American Journal of Computer Science and Technology
2023; 6(3): 102-108
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20230603.12
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Role of Shoulder Surfing in Cyber Security (Experimental Study to the Comparative Framework)

Marran Aldossari, Abdullah Albalawi

Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia

Email address:
Maldossari@su.edu.sa (Marran Aldossari), Aalbalawi@su.edu.sa (Abdullah Albalawi)

To cite this article:
Marran Aldossari, Abdullah Albalawi. Role of Shoulder Surfing in Cyber Security (Experimental Study to the Comparative Framework). *American Journal of Computer Science and Technology*. Vol. 6, No. 3, 2023, pp. 102-108. doi: 10.11648/j.ajcst.20230603.12

Received: August 23, 2023; **Accepted**: September 7, 2023; **Published**: September 18, 2023

Abstract: Shoulder surfing attacks pose a significant threat to the security of sensitive information, such as passwords, social security numbers, and credit card details. In these attacks, malicious individuals strategically position themselves to observe a victim's screen and keyboard inputs covertly. As the security landscape evolves, researchers are actively exploring alternative authentication methods to replace traditional textual passwords. However, evaluating the resilience of these authentication systems against shoulder surfing attacks has been a complex task. This research aims to provide a comprehensive framework for objectively assessing the vulnerability of authentication mechanisms to shoulder surfing attacks. Through a systematic analysis, our study reveals intriguing insights. Notably, it demonstrates that pictorial passwords are more susceptible to shoulder surfing than their textual counterparts. This susceptibility arises from the ease with which attackers can visually capture and recall graphical representations. However, our research also highlights the potential for designing graphical authentication schemes that can resist shoulder surfing attempts effectively. While visual passwords exhibit inherent vulnerability due to their visibility, creative design choices can mitigate these risks. Furthermore, we found that textual passwords, while less susceptible to shoulder surfing, face limitations due to their smaller character pool size. In conclusion, this study sheds light on the nuanced landscape of authentication mechanisms and their susceptibility to shoulder surfing attacks. By providing a robust set of measures for objective analysis, our research serves as a valuable resource for developing and implementing secure authentication solutions. It emphasizes the importance of considering both usability and security factors when designing authentication systems to combat the persistent challenge of shoulder surfing attacks.

Keywords: Shoulder Surfing, Observer, Attacker, Surfer, Security, Privacy

1. Introduction

When attackers can see the device's screen and keyboard, they can perform a shoulder surfing attack and steal sensitive information. As such, it is one of the rare forms of attack that necessitates the attacker to be near the victim. Some attackers will utilize binoculars, small video cameras, or other optical equipment to spy on their victims. Despite the name's implication, all they must do is peek over the victim's shoulder. The target is the user's private information, including their passwords, social security numbers, and credit card details. Most shoulder surfing assaults will be carried out maliciously, although others may be the product of inquisitive onlookers.

Shoulder surfing assaults are typically relatively simple, with the perpetrator just positioning himself so that he can see the victim's screen and the keyboard or keypad, if necessary. The attacker keeps track of what the victim types and sees on the device. The attacker probably uses a similarly simple method, such as writing or entering the information. However, more complex attacks may use optical gadgets, making it impossible for the victim to see the attacker. Shoulder surfing does not include attacks where the hacker can monitor your screen and your data remotely or if the victim has placed a reading device to contain malware (such as a skim reader on an ATM) [1].

Examples:

The following are examples of shoulder surfing that have occurred in real life:

1) Someone stood over you at an ATM and watched you input your PIN. Since you were in a hurry, you did not check to see whether all the money had been taken out

of the ATM before you left with your card and the cash. If the ATM does not need the card to be inserted throughout the whole transaction, then the attacker can use the PIN for more transactions if you do not affirm that you have no more transactions to perform.

2) Why Attackers can easily spy on victim's device screens and overhear their talks on crowded public transportation, when this occurs, the offender is figuratively and physically peering over the victim's shoulder.
3) The victim may leave their gadget alone in a public area. However, suppose an attacker watches a victim type in his password on a computer. In that case, that attacker can access the device and access any private information stored on it.

