# THE USE OF TEXT RECOGNITION, LIP READING, AND OBJECT DETECTION FOR PROTECTING SENSITIVE INFORMATION FROM SHOULDER SURFING ATTACKS

by

Marran Aldossari

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2023

Approved by:

_____
Dr. Dongsong Zhang

_____
Dr. Lina Zhou

_____
Dr. Weichao Wang

_____
Dr. Richard G. Lambert

# ABSTRACT

MARRAN ALDOSSARI. The Use of Text Recognition, Lip Reading, and Object Detection for Protecting Sensitive Information from Shoulder Surfing Attacks
(Under the direction of DR. DONGSONG ZHANG)

The portability and convenience of laptops have propelled their use in public venues. However, the risk of unauthorized view of sensitive information displayed on these devices, including business data, emails, banking information, online trading information, and private chats, raises privacy concerns. In particular, shoulder-surfing attacks pose a significant threat, whereby individuals can steal sensitive information by looking over one's shoulder. While researchers have developed various approaches to protect users' screens, such as text modification-based, gesture-based, and external tool-based, those methods have limitations in terms of effectiveness, protection, and usability. To address these limitations, this dissertation proposes, develops, and evaluates three novel methods for protecting sensitive information from shoulder-surfing attacks: detection and labeling (D&L), recognizing and labeling sensitive information in text entry (RLSITE), and "someone is close" (SIC). D&L is a method designed to protect sensitive information while browsing. It works by recognizing and labeling sensitive information in text entry and replacing it with a category label. The labeled and hidden sensitive information is then read to users through their headphones when they click the label. RLSITE is a method designed to protect sensitive information while typing. It works by automatically capturing and interpreting users' lip movements of the sensitive information, then replacing it with a category label and reading it to users through their headphones when they click the label. Finally, the SIC method automatically detects whether someone is close to a user. If so, it will alert the user while labeling the sensitive information and reading it to users through their headphones. The proposed methods have been empirically evaluated in controlled laboratory settings using various measures,

including usability, effectiveness, and protection. Evaluation results demonstrate that D&L, RLSITE, and SIC outperform baseline methods in all measures. Furthermore, these innovations have significant practical implications, making them more resistant to shoulder-surfing attacks to browse or enter sensitive content on devices without compromising the usability of these devices.

## ACKNOWLEDGMENTS

I would like to extend my deepest gratitude to my respected supervisor, Prof. Dongsong Zhang, for his invaluable guidance, support, and mentorship throughout my Ph.D. journey. His extensive knowledge and vast experience have undoubtedly influenced my research and constructively guided my work. In addition, Prof. Zhang has provided step-by-step directions throughout my research and has always been available to help when needed. I am honored to have had the opportunity to learn from his remarkable knowledge and expertise, which will undoubtedly shape my career.

I would also like to express my appreciation to my dissertation committee members, Dr. Lina Zhou, Dr. Chao Wang, and Dr. Richard Lambert, for their thoughtful and constructive feedback, which greatly enhanced the quality of my research.

Moreover, I extend my sincere gratitude to my parents, Zabin Aldossari and Tarfah Aldossari, for their love, encouragement, and unwavering support throughout my academic journey. Their guidance and support were invaluable, and I am grateful for everything they have done to help me achieve my goals.

I also want to express my heartfelt thanks to my beloved wife, Haya Aldossari, and my sons, Khalid, Rayan, and Abdulelah, for their unwavering support, encouragement, and understanding throughout my Ph.D. journey. Their love and support have been a constant source of motivation and inspiration for me.

Furthermore, I am grateful to my friends and colleagues in the KAIM research group, whose assistance was invaluable in conducting my experimental studies. Their support and encouragement were crucial to the success of my research. Furthermore, I would like to express

my gratitude to my esteemed colleagues, Dr. Mohammed Alziyadi and Dr. Louai Mohammed, for their unwavering support and encouragement during the course of my Ph.D. program.

Finally, I would like to thank my sisters and brothers for their encouragement and support throughout my Ph.D. journey. Their words of wisdom and encouragement helped me stay motivated and focused during challenging times.

Finally, I extend my special thanks to Shaqra University and the Kingdom of Saudi Arabia for providing me with the opportunity to pursue my Ph.D. and for their support throughout my academic journey.

## TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1: INTRODUCTION

## 1.1 Dissertation Motivation

According to Statista, there were more than 15.96 billion portable devices worldwide in 2022 [1]. 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 for many people.

Sending and receiving emails on a laptop are ubiquitous, with many people checking and responding to their emails multiple times throughout a day. It was reported that in 2017, 269 billion emails were sent daily worldwide, and this number is expected to reach 376.4 billion by 2025 [2]. By the end of 2019, more than 3.9 billion users—more than half of the global population—were active email users [3, 4].

Many people use a laptop for work and to browse the internet, but browsing or typing sensitive content in public spaces can entail risks to privacy and information security. Sensitive information is defined as information that must be kept secure from unauthorized access to maintain an individual's privacy [5, 6]. A laptop may contain considerable sensitive information that must be protected from unauthorized viewing. The main privacy challenge when browsing or typing sensitive information on a laptop in a public place is shoulder-surfing attacks, which encompass "behavior where people covertly observe somebody else's screen of those people's electronic devices" [7, p 408]. Shoulder surfing can enable an attacker to illegally obtain sensitive information from a victim's screen.

In the modern world, the upsurge in demand for large-screen tablets has resulted in a significant increase in shoulder-surfing incidents, which pose a risk to the privacy and

confidentiality of the information displayed on these portable devices. Shoulder surfing is not restricted to observing passwords when they are entered. According to the Ponemon Institute [12], there is a risk of shoulder-surfing attacks in public places where sensitive information is visible on laptops and tablets. Researchers at the Ponemon Institute found that 41 out of 45 attackers (91%) obtained sensitive information from users' screens. A total of 53% of this information, such as SSN, personal and employee data, and financial information, was deemed sensitive. In a recent study from New York University, 73% of survey respondents indicated that they had obtained sensitive information from others without their knowledge [8]. Over the past few years, shoulder-surfing attacks have become a serious problem, especially for identity theft, with adverse consequences for millions of people and companies worldwide [9].

Shoulder-surfing attacks are among the most common methods that attackers use for identity theft. A recent report on identity fraud losses involving any use of a consumer's sensitive information amounted to $56 billion in 2020 and involved 15 million U.S. consumers [10, 11]. Financial losses rose 77% from the previous year to more than $6.1 billion [12], emphasizing the importance of vigilantly protecting personal information, particularly in public places. This cost is expected to increase annually, as attackers find new ways of exploiting vulnerabilities in individuals. Shoulder surfing is considered identity theft and fraud in the United States and can be sentenced for up to 15 years in prison [13].

In response to this trend, several solutions have been proposed to protect the textual content displayed on mobile phones, tablets, and laptops from shoulder-surfing attacks. These solutions can be divided into three types based on their approach: text modification-based, gesture-based, and external tool-based. Text-modification methods [14, 15] are designed to protect text from shoulder surfers by rearranging the letters in each word displayed on the screen at various

positions, making the text difficult to interpret. However, researchers have found it ineffective to protect sensitive information because attackers can still recognize the modified text. These techniques also impose a high cognitive workload on users due to the need to rearrange words. Gesture-based methods [14, 16-21] display or hide content, depending on the user's hand movements, but it is slow to recognize gestures and execute the intended commands. Finally, external tools-based [16, 22-25] can display content on a screen in response to eye tracking, but eye tracking is inaccurate and difficult to deploy.

In summary, although various solutions have been proposed for protecting sensitive information from shoulder-surfing attacks in public venues when users browse or type, they all have limitations, including ineffectiveness or insufficient protection of sensitive information, high cognitive load, and difficult deployment.

## 1.2 Research Questions

The main activities that users typically perform on a laptop are browsing and typing sensitive information. A practical, effective method for browsing and typing sensitive information is necessary to overcome these limitations and prevent the disclosure of sensitive information from shoulder-surfing attacks when users are browsing or typing sensitive information in a public venue. To address these limitations simultaneously, there is a need to develop and deploy more effective methods for protecting sensitive information from shoulder-surfing attacks. This dissertation research proposes three novel methods for protecting user's sensitive information.

The first method is detection and labeling (D&L), which is designed to protect sensitive information while browsing. It works by recognizing and labeling sensitive information in text

entry and replacing it with a category label. The labeled and hidden sensitive information is then read to users through their headphones when they click the label. Accordingly, this dissertation aims to answer the following first research question: **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 second proposed method is recognizing and labeling sensitive information in text entry (RLSITE), which is designed to protect sensitive information while typing. It works by automatically capturing and interpreting users' lip movements of the sensitive information, then replacing it with a category label and reading it to users through their headphones when they click the label. Consequently, this dissertation aims to answer the second research question: **How effective is the RLSITE method for protecting sensitive information against shoulder-surfing attacks when a user is entering sensitive information on a laptop? What is the perceived usability of RLSITE compared to that of the virtual shuffling of letters and normal typing methods?**

The third proposed method is called "Someone is Close" (SIC) for protecting sensitive information. SIC is also designed to protect sensitive information while browsing. It automatically detects whether someone is close to a user within 120 cm. If so, it will alert the user while labeling the sensitive information and reading it to users through their headphones. Therefore, the third research question that this dissertation research aims to answer is: **What is the effectiveness of the face detection method in protecting sensitive information against shoulder-surfing attacks when browsing on a laptop, and what is the perceived usability of the SIC method**

**compared to that of the Moving or Hiding Content method and user-driven detection method?**

The proposed methods for protecting sensitive information while browsing and typing present several advantages over existing solutions. First, D&L method is expected to improve user interactions with devices while protecting sensitive information on screens without compromising usability. In contrast to other methods that hide sensitive information by either shuffling the text or providing the content in one area of the screen without distinguishing between restricted and non-restricted data, D&L method uses automated techniques to hide sensitive information. D&L also eliminates the addition of the cognitive workload, which is a common limitation of many previous methods [23, 26], because it neither shuffles the text nor uses other techniques that require interpretation. D&L can be used in public venues owing to a lack of gesture-activated security methods or external hardware requirements [23, 25, 27, 28]. Second, RLSITE uses lip reading as a primary input method to reduce the vulnerability of sensitive written information. Lip reading methods have been used to identify what users are saying by observing and translating their lip movements. Furthermore, RLSITE avoids the additional cognitive workload [23, 26] because it does not shuffle letters on a virtual keyboard or use augmented reality devices. RLSITE can be utilized in public venues because augmented reality or external hardware tools are unnecessary [23, 25, 27, 28]. Finally, SIC is based on automatic face detection to detect others in close proximity, thus reducing the effort required by users for previous solutions based on users' detection ability or based on gestures [25, 27, 29]. SIC allows users to become more comfortable in their surroundings. Finally, SIC can be applied in public venues because it does not require any gestures that could interrupt the user workflow

## 1.3 Dissertation Outline

This dissertation research aims to answer the research questions and achieve the following goals:

1) The design and development of D&L, which is designed to protect sensitive information while browsing by recognizing and labeling sensitive information in text entries, replacing it with a category label, and reading the labeled information to users through their headphones when they click on the label.
2) The design and development of RLSITE, which is designed to protect sensitive information while typing by automatically capturing and interpreting users' lip movements of sensitive information, replacing it with a category label, and reading it to users through their headphones when they click on the label.
3) The design and development of SIC, which is to protects sensitive information while browsing by automatically detecting whether someone is within 120 cm of the user and alerting them while labeling the sensitive information and reading it to them through their headphones.
4) The empirical evaluation of the effectiveness, efficiency, and usability of the proposed methods, as well as the protection of sensitive information, in a controlled laboratory environment.

The research questions and their corresponding techniques and chapters are presented in the following table.

Table 1. Dissertation Research Questions

| Dissertation Research Questions | Techniques | Chapters |
|---|---|---|
| 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 | D&L | 3 |
| How effective is the RLSITE method for protecting sensitive information against shoulder-surfing attacks when a user is entering sensitive information on a laptop? What is the perceived usability of RLSITE compared to that of the virtually shuffling-letter and normal typing methods? | RLSITE | 4 |
| What is the effectiveness of the face detection method in protecting sensitive information against shoulder-surfing attacks when browsing on a laptop, and what is the perceived usability of the SIC method compared to that of the Moving or Hiding Content method and User-driven detection method? | SIC | 5 |

The remaining structure of the dissertation is organized as follows. In Chapter 2, a comprehensive literature review is presented, along with an overview of the existing methods developed to safeguard sensitive information presented on mobile devices, tablets, and laptops from shoulder surfing attacks. Chapter 3 introduces the proposed D&L method, which involves detecting, labeling, and delivering sensitive information, along with its empirically evaluated results. In Chapter 4, the RLSITE method for typing sensitive information is presented, along with the results of its empirical evaluation. Chapter 5 examines the effectiveness of the SIC method in protecting users from shoulder surfing, and presents the evaluation results. Finally, Chapter 6 summarizes the contributions and discuss the limitations of this research.

# CHAPTER 2: LITERATURE REVIEW

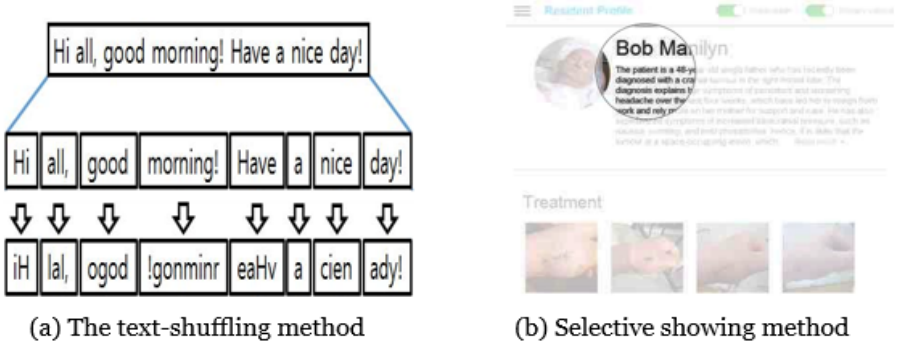
There are two main types of sensitive information: personal and business. Personal sensitive information is defined as any information associated with a specific individual, such as a social security number, the number of a credit card, or a home address. Sensitive business information is any information posing a risk to an organization if released to the public, such as details of a company's financial situation or business decisions. Both types of sensitive information must be protected from shoulder-surfing attacks. A number of 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 when a user logs into his/her device, 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 [30, 31], as text is the primary medium of digital communication.

The literature review focuses on methods of protecting textual content from shoulder surfing when a user is browsing or typing on a mobile device, tablet, or laptop, as opposed to methods of protecting system login credentials (e.g., usernames and passwords). 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*, *Human–Computer Interaction*, and *Computers in Human Behavior*. The searches used multiple keywords, including "shoulder-surfing," "privacy," "usability," "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.

## 2.1 Text Modification-based Methods

This section reviews the existing methods for changing the content displayed on the screen of a user's device, such as changing the text to another format or hiding the content. The main goal of modifying text is to inhibit an observer's ability to comprehend what is displayed on the user's screen [14, 21, 24, 32-35]. Various techniques have been proposed for altering text, including text shuffling [14], Crystallize Filter [33], Selective Showing [24], and My Scrawl Hide It All [36].




(a) The text-shuffling method (b) Selective showing method

Fig. 1. Text modification-based methods

The text-shuffling method rearranges the letters in each word at various positions, making it difficult for an observer to recognize the meaning of words. 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 the user's

handwriting. 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 to the system for recognition. These limitations could hinder the adoption of such methods.

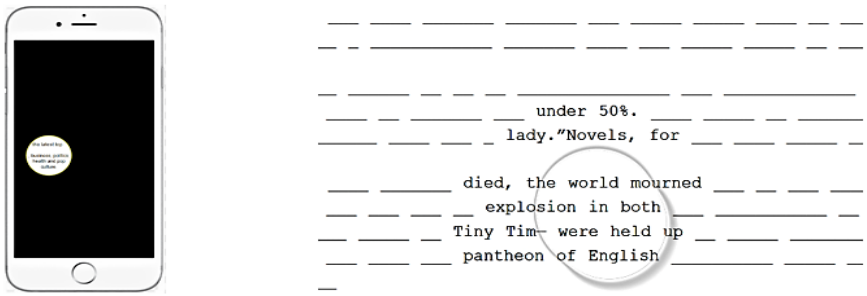
## 2.2 Gesture-Based Methods

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" [16] is a technique that can minimize and hide all on-screen content, including the user's own view, from sight. Similarly, Moving or Hiding Content uses a hand gesture to hide all running content on a device screen [16]. 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.

