Aug 10th, 12:00 AM

D&L: A Natural Language Processing Based Approach for Protecting Sensitive Information from Shoulder Surfing Attacks

Marran Aldossari
University of North Carolina at Charlotte, maldoss2@uncc.edu

Dongsong Zhang
University of North Carolina at Charlotte, dzhang15@uncc.edu

D&L: A Natural Language Processing-Based Approach for Protecting Sensitive Information from Shoulder-Surfing Attacks

Completed Research Full Paper

Marran Aldossari
University of North Carolina at Charlotte
maldoss2@uncc.edu

Dongsong Zhang
University of North Carolina at Charlotte
dzhang15@uncc.edu

Abstract

Despite the increasing attention and research effort, how to protect sensitive information from shoulder surfing attacks is still under studied. Existing methods for protecting sensitive textual content on users' screens from shoulder surfing attacks have various limitations, including ineffectiveness, insufficient protection of sensitive information, low usability, and high cognitive workload. To address those limitations, this paper proposes, develops, and evaluates a new solution called "detection and labeling" (D&L), which uses NLP techniques to automatically detect and label sensitive information in the textual content. The labeled and hidden sensitive information is then read to users through their headphones upon their clicking a label. Evaluation results demonstrate that D&L improves protection, enhances usability, reduces users' cognitive workload, and allows faster browsing speed compared to the baseline methods.

Keywords

Privacy, shoulder surfing, sensitive information protection, detection and labeling (D&L).

Introduction

According to Statista, there were more than 15.96 billion portable and mobile devices worldwide in 2022 (Federica 2022). Those devices, such as mobile phones, laptops, and tablets, have been used for not only information gathering (e.g., navigating news) and entertainment (e.g., gaming), but also communication (e.g., email), business (e.g., trading and online banking), and other personal and work-related activities. They have become an essential part of daily work and life of many people. For example, sending and receiving emails on a laptop are ubiquitous, with many people writing, checking, and responding to emails multiple times throughout a day. In 2017, 269 billion emails were sent daily worldwide, and that number is expected to reach 376.4 billion by 2025 (Deepak et al. 2022).

Despite convenience, browsing with sensitive or private content on those portable devices in public spaces can entail severe risks to privacy and information security. Sensitive information refers to any information that must be kept secure from unauthorized access in order to maintain an individual's privacy. Shoulder-surfing attacks are becoming increasingly common as more people use portable devices in public. This type of attack is referred to as someone covertly observing another person's device screen, which can result in the attacker obtaining sensitive information illegally. According to the Ponemon Institute (Ponemon 2017), 91% of shoulder-surfing attackers obtained sensitive information while a user was browsing. The stolen information, such as SSN, personal and employee data, and financial information, is a major contributor to the $56 billion loss from identity theft in 2020 that affected 15 million U.S. consumers (Buzzard 2022), emphasizing the urgency and importance of protecting personal information from shoulder surfers, particularly in public places.

In response to this need, some technological solutions have been proposed to protect text displayed on mobile and portable devices from shoulder surfers. These solutions can be categorized into three types based on their main characteristics: text modification, gesture-based, and external tool-based. Text modification methods shuffle letters or hide the screen with masks, but some attackers can still identify the masked text. Gesture-based methods recognize user gestures to display or hide content, but they are slow; and external tool-based methods are inaccurate and difficult to deploy. Therefore, a more effective method for protecting sensitive information from shoulder surfers that can maximize information security without satisficing usability is necessary.

This research proposes a method called detection and labeling (D&L), which automatically identifies and replaces sensitive information in textual content with a category label. Users can click on the label to hear the original sensitive information through headphones. D&L is expected to improve user interaction with devices while protecting sensitive information displayed on the screen without compromising usability because it does not hide any non-sensitive content on the screen. This research aims to answer the following research questions: *How effective is the D&L method for protecting sensitive information against shoulder-surfing attacks when a user is browsing on a laptop? What is the perceived usability of D&L compared to that of the selective showing and normal browsing methods?*

The rest of the paper first presents a literature review on methods for protecting sensitive information from shoulder surfing in Section 2. Section 3 introduces the proposed D&L method, while Section 4 describes its evaluation. Section 5 presents the evaluation results, followed by the discussion of major findings and the limitations of this research in Section 6.

