophisticated processing of sensed gaze gestures.

5.5 Observation-Based Attack Results

Evaluation results from the observation-based attack dataset indicate that closed-eye gaze gesture passwords seem to be difficult to attack: 0% of the observation-based attacks (0/18) on closed-eye gaze gesture password videos succeeded. In contrast, with open-eye gaze gesture password videos, the observation-based attack success rate was 61% (11/18). This clearly confirms that it is more difficult to attack closed-eye gaze gestures from observing users' eyes during password input. As a consequence, this makes closed-eye gaze an interesting option to consider for security and authentication related purposes in general.

5.6 Discussion

The combination of EOG sensor positions with the gaze gestures utilized in our study results in low authentication success rates, hence is not yet usable for mobile authentication in its current form. The challenge arises from the EOG sensor positions available with regular glasses frames, without extending the form factor of the glasses towards goggles. Gaze gesture alphabets that would only utilize horizontal eye movements would have a significantly smaller set of possible gaze gestures, hence would reduce the size of the password space of the corresponding gaze gesture passwords. In our setup, EOG sensors on the nose pads of the glasses allow for sensing horizontal eye movements in a robust way. The third EOG sensor, which is included in the bridge of the glasses, is positioned a little higher than the two other sensors. However, utilizing the resulting vertical voltage difference for recognizing vertical eye movements is challenging. This is due the muscles for vertical eye movements not being directly under or next to those sensors, as well as horizontal eye movements also affecting the resulting voltage difference – which both cause noisy data. For this reason, with the sensor setup, gaze gesture alphabet, and processing utilized in our work, we have to reject hypothesis a).

Despite the overall gaze gesture authentication success rates with our setup ranging from 28.6%-54.8% only, recognition of individual gaze gestures reached up to 100%, with an average 74.5%-88.6% (including vertical gestures), depending on the configuration. Observable trends include confusion of gestures that had same horizontal components but different vertical components, as well as that recognition in general seems more accurate for open than for closed eyes. We argue that those results indicate that exploring further combinations of gaze gestures and EOG sensor positions, together with appropriate processing of sensed data, would likely allow for improved gaze gesture recognition rates, hence also for better authentication success rates – while at the same time allowing for a reasonable password space size.

Observation-based attack results clearly indicate that closed-eye gaze gestures are more difficult to attack than open-eye gaze gestures, hence, that hypothesis b) can be accepted. With our evaluation and datasets, attackers – who are aware of the authentication mechanism and the corresponding gaze gesture alphabet – were unable to derive the user's password for any attack attempt with closed-eye gaze gestures, while for open eyes the observation-based attack success rate is 61%. Our findings of gaze gestures being easy to observe for attackers by watching the user's pupils during authentication is in line with findings in previous work [9]. In contrast to those results for open eyes, our closed-eye results confirm intuition in that gaze eye movements are more difficult to observe when eyelids are closed. For gaze gesture authentication, this means that closed eyes better protect the corresponding authentication secret than open eyes. We thereby conclude that closed-eye gaze gestures should in general be considered when dealing with security and authentication critical aspects, such as mobile authentication in environments, where attackers would be able to observe users' eyes and their movements.

Limitations of our study include that user-chosen knowledge-based authentication secrets have been shown to in general have limited entropy [3, 32]. Since they are knowledge-based, this also applies to gaze gesture passwords. However, there exist ways to facilitate users choosing stronger passwords [4, 29], which could also be investigated for both closed and open eye gaze gesture passwords in future work. In the present work we focuses on the technical aspects of EOG-based closed-eye gaze gestures for smart glasses and declare analyzing the user chosen gaze gesture password space inside the theoretical password space out of scope at this time. Our work defines the process of prompting users for their gaze gesture password as an external process. Once users are prompted for a gaze password by this external process, the subsequent eye movements are considered to be gaze gestures. Details on how this process prompts users for their password are left for future investigation. Finally, our work does not investigate the usability of closed and open eye gaze gestures in our approach as perceived by users. This is declared out of scope due to the focus on technical aspects, however is left for future work as an interesting aspect to investigate and evaluate.