## 2.3 External Tool-based Methods

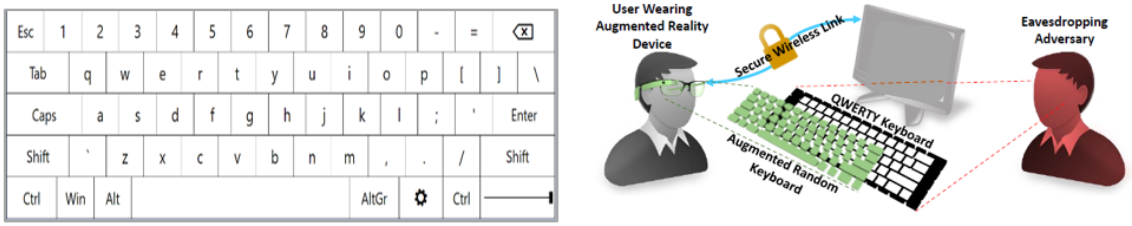
External tools, such as eye-tracking devices, have been used to protect sensitive information. For example, Eyespot (Fig 2(a)) [37] and Private Reader (Fig 2(b)) [22] display only the content at a specific spot on a device screen based on the user's gaze while using overlaid masks to hide

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




(a) EyeSpot method (b) Private Reader method

Fig. 2. Eye-tracking methods




(a) Shuffled-keyboard implementation method (b) Randomized augmented keyboard

Fig. 3. Typing methods

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 unable to capture the exact location of a 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 terms of typing methods, a few techniques and tools are available to enhance security and protect sensitive information. One such a method is the Shuffled-keyboard implementation (Fig 3 (a)), which uses a virtual keyboard that employs a shuffling-letter system. This system shuffles each letter after every keyboard press by the user. Another method is the randomized augmented keyboard (Fig 3(b)), which generates a new keyboard each time the user wants to type using smart glasses. However, using external tools like smart glasses can impose a high cognitive workload on users as they must wear the glasses when they want to type. Additionally, attackers can follow the Shuffled-keyboard implementation to learn what the user typed, reducing the effectiveness of this method. Another limitation of these methods is that users must search for new letter positions every time they type, as the letters change with each keyboard press. This can result in a high cognitive workload and be time-consuming.

Table 2. A Summary of Some Existing Methods for Protecting Sensitive Information from Shoulder-Surfing Attacks

| Approach Name* | | | Method Name | General Description | Sample Studies | Limitations |
|---|---|---|---|---|---|---|
| T | G | E | | | | |
| X | | | Shuffling-Text Method (STM) | It rearranges the letters in each word to make it difficult for an observer to recognize the intended meaning (e.g., “Hi all, good morning!” might become “iH lal, ogod!gonminr”). | [14] | STM may lead to high error rates as rebuilding each word requires extra time and cognitive effort. Additionally, some users may find STM challenging because it is not intuitive. |
| X | | X | My Scrawl Hides It All and CalliScan | It modifies the text displayed on the user’s screen to prevent shoulder-surfing of text messages (e.g., notifications) on mobile devices. | [36, 38] | Reading unfamiliar handwriting takes longer with this method, and users must upload their handwriting for the system to recognize it before it can be used. |
| X | | | DSSYTEM | This application works in the background, periodically taking photos with a front-facing camera equipped with a fish-eye lens to expand the camera's range of view and identify shoulder-surfers. The | [32] | The notifications can be an annoyance because they hide some of the content on the screen. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | system sends awareness signals when a person is discovered near the actual user. | | |
| X | | | Crystallize Filter | This is a mask that uses a crystallizing filter to hide the content on the screen of a smartphone when someone is detected through the front-facing camera. | [33] | Crystallize Filter can make it difficult for both the user and attacker to read the screen's content. This can restrict the user's own interactions with the phone by reducing the usability of the system. |
| X | | | CursorCamouflage | This shows multiple, independently moving dummy cursors on the screen, making it difficult for an attacker to identify which cursor is the one being used. | [34] | Researchers found that the attacker could still identify the real cursor. |
| X | | | Selective-Showing | This offers the option to display the content on the screen in only one position (indicated by the user's movement of the cursor), while hiding the rest of the screen. | [24] | This method can disrupt the user's workflow by presenting an incomplete view, requiring them to move the cursor to view content fully. This could also result in the accidental exposure of sensitive information when it moves into the viewing area. |
| X | | | HideScreen | This uses optical system features to mask on-screen information from shoulder-surfers. This method discretizes the screen into grid patterns to neutralize low-frequency components, allowing the on-screen information to blend into the backdrop outside of the designated range. | [21] | HideScreen is not suitable for reading a long piece of text because it causes readability problems. |
| X | | X | PrivacyScout | This extracts visual features from the attacker's face and uses regression to create a shoulder-surfing risk score, providing a direct measure of the potential risk based on the distance of the attacker from the user. The risk assessment score ranges between zero and three; a higher value means that the user is at higher risk of shoulder-surfing. | [35] | A smartphone only allows information to be captured from the front camera. As users do not usually hold their phone in front of their faces, this technique may yet lead to information disclosure, making it unreliable. |
| | X | X | Hide It All and Moving or Hiding Content | Designed for use in public venues, this recognizes the wave of a user's hand in a given direction as a command to move all content displayed on the screen in that direction. | [16] | Explicit hand movements require extra work, and a user's hand may not be free to make this gesture when required. Moreover, the resulting reorganization (or |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | hiding) of windows can disrupt the user's workflow and hide all content. |
| | X | | PrivacyShield | This application can recognize hand gestures. For example, "For example, if the user swipes his or her hand from bottom to top, this gesture is interpreted as a command to hide all running content. | [17] | Hands movements require extra work, and a user's hand may not be free to make this gesture when required. |
| X | | X | EyeSpot and Private Reader | This displays content only within a circular area on the screen, which follows a user's gaze while using overlaid masks to hide the remainder. | [22, 37] | EyeSpot and Private Reader have usability and navigation issues as the user needs to move masks to different positions, potentially allowing an observer to see the content. Also, mobile-based eye-tracking can be inaccurate and may not capture the exact gaze location due to technological limitations. These methods also expose the content at one point while concealing the rest of the screen, potentially allowing an observer to follow the user's gaze and read the text. |
| | | X | Saturation Laser Attack | This uses lasers to aim colored light beams into a camera, causing it to become saturated and suddenly blind. | [25] | External hardware that must be configured correctly is required for this method. This hardware is unfit for public venues and requires time and effort to recalibrate when a user moves to a new venue. |
| | | X | Human Body and Face Detection (HBFD) | This system relies on face detection and notifies the user when a potentially suspicious person moves near to the user. This is intended to prevent users from encountering a shoulder-surfing attack. | [39] | The notifications can be an annoyance and interrupt user workflow. |
| | X | X | Gaze-Based Typing | A user inputs sensitive information by selecting from an on-screen keyboard using the alignment of their pupils. This technique uses a computer-vision algorithm to determine the position of a user's gaze on a screen. | [27, 40] | An observer would eventually be able to view the content. Moreover, eye-tracking is inaccurate and, for technological reasons, may not capture the exact location of the user's gaze. |

| | | | | | | |
|---|---|---|---|---|---|---|
| X | | | Shuffled-keyboard implementation method | This method uses the shuffling-letters system in which each letter is shuffled after each keyboard press by the user. | [28, 41] | An observer would eventually be able to view the content. Moreover, additional time and cognitive effort are required to look for a new wanted letter. |
| X | | X | Virtual keyboard scheme | The method uses a second level of randomized keys before presenting the hidden keys to the user. | [23, 28, 42] | After the actual keyboard is presented, an observer could see the content, and users need to wait for it, which requires additional time and cognitive effort. |
| | X | X | Pressure Sensitive Stylus | This is a pressure sensor that is detached from an input device and fastened directly to a user's finger to enable pressure values to be entered into a computer, using various devices and in varied locations. | [43] | This method requires external hardware, as well as time and effort to learn how to use it. |
| X | | X | Randomized augmented keyboard | The randomized keyboard method generates a new keyboard every time the user wants to type | [23] | Users are required to find the new position of each letter when they want to type. |

T= Text Modification-based Methods, G= Gesture-Based Methods, and E= External Tool-based Methods

## 2.4 Limitations of the Existing Methods

Although studies have proposed various solutions for reducing the risk of shoulder-surfing attacks in public venues, they all have limitations, including ineffectiveness, insufficient protection of sensitive information, low usability, and high cognitive workload demands. The specific limitations of the existing methods are summarized below.

1) Ineffectiveness or insufficient protection of sensitive information

Several techniques [14, 22, 23, 31, 32, 34, 37, 38, 44] leave sensitive information visible on the screen, making it vulnerable to unauthorized individuals viewing it. These 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. For

example, various researchers [27, 37] have used different layout masks, they have typically reported that attackers can still distinguish sensitive information. In summary, these methods' main limitations are either ineffective at or insufficient for protecting the user's privacy and reducing an attacker's ability to obtain sensitive information from the screen. They either present the screen content in a small area that an attacker can still see, or they hide the whole screen, thus leading to usability problems.

2) Complicated design and high cognitive workload

Users consider many of the existing methods [22, 24, 44] too complicated because they require additional time and effort to accomplish tasks. In some methods [16, 17], users must perform specific gestures, which may not be quickly recognized, or upload their handwriting for recognition, resulting in inefficient browsing. Existing methods can also leave sensitive information vulnerable to attackers and have not been well-designed for distinguishing between restricted and unrestricted data. Although eye tracking using a mobile device's front-facing camera is possible, obstacles remain [37]. Eye-tracking techniques can be inaccurate and may not always recognize the focus of the user's gaze on the screen. Using these inaccurate techniques may lead to revealing information that users wish to hide from attackers. Finally, due to technical and anatomical limitations, mobile eye-tracking devices are often unreliable and do not accurately depict the user's precise gaze position [22]. Numerous methods [14, 35-37] impose a learning curve for users to become familiar with the procedure and spend a substantial amount of time on learning how to use it before they can browse content.

3) Difficulty in deployment

Specific external hardware that must be correctly configured is required for several existing methods [22, 25, 37, 38]. Unfortunately, most systems described in the literature are experimental prototypes that are not yet ready for use in the real world. Additionally, most external hardware is either expensive or unfit for use in public venues and may require time and effort to recalibrate when a user moves to a new venue. An additional problem with gesture-based methods is that they require specific movements from users whose hands might not always be free. They are also slow to recognize hand movements and execute intended commands, meaning that sensitive information might inadvertently be revealed. Eye-tracking systems occupy significant amounts of memory on users' devices, and most require users to maintain a certain distance from the eye-tracking tool, potentially causing inconvenience.

To overcome the limitations of the existing methods mentioned above, this dissertation proposes three novel solutions. The first proposed method, D&L, is designed to protect sensitive information while browsing. It recognizes and labels sensitive information in text entries, replaces it with a category label, and reads the labeled information to users through their headphones when they click on the label.

The second proposed method, RLSITE, is designed to protect sensitive information while typing. It automatically captures and interprets users' lip movements of sensitive information, replaces it with a category label, and reads it to users through their headphones when they click on the label.

The third proposed method, SIC, is an advanced version of D&L that also protects sensitive information while browsing. It automatically detects whether someone is within 120 cm of the

user and alerts them while labeling the sensitive information and reading it to them through their headphones.

All three proposed methods are explained in detail in the following chapters. These novel solutions offer practical and effective ways to protect sensitive information while browsing and typing and aim to provide users with comprehensive protection against shoulder-surfing attacks.

# CHAPTER 3: D&L: A NATURAL LANGUAGE PROCESSING-BASED APPROACH TO PROTECTING SENSITIVE INFORMATION WHILE BROWSING ON LAPTOP SCREENS AGAINST SHOULDER-SURFING ATTACKS

## 3.1 Description of the Proposed Method

### 1) Theoretical Foundation

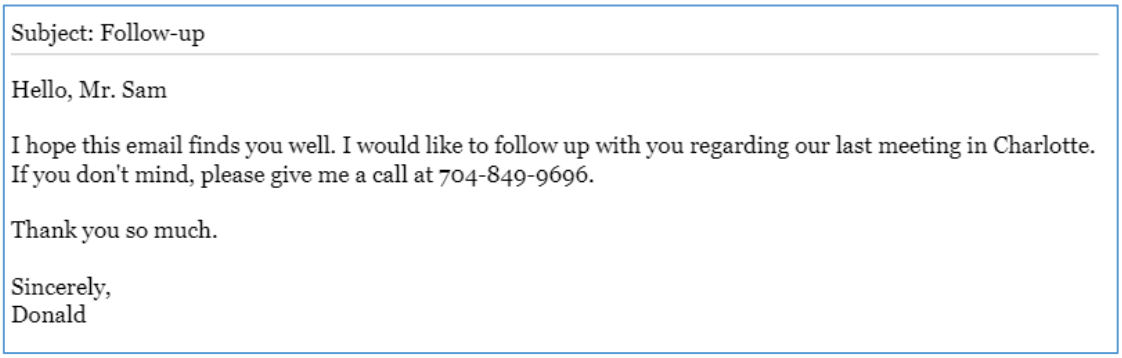
Coding theory, which was proposed by Shannon [45], entails encoding data into various symbols so that when an individual uses a code to send a message or to access information, only specific people can read it. It involves the use of cryptographic techniques to ensure that breaking the code without additional data is difficult. Codes are applied when the information or data are intended to be kept secret.

## 3.2 Design of D&L

There is often a tradeoff between the security and usability of a system [46]. 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 [22, 24]. 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 [14]. Third, it should present a solution that enables a user to interact with a device easily [22]. Fourth, it should not require users to make any body movement, nor require extra hardware or tools [17]. Fifth, it should effectively protect sensitive information from shoulder surfing at all angles. Sixth, it should be usable at any place [37].




(a)


(b)

Fig. 4. The graphical user interface of the D&L method (a) The original content with no protection; (b) The content protected by D&L

Fig 4(a) depicts the original email content with no protection (i.e., in the direct reading or plain mode), in which all sensitive information is visible. By following the above design principles, D&L detects sensitive information in textual content and replaces it with a category label automatically (Fig 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. For instance, it replaced 'Sam' with 'Person', and '704-849-9696' with Communication. Users can click on any label to hear the masked sensitive information through their headphones. The D&L method has the following unique features:

1) It detects most types of sensitive information reported in the literature.
2) It has advanced tools for detecting sensitive information automatically, as text detection by humans is slower.
3) It recognizes the information that has been detected and labels it with a category name to indicate what has been concealed.

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 [47, 48]. To further improve its accuracy, D&L incorporates the SpaCy model [49], 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 headphones are not connected to the user's device, a reminder will be displayed on the screen, prompting the user to connect them. An illustration of this reminder can be seen in the accompanying picture below.

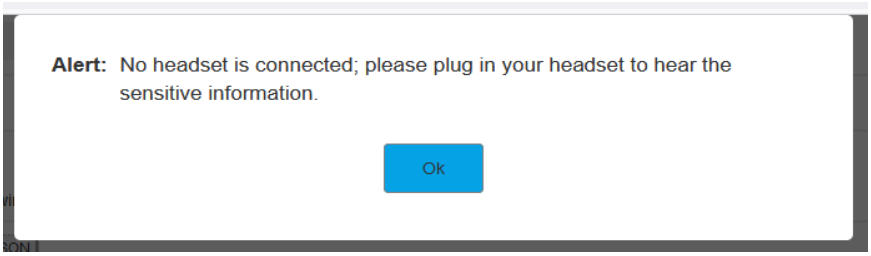



Fig. 5. Message shown if headphone is not connected

## 3.3 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 any protection (i.e., normal browsing), browsing with

selective showing, and browsing with D&L). The normal browsing without protection and selective showing serve as the baseline methods.

### 3.3.1 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.

### 3.3.2 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.

### 3.3.3 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.

### 3.3.4 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 [50]. 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 (see Fig. 6). 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 7-point Likert scales (1 = Extremely Low, 4 = neutral, and 7 = Extremely High).