There has been much work put into inventing alternative authentication mechanisms to textual passwords to solve the age-old password security problem. Their biggest problem is trying to maximize two factors that are intrinsically at odds with one another: security and usability. Examining alternatives to textual passwords is a common topic for research papers, and these papers often include assessments along these two dimensions. However, maintaining comparability across widely varied authentication systems presents a significant challenge. To get around this problem, research has standardized metrics like entropy for gauging password strength (and hence the method's underlying security), login times, and recall accuracy for characterizing some of the usability features. While no one statistic is without flaws, they do allow for reliable comparisons across different approaches. Unfortunately, when comparing authentication systems for their robustness against shoulder surfing, only a few previous articles have attempted to do so empirically. Although shoulder surfing is not as common as some other forms of cyberattack, its simplicity and ease of detection and execution may be to blame.

Shoulder surfing is a well-known security concern in the human-computer interaction world, and the field of password security is crowded with new authentication mechanisms claiming to be immune to such assaults. Lacking metrics that would thoroughly and accurately evaluate the susceptibility of a specific strategy to shoulder surfing assaults hinders fair comparisons. The "security" of a technique against these assaults is generally determined using subjective criteria, such as the number of observations required to guess the password correctly. The researcher argues that evaluating fresh approaches along this dimension is only meaningful if they are assumed safe against shoulder surfing. While it would be ideal if there were no variation in how susceptible different authentication techniques were to shoulder surfing, this is obviously not possible.

Our goal is to give a complete set of measures that will allow for an objective analysis of shoulder surfing resistance. At the same time, other researchers investigate the various study designs of shoulder surfing and emphasize the associated concerns and problems. In this study, we set out to provide a standard by which all knowledge-based authentication techniques may be compared, no matter their specific architecture. Our approach is tested with three distinct forms of authentication: the more common text-based passwords, a graphical authentication system based on the game of chess, and a new hybrid form of both.

We conduct a thorough vulnerability analysis of the selected approaches in one of the most extensive live-observation studies, paying attention to factors like the input type and the observer's purpose. Our data analysis goes beyond the first comprehensive review of the techniques to shed light on the factors at play in a method's vulnerability to these attacks. The findings shed light on the shoulder surfing phenomenon and, by extension, password security and have significant implications for the creation of innovative authentication techniques and research.

2. Literature Review

Shoulder surfing is a phenomenon that receives little empirical examination in password research. Shoulder surfing attacks are a common topic of discussion in academic publications that provide new forms of graphical password authentication. Even because graphical passwords have traditionally been considered particularly vulnerable to shoulder surfing attacks, this vulnerability has become less and less of a concern as authentication methods have evolved. Even though most current articles do not go beyond theoretical justification, it is uncommon to encounter claims that a revolutionary approach is resistant to shoulder surfing. Some of them suggest studying the technique's resistance would be an excellent next step in the field, while others assume the method is immune to the attack because of how it was built.

The articles that have empirically studied shoulder surfing assaults are highlighted here. In Appendix A, we thoroughly analyze how the chosen studies compare to one another. Investigations into shoulder surfing in general. A review of existing shoulder-surfing-resistant graphical authentication techniques was undertaken in 2009. Each of the sixteen publications was detailed in detail, including the research challenges it addressed, the methods employed, the outcomes, and the possible next steps. After that, 12 papers that were shown to be resistant to shoulder surfing were chosen for additional analysis. Insight into shoulder surfing trials might be gained from a quick review of current shoulder surfing-resistant graphical authentication techniques. However, more work was needed to identify and understand any potential research design concerns. The work comes closest to addressing the issue of the difficulties inherent in the study design of shoulder surfing.

Instead of comparing previous studies of shoulder surfing by looking at their results, scientists decided to look at the methodology utilized in each study individually. By contrasting many studies on shoulder surfing, the authors show how seemingly little modifications to an experiment's design may have a profound effect on the reliability and applicability of its findings.

