IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 January 2024, accepted 2 March 2024, date of publication 7 March 2024, date of current version 19 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373662

TOPICAL REVIEW

A Systematic Literature Review on the Security Attacks and Countermeasures Used in Graphical Passwords

LIP YEE POR[1], (Senior Member, IEEE), IAN OUII NG[1], YEN-LIN CHEN[2], (Senior Member, IEEE), JING YANG[1], (Graduate Student Member, IEEE), AND CHIN SOON KU[3]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2]Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei 106344, Taiwan
[3]Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia

Corresponding authors: Yen-Lin Chen (ylchen@mail.ntut.edu.tw), Lip Yee Por (porlip@um.edu.my), and Chin Soon Ku (kucs@utar.edu.my)

This work was supported by National Science and Technology Council in Taiwan under grant numbers NSTC-112-2221-E-027-088-MY2 and NSTC-112-2622-8-027-008 and also supported by the Ministry of Education of Taiwan under Official Document No. 1122302319 entitled "The study of artificial intelligence and advanced semiconductor manufacturing for female STEM talent education and industry-university value-added cooperation promotion" and the UTAR Financial Support for Journal Paper Publication Scheme through Universiti Tunku Abdul Rahman (UTAR), Malaysia.

ABSTRACT This systematic literature review delves into the dynamic realm of graphical passwords, focusing on the myriad security attacks they face and the diverse countermeasures devised to mitigate these threats. The core objective of this paper is to identify existing security threats to graphical password schemes and the corresponding countermeasures developed to mitigate these attacks. The study process begins by identifying the usable databases and search engines to identify all the relevant resources. The inclusion and exclusion criteria were carefully selected to prioritize the study, focusing mostly on attacks and countermeasures related to graphical password schemes between 2009 and 2023. After thorough identification and selection progress, 59 studies met all the criteria. Among these studies, 47 mentioned shoulder surfing as a threat to graphical password schemes, while 20 discussed brute force attacks. Additionally, there were 21 papers on dictionary attacks, 13 on smudge attacks, spyware attacks, and social engineering, and 19 that discussed guessing attacks as threats to graphical password schemes. Furthermore, the papers identified several other attacks, including frequency of occurrence analysis attacks, video recording, eavesdropping, computer vision, sonar, and image gallery attacks, with the corresponding numbers of papers being 9, 17, 5, 2, 2, and 1, respectively. The results also highlight the countermeasures proposed in the study papers to mitigate the aforementioned attacks. Among the various countermeasures identified, most revolve around randomization, obfuscation, and password space complexity as the most commonly used techniques for enhancing the security of graphical password schemes.

INDEX TERMS Graphical passwords, security attacks, countermeasures, authentication, cybersecurity.

I. INTRODUCTION

Graphical passwords have emerged as an alternative authentication mechanism, offering a more user-friendly interface compared to traditional text-based passwords [1]. However, as the use of graphical passwords rapidly increases, so does concern about their vulnerability to security attacks [1]. Understanding the landscape of these threats and the countermeasures used to tackle them is crucial for enhancing the security of graphical password systems. This systematic literature review (SLR) delves into the realm of graphical passwords, aiming to comprehensively analyze existing

The associate editor coordinating the review of this manuscript and approving it for publication was Aneel Rahim.

security attacks and the various types of countermeasures employed to safeguard these systems. By examining a range of scholarly databases and publications, this review seeks to offer an in-depth exploration of the threats posed to graphical passwords and the countermeasures developed to combat these vulnerabilities.

The primary research questions guiding this review explore two key aspects of the security landscape of graphical passwords. Firstly, we delve into the existing security attacks targeting graphical passwords to identify the various threats and vulnerabilities affecting these authentication mechanisms. It is essential for us to understand how these passwords might be vulnerable. Subsequently, the review discusses and evaluates the countermeasures that have been developed to overcome the identified security attacks. By evaluating the developed countermeasures, we aim to enhance the security of graphical password systems, ensuring that graphical passwords are as secure as possible.