Literature Review

There are two main types of sensitive information: personal and business. Personal sensitive information includes data related to an individual, such as a social security number, a credit card number, or a home address, while sensitive business information includes details that could harm an organization if it is made to the public, like financial information. Both types of sensitive information must be protected from shoulder-surfing attacks. Various methods have been developed to protect sensitive textual information on mobile devices, tablets, and laptops from shoulder-surfing attacks. The most common method focuses on password- or PIN-based user authentication, but shoulder surfing is not restricted to the user authentication stage - content-targeted, especially textual content-targeted, shoulder-surfing attacks have also been frequently reported (Binbeshr et al. 2021; Ragozin et al. 2019), as text is the primary medium of digital communication.

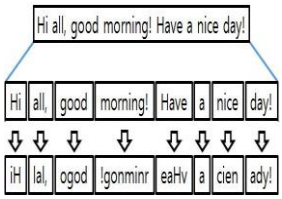
We conducted a literature search in databases including ACM Digital Library, Google Scholar, IEEE Xplore digital library, and ScienceDirect, as well as in individual journals related to human-computer interaction, such as *Usable Security and Privacy*, *Security and Privacy*, and *Human–Computer Interaction*. The searches used multiple keywords, including “shoulder-surfing,” “privacy,” “observer,” “protection,” and “attacker,” and a variety of their combinations. To ensure that the literature review reflects the state-of-the-art research, we only searched and reviewed studies published in the last six years. Our literature search identified 25 relevant papers. Based on how sensitive information is protected from shoulder-surfing attacks, we divided the existing methods into three categories: text modification-based, gesture-based, and external tool-based.

Text Modification-based Methods

The main goal of text modification-based methods is to modify the text displayed on the screen of a user’s device (e.g., hiding the content, changing the text to a handwriting font) to decrease the ability of an observer to comprehend the content displayed on the screen. Various techniques have been proposed for altering text, including text shuffling (Figure 1(a)) (Kim et al. 2015), Crystallize Filter (Farzand et al. 2021), and Selective Showing (Figure 1(b)) (Zhou et al. 2015).

The text-shuffling method rearranges the letters in each word at various positions, making it difficult for an observer to recognize words properly. Crystallize Filter utilizes a crystallizing filter to hide the content on the screen of a smartphone when someone is detected through the front-facing camera. Selective Showing relies on the user's cursor movement to display the content that falls within the cursor's spot

while dimming the rest of the screen. My Scrawl Hide It All is a text-modifying method that changes the font of the displayed text to a user's handwriting font. However, researchers have found that text modification-based methods can interrupt a user's workflow, provide an incomplete view of content, increase browsing time, and potentially reveal sensitive information. As a result, these methods may be ineffective and have limited usability. Additionally, unfamiliar handwriting can make reading challenging, and users must upload their handwriting into the system for recognition. These limitations could hinder the adoption of such methods.

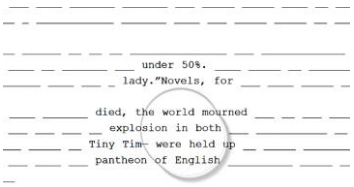


(a) The shuffling-text-method

(b) Selective showing method

Figure 1. Text modification-based methods

(a) EyeSpot method



(b) Private Reader method

Figure 2. Eye-tracking methods

Gesture-Based Methods

Gesture-based methods protect sensitive information by using hand gestures to represent commands that the methods can recognize and respond. For example, "Moving the Content" (Brudy et al. 2016) is a technique that can minimize and hide all on-screen content, including the user's own view, from sight. Similarly, PrivacyShield (Pushp et al. 2018) uses a hand gesture to hide all running content on a device screen. However, gesture-based methods have drawbacks. They require explicit hand movements, which can be inconvenient and restrict a user's hand movements when necessary. Additionally, reorganizing or hiding windows can disrupt a user's workflow and prevent content navigation. Another potential issue is that users may not use hand gestures if they are unaware of the presence of a shoulder surfer nearby, which could limit the effectiveness of the methods.