They were able to pinpoint numerous issues (such as a lack of specific metrics) that have been consistently identified in shoulder surfing studies by comparing and contrasting various methods. They put out a list of suggestions to give future researchers a starting point for achieving consistent findings comparisons. Our research included the recommendations made in this publication. One fascinating research looked at how mental exercise may improve the performance of human rivals. The research team developed an innovative covert attentional shoulder surfing strategy by reducing the opponent's effectiveness by suppressing saccadic eye movement and perceptual grouping. In just five days, the average performance of 10 participants on a shoulder-resistant approach suggested by jumped from 44% to 84% in a live presentation. They modified the original strategy to prevent attentional shoulder surfing and reran the experiment. Over the five days, not a single person guessed more than two digits of the PIN, and in 69.8 percent of attempts, every participant failed to predict any of the PIN's digits. The authors stressed the need to recognize experienced human attackers, especially when sophisticated surveillance methods are not countered.

A mobile device investigation also investigated the vulnerability of swipe passwords to shoulder surfing [8]. The subjects of the two studies were shown videos of the login procedure. According to the authors, the subjects were far more likely to notice symmetrical patterns than asymmetrical ones. Also, they needed help keeping up with the knight's movements, which may have been because the swipe password needed to be more straightforward. They also noted that the guessing accuracy dropped significantly without visual cues (i.e., disappearing lines).

SwiPIN is a gesture-based swipe password technique for mobile devices; Wiese and Roth ran a more extensive experiment to evaluate its resistance against shoulder surfing [4]. Every 162 participants went through as many as ten steps of the online trial. They started with observing a one-digit password and then gradually increased to passwords of two, three, four, and five digits throughout many stages. At least three out of five attempts at guessing a random password had to be successful for the player to go on. Ninety percent of people in the first three experiments guessed the correct password. With only one participant correctly guessing a 7-digit password three out of five times, the success rate suddenly decreased to 56% in experiment four and 18% in experiment five. The authors estimated which participant reports were seen and which would have been inferred using Wilson's 95% confidence intervals. In a subsequent, more limited study, the same method was utilized once more, this time with smartphones. Nineteen people went through 11 tests where they had to keep track of the motions of up to 4 fingers and 4 digits. It was significantly more difficult for the participants to monitor the passwords submitted on the phone, according to a comparison of the first four tests with the web-based study. Additionally, the scientists reported a 90% success rate within 8-14 observations while simulating an opponent guessing 10,000 PINs across 20 sessions in three different circumstances. Finally, five schemes with very similar designs were attacked virtually. The authors compared the strategies based on the likelihood of achieving their goals within a certain number of sessions. By doing additional assessments, researchers in many other studies were able to bolster the reliability of their shoulder surfing research. The picture-based approach suggested by Ho et al. was first put through its paces in a simulation, where it was subjected to a frequency-of-occurrence assault [8]. After making sure the final "target" images are spread out evenly amongst the venues, a thirty people participated in a typical shoulder surfing experiment. None of the participants were able to correctly guess the password after seeing a recording of the login process for an infinite number of times.

For this purpose, Papadopoulos created a human visual perception algorithm to ascertain whether the user's keypad is visible from any particular vantage point [2]. Twenty-one individuals performed the shoulder surfing experiment in pairs to assess the innovative IllusionPIN technique's assessed safety distance. Everyone had to see the login procedure five times from varying vantage points. The authors assessed that no one would have guessed the password correctly within the range [0, 0.1329].

For their 2016 paper, Maqsood et al. thoroughly tested a new gesture-based authentication method they termed Bend passwords [3]. Different features of user-selected and system-generated usability were empirically compared. For example, changing PINs and passwords is easy. In an ancillary survey, they were also asked several questions on the practicality and safety of both approaches, such as how vulnerable they thought each was to shoulder surfing assaults. In a follow-up experiment, 9 people saw eight passwords of each kind in different hand positions and password strengths, and they were given up to three tries to guess the password. The similarity between the original and guessed passwords was measured using the Levenshtein distance; however, due to the limited sample size, no statistically significant differences were identified. Another investigation of the relative strengths of several graphical authentication techniques on handheld devices by Schaub [6]. Six distinct schemes were tested, each representing a different kind of graphical password for their ease of use and vulnerability to shoulder surfing. Each of the sixty people who participated in the shoulder surfing study was randomly allocated to one of two groups, one using the graphical approach and the other using the traditional way, and both were instructed to watch. In comparison, four people entered passwords (strong vs. weak, live vs. video). The authors chose a simple binary measure, rewarding 1 to participants who guessed the correct password within three attempts and 0 otherwise, to account for the variations across authentication mechanisms.