Aligned with these research questions, the objectives of this SLR are to explore the existing landscape of security attacks on graphical passwords and to investigate and assess the efficiency of countermeasures deployed to address these threats. Furthermore, to conduct a thorough systematic literature review, we will employ a systematic approach, leveraging a wide range of renowned academic databases and repositories known for their scholarly articles and studies. By utilizing specific search keywords, this review aims to provide a comprehensive overview of the current state of knowledge, identifying gaps, trends, and emerging directions within the realm of graphical password security.

The paper's structure is arranged as follows: In the subsequent section, the research method is presented. The results of the systematic literature review following PRISMA guidelines are presented in Section III. The discussion of the review is presented in Section IV. Finally, Section V concludes the review.

II. METHODS

This section outlines the methodology employed to conduct a systematic literature review (SLR) focused on exploring security attacks targeting graphical password schemes and the corresponding countermeasures. The methodology closely adhered to the 'Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, as detailed in the PRISMA 2020 checklist (Appendix A). The PRISMA approach ensured a transparent and structured process in the selection of articles, encompassing their identification, screening, and inclusion. Adhering to PRISMA guidelines aimed to enhance the validity and reliability of our findings by providing a clear and visually comprehensive representation of the review's methodology.

The methodology was designed to thoroughly explore the security threats targeting graphical password systems and the solutions proposed to tackle them. We meticulously searched respected academic databases, using specific keywords and criteria, to find relevant studies. These studies were carefully assessed for their quality and relevance to our goals. We then analyzed and combined their findings to understand the various attack methods on graphical passwords and how well the suggested defenses work. This methodological approach aimed to provide a detailed picture of the vulnerabilities inherent in graphical password systems and the effectiveness of strategies designed to mitigate these threats.

A. DEFINING RESEARCH QUESTIONS AND OBJECTIVES

The primary objective of this systematic literature review is to examine the prevailing countermeasures against security attacks employed in the realm of graphical passwords. The research questions and research objectives are as follows:

Research Questions (RQ):

- What are the existing security attacks on graphical passwords?
- What are the countermeasures introduced to tackle the existing security attacks on graphical passwords?

Research Objectives:

- To identify and investigate the existing security attacks on graphical passwords.
- To identify and investigate the countermeasures developed and implemented to mitigate prevalent security attacks targeting graphical passwords.

B. IDENTIFYING INFORMATION SOURCES/DATABASES

We identified and selected a diverse range of databases, including Academic Search Elite @EBSCOhost, The Science and Information Organization (SAI), Education Research Complete @EBSCOhost, Web of Science, IEEE Xplore, IOPScience, MDPI, ProQuest, SAGE Journals, Semantic Scholar, Science Direct, Scopus, and the ACM Digital Library. We conducted a comprehensive search of these databases to retrieve relevant journal articles and conference papers for the study.

C. DEVELOPING THE SEARCH STRATEGY/SEARCH TERMS

Based on the research questions and objectives, we devised a search strategy by combining keywords and controlled vocabulary terms relevant to password security, potential attacks and countermeasures, and graphical passwords. To ensure a comprehensive search result, we employed different combinations of the search terms and used boolean operators, including AND and OR. For each database involved in the searching process, we customized the search strategy based on its syntax and functionalities. The chosen search terms for this study are as follows:

(''graphical passwords'' OR ''picture-based passwords'' OR ''pattern-based authentication'') AND (''security attacks'' OR ''threats to graphical passwords'' OR ''authentication vulnerabilities'') AND (''countermeasures'' OR ''password security'' OR ''usability of graphical passwords'')

TABLE 1. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Studies that were published between 2009 and 2023.	Studies that primarily focus on textual or biometric passwords.
Papers proposing or discussing countermeasures specifically addressing security attacks in graphical passwords.	Studies that disclose or discuss the vulnerabilities of graphical passwords but do not suggest countermeasures.
Papers published in the English language.	Studies that primarily focus on the user experience and usability of graphical passwords
Peer-reviewed papers, articles, and conference	

D. INCLUSION AND EXCLUSION CRITERIA

The formulation of inclusion and exclusion criteria was conducted to define the studies suitable for inclusion in the review and those that warranted exclusion. Table 1 outlines the criteria used to include or exclude papers from this review.