External Tool-based Methods

External tools, such as eye-tracking devices, have been used to protect sensitive information. For example, Eyespot (Figure 2(a)) (Khamis et al. 2018) and Private Reader (Figure 2(b)) (Ragozin et al. 2019) display only the content at a specific spot on a device screen based on the user's gaze while using overlaid masks to hide the rest of the content. Eyespot offers three different masks, including Crystallize, Fake Text, and Blackout, which apply different filters to the area surrounding the user's gaze, such as replacing it with fake text or a chat bubble filter. However, external tool-based methods can impose a high cognitive workload on users as they need to move their gaze to different positions on the screen, potentially exposing sensitive information to attackers. Additionally, mobile-based eye-tracking may be inaccurate and not able to capture the exact location of the user's gaze due to technological limitations. Eyespot users must hold the device in front of their faces so that their gaze can be accurately captured. These techniques require users to know how to use them or differentiate between real and fake text, which can be confusing and reduces the effectiveness of these methods.

In sum, although prior studies have proposed various solutions for protecting sensitive information from shoulder surfing, they all have limitations. First, many existing methods are ineffective or insufficient in protecting sensitive information. This happens because those methods do not distinguish between sensitive and non-sensitive information, making it easy for attackers to access screen content, regardless of whether a method is based on a user's gaze or cursor. Second, the current methods tend to have complicated designs and incur high cognitive workload. For example, some methods (Kim et al. 2015; Ragozin et al. 2019) may be overly complex and require significant time and effort to complete tasks involving text shuffling or eye tracking. Additionally, while mobile devices can use front-facing cameras

for eye tracking, the techniques can be imprecise and time-consuming in capturing a user's gaze on the screen. Third, numerous methods (Khamis et al. 2018; Kim et al. 2015) incur a high cognitive workload and impose a learning curve for users to become familiar with the procedure.

Description of the Proposed Method

Theoretical Foundation

Coding theory, which was proposed by Shannon (Shannon 1948), entails encoding data into various symbols so that when an individual uses a code to send a message or to access information, only specific people can read it. It involves the use of cryptographic techniques to ensure that breaking the code without additional data is difficult. Codes are applied when the information or data are intended to be kept secret.

Design of D&L

There is often a tradeoff between the security and usability of a system (Zhou et al. 2016). The rationale of the D&L design in this study is to allow users to interact with their devices effectively and efficiently while protecting user privacy without sacrificing usability. Specifically, we aim to protect sensitive information from shoulder surfers without obstructing content browsing significantly. The design of D&L is guided by coding theory by encoding information in such a way that sensitive information can be hidden from view while non-sensitive information can be displayed normally. This is critical in situations where it is important to protect sensitive information from shoulder surfing attacks.

When designing the D&L method, we considered six design principles. First, design should address the problem of hidden screen content that many previous studies have identified (Ragozin et al. 2019; Zhou et al. 2015). Making all or part of content completely inaccessible would disrupt a user's content browsing and workflow. Second, D&L should minimize the user's cognitive workload (Kim et al. 2015). Third, it should present a solution that enables a user to interact with a device easily (Ragozin et al. 2019). Fourth, it should not require users to make any body movement, nor require extra hardware or tools (Pushp et al. 2018). Fifth, it should effectively protect sensitive information from shoulder surfing at all angles. Sixth, it should be usable at any place (Khamis et al. 2018).