Weak passwords, as predicted, were simpler to shoulder surf than strong ones. In all likelihood, the participants' poor performance was because the camera and hands were fixed throughout the movie, as was the lighting. Finally, cued-recall schemes were the most secure. In contrast,

approaches involving drawing interaction (such as the recall-based Pass-Go [3, 7] were the most vulnerable to shoulder surfing assaults.

Only Tari et al. assessed the vulnerability of a graphical authentication technique to that of traditional textual passwords, as far as we are aware [10]. A total of 20 individuals were put in the attacker's position and instructed to spy on one of four password setups (dictionary and non-dictionary textual passwords and Pass faces input by a mouse or a keyboard). The proportion of correctly predicted characters in the correct order was used to evaluate their performance. Most participants had the worst time predicting the key-board-input Pass faces, whereas it was much simpler for them to follow the characters input by a mouse. Somewhat unexpectedly, dictionary passwords seemed more complicated to shoulder surf than non-dictionary ones. To crack non-dictionary passwords, participants had to concentrate on each character, which led to their success, according to the authors. However, a single primary metric could obscure the true motivation behind the score and the accurate vulnerability levels of the existing approaches under consideration. In our research, we take great pains to ensure the reliability of our findings by using several different criteria. The primary addition made by Tari et al. is a contrast between the actual dangers of shoulder surfing and the participants' perceptions of such risks, regardless of the method used [12]. In several ways, they had similar views: After the fact, correlation analysis revealed that their expectations were incorrect for the other two techniques. At the same time, their perceptions were spot on for mouse-input Pass faces and dictionary passwords.

Shoulder Surfing Studies of Novel and Existing Method

Using doodles as pass-images in a recognition-based graphical password system has been the subject of much research on its security and usability against shoulder surfing. Thirty people were split into ten pairs, including a victim and an observer. While an observer observed, the victims typed in four randomly generated doodle passwords. The experiment was replicated with the individuals' switching roles. The participants correctly guessed 54.4% of passwords overall and almost 75% of mouse-input password-guessing attempts, indicating that the input modality influences the attacker's efficacy. Defended the Draw-AS-Secret (DAS) recall-based graphical password scheme with three different methods of shoulder surfing protection. Usability and vulnerability to shoulder surfing were tested in two independent trials. Each participant in the shoulder surfing experiment took on the role of an attacker attempting to steal one of three DAS passwords (weak, medium, or strong) during a single login attempt and was randomly assigned to one of four experimental groups (three defensive groups and a control group) [13]. The data was split in half depending on how often shoulder surfing was used: About 77% of strokes could be estimated using DAS alone with the Decoy Stroke defense, but only 40% to 50% could be guessed with the Disappearing Stroke and Line Snaking defenses, respectively. Passwords that were secure against shoulder surfing were also recorded, along with the total number of times they were stolen, cracked, or otherwise compromised.

The correlation between password complexity and guess rate was also analyzed. A recognition-based authentication approach called EvoPass was described. It gradually adapts pass pictures such that they become more secure against shoulder surfing. Twenty volunteers in a shoulder surfing experiment saw an experimenter enter numerous passwords into three different implementations of the EvoPass system as part of the authors' comprehensive investigation of the unique scheme [11]. When asked how many times they had to look at each passing picture during a single assault, participants reported the number of observations needed. Participants were also asked to provide an estimate of their memory's accuracy so that researchers could examine how well this estimate matched their actual memorability during shoulder surfing. Standard pass photos were used in a mobile device study with identical results. After enrolling in usability research, 16 people participated in a shoulder surfing experiment to see what it would be like to use the system from someone else's perspective. Participants played the roles of both attackers and victims, just like in. The average number of observations needed to log in for low-entropy passwords was 4.5, whereas for high-entropy passwords, it was 7.5. At the same time, a model of a shoulder surfer was created, and 10,000 attacks were simulated.