### 3.3.5 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 [32, 51]. Afterwards, participants were required to complete the tasks explained in Section 'Experimental Tasks'. The figure below provides an overview of the study procedure and tasks.

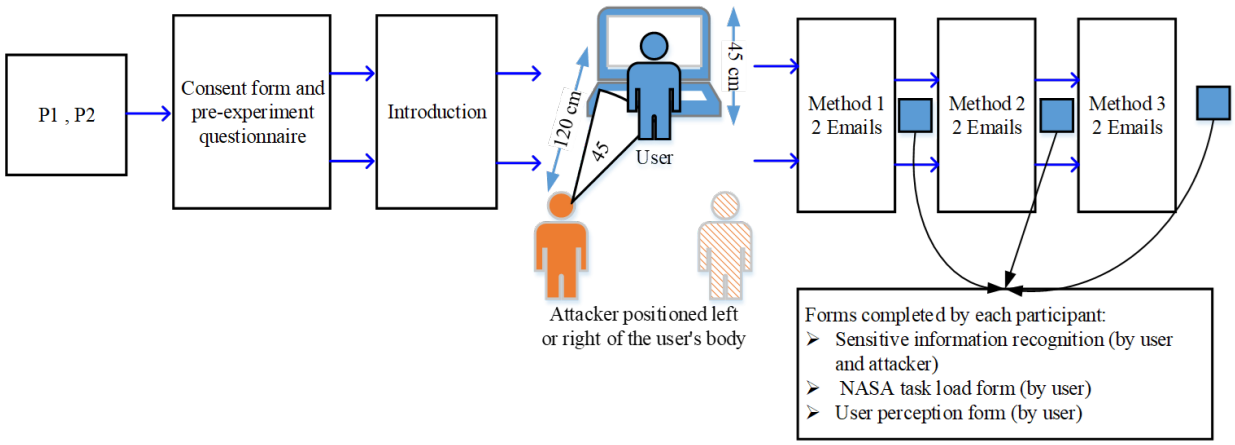



Fig. 6. Study Procedure and Tasks Overview for D&L

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).

### 3.3.6 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 [37, 52], this variable measures the accuracy of sensitive information recognition through two multiple-choice questions that ask participants to recall 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 would receive a 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 multidimensional scales measuring perceived workload (including mental, physical, and temporal demand) and overall performance of completing the task [53].

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

User perception included the variables of perceived ease-of-use, perceived effectiveness, and participants' overall satisfaction with each method. This was assessed using a post-experiment survey consisting of five questions and 7-point Likert scales (1 = totally disagree, 4 = neutral, and 7 = totally agree) (see Table 3). The questions, grouped by these three variables, were adapted from the IBM post-study system usability questionnaire [54], which was initially developed by applying psychometric methods to measure users' satisfaction and subjective assessments of system usability [54]. The following table presents the questionnaire items measuring user perceptions for the D&L method. The same questionnaire items were used to evaluate users' perceptions of the other two methods.

Table 3. Questionnaire Items Measuring User Perceptions for the D&L Method

| Factors | Items based on a 7-point Likert scale (1 = totally disagree, 4 = neutral, and 7 = totally agree) |
|---|---|
| Perceived ease-of-use | Overall, I am satisfied with the simplicity of the D&L method.<br>The D&L method was simple to use.<br>It was easy to learn how to use the D&L method. |
| Perceived effectiveness | I was able to accomplish the tasks using the D&L method. |
| Overall satisfaction | Overall, I am satisfied with the D&L method. |

## 3.4 Results

### 3.4.1 Responses to the Pre-experiment Questionnaire

The responses to the pre-experiment questionnaire provide valuable insights into participants' attitudes towards using laptops in public venues. All participants indicated that they currently use a laptop in public for browsing, and the majority (87.5%) reported browsing emails on their laptops multiple times per day. 94% 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 (72%) 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.

Table 4. Responses to Pre-Experiment Questionnaire on Browsing on Laptops

| Variables | Sub-Variables | Frequency | Percentage (%) |
|---|---|---|---|
| Do you currently use a laptop (e.g., Apple Mac, Dell, HP, or Lenovo)? | Yes | 72 | 100.0 |
| How often do you browse/access personal or work emails on your laptop? | Multiple times per day | 63 | 87.5 |
| | Once a daily | 2 | 2.8 |
| | Weekly | 4 | 5.6 |
| | Monthly | 2 | 2.8 |
| | Once or twice a quarter | 1 | 1.4 |
| | Rarely (once a year or less) | 0 | 0 |
| | Never | 0 | 0 |
| Browsing sensitive information on a laptop device in a public venue entails significant privacy concerns. | Strongly disagree | 1 | 1.4 |
| | Somewhat disagree | 2 | 2.8 |
| | Disagree | 1 | 1.4 |
| | Neither agree nor disagree | 1 | 1.4 |
| | Somewhat agree | 8 | 11.1 |

| | | | |
|---|---|---|---|
| | Agree | 32 | 44.4 |
| | Strongly agree | 28 | 38.9 |
| I can hide my sensitive information on the screen without any assistive technology. | Strongly disagree | 8 | 11.1 |
| | Somewhat disagree | 13 | 18.1 |
| | Disagree | 31 | 43.1 |
| | Neither agree nor disagree | 5 | 6.9 |
| | Somewhat agree | 7 | 9.7 |
| | Agree | 6 | 8.3 |
| | Strongly agree | 2 | 2.8 |
| I can easily read sensitive information on a laptop in a public venue without any privacy concerns. | Strongly disagree | 9 | 12.5 |
| | Somewhat disagree | 15 | 20.8 |
| | Disagree | 33 | 45.8 |
| | Neither agree nor disagree | 4 | 5.6 |
| | Somewhat agree | 3 | 4.2 |
| | Agree | 4 | 5.6 |
| | Strongly agree | 4 | 5.6 |

Finally, the majority of participants (79%) also disagreed or strongly disagreed with the statement that they could easily read sensitive information on their laptop in a public venue without any privacy concerns. These findings suggest that participants are aware of the privacy risks associated with using laptops in public venues, and that they may need additional support or tools to protect their sensitive information.

We first conducted a Kruskal-Wallis test to analyze how browsing methods affect the recognition of sensitive information for both users and attackers. We also evaluated how browsing methods impact cognitive workload, browsing speed, and user perception for users. Afterward, we performed Pairwise Comparisons on each dependent variable to identify any differences between the three browsing methods.

### 3.4.2 Sensitive Information Recognized by Attackers

The summary of attackers' response scores can be found in Table 5. Attackers who answered both questions correctly received a score of "1". Those who answered one question correctly received a score of "0.5". Those who did not answer any questions correctly received a score of "0". Table 6 showed that there was a significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The null hypothesis can be rejected due to the significant p-value ($p < 0.001$). The results of the pairwise comparisons of browsing methods were shown in Table 7. The table indicated that significant differences were observed when attackers used D&L compared to the normal browsing method ($p < 0.001$), as well as when they used D&L compared to selective showing method ($p < 0.001$). Based on the findings, attackers were less able to identify sensitive information when using D&L compared to the normal browsing method and selective showing method ($p < 0.01$). Additionally, Table 8 displayed the mean rank, suggesting that D&L was highly effective in protecting sensitive information from shoulder surfing attacks, as attackers recognized the least amount of sensitive information. In summary, the D&L method demonstrated higher effectiveness in protecting sensitive information against shoulder surfing attacks compared to other methods.

Table 5. Attackers' Response Summary for Browsing Methods

| | | Normal browsing | Selective showing | D&L |
|---|---|---|---|---|
| Correct | 1 | 51 | 25 | 0 |
| | 0.5 | 11 | 28 | 12 |
| Incorrect | 0 | 0 | 9 | 50 |
| Total | | 62 | 62 | 62 |

Table 6. Independent-Samples Kruskal-Wallis Test Summary for Browsing Methods (Results from Attackers' Perspectives)

| | |
|---|---|
| Total N | 186 |
| Test Statistic | 116.515a |
| Degree Of Freedom | 2 |

| Asymptotic Sig.(2-sided test) | .000 |
|---|---|

Table 7. Pairwise Comparisons of Browsing Methods from Attackers' Perspective

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.a |
|---|---|---|---|---|---|
| D&L – Selective showing | 61.976 | 9.067 | 6.835 | .000 | .000 |
| D&L –Normal browsing | 96.589 | 9.067 | 10.653 | .000 | .000 |

Table 8. Mean Rank of Sensitive Information Recognized by Attackers for Different Browsing Methods

| Browsing Method | N | Mean Rank |
|---|---|---|
| Normal browsing | 62 | 137.23 |
| Selective showing | 62 | 102.62 |
| D&L | 62 | 40.65 |

### 3.4.3 Sensitive Information Recognized by Users

The summary of users' response scores can be found in Table 9. Users who answered both questions correctly received a score of "1". Those who answered one question correctly received a score of "0.5". Those who did not answer any questions correctly received a score of "0". Table 10 showed that there was a significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The results of the pairwise comparisons of browsing methods were shown in Table 11. The table indicated that there was a significant differences were observed when users used these methods. Based on the findings, D&L did not negatively impact a user's ability to access sensitive information when browsing. Additionally, Table 12 displayed the mean rank, suggesting that all the methods close to each other which indicated that users were able to recognize the most of the sensitive information regardless of the method that was used.

Table 9. Users' Response Summary for Browsing Methods

| | | Normal browsing | Selective showing | D&L |
|---|---|---|---|---|
| Correct | 1 | 64 | 53 | 62 |
| | 0.5 | 8 | 18 | 10 |
| Incorrect | 0 | 0 | 1 | 0 |
| Total | | 72 | 72 | 72 |

Table 10. Independent-Samples Kruskal-Wallis Test Summary for Browsing Methods (Results from Users' Perspectives)

| | |
|---|---|
| Total N | 216 |
| Test Statistic | 6.842a |
| Degree Of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .033 |

Table 11. Pairwise Comparisons of Browsing Methods from Users' Perspective

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.a |
|---|---|---|---|---|---|
| D&L - Selective showing | -13.694 | 6.801 | -2.014 | .044 | .132 |
| D&L – Normal browsing | 2.986 | 6.801 | .439 | .661 | 1.000 |

Table 12. Mean Rank of Sensitive Information Recognized by users for Different Browsing Methods

| Browsing Method | N | Mean Rank |
|---|---|---|
| Normal browsing | 72 | 115.06 |
| Selective showing | 72 | 98.38 |
| D&L | 72 | 112.07 |

Table 13. 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 14. Pairwise Comparisons of Dependent Variables among Browsing Methods (Users Only)

| 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 |

### 3.4.4 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 9) revealed that the participants finished reading the emails with the least time when they used normal browsing, followed by D&L, which was faster than selective showing.

### 3.4.5 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 9) showed that normal browsing resulted in the lowest perceived cognitive workload, followed by D&L, which was lower than selective showing.

### 3.4.6 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 9), 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, while selective showing was rated as the least effective and satisfying.

## 3.5 Discussion

The study discovers that using D&L for browsing content provides greater protection of sensitive information against shoulder-surfing attacks than normal browsing and selective showing because D&L does not display sensitive information on the screen. Therefore, Table 5 and Table 8 show that D&L is the most effective method for protecting sensitive information from attackers. It protects sensitive information against attackers better, while not hinder users from recognizing sensitive information.

According to Table 14, this study found that the users who used D&L had faster browsing speed than those using selective showing, the analysis found that the average mean browsing speeds of normal browsing and D&L were not significantly different, suggesting that D&L does not have a negative impact on browsing speed. D&L automatically hides and labels sensitive information, making it easier for users to navigate without having to learn new techniques or perform 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. To our best knowledge, 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.

# CHAPTER 4: RLSITE: A LIP READING-BASED APPROACH FOR PROTECTING SENSITIVE INFORMATION WHILE TYPING ON LAPTOP FROM SHOULDER-SURFING ATTACKS

## 4.1 Description of the Proposed Method

Cohort theory posits that a word can be identified when it is distinguishable from all other words [55]. In the context of speech recognition, this theory is particularly relevant, as this subfield of computer science involves developing methodologies and technologies for translating spoken language into text using advanced models, such as lip learning. The implementation of lip reading in various contexts has appeared as an innovative solution with significant potential. We have developed a novel approach to protecting sensitive information during user input that uses lip reading, which has not been employed in this context before. By utilizing this innovative technique, we can provide a more secure and efficient way of protecting sensitive information from shoulder surfing attacks. Moreover, our method can enhance accessibility for visually impaired or hard of hearing users by recording their lip movements and providing an audio output through their headphones. Lip reading also adds an extra layer of security, making it difficult for bystanders or surveillance cameras to capture sensitive information. Our approach offers significant advantages, making it a promising solution for securing sensitive information while typing. Lip reading techniques rely heavily on word recognition and comprehension. Thus, if inputting data into a computer involves reading lips and typing, a computer can likely perform the task more quickly than a human. In fact, Fernandez [56] found that the accuracy of automatic lip reading improves with experience. In this context, cohort theory influenced the design of the RLISTE system, which aimed to prevent shoulder-surfing attacks through the use of speech recognition technology.

- Lip Reading Recognition (TCN) Model

We adapted a state-of-the-art model known as lip reading using Temporal Convolutional Networks (TCN) model [57]. They used the LRW and LRW1000 databases, which are the most extensive and publicly available lip-reading datasets in English. LRW consists of segments from BBC programs, mainly news and talk shows, and includes 1,000-word classes and 718,018 samples with a total running time of approximately 57 hours**.** The TCN model was published in 2020, reporting an 82% recognition success rate. However, on the author's website, better results are displayed as a result of further model fine-tuning, with a 93.4% recognition success rate [58]. We obtained permission to reuse the latest version of the model, which we used for our study. Temporal Convolutional Networks (TCN) model analyzes video clip data to extract users' lip movements within frames, to determine the spoken words, achieving state-of-the-art lip-reading accuracy [58].

## 4.2 Design of RLSITE

Many existing methods for protecting sensitive information during typing are ineffective or insufficient, leaving sensitive information vulnerable to attackers [28, 59-61]. Additionally, many of these methods rely on high cognitive workload and complex interfaces, requiring users to wear external hardware that leaves them unaware of their surroundings. To overcome these limitations, lip reading can be used to protect sensitive information. By considering lip movements, it becomes possible to protect sensitive information without relying on external hardware or complex interfaces. This highly effective and efficient approach makes it an attractive option for many users. Furthermore, lip-reading does not require users to wear external devices, allowing them to remain aware of their surroundings while protecting sensitive information.

During the development of the RLSITE method, we incorporated five fundamental design principles. First, the design should address the problem of wearing external hardware, a common issue in previous studies [23, 62-64]. Second, the design should minimize cognitive workload, which previous studies had struggled to achieve [23, 25]. Third, the design should ensure that the method does not require any bodily movement from the user. Fourth, the design should be effective in protecting sensitive information from shoulder surfing at all viewing angles. Finally, the design should ensure that the method is usable in any location, making it more versatile overall. It is important to note that these design principles were informed by the unique needs and challenges of our users.

The proposed RLSITE method is aimed to allow users to interact efficiently with their devices while enhancing usability and protecting privacy. Guided by cohort theory, the RLSITE method is a novel approach for inputting sensitive information. The method involves using an integrated camera to record participants' lip movements without producing any sound. Once users completed the task, the video clip was sent to the TCN model for processing. The TCN model's output was then used as input to the NPL model in the backend, which labeled the sensitive information using SpaCy. The labeled information was then displayed to the participants, along with a label name. Clicking on the label delivered the information to their headphones.

Fig 6 shows the graphical user interface of the RLSITE method. This approach records participants' lip movements when they silently mouth sensitive information and feeds the resulting video to the TCN model for recognition. RLSITE then protects the recognized sensitive information by replacing it with corresponding category labels. These labels are displayed in the main body.