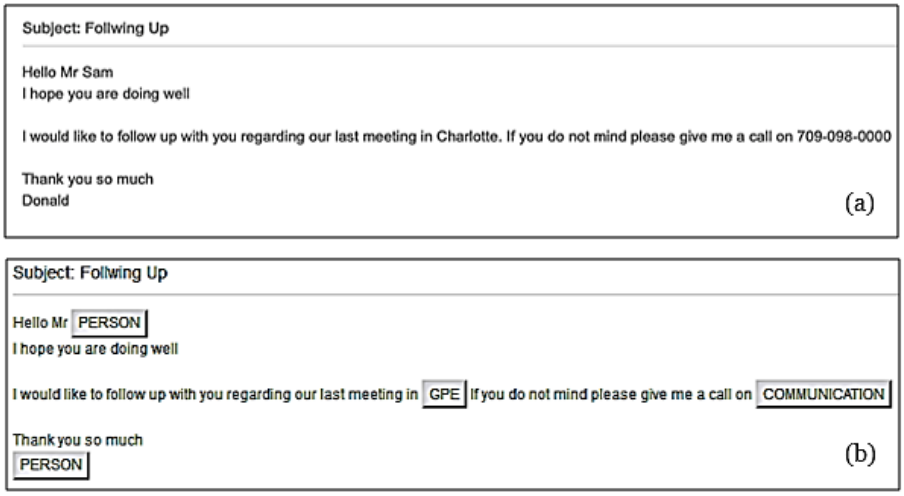


Figure 3. The graphical user interface of the D&L method (a) The original content with no protection; (b) The content protected by D&L

By following the above design principles, D&L detects sensitive information in textual content and replaces it with a category label automatically (Figure 3 (b)). The replaced sensitive content will be read to the user through headphones when he or she clicks the label.

The D&L method incorporates several advanced techniques, including sensitive information detection, labeling, and speech synthesis. Sensitive information detection from text is a process in which an algorithm takes a string of text as input and separates it into smaller components based on certain rules. D&L employs a set of rules to accurately identify various components within a text. For instance, it identifies any sequence of 10 digits with common patterns as a phone number. Similarly, it identifies any sequence with a nine-digit pattern as a social security number; any sequence containing the symbol "@" and end with '.com', '.edu', etc. as a form of email. In addition, any sequence containing a combination of numbers, letters, and digits, such as 14$&L, as private data. These different types of sensitive information were adopted from prior research studies (Ahmed et al. 2021; Cloos et al. 2019). To further improve its accuracy, D&L incorporates the SpaCy model (SpaCy 2021), which processes a given string of text and effectively identifies nouns referring to people, places, or organizations. Then, a parsing function masks these nouns with the appropriate category name. Finally, when the user clicks on a label, a speech-synthesis API will read out the hidden sensitive information to the user through his headphone. The speech-synthesis API converts this written information into aural information. After confirming that the user's headphone is connected to the device, D&L delivers the hidden information through the headphone. If the headphone is not connected to the user's device, a reminder will be shown on the screen asking the user to connect them.

Evaluation

A controlled laboratory experiment with a 3 × 2 × 2 within-subjects factorial design was conducted to evaluate the efficacy and usability of D&L. The independent variables were the two types of roles (user and attacker), two shoulder surfing positions (right and left), and three browsing methods (browsing without protection, browsing with selective showing, and browsing with D&L).

Participants

72 participants who met the study's inclusion criteria were included in the experiment. They had previously used a laptop to access emails in public venues and were recruited from a public university on the east coast of the U.S. Among them, 45 were male. 48 were undergraduate or graduate students, and 24 were university employees. Among the participants, 22 were aged between 18–20 years old, 17 were 21–25, 11 were 36–30, nine were 31–35, seven were 36–40, and 6 were older than 40. All 72 participants played the role of a user, while 62 of them also took on the role of an attacker. To incentivize participation in the study, each participant was provided with a $10 Amazon gift card at the end of the study. A random draw was conducted at the end of the study to encourage participants to fully engage with the experimental tasks seriously. To motivate participants to complete the experimental tasks and take them seriously, a random draw was held at the end of the study. Those who answered all the questionnaire questions properly, including the check questions, were eligible to enter the draw. Four participants were randomly chosen to receive an extra $25 Amazon gift card each for their effort.

Browsing methods

Three browsing methods were used: normal browsing without protection, selective showing, and D&L. Normal browsing refers to browsing content without any protection mechanism. We chose the selective showing method as a baseline primarily because D&L is a text-modification based method as well. In addition, selective showing is not complex and easy to implement. On the other hand, considering that external tool-based and gesture-based methods have some major limitations, such as requiring additional hardware/software or hand movements, which not only require more participant training, but also bring confounding factors. Therefore, we excluded external tool-based methods and gesture-based methods from this study.