The model predicted that an attacker would require less than five observations to log in once successfully and that an attacker with the tools for perfect recall (such as a camera) would correctly identify all crucial pictures 84% of the time, on average. The vulnerability of swipe passwords to shoulder surfing was also investigated in a mobile device investigation. The subjects of the two studies were shown videos of the login procedure. According to the authors, the subjects were far more likely to notice symmetrical patterns than asymmetrical ones. Also, they needed help keeping up with the knight's movements, which may have been because the swipe password needed to be more straightforward. They also noted that the guessing accuracy dropped significantly without visual cues (i.e., disappearing lines). SwiPIN is a gesture-based swipe password solution for mobile phones, and its resistance to shoulder surfing was tested in a more extensive study. Every 162 participants went through as many as ten steps of the online trial. A one-digit password was shown to them in the first step; from there on out, they would need to see passwords with one additional digit. At least three out of five attempts at guessing a random password had to be successful for the player to go on [7].

Table 1. *Bonferroni-corrected p-values for pairwise comparisons between all authentication methods, with respect to observer type. All p-values, significant at .05 level, are shaded. Metrics marked with an asterisk are complementary.*

Metric	Active Participants						Passive Participants					
	P-C	P-L_k	P-L_m	C-L_k	C-L_m	L_k-L_m	P-C	P-L_k	P-L_m	C-L_k	C-L_m	L_k-L_m
Length Dif	1	0	0	0	0	1	0	0.384	1	0	0	1
Same Chars	1	0.414	1	1	1	0.63	0.186	0.57	0.006	1	1	0.456
Correct First	1	0	1	0	1	0	0	0.132	1	0	0	0.252
Right Spot	1	0	0.042	0	0.114	0	0.318	0	0.006	0	0	0.636
LCS	1	0	0	0	1	0	0.252	1	1	0.006	0.036	1
Dif in Guess*	1	0	0	0	0	0.36	1	0	0	0	0	0.168
Characteristics	1	0.054	1	1	1	0	0.246	1	0.024	1	1	0.042
Jaccard	1	1	0.108	1	0.252	0.222	0.204	0.024	0	1	0.084	0.504
Jaro-Winkler	1	1	0	1	0	0	0.366	0.156	0.036	1	1	1
Cosine	0.228	1	1	0.846	0.042	0.12	1	0.126	0	0.66	0.006	0.252
Levenshtein	1	0	1	0.336	1	0	1	1	1	0.102	0.408	1
N-grams	1	0.006	1	0.156	1	0	0.51	0.948	1	0.03	0.372	0.816
Distance	1	0	0.288	1	0.264	0	0.612	0.6	0.018	1	1	0.27
Pool Guess*	0.486	0.048	0.356	0.294	0.486	0.228	1	1	1	0.348	0.066	1
Position Guess*	0.024	1	0.012	1	1	0	0.018	0.216	0.876	0.042	0.096	1
Entropy*	0.192	0	0	0	0	1	0	1	1	0	0	1
Guessing Order*	0.012	0.006	0.084	0	0	1	0	1	1	0	0	1

Ninety percent of people in the first three experiments guessed the correct password. With only one participant correctly guessing a 7-digit password three out of five times, the success rate suddenly decreased to 56% in experiment four and 18% in experiment five. The authors estimated which participant reports were seen and which would have been inferred using Wilson's 95% confidence intervals. In a subsequent, more limited study, the same method was utilized again, this time with smartphones. Nineteen people went through 11 tests where they had to keep track of the motions of up to 4 fingers and four digits. It was significantly more difficult for the participants to monitor the passwords submitted on the phone, according to a comparison of the first four tests with the web-based study. The authors also ran a simulation in which an adversary tried to guess 10,000 PINs throughout 20 sessions across three different situations, claiming they were 90% successful after 8-14 observations. Finally, five schemes with very similar designs were attacked virtually. The authors compared the strategies based on the likelihood of achieving their goals within a certain number of sessions.