6 CONCLUSION

In this paper we presented an approach to sense closed-eye gaze gestures with EOG sensors for password authentication with smart glasses. EOG sensors are embedded in the bridge as well as the left and right nose pad of the frame, which does not extend the form factor of the frame beyond that of regular glasses. We utilized gaze gesture alphabets consisting of 7 and 9 gestures, which leave out gestures that go towards the upper boundary of users' vision. Our processing senses EOG timeseries in horizontal and vertical direction, then detects and recognizes gaze gestures in them. We evaluated gaze gesture detection and recognition rates with 81 password samples of 15 users, containing a total of 380 gaze gestures. Results show an average recognition accuracy of 71.2% and 76.3% for closed and open eyes, when including "up" and "down" as the only pure vertical gaze gestures, and 80.0% and 86.5% when excluding those two gestures. We found the challenging aspects of recognition to be the combination of the utilized sensor positions – which make robust recognition of vertical eye movements difficult – with using gaze gestures that (partially) contain vertical eye movements. While the setup used in this work is not yet ready for being employed in mobile authentication, we argue that with fine tuning EOG sensor positions in smart glasses and evaluating different corresponding gaze gesture sets, combinations can be found that allow for more robust sensing of vertical gaze gestures as well.

We further evaluated the success of observation-based attacks, in which attackers observe the eyelids or pupils during password input, with 18 attackers and a total of 36 attack attempts. Results clearly show that closed-eye gaze gesture passwords are more difficult to attack than their open eye counterparts. Not a single closed-eye attack succeeded, while for open eyes the attack success rate in our evaluation is 61%. Closed-eye gaze gestures seems to protect authentication secrets better than their open eye counterparts. As a consequence, we argue that closed-eye gaze should be considered in future security and authentication related gaze aspects, especially in situations in which attackers are potentially able to observe users' eyes.

Future work could investigate different combinations of EOG sensor positions in smart glasses – without extending the form factor beyond glasses – with corresponding gaze gesture alphabets. It could further investigate and compare the usability of closed and open eye gaze gestures, as well as the easiness of observation-based attacks (observing eye movements during password input and to derive the password from it) – as perceived by attackers. It could also investigate and evaluate options for prompting users for gaze gesture passwords and limiting user input to gaze gestures relevant for authentication. Furthermore, investigating and comparing the password spaces of user chosen closed and open eye gaze gestures could be in the focus of future work as well.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In *Proc. of the 4th USENIX conference on offensive technologies*. Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[3] 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

[4] 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 (CHI '12)*. ACM, New York, NY, USA, 3011–3020. https://doi.org/10.1145/2207676.2208712

[5] Andreas Bulling, Daniel Roggen, and Gerhard Tröster. 2008. It's in Your Eyes - Towards Context-Awareness and Mobile HCI Using Wearable EOG Goggles. In *Proc. of the 10th International Conference on Ubiquitous Computing (UbiComp 2008) (ACM International Conference Proceeding Series)*, Vol. 344. 84–93. https://doi.org/10.1145/1409635.1409647 acceptance rate: 18.6%.

[6] Andreas Bulling, Daniel Roggen, and Gerhard Tröster. 2009. Wearable EOG Goggles: Eye-based Interaction in Everyday Environments. In *CHI '09 Extended Abstracts on Human Factors in Computing Systems (CHI EA '09)*. ACM, New York, NY, USA, 3259–3264. https://doi.org/10.1145/1520340.1520468

[7] Andreas Bulling, J. A. Ward, Hans Gellersen, and Gerhard Tröster. 2011. Eye Movement Analysis for Activity Recognition Using Electrooculography. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 33, 4 (April 2011), 741–753. https://doi.org/10.1109/TPAMI.2010.86

[8] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password?. In *Proc. 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

[9] 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 (OZCHI '07)*. ACM, New York, NY, USA, 199–202. https://doi.org/10.1145/1324892.1324932

[10] Heiko Drewes, Alexander De Luca, and Albrecht Schmidt. 2007. Eye-gaze Interaction for Mobile Phones. In *Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology (Mobility '07)*. ACM, New York, NY, USA, 364–371. https://doi.org/10.1145/1378063.1378122

[11] Heiko Drewes and Albrecht Schmidt. 2007. Interacting with the Computer Using Gaze Gestures. In *Human-Computer Interaction – INTERACT 2007*, Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 475–488. https://doi.org/10.1007/978-3-540-74800-7_43

[12] Rainhard Dieter Findling and René Mayrhofer. 2013. Towards Pan Shot Face Unlock: Using Biometric Face Information from Different Perspectives to Unlock Mobile Devices. *International Journal of Pervasive Computing and Communications* 9, 3 (Sept. 2013), 190–208. https://doi.org/10.1108/IJPCC-05-2013-0012

[13] 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

[14] 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)*, Vol. 11506. Springer, 322–334.