Apparatus

A D&L prototype was developed using Python programming language on a MacBook Pro. The laptop was equipped with 16 GB of RAM, an Apple M1 processor, and a 13.3-inch display running MacOS Monterey. The same laptop was used by all the participants in the experiments.

Experimental task

The participants were asked to browse six emails displayed on the MacBook Pro one by one without using the keyboard to search for any words or to return to previous emails. They were required to read the whole content of two different emails with each of the three browsing methods. The order of the methods was randomized and balanced. The emails contained 120 words on average and two pieces of sensitive information per email, adapted from a corpus dataset (Tatman 2017). All emails were presented in Times New Roman font with a font size of 12. During the experiment, an attacker stood behind the sitting user, either to the left or right of the user, and was asked to look at the laptop screen over the user's shoulder and obtain sensitive information. After browsing a pair of emails using one method, both the user and attacker filled out a form with two multiple-choice questions about the sensitive information that they had read or memorized from the previous emails. The user then filled out a questionnaire about their experience with the browsing method, including ease of use, effectiveness, and satisfaction, as well as a NASA Task Load Index questionnaire using a 7-point scales.

Procedure

Prior to the formal experiment, the participants completed a pre-questionnaire about their email browsing frequency and concerns about shoulder-surfing attacks with 7-point Likert scales. After obtaining informed consent, participants were given a training session to familiarize themselves with the browsing methods and with the D&L and selective showing methods. Then, each participant was assigned a role (user or attacker) and remained in their position till the end of the experiment. The setup involved an attacker positioned at a 45° angle standing behind the sitting user, randomly assigned to either the left or right side. The distance between the attacker and the user's screen was 120 cm, and the distance between the user and the laptop screen was 45 cm. These positions were adopted from previous shoulder-surfing studies (Aviv et al. 2018; Saad et al. 2018). Afterwards, participants were required to complete the tasks explained in Section 'Experimental Tasks'. In the second session, which was essentially the same as the first except involving different email content, the participants switched roles. All participants completed the required forms independently, ensuring that there were no external influences on the study's outcomes.

The study design was reviewed and approved by the Office of Research Protections and Integrity of the authors' university (under IRB number 25-5955).

Dependent Variables

The dependent variables include accuracy of sensitive information recognition, perceived cognitive workload, browsing speed, and user perception.

1) Accuracy of sensitive information recognition
To make it consistent and comparable with previous studies (Abrar et al. 2014; Khamis et al. 2018), this variable measures the accuracy of sensitive information recognition through two multiple-choice questions that ask participants to recognize sensitive information obtained or remembered from previous emails. Correct answers were scored 0.50, while incorrect answers were scored 0. If the participant answered both questions correctly, they received a full score of 1 out of 1. The final score for each method was calculated by averaging the scores for all participants.

2) Perceived cognitive workload
This variable was measured using the NASA–TLX, a multi-dimensional scale measuring perceived workload and overall performance of completing the task (Lai 2016).

3) Browsing speed
A user's browsing speed was measured by the time duration between the time when a user pressed the "display email" button to starting browsing an email and the time when he/she pressed the "move on" button. To ensure accuracy of the collected data, the primary investigator observed the participants scrolling to the bottom of the page and monitored their scrolling position to make sure that they had read each email rather than just skimming the content.

4) User perception
The post-experiment survey assessed user perception through three variables: perceived ease of use, perceived effectiveness, and overall satisfaction with each method. These questions were adapted from the IBM post-study system usability questionnaire (Gore and Kim 2020). To ensure the quality of the responses, the survey was designed with established quality assurance methods, including attention check questions. We evaluated users' perceptions of all three methods through a questionnaire that consisted of items based on 7-point Likert scales (1 = totally disagree, 4 = neutral, and 7 = totally agree). For example, we assessed users' perceptions of the D&L method with regard to perceived ease of use using the following items: "I am satisfied with the simplicity of the D&L method."; "Using the D&L method was simple."; and "Learning to use the D&L method was easy." Additionally, we measured perceived effectiveness using the items "I could accomplish the designated tasks using the D&L method" and "I could complete the designated tasks efficiently using the D&L method." Finally, we measured overall satisfaction with the item "I am satisfied with the D&L method." Likewise, we used the same questionnaire items to evaluate users' perceptions of the other two methods.