By doing additional assessments, researchers in many other studies were able to bolster the reliability of their shoulder surfing research. First, a simulated assault based on the frequency of occurrence was used to check the strength of a suggested picture-based method. Once it was established that the "target" images were spread relatively throughout the many sites, a standard shoulder surfing experiment was run with a group of 30 participants [14].

The participants could only correctly guess the password after seeing a recording of the login process an infinite number of times. Scientists devised an algorithm based on human visual perception to ascertain whether the user's keypad is visible from any vantage point. Twenty-one individuals performed the shoulder surfing experiment in pairs to assess the innovative IllusionPIN technique's assessed safety distance. Everyone had to see the login procedure five times from varying vantage points. The authors assessed that no one would have guessed the password correctly within the range [0, 0.1329]. Rigorously tested a new gesture-based authentication method dubbed Bend passwords.

By doing additional assessments, researchers in many other studies were able to bolster the reliability of their shoulder surfing research. In, a simulated assault based on the frequency of occurrence was used to check the strength of a suggested picture-based method. Once it was established that the "target" images were spread fairly throughout the many sites, a normal shoulder surfing experiment was run with a group of 30 participants. None of the participants were able to correctly guess the password after seeing a recording of the login process for an infinite number of times. Scientists devised an algorithm based on human visual perception to ascertain whether or not the user's keypad is visible from any vantage point. Twenty-one individuals performed the shoulder surfing experiment in pairs to assess the innovative IllusionPIN technique's assessed safety distance. Everyone had to see the login procedure five times from varying vantage points. The authors assessed that no one would have guessed the password correctly within the range [0, 0.1329]. rigorously tested a new gesture-based authentication method dubbed Bend passwords.

However, it seems far more difficult to shoulder surf a 6-digit PIN. Only 10.8 percent of people could identify the PIN after only one trial, and 26.5 percent after two or more. The attacker's ability to see the password also varied with viewing angle and phone size, but not with hand position. The research supplements some of the earlier work on the topic. It sheds light on the kinds of environments and adjustments that could make the approaches less vulnerable to shoulder surfing assaults. Another look at mobile graphical authentication methods was conducted by [4], who compared several different approaches. Six distinct schemes were tested, each representing a different kind of graphical password for their ease of use and vulnerability to shoulder surfing. Each of the sixty people who participated in the shoulder surfing

study was randomly allocated to one of two groups, one using the graphical approach and the other using the traditional way, and both were instructed to watch.

In comparison, four people entered passwords (strong vs. weak, live vs. video). The authors chose a simple binary measure, rewarding 1 to participants who guessed the correct password within three attempts and 0 otherwise, to account for the variations across authentication mechanisms. Weak passwords, as predicted, were simpler to shoulder surf than strong ones. Likely, the participants' poor performance was because the camera and hands were fixed throughout the movie, as was the lighting [5].

3. Discussion

Shoulder surfing vulnerability was studied using a variety of approaches, but overall, there were few discernible variations between them. However, they all show that visual passwords are more susceptible to observational assaults than textual ones. The association lists variant in which the password was entered using a mouse, for instance, consistently performed worse than the other three approaches, regardless of the measure being compared (distance or characteristics). The GCPS password guesses would have significantly reduced the guessing effort needed compared to the other techniques. The contrast between the two forms of association lists is the most persuasive piece of evidence.

The primary motivation for comparing two variants of the identity authentication mechanism was to exclude the influence of any additional confounding factors that may increase the likelihood of shoulder surfing. Furthermore, despite sharing the same output type, the two groups demonstrated the different human-computer interaction that defines textual and graphical passwords. In this regard, practically all vulnerability measures found that graphical variety (i.e., mouse input) was inferior to textual variation (i.e., keyboard input). Therefore, given the highlighted influence of the textual-graphical discrepancy on the measure, it may be predicted that the shoulder surfing susceptibility levels would differ more noticeably between the techniques.