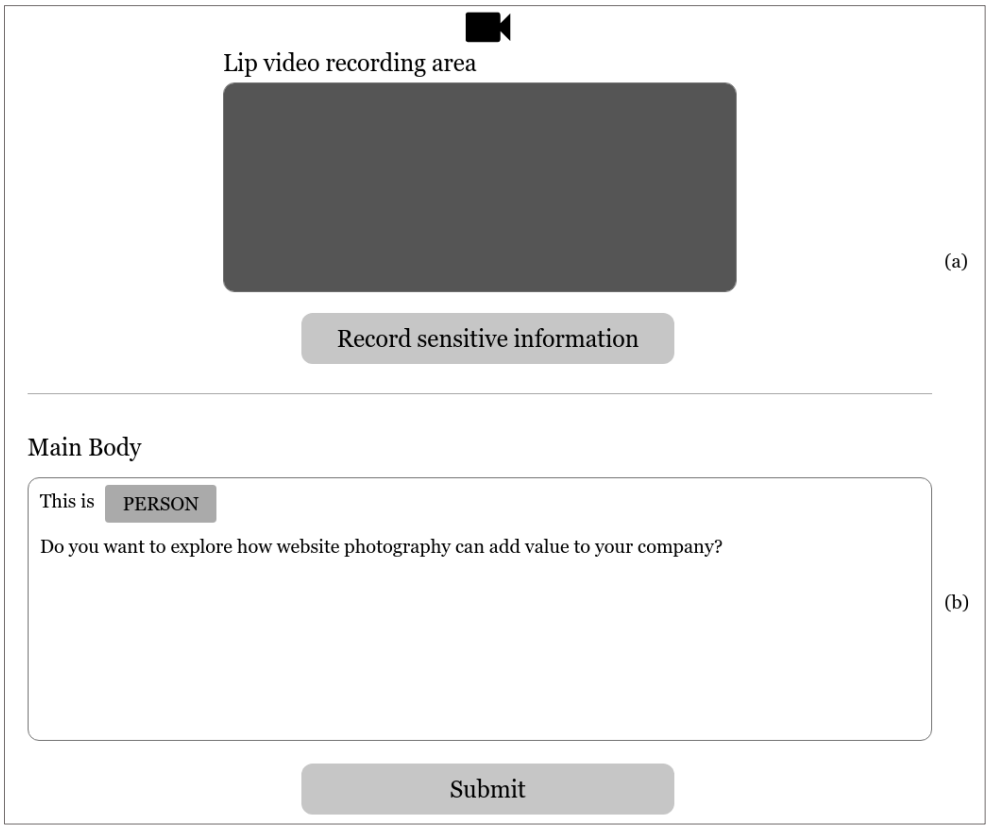



Fig. 7. The graphical user interface of the RLSITE method, where (a) the area of a webcam's view where lip movements are recorded; (b) the content protected by RLSITE appears on the screen after recognizing the user's lip movement

RLSITE provides several advantages over existing methods. First, it effectively addresses cost-related issues associated with other methods, such as randomization methods or smart glasses [23, 65]. Second, RLSITE eliminates the additional cognitive load or time effort required by other methods [22, 63, 66], as it does not shuffle letters or require certain gestures from users. Instead, the method recognizes users' lip movements. Third, RLSITE's design enables faster typing than existing methods as it does not involve shuffling text or requiring a virtual keyboard. Fourth, RLSITE can be used in public venues without any restrictions that required by other methods [23, 62-64], it does not require any external hardware that leaves users unaware of their surroundings.

Fifth, RLSITE effectively protects sensitive information, which is not always the case with other methods. With these benefits, RLSITE emerges as a reliable, secure, and efficient method for inputting sensitive information.

## 4.3 Evaluation

A controlled laboratory experiment with a 3 × 2 × 2 within-subjects factorial design was conducted to evaluate the efficacy and usability of RLSITE. The independent variables were the two types of roles (user and attacker), two shoulder surfing positions (right and left), and three typing methods (normal typing, typing with the Shuffled-keyboard method, and typing with RLSITE). The normal typing without protection and Shuffled-keyboard methods serve as the baseline methods.

### 4.3.1 Participants

During a questionnaire about user perceptions, an attention check was conducted resulting in four participants being deemed ineligible and removed from the study. Therefore, the final analysis was conducted on a sample of 71 participants. Among them, 45 were male. 48 were undergraduate or graduate students, and 23 were university employees. Among the participants, 22 were aged between 18–20 years old, 17 were 21–25, 10 were 36–30, nine were 31–35, seven were 36–40, and 6 were older than 40. 71 individuals 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. A random draw was conducted at the end of the study to encourage participants to fully engage with the experimental tasks and take them 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 a $25 Amazon gift card each as a gesture of appreciation for their effort and diligence.

### 4.3.2 Typing methods

In our study, three typing methods were used: normal typing without additional protection, the Shuffled-keyboard method, and RLSITE (with the first two used as baseline methods). The Shuffled-keyboard method uses a letter-shuffling system, in which each letter is shuffled after every keyboard press by the user. This method was chosen due to the lack of existing methods designed to protect sensitive information during typing. While several other methods also aim to protect sensitive information during typing [14, 23], they often rely on external tools such as augmented reality and virtual keyboards, which can be expensive and challenging to deploy, and introduce additional complexity and user training requirements. Therefore, we selected the Shuffled-keyboard method and excluded external tool-based methods from our study due to their added complexity and training requirements.

### 4.3.3 Apparatus

A RLSITE 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.

### 4.3.4 Experimental task

Participants who undertook the role of user were asked to type two designated emails per a method, with 6 emails in total, adapted from a corpus dataset [50]. The order in which the typing methods were used was randomized and balanced to minimize any sequential impact and bias. Each email contained an average of 80 words and two pieces of sensitive information. Participants

were instructed to type an email and not to return to previous email. All emails were entered in the Times New Roman font with size 12. For the normal typing method, users were instructed to use the physical keyboard to type two emails on a website designed for the study. For the virtual shuffling-letters keyboard method, users were asked to use a keyboard with shuffled letters where the positions of the letters changed after each key press. During the RLSITE experiment, users were instructed to use the physical keyboard to type non-sensitive information found in a provided email. Then, when they needed to insert any sensitive information, they were asked to click the 'Record sensitive information' button and were instructed to silently mouth the information within two seconds. The sensitive information was then inserted into the model.

After typing a pair of emails using a method, both the user and attacker filled out a form with two multiple-choice questions about the sensitive information they had read or memorized from the emails (see Fig. 7). The user then filled out a questionnaire about their experience with the typing methods, including ease of use, effectiveness, and satisfaction. The user also completed a NASA Task Load Index questionnaire using 7-point scales (1 = Extremely Low, 4 = neutral, and 7 = Extremely High).

### 4.3.5 Procedure

After providing informed consent, the participants received instructions on how to use the RLSITE and Shuffled-keyboard methods during a training session. Then, each participant was assigned a role (user or attacker) and asked to remain in that role for the duration 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, as adopted from previous studies on shoulder-surfing [67, 68]. Afterwards, participants were required to complete

the tasks explained in the "Experimental Task" section. The figure below provides an overview of the study procedure and tasks.

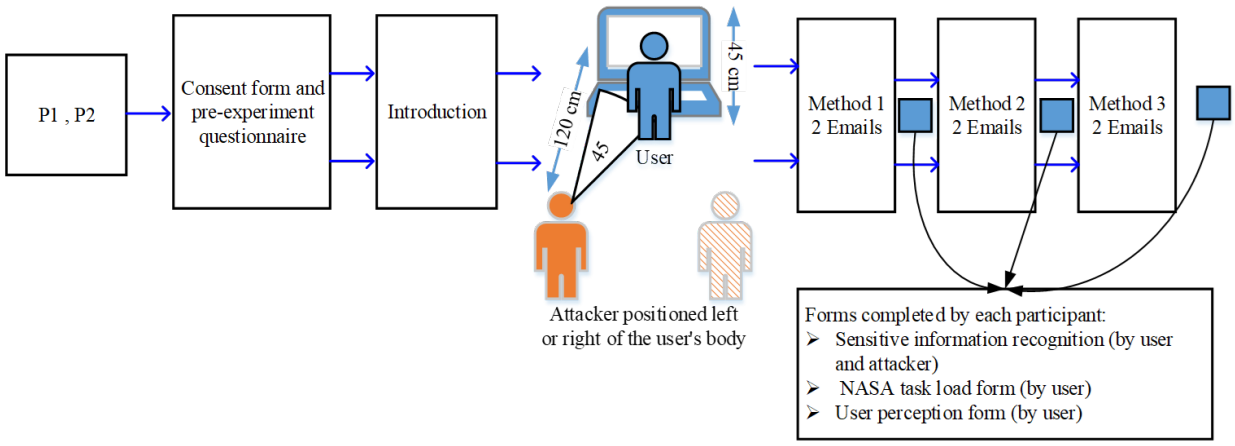



Fig. 8. Study Procedure and Tasks Overview of RLSITE

In the second session, the participants switched roles so that an attacker became a user typing the content, and a user became an attacker. This session was essentially the same as the first except involving different email content. All participants completed the forms for the multiple-choice questions and questionnaires 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 University of North Carolina at Charlotte (under IRB number 25-5955).

### 4.3.6 Independent and Dependent Measures

This study evaluated the RSLTIE method using multiple dependent and independent variables from the perspectives of both the user (victim) and the attacker (observer). The measures used for the dependent variables were adopted from previous studies that had evaluated both perspectives

across many variables [22, 33, 37, 51, 69], including sensitive information recognition, perceived cognitive workload, typing speed, and user perception. The independent variables were the two types of participant (user and attacker), observation angles (right and left), and typing methods (normal typing, the Shuffled-keyboard method [61], and RLSITE, with the first two used as baseline methods). The variables and the methods used to evaluate them are explained in detail below.

1) Accuracy of sensitive information recognition

To measure the accuracy of sensitive information recognition, this variable uses two multiple-choice questions that ask participants to recall sensitive information obtained or remembered from previous emails, as done in previous studies [37, 52]. Each correct answer for one email would receive 0.50, while incorrect answers would be scored 0. If a participant answered both questions correctly, he would receive a 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 multidimensional scales measuring perceived workload (including mental, physical, and temporal demand) and overall performance of completing the task [53].

3) Typing speed

This variable was measured as the time between the moment when a user entered the first letter of an email and the moment that they finished typing and clicked the “Submit” Button on the user interface. The system then showed the “Start” button again, which could be clicked to bring up the next email.

4) Observation angle

The observation angle of an attacker was an independent variable. Two observation angles were considered: a 45° angle behind the user either from left or from right. Each attacker was assigned to a position (right or left) and asked to remain in that position until the end of the experiment. These observation positions were adopted from previous studies that reported an optimal viewing angle of slightly to the right or left of the experimenter, suggesting that the angle influenced the feasibility of a shoulder-surfing attack [51, 69-73]. The sequence of observation angles used by the attackers was randomized and balanced to minimize any sequential impact and bias.

5) User perception

User perception included the variables of perceived ease-of-use, perceived effectiveness, and participants' overall satisfaction with each method. This was assessed using a post-experiment survey consisting of five questions and a 7-point Likert scale (1 = totally disagree, 4 = neutral, and 7 = totally agree) (see Table 15). The questions, grouped by these three variables, were adapted from the IBM post-study system usability questionnaire [54], which was initially developed by applying psychometric methods to measure users' satisfaction and subjective assessments of system usability [54]. The following table presents the questionnaire items measuring user perceptions for the RLSITE method. The same questionnaire items were used to evaluate users' perceptions of the other two methods.

Table 15. Questionnaire Items Measuring User Perceptions for the RLSITE Method

| Factors | Items based on a 7-point Likert scale (1 = totally disagree, 4 = neutral, and 7 = totally agree) |
|---|---|
| Perceived ease-of-use | Overall, I am satisfied with the simplicity of the RLSITE method.<br>The RLSITE method was simple to use.<br>It was easy to learn how to use the RLSITE method. |
| Perceived effectiveness | I was able to accomplish the tasks using the RLSITE method. |
| Overall satisfaction | Overall, I am satisfied with the RLSITE method. |

## 4.4 Results

### 4.4.1 Responses to the Pre-experiment Questionnaire

The responses to the pre-experiment questionnaire provided insightful findings regarding participants' laptop use in public venues. All participants indicated that they used a laptop, with the majority reporting typing personal or work emails on their laptops multiple times per day (69%) or once a day (16.9%). However, the results also revealed significant privacy concerns related to typing sensitive information on a laptop device in a public venue, with an overwhelming majority of participants (97.2%) agreeing or strongly agreeing with this statement. This finding suggests that the participants were aware of the risks associated with typing sensitive information in public settings and highlighted the importance of implementing measures to protect personal information when using laptops outside of private spaces. Overall, these results provided important insights into the use of laptops in public venues and underscored the need for improved privacy protections in these settings.

Table 16. Responses to Pre-Experiment Questionnaire on Typing on Laptops in Public Venues

| Variables | Sub-Variables | Frequency | Percentage (%) |
|---|---|---|---|
| Do you currently use a laptop (e.g., Apple Mac, Dell, HP, or Lenovo)? | Yes | 71 | 100.0 |
| How often do you type/write personal or work emails on your laptop? | Multiple times per day | 60 | 84.5 |
| | Once a daily | 1 | 1.4 |

| | | | |
|---|---|---|---|
| | Weekly | 9 | 12.7 |
| | Monthly | 1 | 1.4 |
| | Once or twice a quarter | 0 | 0.0 |
| | Rarely (once a year or less) | 0 | 0.0 |
| | Never | 0 | 0.0 |
| Typing sensitive information on a laptop device in a public venue entails significant privacy concerns. | Strongly disagree | 0 | 0 |
| | Somewhat disagree | 1 | 1.4 |
| | Disagree | 1 | 1.4 |
| | Neither agree nor disagree | 0 | 0 |
| | Somewhat agree | 8 | 11.3 |
| | Agree | 33 | 46.5 |
| | Strongly agree | 28 | 39.4 |

We first conducted a Kruskal-Wallis test to analyze how typing methods affect the recognition of sensitive information for both users and attackers. We also evaluated how browsing methods impact cognitive workload, typing speed, and user perception for users. Afterward, we performed Pairwise Comparisons on each dependent variable to identify any differences between the three typing methods.

### 4.4.2 Sensitive Information Recognized by Attackers

The summary of attackers' response scores can be found in Table 17. Table 18 showed that there was a significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The null hypothesis can be rejected due to the significant p-value ($p < 0.001$). The results of the pairwise comparisons of typing methods were shown in Table 19. The table indicated that significant differences were observed when attackers used RLSITE compared to the normal typing method ($p < 0.001$), as well as when they used RLSITE compared to Shuffled-keyboard method ($p < 0.001$). Based on the findings, attackers were less able to remember sensitive information when using RLSITE compared to the other methods ($p < 0.01$). Furthermore, the

results presented in Table 20 indicate that RLSITE proved to be highly proficient in protecting sensitive information against shoulder surfing attacks, as attackers were able to identify the smallest amount of sensitive information. In summary, the RLSITE method demonstrated higher effectiveness in protecting sensitive information against shoulder surfing attacks compared to other methods.

Table 17. Attackers' Response Summary for Typing Methods

| | | Normal typing | Shuffled-keyboard method | RLSITE |
|---|---|---|---|---|
| Correct | 1 | 46 | 31 | 0 |
| | 0.5 | 15 | 27 | 9 |
| Incorrect | 0 | 0 | 3 | 52 |
| Total | | 61 | 61 | 61 |

Table 18. Independent-Samples Kruskal-Wallis Test Summary for Typing Methods (Results from Attackers' Perspectives)

| | |
|---|---|
| Total N | 182 |
| Test Statistic | 121.800a |
| Degree Of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .000 |

Table 19. Pairwise Comparisons of Typing Methods from Attackers' Perspective

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.a |
|---|---|---|---|---|---|
| RLSITE - Shuffled-keyboard method | 74.443 | 8.928 | 8.338 | .000 | .000 |
| RLSITE - Normal typing method | 93.437 | 8.965 | 10.422 | .000 | .000 |

Table 20. Mean Rank of Sensitive Information Recognized by Attackers for Different Typing Methods

| Method | N | Mean Rank |
|---|---|---|
| Normal typing method | 61 | 129.18 |
| Shuffled-keyboard method | 61 | 110.19 |
| RLSITE | 61 | 35.75 |

### 4.4.3 Sensitive Information Recognized by Users

The summary of users' response scores can be found in Table 21. Users who answered both questions correctly received a score of "1". Those who answered one question correctly received a score of "0.5". Those who did not answer any questions correctly received a score of "0". Table 22 showed that there was no significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The table indicated that there was no significant differences were observed when users used these methods. Based on the findings, RLSITE did not negatively impact a user's ability to remember their sensitive information when typing.