Results

Responses to the Pre-experiment Questionnaire

According to the pre-experiment questionnaire, all participants reported that they had used a laptop in public for browsing. 93% of those surveyed either totally agreed or partially agreed that browsing sensitive information on a device in a public venue would raise their privacy concerns. Additionally, most respondents (68%) indicated that they could not hide sensitive information on their screens without assistive technology. In the meantime, some participants (28%) claimed that they could protect sensitive information on their laptop screen without assistive technology. When asked how, those participants responded that they used traditional methods, such as turning their device in a different direction, moving their body closer to the screen to cover it, or walking away from potential attackers.

Initially, we conducted a one-way ANOVA to examine the effects of browsing methods on sensitive information recognition for both users and attackers. Additionally, we assessed the impact of browsing methods on cognitive workload, the browsing speed, and user perception for users. Then, we conducted a post hoc Tukey test on each of these dependent variables to determine the differences in performance measures and participants' perceptions among the three browsing methods.

Sensitive Information Recognized by Attackers

The results of ANOVA showed that the effect of browsing method on the accuracy of sensitive information recognition was statistically significant ($F [2, 183] = 159.758$, $p = .001$). Table 3 shows the results of the post hoc Tukey test, which revealed that attackers recognized significantly less sensitive information when using D&L compared to using normal browsing and selective showing methods ($p < 0.01$), implying that D&L can better protect sensitive information from shoulder surfers than the other two browsing methods.

Sensitive Information Recognized by Users

The results of ANOVA indicated that the effect of browsing method on recognition of sensitive information was statistically significant ($F [2, 213] = 3.801$, $p = .024$). The post hoc LSD test results, as shown in Table 4, revealed that users recognized the least amount of sensitive information when using selective showing. No significant differences were found between normal browsing and D&L, suggesting that D&L did not negatively impact a user's ability to access sensitive information when browsing.

Table 1. Accuracy of sensitive information recognized by attackers (0~1)

Browsing Methods	Mean	Std. Dev.
Normal browsing	0.911	0.192
Selective showing	0.629	0.349
D&L	0.096	0.199

Table 2. Accuracy of sensitive information recognized by users (0~1)

Browsing Methods	Mean	Std. Dev.
Normal browsing	0.944	0.158
Selective showing	0.861	0.240
D&L	0.930	0.174

Table 3. Pair-Comparisons of sensitive information recognized by attackers

(I) Browsing Method	(J) Browsing Method	Mean Difference (I-J)	Std. Error	Sig.
D&L	Normal browsing	-.8145*	.0462	.000
	Selective showing	-.5323*	.0462	.000

Table 4. Pair-Comparisons of sensitive information recognized by users

(I) Browsing Method	(J) Browsing Method	Mean Difference (I-J)	Std. Error	Sig.
D&L	Normal browsing	-.0139	.0323	.668
	Selective showing	.0694*	.0323	.033

Table 5. Mean values of variables for three browsing methods (from users only)

Variables	Browsing Methods	Mean	Std. Dev.
Cognitive workload	Normal browsing	2.588	0.677
	Selective showing	4.041	0.973
	D&L	3.005	0.737
Browsing speed (in seconds)	Normal browsing	28.527 sec	3.011
	Selective showing	56.416 sec	6.458
	D&L	37.263 sec	5.5156
Perceived ease of use	Normal browsing	5.810	0.996
	Selective showing	3.897	1.330
	D&L	5.092	1.301
Perceived effectiveness	Normal browsing	5.944	0.966
	Selective showing	3.736	1.406
	D&L	5.259	1.406
Satisfaction	Normal browsing	5.240	0.813
	Selective showing	3.740	1.311
	D&L	5.690	1.229

Table 6. Pairwise Comparisons of Dependent Variables among Browsing Methods (Users)