The intricacy of the susceptibility measure is to blame for this discrepancy. Regarding shoulder surfing assaults, it is not just the password format that makes a difference; other aspects, such as the mapping between the remembered idea and the encoded password characters, or the scheme's underlying security, might also have an impact. It is simple to make a mistake and conclude, for instance, that the approach with the highest percentage of predicted characters is also the most susceptible to shoulder surfing assaults when this is not the case. An attacker may have an easier time making correct guesses, but it does not mean they will have an easier time finding the correct password if you use this strategy because the character pool is so big [9, 15].

As a result, much time and effort were spent before the experiment began to account for technique inequalities and normalize such discrepancies to provide a fair comparison. Therefore, we considered how much the attackers could see, memorize, and repeat and how much help their guess may give them in obtaining the actual password when gauging how vulnerable a system was to shoulder surfing assaults. Due to our well-designed experiments and incorporation of different vulnerability measures, we were able to evaluate the causes of the observed variation in vulnerability. The susceptibility score went up because of the visual element, but it went down as the character pool got more extensive or the password got longer. Over time, the disparities in susceptibility were even out due to the inversely proportional factors, leaving only subtle variations between the authentication strategies to be emphasized. However, that in no way lessens the significance of the findings of this study.

Our study's main contribution is empirical proof of the detrimental effect of pictorial passwords on susceptibility to shoulder surfing assaults. Furthermore, only because of their mathematical stability and improved security could the evaluated graphical approaches compete with textual ones regarding vulnerability to shoulder surfing. This has crucial implications for future graphical password studies; researchers should be mindful of graphical passwords' intrinsic propensity to shoulder surfing assaults, but they should not let that deter them from designing graphical schemes resistant to shoulder surfing. Any scheme's susceptibility to shoulder surfing attacks will vary depending on its specific design and implementation details. Increasing the search space (both theoretical and practical) can help strengthen the scheme's security and make it less likely that an attack of this type would succeed. The scheme's usefulness will suffer, as was briefly demonstrated with login timings. Password security, especially graphical passwords, continues to center on striking a balance while working to enhance all elements (security, usability, and deployment ability). We advocate for an empirical evaluation of each new authentication mechanism to see how vulnerable it is to shoulder surfing. The threat model should inform the experimental design. Given our goal of figuring out how little an attacker may learn by watching a victim type in a password, we found that a single live observation was the most effective method. A more nuanced examination of the examined authentication techniques was made possible by classifying the participants as either opportunistic or purposeful observers; this helped to illuminate the susceptibility of graphical passwords to contextual observations. It will be necessary for future studies to modify their experimental design to meet their specific needs and areas of inquiry.

4. Conclusion

Conclusion Shoulder surfing vulnerability is difficult to quantify since it depends not only on whether a method is textual or graphical but also on the design aspects of each method that impact the attacker's observation technique. We offer a set of metrics in this study to reflect the many factors contributing to a method's vulnerability to observational assaults. We normalize the data depending on the original

password length and adjust the account for incomplete guesses. Password features, distance metrics, and guessing order are the groups into which we group the many data we have collected. We use this model to compare four authentication strategies across two observation settings. That lets us evaluate each technique from several angles, such as authentication strategy, input method, and observer motivation. Passwords for association lists entered using a mouse were consistently easier for the participants to guess than those entered with a keyboard. As shown in table 1, active participants fared better than their passive counterparts. Both results corroborate information from prior research. There was little distinction between the various authentication techniques measured by composite metrics.

It would be easy to jump to the incorrect conclusion that graphical approaches are just as vulnerable to shoulder surfing as textual ones. Thankfully, an in-depth examination of the data was made possible by the availability of different measures. In this case, the attackers had more conviction in their guesses since they had seen and memorized more accurate characters occurring in proper locations in graphical passwords. In addition, several of their estimates were only half true, suggesting that the visual element helped people remember at least some of what they saw in the characters. However, the more considerable vulnerability disparities were evened out because textual passwords had a much more minor character pool size, making the approach more susceptible to successful blind guessing. Meaningful inferences may be made from that. Because attackers (whether intentional or not) may more easily see and recall graphical constructions than textual ones, graphical passwords are more susceptible to observational assaults. Shoulder attacks on graphical passwords may be more effective than on textual passwords in the future, although this is not yet guaranteed.