Table 21. Users' Response Summary for Typing Methods

| | | Normal typing | Shuffled-keyboard method | RLSITE |
|---|---|---|---|---|
| Correct | 1 | 56 | 53 | 45 |
| | 0.5 | 15 | 16 | 24 |
| Incorrect | 0 | 0 | 2 | 2 |
| Total | | 71 | 71 | 71 |

Table 22. Independent-Samples Kruskal-Wallis Test Summary for Typing Methods (Results from Users' Perspectives)

| | |
|---|---|
| Total N | 213 |
| Test Statistic | 4.696 |
| Degree Of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .096 |

Table 23. Mean Values of Variables for Three Typing Methods (Users Only)

| Variables | Typing Methods | Mean | Std. Dev. |
|---|---|---|---|
| Cognitive workload | Normal typing | 2.676 | 0.627 |
| | Shuffled-keyboard | 4.534 | 0.690 |
| | RLSITE | 3.049 | 0.767 |
| typing speed (in seconds) | Normal typing | 125.309 | 2.759 |
| | Shuffled-keyboard | 256.085 | 2.974 |
| | RLSITE | 190.436 | 5.525 |
| Perceived ease of use | Normal typing | 5.830 | 1.048 |
| | Shuffled-keyboard | 3.035 | 0.957 |
| | RLSITE | 5.116 | 0.890 |
| Perceived effectiveness | Normal typing | 5.739 | 1.161 |

| | | | |
|---|---|---|---|
| | Shuffled-keyboard | 2.887 | 1.153 |
| | RLSITE | 4.9155 | 1.224 |
| Satisfaction | Normal typing | 5.633 | 1.233 |
| | Shuffled-keyboard | 2.901 | 1.277 |
| | RLSITE | 5.2254 | 1.343 |

Table 24. Variable Pairwise Comparisons for Typing Methods (Users Only)

| Variables | (I) Typing Method | (J) Typing Method | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Cognitive workload | RLSITE | Normal Typing | 0.372 | 0.117 | .005 |
| | | Shuffled-keyboard | -1.485 | 0.117 | .000 |
| Typing speed (in seconds) | RLSITE | Normal Typing | 65.126 | 0.664 | .000 |
| | | Shuffled-keyboard | -65.647 | 0.664 | .000 |
| Perceived ease of use | RLSITE | Normal Typing | -0.714 | 0.162 | .001 |
| | | Shuffled-keyboard | 2.080 | 0.162 | .000 |
| Perceived effectiveness | RLSITE | Normal Typing | -0.823 | 0.198 | .001 |
| | | Shuffled-keyboard | 2.028 | 0.198 | .000 |
| Satisfaction | RLSITE | Normal Typing | -0.408 | 0.215 | .143 |
| | | Shuffled-keyboard | 2.323 | 0.215 | .001 |

### 4.4.4 Cognitive Workload

The ANOVA results indicated a significant impact of typing method on cognitive load (F [2, 210] =141.191, $p$ = .001). The Tukey test results (Table 23. Mean Values of Variables for Three Typing Methods (Users Only)

| Variables | Typing Methods | Mean | Std. Dev. |
|---|---|---|---|
| Cognitive workload | Normal typing | 2.676 | 0.627 |
| | Shuffled-keyboard | 4.534 | 0.690 |
| | RLSITE | 3.049 | 0.767 |
| typing speed (in seconds) | Normal typing | 125.309 | 2.759 |
| | Shuffled-keyboard | 256.085 | 2.974 |
| | RLSITE | 190.436 | 5.525 |
| Perceived ease of use | Normal typing | 5.830 | 1.048 |
| | Shuffled-keyboard | 3.035 | 0.957 |
| | RLSITE | 5.116 | 0.890 |
| Perceived effectiveness | Normal typing | 5.739 | 1.161 |
| | Shuffled-keyboard | 2.887 | 1.153 |
| | RLSITE | 4.9155 | 1.224 |
| Satisfaction | Normal typing | 5.633 | 1.233 |

| | | | |
|---|---|---|---|
| | Shuffled-keyboard | 2.901 | 1.277 |
| | RLSITE | 5.2254 | 1.343 |

Table 24) showed that normal typing resulted in the lowest perceived cognitive workload, followed by RLSITE, which was lower than Shuffled-keyboard method.

### 4.4.5 Typing Speed

The ANOVA results showed a significant impact of typing method on users' typing speed (F [2, 210] = 19357.45, $p$ = .001). The Tukey test results (Table 23. Mean Values of Variables for Three Typing Methods (Users Only)

| Variables | Typing Methods | Mean | Std. Dev. |
|---|---|---|---|
| Cognitive workload | Normal typing | 2.676 | 0.627 |
| | Shuffled-keyboard | 4.534 | 0.690 |
| | RLSITE | 3.049 | 0.767 |
| typing speed (in seconds) | Normal typing | 125.309 | 2.759 |
| | Shuffled-keyboard | 256.085 | 2.974 |
| | RLSITE | 190.436 | 5.525 |
| Perceived ease of use | Normal typing | 5.830 | 1.048 |
| | Shuffled-keyboard | 3.035 | 0.957 |
| | RLSITE | 5.116 | 0.890 |
| Perceived effectiveness | Normal typing | 5.739 | 1.161 |
| | Shuffled-keyboard | 2.887 | 1.153 |
| | RLSITE | 4.9155 | 1.224 |
| Satisfaction | Normal typing | 5.633 | 1.233 |
| | Shuffled-keyboard | 2.901 | 1.277 |
| | RLSITE | 5.2254 | 1.343 |

Table 24) revealed that normal typing was the fastest, followed by RLSITE, which was faster than the Shuffled-keyboard method.

### 4.4.6 User Perceptions

The results of the ANOVA revealed a significant impact of typing method on participants' perceived ease of use (F [2, 210] = 159.982, $p$ = .001), perceived effectiveness (F [2, 210] =

109.815, $p = .001$), and overall satisfaction (F [2, 210] =93.286, $p = .001$). According to the Tukey test results (Table 23. Mean Values of Variables for Three Typing Methods (Users Only)

| Variables | Typing Methods | Mean | Std. Dev. |
|---|---|---|---|
| Cognitive workload | Normal typing | 2.676 | 0.627 |
| | Shuffled-keyboard | 4.534 | 0.690 |
| | RLSITE | 3.049 | 0.767 |
| typing speed (in seconds) | Normal typing | 125.309 | 2.759 |
| | Shuffled-keyboard | 256.085 | 2.974 |
| | RLSITE | 190.436 | 5.525 |
| Perceived ease of use | Normal typing | 5.830 | 1.048 |
| | Shuffled-keyboard | 3.035 | 0.957 |
| | RLSITE | 5.116 | 0.890 |
| Perceived effectiveness | Normal typing | 5.739 | 1.161 |
| | Shuffled-keyboard | 2.887 | 1.153 |
| | RLSITE | 4.9155 | 1.224 |
| Satisfaction | Normal typing | 5.633 | 1.233 |
| | Shuffled-keyboard | 2.901 | 1.277 |
| | RLSITE | 5.2254 | 1.343 |

Table 24), users rated normal typing as the easiest, followed by RLSITE, with Shuffled-keyboard method being the most difficult. Additionally, RLSITE was perceived as the most effective and satisfying typing method, while Shuffled-keyboard method was rated as the least effective and satisfying.

### 4.4.7 Attacker position and demographics

The results of the ANOVA analysis indicate that there was no significant effect of attacker positions, attacker ages, or attacker gender on the ability to recall sensitive information.

Table 25. ANOVA Results for Attacker Position, Age, And Gender on Recall of Sensitive Information for Typing Methods

| Variables | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Attacker Position | Between Groups | .462 | 2 | .231 | .926 | .398 |
| | Within Groups | 45.694 | 183 | .250 | | |
| Attacker Gender | Between Groups | .009 | 2 | .005 | .020 | .980 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Within Groups | 49.944 | 210 | .238 | | |
| Attacker Age | Between Groups | .000 | 2 | .000 | .000 | 1.000 |
| | Within Groups | 592.310 | 210 | 2.821 | | |

## 4.5 Discussion

The study found that RLSITE provided better protection of sensitive information against shoulder-surfing attacks than normal typing and the Shuffled-keyboard method because it does not display sensitive information on the screen. According to the results presented in Table 17 and Table 21, it is evident that RLSITE was the most effective method for protecting sensitive information from attackers while still enabling users to identify and recognize sensitive information. Furthermore, the study found that the mean value of users who used RLSITE showed a reduced ability to recall sensitive information compared to other tested methods. This is due to the fact that RLSITE users were instructed to select sensitive information based on the lip-reading model's output. If the model's detection was inaccurate, users were instructed to select the "the output is not accurate" option, even if they still remembered the sensitive information. Future research should explore the use of improved models to address these issues.

Additionally, no significant differences were observed in attackers' ability to recall sensitive information based on their education level, gender, or age. This finding is not surprising, as shoulder-surfing attacks do not require specialized skills or knowledge [74, 75]. Although normal typing was faster than RLSITE and the Shuffled-keyboard method, it was also expected to result in more significant information leakage. RLSITE was faster than the Shuffled-keyboard method because it utilized a lip-reading model installed on a host with a high GPU, the NVIDIA GeForce GTX 1080 Ti.

The study also evaluated cognitive workload to determine which method resulted in higher workload. The results showed that normal typing had the lowest workload, followed by RLSITE and the Shuffled-keyboard method. Users may have rated RLSITE slightly higher than normal typing and lower than shuffled-keyboard implementation due to its novelty and the unfamiliarity of inputting lip movements using the webcam. In our comparison study, RLSITE was evaluated against the Shuffled-keyboard implementation for ease of use, effectiveness, and user satisfaction. RLSITE scored higher than the Shuffled-keyboard method in each of these aspects, and achieved a score very close to that of the normal typing method. These results suggest that RLSITE is more effective and user-friendly compared to the Shuffled-keyboard method. The findings confirmed that RLSITE's use of labeling and automatic lip-reading detection and recognition enhances ease of use, effectiveness, and user satisfaction.

In summary, the study found that RLSITE was the most effective method for protecting sensitive information, outperforming the other two methods in many of the dimensions evaluated. RLSITE provided the highest level of security for sensitive information since it resulted in attackers recalling less information compared to the other tested methods. Additionally, RLSITE users reported a low cognitive workload while typing and found it to be the most effective method. Consequently, users expressed greater satisfaction with RLSITE than with the Shuffled-keyboard method. Furthermore, the typing speeds with RLSITE were significantly faster than with the Shuffled-keyboard implementation. Therefore, RLSITE is considered an effective and straightforward method for protecting privacy in public places.

# CHAPTER 5: SIC: AUTOMATIC FACE DETECTION-BASED APPROACH FOR PROTECTING SENSITIVE INFORMATION WHILE BROWSING ON LAPTOP FROM SHOULDER SURFING ATTACKS

## 5.1 Description of SIC

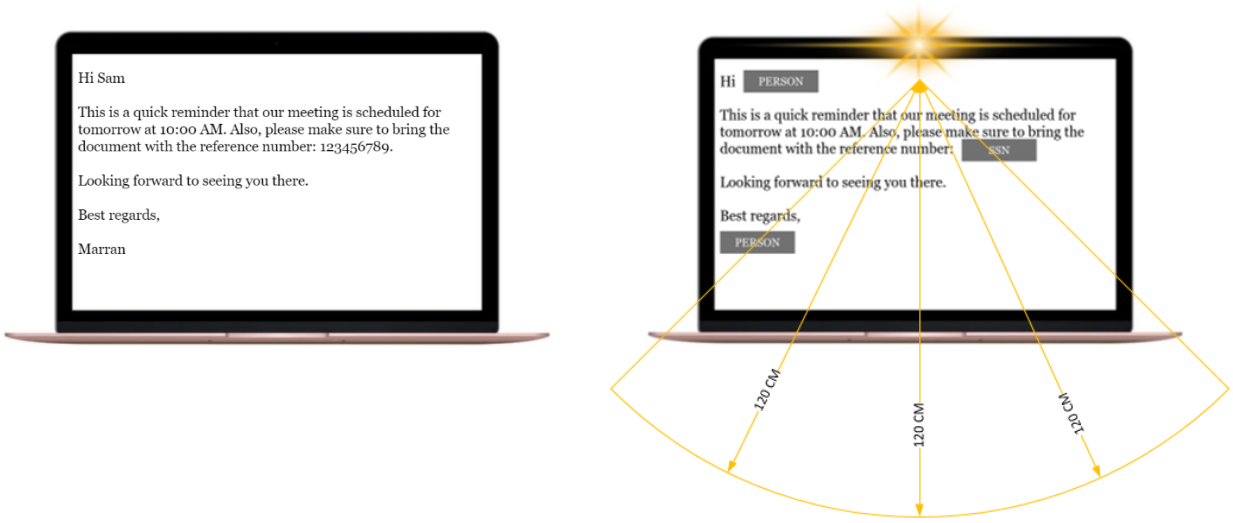
The speed at which humans can detect people behind them is limited due to the physical limitations of the human body and the cognitive processes of the human brain. Debnath [76] found that automatic object detection using computer vision algorithms could achieve faster and more accurate results than human detection in certain scenarios. It provided the foundation for the design of the SIC system, which involves automatic object detection to identify when a person moves closer to a user and in view of the screen. The next section presents the design of SIC.

## 5.2 Design of SIC

The purpose of SIC is to enable users to interact with their devices while reducing their concerns and risks of getting shoulder surfing by alerting users when someone behind them is in close proximity. Although a few methods rely on automatic detection to protect sensitive information [14, 77], most existing approaches use static modes or non-technical solutions, such as user awareness and education. Therefore, a technical system that can automatically detect an attacker's proximity is essential for effective protection of sensitive information.

To overcome the limitations of existing methods, a practical and effective solution is necessary. The proposed SIC automatically detects when someone is in close proximity to a user, labels sensitive information, and notifies users by activating an audible alarm. Users can then click on the label name to have the SIC read the sensitive information to them through their headphones.

The SIC method employs several advanced techniques, including single-shot object detection (SSD) for detecting people, text labeling, and speech synthesis.




(a) (b)

Fig. 9. The graphical user interface of the SIC method (a) The original content with no protection; (b) content protected by SIC when the camera detects someone's face within a range of 120 cm

Fig. 9 (a) shows the content without any protection measure, while (b) shows the SIC with protected sensitive information. The SIC uses a webcam camera to detect anyone within 120 cm of the user's screen. If someone gets too close, the SIC labels sensitive information and notifies users by activating an audible alarm. Users can then click on the label name to have the SIC read the sensitive information to them through their headphones. We utilized the triangle similarity technique to measure the distance between the user's webcam and the potential attacker. Previous studies suggested that a potential attacker could view the victim's screen from up to 120 cm away. However, because of the limited space in our laboratory, we were unable to confirm whether SIC will function beyond this specific distance or not. Nonetheless, the SIC remained operational for detection and successfully accomplished its intended purpose. Overall, we sought to prevent

shoulder surfers from accessing sensitive information and increase perceived ease of use. The design was also intended to reduce the need for users to make extra movements, such as turning around to check for people behind them. Close proximity to users in public spaces could enable shoulder surfers obtaining private information from users' laptop screens.

## 5.3 Evaluation

We conducted a controlled laboratory experiment using a 3 × 2 × 2 within-subjects factorial design to evaluate the efficacy and usability of SIC. The independent variables were the two types of roles (user and attacker), two shoulder surfing positions (right and left), and three methods of detecting attackers while browsing: browsing with User-driven detection, browsing with Moving or Hiding Content, and browsing with SIC. The User-driven detection and Moving or Hiding Content methods were used as baseline methods.

### 5.3.1 Participants

The experiment included 69 participants who met the inclusion criteria. They had previously used a laptop to access emails in public venues were recruited from a public university on the east coast of the U.S. Among them, 45 were male. 45 were undergraduate or graduate students, and 24 were university employees. Among the participants, 19 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. 69 individuals played the role of a user, while 60 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. A random draw was conducted at the end of the study to encourage participants to fully engage with the experimental tasks and take them 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 a $25 Amazon gift card each as a gesture of appreciation for their effort and diligence.