Variables	(I) Browsing Method	(J) Browsing Method	Mean Difference (I-J)	Std. Error	Sig.
Cognitive workload	D&L	Normal browsing	.4165	.1343	.006
		Selective showing	-1.036	.1343	.000
Browsing speed (in seconds)	D&L	Normal browsing	8.736	.8671	.000
		Selective showing	-19.152	.8671	.000
Perceived ease of use	D&L	Normal browsing	-.7174*	.2031	.001
		Selective showing	1.1953*	.2031	.000
Perceived effectiveness	D&L	Normal browsing	-.6980*	.2128	.004
		Selective showing	1.5104*	.2128	.000
Satisfaction	D&L	Normal browsing	.460	.190	.044
		Selective showing	1.960	.190	.001

Browsing Speed

The ANOVA results showed a significant impact of browsing method on users' browsing speed (F [2, 213] = 541.281, p = .001). The Tukey test results (Table 6) revealed that the "user" participants finished reading the emails with the least time when they used normal browsing, followed by D&L, which was faster than selective showing, as confirmed by Table 5.

Cognitive Workload

The ANOVA results indicated a significant impact of browsing method on cognitive load (F [2, 213] =40.303, p = .001). The Tukey test results (Table 6) showed that normal browsing resulted in the lowest perceived cognitive workload, followed by D&L, which was lower than selective showing,

User Perceptions

The results of the ANOVA revealed a significant impact of browsing method on participants' perceived ease of use (F [2, 213] = 45.242, p = .001), perceived effectiveness (F [2, 213] = 54.398, p = .001), and overall satisfaction (F [2, 213] = 58.246, p = .001). According to the Tukey test results (Table 6), users rated normal browsing as the easiest, followed by D&L, with selective showing being the most difficult. Additionally, D&L was perceived as the most effective and satisfying browsing method.

Discussion

The study discovered that using D&L for browsing content on a laptop provides greater protection of sensitive information against shoulder-surfing attacks than normal browsing and selective showing because it does not display sensitive information on the laptop screen. Table 1 shows that D&L is the most effective method for protecting sensitive information from attackers. It protects sensitive information against attackers better while not hindering users from recognizing sensitive information. Furthermore, we did not find any significant relationship between the attackers' ability to recognize sensitive information and their educational background, gender, or age group.

The results of the Least Significant Difference (LSD) test, presented in Table 4, indicate a significant p-value, suggesting that users are able to recall less sensitive information when using the selective showing method, as corroborated by Table 2. Nevertheless, the study found that D&L does not negatively impact browsing speed, as users using D&L had faster browsing speeds than those using selective showing. While normal browsing was the fastest method, D&L automatically hides and labels sensitive information, making it easier for users to navigate without learning new techniques or performing additional gestures. As a result, users found D&L to be more user-friendly than selective showing. These results confirm that the automatic detection and labeling features of D&L make it an effective, easy-to-use, and satisfying browsing method for end-users. D&L improves protection, enhances usability, reduces cognitive workload, and maintains browsing speed compared to the selective showing method. This is the first method to use NLP techniques for this purpose, and this research advances our understanding of privacy protection when using laptops in public venues.

Theoretical and Practical Implications

The D&L method has theoretical implications, demonstrating the potential of NLP in enhancing data privacy and security in contexts where sensitive information is present in the text. Automating the detection and labeling processes reduces the likelihood of human errors and increases the efficiency of protecting sensitive information. D&L's ability to reduce users' cognitive workload and improve browsing speed may facilitate more efficient and effective engagement with sensitive information. Furthermore, this research has practical implications for protecting sensitive information on smart devices. D&L can be applied for this purpose, providing benefits for individuals and companies in sensitive sectors such as government, finance, and healthcare. D&L reduces the risk of unauthorized viewing and improves accessibility for visually impaired users through audio transmission. Social media platforms can also utilize these findings to enhance their privacy protection features.

Limitations and Future Work

This research has limitations that offer future research opportunities. The study's participants may not be representative of the general population, although the sample size was larger than that of some other similar studies (Khamis et al. 2018; Ragozin et al. 2019). Future research opportunities include developing a customized version of D&L tailored to the sensitivity level of information that users want to protect, and exploring methods for protecting image-based content by analyzing image sensitivity.

Acknowledgements

This work was partly supported by the National Science Foundation (Award #: CNS 1917537) and the School of Data Science at UNC Charlotte. Any opinions, findings, and conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the above funding agency.