[15] Henna Heikkilä and Kari-Jouko Räihä. 2009. Speed and Accuracy of Gaze Gestures. *Journal of Eye Movement Research* 3, 2 (Nov. 2009), 1–14. https://doi.org/10.16910/jemr.3.2.1

[16] Daniel Hintze, Rainhard Dieter Findling, Muhammad Muaaz, Eckhard Koch, and René Mayrhofer. 2015. CORMORANT: Towards Continuous Risk-Aware Multi-Modal Cross-Device Authentication. Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp 2015), Osaka, Japan. In *Proc. 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp 2015)*. ACM, Osaka, Japan, 169–172. https://doi.org/10.1145/2800835.2800906

[17] Daniel Hintze, Rainhard Dieter Findling, Sebastian Scholz, and René Mayrhofer. 2014. Mobile Device Usage Characteristics: The Effect of Context and Form Factor on Locked and Unlocked Usage. In *Proc. MoMM 2014: 12th International Conference on Advances in Mobile Computing and Multimedia*. ACM Press, New York, NY, USA, 105–114. https://doi.org/10.1145/2684103.2684156

[18] 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

[19] 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

[20] M. S. Hossain, Kristie Huda, S M. Sadman Rahman, and Mohiuddin Ahmad. 2015. Implementation of an EOG based security system by analyzing eye movement patterns. https://doi.org/10.1109/ICAEE.2015.7506818

[21] Aulikki Hyrskykari, Howell Istance, and Stephen Vickers. 2012. Gaze Gestures or Dwell-based Interaction?. In *Proceedings of the Symposium on Eye Tracking Research and Applications (ETRA '12)*. ACM, New York, NY, USA, 229–232. https://doi.org/10.1145/2168556.2168602

[22] Shoya Ishimaru, Kai Kunze, Katsuma Tanaka, Yuji Uema, Koichi Kise, and Masahiko Inami. 2015. Smart Eyewear for Interaction and Activity Recognition. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 307–310. https://doi.org/10.1145/2702613.2725449

[23] Howell Istance, Aulikki Hyrskykari, Lauri Immonen, Santtu Mansikkamaa, and Stephen Vickers. 2010. Designing Gaze Gestures for Gaming: An Investigation of Performance. In *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications (ETRA '10)*. ACM, New York, NY, USA, 323–330. https://doi.org/10.1145/1743666.1743740

[24] Moritz Kassner, William Patera, and Andreas Bulling. 2014. Pupil: An Open Source Platform for Pervasive Eye Tracking and Mobile Gaze-based Interaction. In *Proc. UbiComp 2014, Adjunct Publication*. ACM, 1151–1160.

[25] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[26] 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 (ICMI 2017)*. ACM, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[27] Abraham. Savitzky and M. J. E. Golay. 1964. Smoothing and Differentiation of Data by Simplified Least Squares Procedures. *Analytical Chemistry* 36, 8 (1964), 1627–1639.

[28] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proc. of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, New York, NY, USA, Article 13, 10 pages. https://doi.org/10.1145/2406367.2406384

[29] Youngbae Song, Geumhwan Cho, Seongyeol Oh, Hyoungshick Kim, and Jun Ho Huh. 2015. On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks. In *Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2343–2352. https://doi.org/10.1145/2702123.2702365

[30] Melanie Swan. 2012. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks (JSAN)* 1, 3 (Nov. 2012), 217–253.

[31] Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R. Crowell, and John D'Arcy. 2013. Modifying Smartphone User Locking Behavior. In *Proc. SOUPS 2013*. ACM, NY, USA, Article 10, 14 pages. https://doi.org/10.1145/2501604.2501614

[32] 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

[33] Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proc. 5th Nordic Conference on Human-computer Interaction: Building Bridges (NordiCHI '08)*. ACM, New York, NY, USA, 383–392. https://doi.org/10.1145/1463160.1463202

[34] Jacob O. Wobbrock, Brad A. Myers, and John A. Kembel. 2003. EdgeWrite: A Stylus-based Text Entry Method Designed for High Accuracy and Stability of Motion. In *Proceedings of the 16th Annual ACM Symposium on User Interface Software and Technology (UIST '03)*. ACM, New York, NY, USA, 61–70. https://doi.org/10.1145/964696.964703

[35] Jacob O. Wobbrock, James Rubinstein, Michael W. Sawyer, and Andrew T. Duchowski. 2008. Longitudinal Evaluation of Discrete Consecutive Gaze Gestures for Text Entry. In *Proceedings of the 2008 Symposium on Eye Tracking Research & Applications (ETRA '08)*. ACM, New York, NY, USA, 11–18. https://doi.org/10.1145/1344471.1344475