### 5.3.2 Detecting attackers while browsing

Three detecting attackers while browsing were used: User-driven detection method without any additional protection, Moving or Hiding Content method, and SIC. The User-driven detection method refers to browsing content without any additional protection measures. Moving or Hiding Content [16] is a gesture-based method that uses simple swiping gestures to hide screen content. When the user swipes one hand from the bottom to the top of the screen, the system can hide the screen content. We chose Moving or Hiding Content as our baseline approach for several reasons. One is that it is a user-friendly and straightforward method that is relatively easy to implement. Second, it employs simple swiping gestures to hide screen content, which can be easily understood and used by users without requiring extensive training.

In contrast, external tool-based methods may not be practical for certain situations due to major limitations. They often require additional hardware or software, which can be costly and may not be readily available to all users. Moreover, these requirements can create confounding factors that may impact the accuracy and effectiveness of the method. Therefore, we chose to exclude external tool-based methods from our study and focused on more practical and accessible approaches, such as Moving or Hiding Content.

### 5.3.3 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.

### 5.3.4 Experimental task

The users in the study were instructed to browse through six emails displayed on a MacBook Pro without using the keyboard to search for specific words or to return to previous emails. For each of the three detecting attackers while browsing methods (User-driven detection method, Moving or Hiding Content method, and SIC).

In the User-driven detection method, participants were asked to rely on their own awareness and detection skills to protect their screen content. They were instructed to move on to the following email if they detected an attacker in their area, even if they had not finished reading the current email. The Moving or Hiding Content method required participants to perform a simple swipe from bottom to top using one hand if they detected the presence of someone within a close range of 120 cm from their location. To clarify this distance, the primary researcher indicated the 120 cm mark on the floor. During the SIC experiment, participants were instructed to browse through their emails, and an audible alarm would be triggered by the SIC when someone approached them closely. Participants were required to wear headphones in order to hear the sensitive information being protected.

The order of the browsing methods was randomized and balanced to avoid any order effects. The emails used in the experiment contained an average of 120 words and two pieces of sensitive information per email, which were adapted from a corpus dataset [50]. All emails were presented in Times New Roman font with a font size of 12.

During the experiment, the attacker stood behind the sitting user, either to the left or right, and was asked to look at the laptop screen over the user's shoulder and obtain sensitive information (see Fig. 10). After browsing a pair of emails using each method, both the user and attacker completed a questionnaire with two multiple-choice questions about the sensitive information that they just read or memorized from the previous emails. Additionally, the user was asked to fill out a questionnaire about their experience with the browsing method, including ease of use, effectiveness, and satisfaction. The user also completed a NASA Task Load Index questionnaire using a 7-point scale to evaluate the cognitive workload associated with each browsing method.

### 5.3.5 Procedure

After providing informed consent, the participants received a training session that familiarized them with the methods, including instructions on using Moving or Hiding Content method and SIC. Each participant was then assigned a role as either a user or attacker and remained in that position for the duration of the experiment. The setup involved an attacker standing at a 45° angle behind the seated user, randomly assigned to either the left or right side. The distance between the attacker and the user's screen was 120 cm, while the distance between the user and the laptop screen was 45 cm. These positions were adopted from previous shoulder-surfing studies [67, 68]. Afterwards, participants were required to complete the tasks explained in Section 'Experimental Tasks'. The figure below provides an overview of the study procedure and tasks.

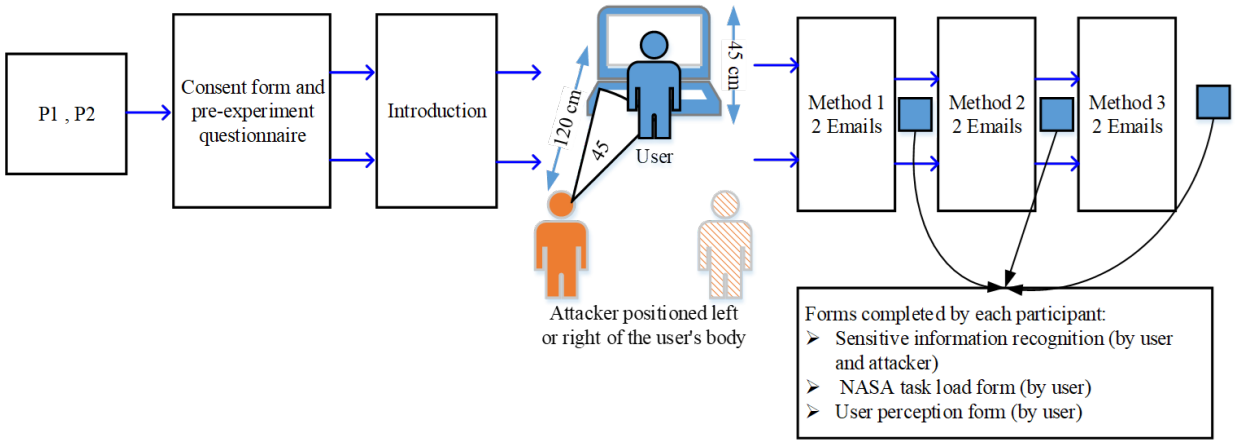



Fig. 10. Study Procedure and Tasks Overview of SIC

In the second session, the participants switched roles, with attackers becoming users and users becoming attackers. The session was essentially the same as the first, except it involved different email content. 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).

### 5.3.6 Dependent Variables

The dependent variables in this study included the accuracy of sensitive information recognition, perceived cognitive workload, detection speed, and user perception.

1) Accuracy of sensitive information recognition

To make it consistent and comparable with previous studies [37, 52], this variable measures the accuracy of sensitive information recognition through two multiple-choice questions that ask participants to recall 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 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 multidimensional scales measuring perceived workload (including mental, physical, and temporal demand) and overall performance of completing the task [53].

3) Detection speed

Detection speed was measured by recording the time duration between when a user pressed the "display email" button to start reading an email and when they pressed the "next email" button. For Moving or Hiding Content, the time duration was recorded between when a user pressed the "display email" button to start reading an email and when they hid the screen. For SIC, the time duration was recorded between when a user pressed the "display email" button to start reading an email and when the system launched an audible alarm indicating the presence of a nearby attacker. To ensure data accuracy, the primary investigator observed participants as they scrolled to the bottom of the page and monitored their scrolling position to ensure that they had thoroughly read each email rather than just skimmed the content.

4) User perception

User perception included the variables of perceived ease-of-use, perceived effectiveness, and participants' overall satisfaction with each method. This was assessed using a post-experiment survey consisting of five questions and a 7-point Likert scale (see Table 20). The questions, grouped by these three variables, were adapted from the IBM post-study system usability

questionnaire [54], which was initially developed by applying psychometric methods to measure users' satisfaction and subjective assessments of system usability [54]. The following table presents the questionnaire items measuring user perceptions for the SIC method. The same questionnaire items were used to evaluate users' perceptions of the other two methods.

Table 26. Questionnaire Items Measuring User Perceptions for the SIC Method

| Factors | Items based on a 7-point Likert scale (1 = totally disagree, 4 = neutral, and 7 = totally agree) |
|---|---|
| Perceived ease-of-use | Overall, I am satisfied with the simplicity of the SIC method.<br>The SIC method was simple to use.<br>It was easy to learn how to use the SIC method. |
| Perceived effectiveness | I was able to accomplish the tasks using the SIC method. |
| Overall satisfaction | Overall, I am satisfied with the SIC method. |

## 5.4 Results

### 5.4.1 Sensitive Information Recognized by Attackers

The summary of attackers' response scores can be found in Table 28. Table 29 showed that there was a significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The null hypothesis can be rejected due to the significant p-value ($p < 0.001$). The results of the pairwise comparisons of browsing methods were shown in Table 30. The table indicated that significant differences were observed when attackers used SIC compared to the User-driven detection method ($p < 0.001$), as well as when they used SIC compared to the Hiding Content method ($p < 0.001$). Based on the findings, attackers were less able to identify sensitive information when using SIC compared to the User-driven detection method and the Hiding Content method ($p < 0.01$). Table 31 showed that the SIC method was very effective in protecting sensitive information from shoulder surfing attacks. Attackers were able to recognize the least amount of sensitive

information using this method, as indicated by the high mean rank. Overall, SIC proved to be more effective in protecting sensitive information against shoulder surfing attacks than other methods.

Table 27. Attackers' Response Summary for Detection Methods

| | | User-driven detection method | Hiding Content method | SIC |
|---|---|---|---|---|
| Correct | 1 | 17 | 32 | 11 |
| | 0.5 | 25 | 11 | 0 |
| Incorrect | 0 | 19 | 18 | 50 |
| Total | | 61 | 61 | 61 |

Table 28. Independent-Samples Kruskal-Wallis Test Summary for Detection Methods (Results from Attackers' Perspectives)

| | |
|---|---|
| Total N | 183 |
| Test Statistic | 32.735a |
| Degree Of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .000 |

Table 29. Pairwise Comparisons of Detection Methods Attackers' Perspective

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.a |
|---|---|---|---|---|---|
| SIC - User-driven detection method | 35.975 | 8.842 | 4.069 | .000 | .000 |
| SIC - Hiding Content method | 48.787 | 8.842 | 5.518 | .000 | .000 |

Table 30. Mean Rank of Sensitive Information Recognized by Attackers for Different Detection Methods

| Method | N | Mean Rank |
|---|---|---|
| User-driven detection method | 61 | 99.72 |
| Hiding Content method | 61 | 112.53 |
| SIC | 61 | 63.75 |

### 5.4.2 Sensitive Information Recognized by Users

The summary of user's response scores can be found in Table 32. Table 33 showed that there was a significant difference between the compared groups, as determined by the Kruskal-Wallis test results. The results of the pairwise comparisons of detection methods were shown in Table 34. The table indicated that there was a significant differences were observed when users used SIC

and User-driven detection method. Based on the findings, SIC did not negatively impact a user's ability to access sensitive information when browsing. Additionally, Table 35 displayed the mean rank, suggesting that users recognized the least amount of sensitive information when using User-driven detection method followed by Moving or Hiding Content then SIC, suggesting that SIC did not negatively impact a user's ability to know the sensitive information when browsing.

Table 31. Users' Response Summary for Different Detection Methods

| | | User-driven detection method | Hiding Content method | SIC |
|---|---|---|---|---|
| Correct | 1 | 30 | 39 | 56 |
| | 0.5 | 15 | 14 | 1 |
| Incorrect | 0 | 24 | 16 | 12 |
| Total | | 69 | 69 | 69 |

Table 32. Independent-Samples Kruskal-Wallis Test Summary for Detection Methods (Results from Users' Perspectives)

| | |
|---|---|
| Total N | 207 |
| Test Statistic | 15.568 |
| Degree Of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .000 |

Table 33. Pairwise Comparisons of Detection Methods from Attackers' Perspective

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.a |
|---|---|---|---|---|---|
| SIC - User-driven detection method | -34.942 | 8.898 | -3.927 | .000 | .000 |
| SIC - Hiding Content method | -20.406 | 8.898 | -2.293 | .022 | .065 |

Table 34. Mean Rank of Sensitive Information Recognized by Users for Different Detection Methods

| Method | N | Mean Rank |
|---|---|---|
| User-driven detection method | 69 | 87.51 |
| Hiding Content method | 69 | 102.04 |
| SIC | 69 | 122.45 |

Table 35. Mean Values of Variables for Three Detection Methods (Users Only)

| Variables | Detection Methods | Mean | Std. Dev. |
|---|---|---|---|
| Cognitive workload | User-driven detection method | 5.805 | .211 |
| | Moving or Hiding Content | 5.008 | .362 |
| | SIC | 3.610 | .379 |

| | | | |
|---|---|---|---|
| Detection speed (in seconds) | User-driven detection method | 29.798 | 2.756 |
| | Moving or Hiding Content | 77.289 | 11.665 |
| | SIC | 30.414 | 7.960 |
| Perceived ease of use | User-driven detection method | 4.143 | .718 |
| | Moving or Hiding Content | 3.047 | .459 |
| | SIC | 4.581 | .679 |
| Perceived effectiveness | User-driven detection method | 3.272 | .490 |
| | Moving or Hiding Content | 3.755 | .501 |
| | SIC | 5.291 | . 724 |
| Satisfaction | User-driven detection method | 3.579 | 0.914 |
| | Moving or Hiding Content | 4.246 | 0.945 |
| | SIC | 5.275 | 0.745 |

Table 36. Variable Pairwise Comparisons for Detection Methods (users Only)

| Variables | (I) Detection Method | (J) Detection Method | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Cognitive workload | SIC | User-driven detection method | -2.1957 | .055 | .000 |
| | | Moving or Hiding Content | -1.3986 | .055 | .000 |
| Detection speed (in seconds) | SIC | User-driven detection method | .6161 | 1.414 | .901 |
| | | Moving or Hiding Content | -46.875 | 1.414 | .000 |
| Perceived ease of use | SIC | User-driven detection method | .4375 | .107 | .000 |
| | | Moving or Hiding Content | 1.5333 | .107 | .000 |
| Perceived effectiveness | SIC | User-driven detection method | 2.0188 | .099 | .000 |
| | | Moving or Hiding Content | 1.5362 | .099 | .000 |
| Satisfaction | SIC | User-driven detection method | 1.6957* | .14859 | .000 |
| | | Moving or Hiding Content | 1.0290* | .14859 | .000 |

### 5.4.3 Cognitive Workload

The ANOVA results indicated a significant impact of browsing method on cognitive load ($F[2, 204] = 797.546$, $p = .001$). The Tukey test results (Table 36) showed that SIC resulted in the lowest perceived cognitive workload, followed by Moving or Hiding Content, which was lower than User-driven detection method.

### 5.4.4 Detection Speed

The ANOVA results showed a significant impact of browsing method on detection speed (F [2, 204] = 741.980, $p$ = .001). The Tukey test results (Table 36) revealed that user detection was the fastest, followed by SIC, which was faster than selective showing.

### 5.4.5 User Perceptions

The results of the ANOVA revealed a significant impact of browsing method on participants' perceived ease of use (F [2, 204] = 108.598, $p$ = .001), perceived effectiveness (F [2, 204] = 226.273, $p$ = .001), and overall satisfaction (F [2, 204] = 66.104, $p$ = .001). According to the Tukey test results (Table 36), users rated SIC the easiest, followed by User-driven detection method then Moving or Hiding Content method being the lowest of ease of use. Additionally, SIC was perceived as the most effective and satisfying browsing method.

### 5.4.6 Attacker position and demographics

The results of the ANOVA analysis indicate that there was no significant effect of attacker positions, attacker ages, or attacker gender on the ability to recall sensitive information.

Table 37. ANOVA Results for Attacker Position, Age, and Gender on Recall of Sensitive Information for Detection Methods

| Variables | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Attacker Position | Between Groups | .001 | 2 | .000 | .002 | .998 |
| | Within Groups | 38.488 | 185 | .208 | | |
| Attacker Gender | Between Groups | .000 | 2 | .000 | .000 | 1.000 |
| | Within Groups | 47.826 | 204 | .234 | | |
| Attacker Age | Between Groups | .000 | 2 | .000 | .000 | 1.000 |
| | Within Groups | 582.870 | 204 | 2.857 | | |

## 5.5 Discussion

The study's results suggest that SIC is a more effective method than User-driven detection for protecting sensitive information during content browsing from shoulder-surfing attacks. Furthermore, the study found that users who used SIC were better able to recall sensitive information than those who used the User-driven detection and Moving or Hiding Content methods, as evidenced by Table 32 and Table 35. Further analysis indicated that the attackers' ability to recall sensitive information was not related to their educational background, gender, or age group. This finding is consistent with previous studies [74, 75], which suggest that shoulder-surfing attacks do not require any specific skills or knowledge. The results highlight the importance of technical solutions like SIC in protecting users' privacy and improving the usability of portable devices. Whether attackers' angle of observation (left or right) affected their information recall was also analyzed. No significant differences were observed. This result agrees with a previous study's findings [38].

Additionally, we found that SIC was faster than Moving or Hiding Content as it does not rely on a user gesture to hide the screen. SIC employs automatic detection of people in proximity and hides sensitive information without any user input, allowing for faster browsing speeds. Furthermore, there was no statistically significant difference in detection speed between SIC and the User-driven detection method, even though the latter method leaves users with usability issues since they must rely on their own detection abilities.