REFERENCES

Abrar, U., Hannan, X., Trevor, B., and Mariana, L. 2014. "Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations," in: *International Conference for Internet Technology and Secured Transactions*. London, UK: IEEE, pp. 302-308.

Ahmed, H., Traore, I., Saad, S., and Mamun, M. 2021. "Automated Detection of Unstructured Context-Dependent Sensitive Information Using Deep Learning," *Internet of Things* (16), p. 100444.

Aviv, A. J., Wolf, F., and Kuber, R. 2018. "Comparing Video Based Shoulder Surfing with Live Simulation," in: *Proceedings of the 34th annual computer security applications conference*. San Juan, PR, USA.

Binbeshr, F., Kiah, M., Por, L. Y., and Zaidan, A. A. 2021. "A Systematic Review of Pin-Entry Methods Resistant to Shoulder-Surfing Attacks," *Computers & Security* (101), p. 102116.

Brudy, F., Ledo, D., Greenberg, S., and Butz, A. 2016. "Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays through Awareness and Protection," in: *Proceedings of The International Symposium on Pervasive Displays*. Copenhagen, Denmark: Association for Computing Machinery, pp. 1-6.

Buzzard, J. 2022. "Identity Fraud Study: The Virtual Battleground." United States: Javelin strategy, p. 64.

Cloos, J., Frank, r., Kampenhuber, L., Karam, S., Luong, N., Monge-Larrain, M., Dat, N. T., and Nilgen, M. 2019. "Is Your Privacy for Sale? An Experiment on the Willingness to Reveal Sensitive Information," *Games*).

Deepak, S. A., Naresh, K. N., and Pradeep, S. 2022. "Exploring the Effectiveness of Word Embedding Based Deep Learning Model for Improving Email Classification," *Data Technologies and Applications* (56), p. 23.

Farzand, H., Bhardwaj, K., Marky, K., and Khamis, M. 2021. "The Interplay between Personal Relationships & Shoulder Surfing Mitigation," in: *Proceedings of Mensch und Computer*. Ingolstadt, Germany.

Federica, L. 2022. "Forecast Number of Mobile Devices Worldwide from 2020 to 2025," Statista Research.

Khamis, M., Eiband, M., Zürn, M., and Hussmann, H. 2018. "Eyespot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing," *Multimodal Technologies and Interaction* (2:3), p. 45.

Lai, J. 2016. "Thumb-Based Approaches to Target Acquisition, Zooming, and Text Entry in Single-Handed Interaction with Mobile Phones." ProQuest Dissertations: University of Maryland, Baltimore County.

Ponemon, I. 2017. "Public Spaces Survey Study," Ponemon Institute LLC, p. 17.

Pushp, S., Liu, Y., Xu, M., Koh, C., and Song, J. 2018. "Privacyshield: A Mobile System for Supporting Subtle Just-in-Time Privacy Provisioning through Off-Screen-Based Touch Gestures," *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (2:2), pp. 1-38.

Ragozin, K., Pai, Y. S., Augereau, O., Kise, K., Kerdels, J., and Kunze, K. 2019. "Private Reader: Using Eye Tracking to Improve Reading Privacy in Public Spaces," in: *International Conference on Human-Computer Interaction with Mobile Devices and Services*. Taipei, Taiwan: Association for Computing Machinery, pp. 1-6.

Shannon, C. E. 1948. "A Mathematical Theory of Communication," *The Bell System Technical Journal* (27:3).

Tatman, R. 2017. "Fraudulent E-Mail Corpus (Clair Collection of "Nigerian" Fraud Emails)." Kaggle.

Zhou, H., Ferreira, V., Alves, T., Hawkey, K., and Reilly, D. 2015. "Somebody Is Peeking! A Proximity and Privacy Aware Tablet Interface," in: *Conference on Human Factors in Computing Systems* Seoul, Republic of Korea: Association for Computing Machinery, pp. 1971-1976.

Zhou, L., Yin, K., Dongsong, Z., and Jianwei, L. 2016. "Harmonized Authentication Based on Thumbstroke Dynamics on Touch Screen Mobile Phones," *Decision Support Systems* (92).