Acknowledgments

We would like to extend our sincere gratitude to Shaqra University for their unwavering support throughout the research and preparation of this publication. The resources and academic environment provided by the university have played an integral role in shaping the outcome of this work. We are thankful for the opportunity to contribute to the scholarly community, and we recognize the invaluable contribution of Shaqra University in making this endeavor possible.

References

[1] Angeli, A. D., Coventry, L., Johnson, G., Renaud, K., (2005). Is a picture worth a thousand words? Exploring the feasibility of graphical authentication systems. Int. J. Hum.-Comput. Stud. 63 (1), 128–152. https://doi.org/10.1016/j.ijhcs.2005.04.020.

[2] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies 63, 1 (2005), 128–152. https://doi.org/ 10.1016/j.ijhcs.2005.04.020 HCI research in privacy and security.

[3] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. (2017). Towards Baselines for Shoulder Surfing on Mobile Authentication. In Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017). ACM, New York, NY, USA, 486–498. https://doi.org/10.1145/ 3134600.3134609

[4] Leon Bo˘snjak and Bo˘stjan Brumen. (2019). Rejecting the Death of Passwords: Advice for the Future. Computer Science and Information Systems 16, 1 (2019), 313332.

[5] Botjan Brumen. (2019). Security analysis of Game Changer Password System. International Journal of Human-Computer Studies 126 (2019), 44–52. https://doi.org/10.1016/j.ijhcs.2019.01.004

[6] Ashley A. Cain, Liya Chiu, Felicia Santiago, and Jeremiah D. (2016) Still. 2016. Swipe Authentication: Exploring Over-the-Shoulder Attack Performance. In Advances in Human Factors in Cybersecurity, Denise Nicholson (Ed.). Springer International Publishing, Cham, 327–336.

[7] H. Sun, S. Chen, J. Yeh, and C. Cheng. (2018). A Shoulder Surfing Resistant Graphical Authentication System. IEEE Transactions on Dependable and Secure Computing 15, 2 (March 2018), 180–193. https://doi.org/10. 1109/TDSC.2016.2539942

[8] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. (2010). Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10). ACM, New York, NY, USA, 162–175.

[9] Marran Zabin Aldossari, "A Survey on Phishing Attacks in Cyberspace", IJC, vol. 41, no. 1, pp. 46–58, Dec. 2021.

[10] Aldossari, Marran and Zhang, Dongsong, "D&L: A Natural Language Processing Based Approach for Protecting Sensitive Information from Shoulder Surfing Attacks" (2023). AMCIS 2023 Proceedings. 7.

[11] Tabassum, M., Alqhatani, A., Aldossari, M., & Richter Lipford, H. (2018, April). Increasing user attention with a comic-based policy. In Proceedings of the 2018 chi conference on human factors in computing systems (pp. 1-6).

[12] Aldossari, M. (2023). The use of text recognition, lip reading, and object detection for protecting sensitive information from shoulder surfing attacks (Order No. 30529612). Available from ProQuest Dissertations & Theses Global. (2840101210). Retrieved from https://www.proquest.com/dissertations-theses/use-text-recognition-lip-reading-object-detection/docview/2840101210/se-2

[13] Zimmeck, Sebastian, Rafael Goldstein, and David Baraka. "PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps." NDSS. Vol. 2. 2021.

[14] Bui, D., Shin, K. G., Choi, J. M., & Shin, J. (2021). Automated Extraction and Presentation of Data Practices in Privacy Policies. Proc. Priv. Enhancing Technol., 2021 (2), 88-110.

[15] Kitkowska, A., Warner, M., Shulman, Y., Wästlund, E., & Martucci, L. A. (2020). Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 437-456).