SIC imposes no additional cognitive workload on users and does not require them to perform any extra tasks. Furthermore, we found that the User-driven detection method was the fastest in terms of detection speed. The main reason for this was that we instructed users to rely on their awareness to protect their sensitive information. However, we also found that many users moved

on to display the following email when displayed their email when potential attackers appeared in their area, regardless of the attacker's position or ability to see the screen content. This assumption was confirmed by the fact that users remembered less of their sensitive information when relying on their awareness. Our results indicated that SIC outperformed the User-driven detection method in terms of ease of use, effectiveness, and user satisfaction. This highlights users' desire for a system that helps them protect sensitive information while browsing in public spaces. With SIC, users do not need to make any gestures or hide non-sensitive information, and they can use their devices without interruption.

In summary, SIC was found to be the most effective method for detecting and protecting sensitive information. Attackers were less successful at recalling information with this method compared to the other techniques. Furthermore, SIC users reported the lowest cognitive workload and rated it as the most effective browsing method. Overall, users expressed higher satisfaction with SIC than with the User-driven detection method.

Therefore, SIC appears to be a promising and straightforward method for protecting the privacy of laptop users in public spaces. It efficiently protects sensitive information without requiring users to learn new skills or interrupting their browsing. The method automatically detects nearby individuals and labels sensitive information, ensuring ease of use, effectiveness, and user satisfaction. In summary, SIC is an effective and promising solution for protecting sensitive information on laptop screens while maintaining usability.

# CHAPTER 6: DISSERTATION CONTRIBUTIONS AND LIMITATIONS

## 6.1 Research Contributions

This dissertation addresses fundamental privacy challenges that arise when users interact with laptops in public environments. It makes innovative, novel contributions to the study of privacy challenges and protection. From a research perspective, we improve the understanding of user behavior and the privacy obstacles that arise when interacting with laptops in public venues. We also present the design and evaluation of new technical methods for protecting sensitive information when interacting with laptops in such circumstances.

Our research offers significant contributions. First, we provide an overview of various methods for protecting sensitive information during browsing and typing from shoulder-surfing attacks and related practices. Second, we present a technical solution called D&L. This solution detects sensitive information in textual content and automatically labels it with a category name using advanced natural language processing techniques. It then uses a TTS function to read the information to users through their headphones when they click on the label name. D&L is the first method to apply NLP techniques to protect sensitive information from shoulder-surfing attacks. Third, we present a technical solution called RLSITE. This solution captures and interprets lip movements, allowing users to employ them to input sensitive information. It then labels the information with a category name and reads it to users through their headphones when they click on a label. Therefore, no virtual or physical keyboards will be needed or involved, which could enable attackers to see what is being typed, are necessary. To our knowledge, RLSITE is the first system to employ lip reading techniques to protect sensitive information from shoulder-surfing attacks. Fourth, this dissertation describes the design, development, and evaluation of the SIC method, which employs image analysis tools to detect when unauthorized individuals are situated

near laptop users. The system then notifies users by activating an audible alarm and automatically labels sensitive information. Empirical evaluation through three controlled laboratory experiments demonstrates the superiority of sensitive information protection and higher levels of user perceptions and satisfaction than the baseline methods.

## 6.2 Theoretical and Practical Implications

The proposed methods, D&L, RLSITE, and SIC, have significant practical implications for protecting sensitive information displayed on smart devices. These methods detect sensitive information in textual content and categorize it by labeling it with a specific category name. Users can access this information by clicking on the corresponding label, and it is read to them through headphones, which reduces the risk of unauthorized access. Additionally, labeling sensitive information can help users categorize information based on its type, making it easier to manage information securely.

Furthermore, the proposed methods provide valuable insights that portable device designers and manufacturers can use to design more secure techniques for protecting sensitive information. They can be easily implemented on most portable and smart devices in public venues, making them widely accessible. The proposed methods offer enhanced security for sensitive information displayed on smart devices, which is crucial in industries such as finance, healthcare, and government, where secure data management is important. They can provide an added layer of security, helping to ensure that sensitive information is handled securely and efficiently.

The study results showed that the proposed methods can reduce the risk of interception of sensitive information through shoulder-surfing attacks. The proposed methods can benefit individuals seeking to protect sensitive information and companies and organizations wishing to

secure sensitive information from shoulder-surfing attacks on their employees. They provide practical benefits for individuals and companies by helping users easily review sensitive information. They improve the user experience by automatically detecting and labeling sensitive information. As a result, users can quickly access the information they need. Using headphones to read the information can also make it easier for users to review it in private or noisy environments, saving time and increasing efficiency. Using headphones eliminates the need for users to view the information on a screen, reducing the risk of visual distraction and increasing the user's focus on the task at hand.

The proposed methods can also improve data management by making organizing and categorizing sensitive information easier. Labeling sensitive information can provide valuable insights into the types of sensitive information displayed on a device, which can help organizations identify areas for improvement in their data management practices. The proposed methods can help organizations ensure that sensitive information is handled securely and efficiently by making it easier to manage sensitive information.

Another benefit of the proposed methods is that they provide visually impaired users with increased accessibility to sensitive information. Using headphones to read information eliminates the need for users to view information on a screen, making it easier for visually impaired users to access and review the information, especially in private or noisy environments. They are designed to be non-intrusive and easy to use, helping increase the likelihood that individuals and companies will adopt them. They can be incorporated into mobile apps and other software that handle sensitive information, making it easier for users to access and protect their data. The RLSITE and SIC methods integrated with D&L can offer many benefits for both users and organizations. By enhancing security, improving the user experience, improving data management, and increasing

accessibility for visually impaired users, the system can help ensure that sensitive information is handled securely and efficiently. They benefit companies and organizations looking to secure sensitive information from shoulder-surfing attacks on their employees. The ease of review and increased accessibility that RLSITE and SIC with D&L offer can provide a simple but effective solution for companies and organizations at risk of losing sensitive information through shoulder-surfing attacks. The RLSITE method allows users to input sensitive information using lip reading, thus improving security and ease of use over typing on a physical or virtual keyboard. Using RLSITE can also help reduce the risk of keyboard-logging malware and other keyloggers used to steal sensitive information. Finally, social media applications like WhatsApp and Twitter could utilize this study's results to develop more efficient methods for protecting user privacy.

Finally, The D&L method and RLSITE method have theoretical implications for enhancing data privacy and security in contexts where sensitive information is present in text. The D&L method showcases the potential of NLP, while the RLSITE method demonstrates the potential of lip-reading approaches.

## 6.3 Limitations and Future Work

While this research makes significant progress in protecting against shoulder-surfing attacks, it is important to acknowledge its limitations. One limitation is that shoulder-surfing attacks are influenced by various factors, such as the attacker and user's positions, height, body size, and laptop screen size. These factors can create different levels of protection against shoulder-surfing attacks. Additionally, the study involved full-face detection, while real-world situations may have partially concealed faces. Therefore, there is a need for detecting partially visible faces to improve the effectiveness of the proposed method.

Another limitation of the study is that the subjects were mostly students, which may not accurately represent the general population. However, this study had a larger sample size compared to similar studies. Future studies could use more diverse and larger samples to validate the results obtained in this dissertation.

However, this dissertation presents a solid foundation for evaluating shoulder-surfing attacks. A customized version of D&L could be designed to protect specific types of sensitive information. Evaluating a method that protects image-based content by analyzing image sensitivity would also be beneficial. Since this study only involved English-language information, future studies could explore other languages to determine if the proposed method is effective across different languages and cultures.

In conclusion, this research has limitations but provides a foundation for improving protection against shoulder-surfing attacks. Future studies can build upon this work by addressing the limitations and exploring further applications of the proposed method.

# REFERENCES


[1] L. Federica, *Forecast number of mobile devices worldwide from 2020 to 2025*, Statista Research, 2022.

[2] S. A. Deepak, K. N. Naresh, and S. Pradeep, "Exploring the effectiveness of word embedding based deep learning model for improving email classification," *Data Technologies and Applications,* vol. 56, pp. 23, 2022.

[3] C. Monitor. "Email Usage Statistics in 2021," March/1/2022; https://tinyurl.com/yc65swax.

[4] Marigold. "How many people in the world use email," March/12/2022; https://tinyurl.com/3s459fwc.

[5] H. M. Tarallo, "Social engineering—countermeasures and Controls to Mitigate Hacking," Social Science, Utica College, United States, New York, ProQuest Dissertations & Theses Global, 2015.

[6] J. Obuhuma, Zivuku, Shingai, "Social Engineering Based Cyber-Attacks in Kenya." pp. 1-9.

[7] M. Langer, R. Siegel, M. Schilling, T. Hunsicker, and Cornelius, "An open door may tempt a saint: Examining situational and individual determinants of privacy-invading behavior," in Eighteenth Symposium on Usable Privacy and Security Boston, MA, USA, 2023, pp. 407-426.

[8] K. Austin. "What Is Shoulder Surfing?," February/14/2022; https://tinyurl.com/3deppj8z.

[9] P. P. Shi, "Methods and Techniques to Protect Against Shoulder Surfing and Phishing Attacks," Information Systems Engineering, Concordia University, 2010.

[10] L. Muntingh, "Identity Theft Statistics," https://tinyurl.com/5n7w52hm, [February/14/2022, 2022].

[11] J. Buzzard, "Identity Fraud Study: The Virtual Battleground," 1, https://tinyurl.com/ycxpzc94, [August/11/2022, 2022].

[12] J. Akin, "Identity Theft Is on the Rise, Both in Incidents and Losses," 1, https://tinyurl.com/2d67tn9w, 2022].

[13] IONOS, "Shoulder surfing – an underestimated threat?," 1, https://tinyurl.com/44u3hbtx, 2020].

[14] H. Kim, H. Kim, and J. W. Yoon, "A New Technique Using a Shuffling Method to Protect Confidential Documents from Shoulder Surfers," in International Conference on Software Security and Assurance (ICSSA), Suwon, Korea (South), 2015, pp. 7-12.

[15] S. Beier, and K. Larson, "How does typeface familiarity affect reading performance and reader preference?," *Information Design Journal,* vol. 20, no. 1, pp. 16-31, 2013.

[16] F. Brudy, D. Ledo, S. Greenberg, and A. Butz, "Is anyone looking? Mitigating shoulder surfing on public displays through awareness and protection," in Proceedings of The International Symposium on Pervasive Displays, Copenhagen, Denmark, 2016, pp. 1-6.

[17] S. Pushp, Y. Liu, M. Xu, C. Koh, and J. Song, "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,* vol. 2, no. 2, pp. 1-38, 2018.

[18] H. Zhou, V. Ferreira, T. Alves, B. MacKay, K. Hawkey, and D. Reilly, "Exploring Privacy Notification and Control Mechanisms for Proximity-Aware Tablets," *International Journal of Mobile Human Computer Interaction (IJMHCI),* vol. 7, pp. 1--19, 2016.

[19] T. Van Nguyen, N. Sae-Bae, and N. Memon, “DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices,” *computers & security,* vol. 66, pp. 115-128, 2017.
[20] O. Wiese, and V. Roth, "See you next time: A model for modern shoulder surfers." pp. 453-464.
[21] C.-Y. Chen, B.-Y. Lin, J. Wang, and K. G. Shin, “Keep Others from Peeking at Your Mobile Device Screen!,” in International Conference on Mobile Computing and Networking, Los Cabos, Mexico, 2019, pp. 1-16.
[22] K. Ragozin, Y. S. Pai, O. Augereau, K. Kise, J. Kerdels, and K. Kunze, “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, 2019, pp. 1-6.
[23] A. Maiti, M. Jadliwala, and C. Weber, “Preventing shoulder surfing using randomized augmented reality keyboards,” *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, pp. 630-635, 2017.
[24] H. Zhou, V. Ferreira, T. Alves, K. Hawkey, and D. Reilly, “Somebody is peeking! A proximity and privacy aware tablet interface,” in Conference on Human Factors in Computing Systems Seoul, Republic of Korea, 2015, pp. 1971-1976.
[25] F. Lan, G. Zhai, Z. Gao, and X. Yang, "Live demonstration: Screen piracy protection using saturation laser attack and tpvm." pp. 2376-2376.
[26] I. Editor, "10 Things to Know About Visual Hacking," 1, https://tinyurl.com/438srza8, [March/04/2020, 2018].
[27] K. Mohamed, L. Trotter, M. Tessmann, C. Dannhart, A. Bulling, and F. Alt, “EyeVote in the wild: Do Users bother correcting system errors on public displays?,” *ACM International Conference Proceeding Series,* vol. 10, pp. 57-62, 2016.
[28] S. Rajarajan, K. Maheswari, R. Hemapriya, and S. Sriharilakshmi, “Shoulder surfing resistant virtual keyboard for internet banking,” *World Applied Sciences Journal,* vol. 31, no. 7, pp. 1297-1304, 2014.
[29] A. U. Zulkurnain, A. Kamal, B. Kamarun, A. B. Husain, and H. Chizari, “Social Engineering Attack Mitigation,” *International Journal of Mathematics and Computational Science,* vol. 1, no. 4, pp. 188-198, 2015.
[30] F. Binbeshr, M. Kiah, L. Y. Por, and A. A. Zaidan, “A systematic review of PIN-entry methods resistant to shoulder-surfing attacks,” *Computers & Security,* vol. 101, pp. 102116, 2021, 2021.
[31] H. Farzand, K. Marky, and M. Khamis, “I hate when people do this; there’s a lot of sensitive content for me" - A Typology of Perceived Privacy-Sensitive Content in Shoulder Surfing Scenarios,” in Eighteenth Symposium on Usable Privacy and Security, Boston, MA, United States, 2022.
[32] A. Saad, M. Chukwu, and S. Schneegass, “Communicating Shoulder Surfing Attacks to Users,” in 17th Intl. Conf. on Mobile and Ubiquitous Multimedia, Egypt, 2018.
[33] H. Farzand, K. Bhardwaj, K. Marky, and M. Khamis, “The Interplay between Personal Relationships & Shoulder Surfing Mitigation,” in Proceedings of Mensch und Computer, Ingolstadt, Germany, 2021.
[34] K. Watanabe, F. Higuchi, M. Inami, and T. Igarashi, “CursorCamouflage: Multiple Dummy Cursors as A Defense against Shoulder Surfing,” in SIGGRAPH Emerging Technologies, Singapore, Singapore, 2017, pp. 1-2.

[35] Mihai Bâce, Alia Saad, Mohamed Khamis, Stefan Schneegass, and A. Bulling, “PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices,” in Privacy Enhancing Technologies Symposium 2022 (PETS 2022), Sydney, Australia, 2022, pp. 650-669.

[36] E. Malin, E. von, D. Buschek, and H. Hußmann, “My Scrawl Hides It All: Protecting Text Messages Against Shoulder Surfing With Handwritten Fonts,” in Conference on Human Factors in Computing Systems San Jose, California, USA, 2016, pp. 2041–2048.

[37] M. Khamis, M. Eiband, M. Zürn, and H. Hussmann, “EyeSpot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing,” *Multimodal Technologies and Interaction,* vol. 2, no. 3, pp. 45, 2018.

[38] O. Viatchaninov, V. Dziubliuk, O. Radyvonenko, Y. Yakishyn, and M. Zlotnyk, “CalliScan: On-device privacy-preserving image-based handwritten text recognition with visual hints,” *UIST 2019 Adjunct - Adjunct Publication of the 32nd Annual ACM Symposium on User Interface Software and Technology*, pp. 72-74, 2019.

[39] Chen Li, Mengti Liang, Ke Xiao, Simon Fong, Qianli Wang, and W. Song, “Human Body and Face Detection based Anti-shoulder Attack System on ATM,” *Association for Computing Machinery*, 2017.

[40] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, “Reducing shoulder-surfing by using gaze-based password entry,” *ACM International Conference Proceeding Series,* vol. 229, pp. 13-19, 2007.

[41] A. Dib, and S. Ghazi, “Anti-Shoulder Surfing Login Based on Multi-Entry Models on Onscreen Keyboard,” *Proceedings - ICNAS 2019: 4th International Conference on Networking and Advanced Systems*, pp. 1-5, 2019.

[42] E. Reed, “A FRAMEWORK FOR DESCRIBING ALTERNATIVE KEYBOARD STRUCTURES IN AUGMENTED REALITY,” *e Southern Association for Information Systems Conference*, 2020.

[43] M. Omata, “A Multi-level Pressure-Sensing Two-Handed Interface with Finger-Mounted Pressure Sensors,” *Graphics Interface Conference* 2009.

[44] P. Mayer, N. Gerber, B. Reinheimer, P. Rack, K. Braun, and M. Volkamer, “I (Don't) See What You Typed There! Shoulder-surfing Resistant Password Entry on Gamepads,” in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19, Glasgow, Scotland Uk, 2019, pp. 1-12.

[45] C. E. Shannon, “A Mathematical Theory of Communication,” *The Bell System Technical Journal,* vol. 27, no. 3, 1948.

[46] L. Zhou, K. Yin, Z. Dongsong, and L. Jianwei, “Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones,” *Decision Support Systems,* vol. 92, 2016.

[47] H. Ahmed, I. Traore, S. Saad, and M. Mamun, “Automated detection of unstructured context-dependent sensitive information using deep learning,” *Internet of Things,* vol. 16, pp. 100444, 2021.

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

[49] SpaCy. "Industrial-Strength Natural Language Processing," May/16/2021; https://spacy.io/usage/linguistic-features.

[50] R. Tatman, "Fraudulent E-mail Corpus (CLAIR collection of "Nigerian" fraud emails)," 2017.
[51] A. J. Aviv, F. Wolf, and R. Kuber, “Comparing Video Based Shoulder Surfing with Live Simulation,” in Proceedings of the 34th annual computer security applications conference, San Juan, PR, USA, 2018.
[52] U. Abrar, X. Hannan, B. Trevor, and L. Mariana, “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, 2014, pp. 302-308.
[53] K. Macnish, “Government surveillance and why defining privacy matters in a post-snowden world,” *Journal of Applied Philosophy,* vol. 35, pp. 417-432, 2018.
[54] B. F. Gore, and R. H. Kim, "NASA Task Load Index," 1, https://tinyurl.com/mrybkapu, [November/6/2021, 2020].
[55] W. D. Marslen-Wilson, & Welsh, A, “Processing interactions and lexical access during word recognition in continuous speech,” *Cognitive Psychology*, 1978.
[56] A. F.-L. a. F. Sukno, “Survey on automatic lip-reading in the era of deep learning,” *Image and Vision Computing*, 2018.
[57] P. Ma, Y. Wang, S. Petridis, J. Shen, M. Pantic, and M. Ai, “Training strategies for improved lip-reading,” *IEEE*, pp. 8472-8476, 2022.
[58] B. Martinez, P. Ma, S. Petridis, and M. Pantic, “Lipreading Using Temporal Convolutional Networks,” *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings,* vol. 2020-May, pp. 6319-6323, 2020.
[59] H.-m. Sun, S.-t. Chen, J.-h. Yeh, and C.-y. Cheng, “A Shoulder Surfing Resistant Graphical Authentication System,” vol. 15, no. 2, pp. 180-193, 2018.
[60] B. Gurung, P. W. C. Prasad, A. Alsadoon, and A. Elchouemi, “Enhanced Virtual Password Authentication Scheme Resistant to Shoulder Surfing,” 2015.
[61] M. Agarwal, M. Mehra, R. Pawar, and D. Shah, “Secure authentication using dynamic virtual keyboard layout,” in International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings, Mumbai, Maharashtra, India, 2011, pp. 288-291.
[62] D. Zhang, Z. Yan, H. Jiang, and T. Kim, “A domain-feature enhanced classification model for the detection of Chinese phishing e-Business websites,” *Information & Management,* vol. 51, no. 7, pp. 845-853, 2014.
[63] R. Eric Tanner, “THE USE OF ALTERNATIVE KEYBOARD STRUCTURES TO PREVENT SHOULDER SURFING ATTACKS IN AUGMENTED REALITY,” 2020.
[64] H. I. Koo, B. S. Kim, Y. K. Baik, and N. I. Cho, “Fast and Simple Text Replacement Algorithm for Text-based Augmented Reality,” *2016 Visual Communications and Image Processing (VCIP)*, no. c, pp. 1-4, 2016.
[65] M. Agarwal, M. Mehra, R. Pawar, and D. Shah, “Secure authentication using dynamic virtual keyboard layout,” *International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings,* vol. 8, no. 5, pp. 288-291, 2011.
[66] Y. B. B, and G. Visvanathan, “Implementing Black hole Password Entry Technique For Mitigating Shoulder-surfing Threat,” *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, no. 1, pp. 1221-1229, 2014.
[67] S. Ali, N. Islam, A. Rauf, and I. U. Din, “Privacy and Security Issues in Online Social Networks,” *Journal of Future Internet,* vol. 10, pp. 1-12, 2018.

[68] L. Prasanna, "Secure Internet Banking Authentication," *Journal of Engineering Sciences,* vol. 11, no. 2, 2020.

[69] J. T. D. Adam J. Aviv, Flynn Wolf, Ravi Kuber, "Towards Baselines for Shoulder Surfing on Mobile Authentication," *ACSAC 2017, San Juan, PR, USA*, 2017.

[70] S. Schneegass, A. Saad, R. Heger, S. Delgado Rodriguez, R. Poguntke, and F. Alt, "An Investigation of Shoulder Surfing Attacks on Touch-Based Unlock Events," *Proceedings of the ACM on Human-Computer Interaction,* vol. 16, pp. 1-14, 2022.

[71] H. Khan, U. Hengartner, and D. Vogel, "Evaluating Attack and Defense Strategies for Smartphone PIN Shoulder Surfing," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montréal, QC, Canada, 2018, pp. 1--10.

[72] H. F. Mohamed Khamis, Karola Marky, "Shoulder Surfing through the Social Lens: A Longitudinal Investigation & Insights from an Exploratory Diary Study," *EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany*, 2022.

[73] S. Maqsood, "Shoulder Surfing Susceptibility of Bend Passwords," *CHI 2014, April 26–May 1, 2014, Toronto, Ontario, Canada*, 2014.

[74] B. Leon, and B. Boštjan, "Shoulder surfing: From an experimental study to a comparative framework," *International Journal of Human Computer Studies,* vol. 130, pp. 1-20, 2019.

[75] M. Eiband, M. Khamis, E. Von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in Conference on Human Factors in Computing Systems, Denver, Colorado, USA, 2017, pp. 4254–4265.

[76] R. D. M. K. Bhowmik, "A comprehensive survey on computer vision based concepts, methodologies, analysis and applications for automatic gun/knife detection," *Journal of Visual Communication and Image Representation*, 2021.

[77] L. Ghemri, "Increasing Students Awareness of Mobile Privacy and Security Using Modules," *Journal of Learning and Teaching in Digital Age*, 2019.

## APPENDIX A: PRE-QUESTIONNAIRE QUESTIONS

1. What is your name?
2. What is your email?
3. What is your gender?
    - Female
    - Male
    - Prefer not to say
4. What is your age group?
    - 18-20 years
    - 21-25 years
    - 26-30 years
    - 31 -35 years
    - 36-40 years
    - 41-45 years
    - 46 years
    - Prefer not to say
5. What is your current employment status?
    - Full-time employment
    - Part-time employment
    - Unemployed
    - Student
    - Retired
6. What is the highest level of education you have completed?
    - High school degree
    - Diploma degree
    - Undergraduate degree
    - Master degree
    - Ph.D. degree
7. What is your ID number that provided to you by the researcher?
8. Do you currently use a laptop device (e.g., Apple Mac, Dell, HP, Lenovo)?
    - Yes
    - No
9. Have you ever used a laptop device to do the following activities in public venues within the past year? (Browsing/reading an email)
    - Multiple times per day
    - Once a daily
    - Weekly
    - Monthly
    - Once or twice a quarter
    - Rarely (once a year or less)
    - Never
10. If the answer to the above question is yes, how often do you browse Web pages/sites on your laptop device?
    - Yes

- No

11. If the answer to the above question is yes, how often do you typing/ writing an email on your laptop device?
    - Multiple times per day
    - Once a daily
    - Weekly
    - Monthly
    - Once or twice a quarter
    - Rarely (once a year or less)
    - Never

## APPENDIX B: NORMAL BROWSING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the Normal browsing method | | | | | | | |
| It was simple to use the Normal browsing method. | | | | | | | |
| Choose number 5, please | | | | | | | |
| It was easy to learn to use the Normal browsing method | | | | | | | |
| I was able to complete the tasks quickly using this Normal browsing method | | | | | | | |
| Overall, I am satisfied with the Normal browsing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX C: ONESPOT BROWSING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the OneSpot browsing method | | | | | | | |
| It was simple to use the OneSpot browsing method. | | | | | | | |
| It was easy to learn to use the OneSpot browsing method | | | | | | | |
| I was able to complete the tasks quickly using this OneSpot browsing method | | | | | | | |
| I was able to efficiently complete the tasks using this OneSpot browsing method | | | | | | | |
| Choose number 2, please | | | | | | | |
| Overall, I am satisfied with the OneSpot browsing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX D: D&L BROWSING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the D&L browsing method | | | | | | | |
| It was simple to use the D&L browsing method. | | | | | | | |
| Choose number 6, please | | | | | | | |
| It was easy to learn to use the D&L browsing method | | | | | | | |
| I was able to complete the tasks quickly using this D&L browsing method | | | | | | | |
| I was able to efficiently complete the tasks using this D&L browsing method | | | | | | | |
| Overall, I am satisfied with the D&L browsing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

# APPENDIX E: NORMAL TYPING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the Normal typing method | | | | | | | |
| It was simple to use the Normal typing method. | | | | | | | |
| It was easy to learn to use the Normal typing method | | | | | | | |
| I was able to complete the tasks quickly using this Normal typing method | | | | | | | |
| I was able to efficiently complete the tasks using this Normal typing method | | | | | | | |
| Overall, I am satisfied with the Normal typing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

# APPENDIX F: VK TYPING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the VK typing method | | | | | | | |
| It was simple to use the VK typing method. | | | | | | | |
| It was easy to learn to use the VK typing method | | | | | | | |
| I was able to complete the tasks quickly using this Normal typing method | | | | | | | |
| I was able to efficiently complete the tasks using this VK typing method | | | | | | | |
| Overall, I am satisfied with the VK typing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX G:RLSITE TYPING METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the RLSITE typing method | | | | | | | |
| It was simple to use the RLSITE typing method. | | | | | | | |
| Choose number 5, please | | | | | | | |
| It was easy to learn to use the RLSITE typing method | | | | | | | |
| I was able to complete the tasks quickly using this RLSITE typing method | | | | | | | |
| I was able to efficiently complete the tasks using this RLSITE typing method | | | | | | | |
| Overall, I am satisfied with the RLSITE typing method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX H: USER-DRIVEN DETECTION METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the User-driven detection method | | | | | | | |
| It was simple to use the User-driven detection method | | | | | | | |
| It was easy to learn to use the User-driven detection method | | | | | | | |
| I was able to complete the tasks quickly using this User-driven detection method | | | | | | | |
| I was able to efficiently complete the tasks using this User-driven detection method | | | | | | | |
| Overall, I am satisfied with the User-driven detection method | | | | | | | |
| Choose number 3, please | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX I: SIC METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat | Agree | Strongly |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the SIC method | | | | | | | |
| It was simple to use the SIC method. | | | | | | | |
| Choose number 5, please | | | | | | | |
| It was easy to learn to use the SIC method | | | | | | | |
| I was able to complete the tasks quickly using this SIC method | | | | | | | |
| I was able to efficiently complete the tasks using this SIC method | | | | | | | |
| Overall, I am satisfied with the SIC method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| Effort / How hard did you have to work to accomplish your level of performance? | | | | | | | |

## APPENDIX K: MOVING OR HIDING CONTENT METHOD QUESTIONNAIRE QUESTIONS

User ID:

| Question | Strongly disagree | Somewhat disagree | Disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| Overall, I am satisfied with how easy it is to use the Moving or Hiding Content method | | | | | | | |
| It was simple to use the Moving or Hiding Content method. | | | | | | | |
| Choose number 5, please | | | | | | | |
| It was easy to learn to use the Moving or Hiding Content method | | | | | | | |
| I was able to complete the tasks quickly using this Moving or Hiding Content method | | | | | | | |
| I was able to efficiently complete the tasks using this Moving or Hiding Content method | | | | | | | |
| Overall, I am satisfied with the Moving or Hiding Content method | | | | | | | |

| Question | Extremely Low | Very Low | Low | Neutral | High | Very High | Extremely High |
|---|---|---|---|---|---|---|---|
| Mental Demand / how mentally demanding was the task? | | | | | | | |
| Physical Demand / how physically demanding was the task? | | | | | | | |
| Temporal Demand / How hurried or rushed was the pace of the task? | | | | | | | |
| Performance / How successful were you in accomplishing what you were asked to do? | | | | | | | |
| **Effort / How hard did you have to work to accomplish your level of performance?** | | | | | | | |

## APPENDIX L: SOME OF THE MULTIPLE-CHOICE QUESTIONS USED IN THE EXPERIMENTS

**Please choose the correct answer to the following questions**

1) Who is the founder of Gifted Pictures Company?
   - ☐ Obama
   - ☐ Keyla
   - ☐ Joy
   - ☐ I do not remember
2) What is the cost of the project design?
   - ☐ $4000
   - ☐ $700
   - ☐ $60
   - ☐ I do not remember

3) Who is the founder of Gifted Pictures Company?
   - ☐ Obama
   - ☐ Keyla
   - ☐ Joy
   - ☐ I do not remember
4) What is the cost of the project design?
   - ☐ $4000
   - ☐ $700
   - ☐ $60
   - ☐ I do not remember
5) From where did Lynette earn her master's degree?
   - ☐ North Dakota State University
   - ☐ Lawrence Technological University
   - ☐ Ohio University
   - ☐ I do not remember
6) How much is the cost for the Intermediate package?
   - ☐ $10000
   - ☐ $54600
   - ☐ $600
   - ☐ I do not remember
7) How much is the monthly full coverage quote that State Farm Insurance offered to that specific vehicle?
   - ☐ $180
   - ☐ $150
   - ☐ $80
   - ☐ I do not remember
8) How much is the cancelation fee on the McNeely Family Dentistry?
   - ☐ $10
   - ☐ $15

- ☐ $50
- ☐ I do not remember

9) What is the name of the person who referred you, who was working at the Bank of America?
   - ☐ John
   - ☐ Adam
   - ☐ Sam
   - ☐ I do not remember
10) What is the organization's name that offered the teaching assistant job?
   - ☐ UNCC
   - ☐ Central Piedmont Community College
   - ☐ Queens University
   - ☐ I do not remember
11) Where are the Bookmark Editors located?
   - ☐ USA
   - ☐ UK
   - ☐ Canada
   - ☐ I do not remember
12) How much is the discount that is offered to support vulnerable children's organizations?
   - ☐ $600
   - ☐ $800
   - ☐ $700
   - ☐ I do not remember
13) What is the sender's name who offered to distribute marketing materials to customers?
   - ☐ Tim
   - ☐ Daniel
   - ☐ Obama
   - ☐ I do not remember
14) How much is the cost for the car repair that you wrote or remembered from your last typing?
   - ☐ $4000
   - ☐ $5460
   - ☐ $10000
   - ☐ I do not remember
15) Which country would you import products from that you wrote or remembered from your last typing?
   - ☐ China
   - ☐ U.K.
   - ☐ Russia
   - ☐ I do not remember
16) Where is the furniture brand shop location that you wrote or remembered from your last typing?
   - ☐ Minnesota
   - ☐ Chicago
   - ☐ New York
   - ☐ I do not remember

17) What is the name of the person who offered to design a mobile app that you wrote or remembered from your last typing?
    - ☐ Obama
    - ☐ Emily
    - ☐ Donald
    - ☐ I do not remember
    - ☐ Predication is not accurate
18) Where is the location of ZinZin's Company that you wrote or remembered from your last typing?
    - ☐ USA
    - ☐ Tokyo
    - ☐ China
    - ☐ I do not remember
    - ☐ Predication is not accurate
19) Where did the gift card comes from that that you wrote or remembered from your last typing?
    - ☐ America
    - ☐ Mexico
    - ☐ Africa
    - ☐ I do not remember
    - ☐ Predication is not accurate
20) Who is the smartphone developer that offered to design a new application?
    - ☐ Tim
    - ☐ Donald
    - ☐ Sam
    - ☐ I do not remember