The decision to focus on the most recent 15 years, from 2009 to 2023, is based on several considerations. This period reflects a crucial phase of technological evolution, marked by substantial advancements in graphical password systems and security technologies. By centering the literature review on this timeframe, the study aims to encompass the latest developments and vulnerabilities in graphical passwords, thereby contributing to a comprehensive understanding of contemporary challenges and emphasizing security attacks and countermeasures relevant to the current threat environment. Meanwhile, the selected 15-year range strikes a balance between capturing a substantial body of relevant literature and preventing information overload, ensuring that the review remains manageable and that the selected studies are both recent and impactful.

E. SCREENING AND SELECTION PROCESS

The selection process consisted of four phases: identification, screening, eligibility, and inclusion. Phases 1 and 2 were conducted by all team members for the initial identification and screening of papers. Phases 3 and 4 involved all team members in the full-text screening and selection of the most pertinent studies.

During the identification process, we used search terms in the title, abstract, and keyword filters to locate relevant studies in the selected databases. All team members manually recorded the titles, DOIs, or URLs of the papers in a Google Sheets document. In the screening phase, we evaluated the papers for applicability and suitability by analyzing their titles and abstracts in relation to our research questions and objectives. Additionally, we manually excluded duplicated studies and those deemed inconsistent or irrelevant to our research topic.

Moving on to the eligibility phase, a team of seven members was assigned to conduct full-text screening to assess the appropriateness of the remaining papers based on the inclusion and exclusion criteria. They also summarized the studies according to the research topic and scope. Finally, in the inclusion stage, the remaining team members evaluated the shortlisted papers based on the summaries made and eliminated those that did not meet the predetermined inclusion and exclusion criteria or were found to be irrelevant to the research question.

F. QUALITY ASSESSMENT

We conducted a comprehensive evaluation to assess the selected papers' quality, aiming to thoroughly analyze both the strengths and weaknesses of the quantitative and qualitative studies. This evaluation focused on closely examining their design and analysis methodologies.

To assess the quality of our quantitative studies, we opted for the Mixed Methods Appraisal Tool (MMAT), a reliable instrument known for effectively evaluating the quality and potential bias within quantitative research studies. Conversely, for the qualitative studies, we chose to utilize the Critical Appraisal Skills Programme (CASP) checklists (CASP, 2020) as our tool for evaluating the research studies. These checklists facilitate a meticulous and systematic examination of research evidence, enabling us to assess its trustworthiness, relevance, and value within a specific context.

Both MMAT and CASP checklists consist of five criteria, ensuring a comprehensive assessment of the quality of quantitative and qualitative studies and strengthening the depth and integrity of our evaluation.

G. DATA EXTRACTION

Data extraction is a critical component of this study, addressing research questions related to existing security attacks on graphical passwords and the countermeasures introduced to mitigate these attacks. Extracted elements, such as research titles, types of attacks, and specific countermeasures, will form a comprehensive foundation for analyzing and understanding the security aspects of graphical passwords. This will enable a thorough investigation into the proposed or existing countermeasures against various attack vectors.

H. DATA SYNTHESIS AND ANALYSIS

The purpose of the data synthesis methodology was to evaluate and summarize the insights obtained from the selected papers and to present the data through tables. This synthesized data forms the primary body of evidence used to address the research questions, which specifically focus on the types of attacks on graphical passwords and the corresponding countermeasures.

Content analysis emerges as the most suitable analytical approach for our study, as our primary objective is to explore and discuss the types of attacks on graphical passwords and their corresponding countermeasures. It is important to note that specific statistical techniques, such as measures of effect and meta-regression, were not within the scope of our study. Therefore, the review is specifically designed to provide an in-depth analysis and discussion of the types of attacks on

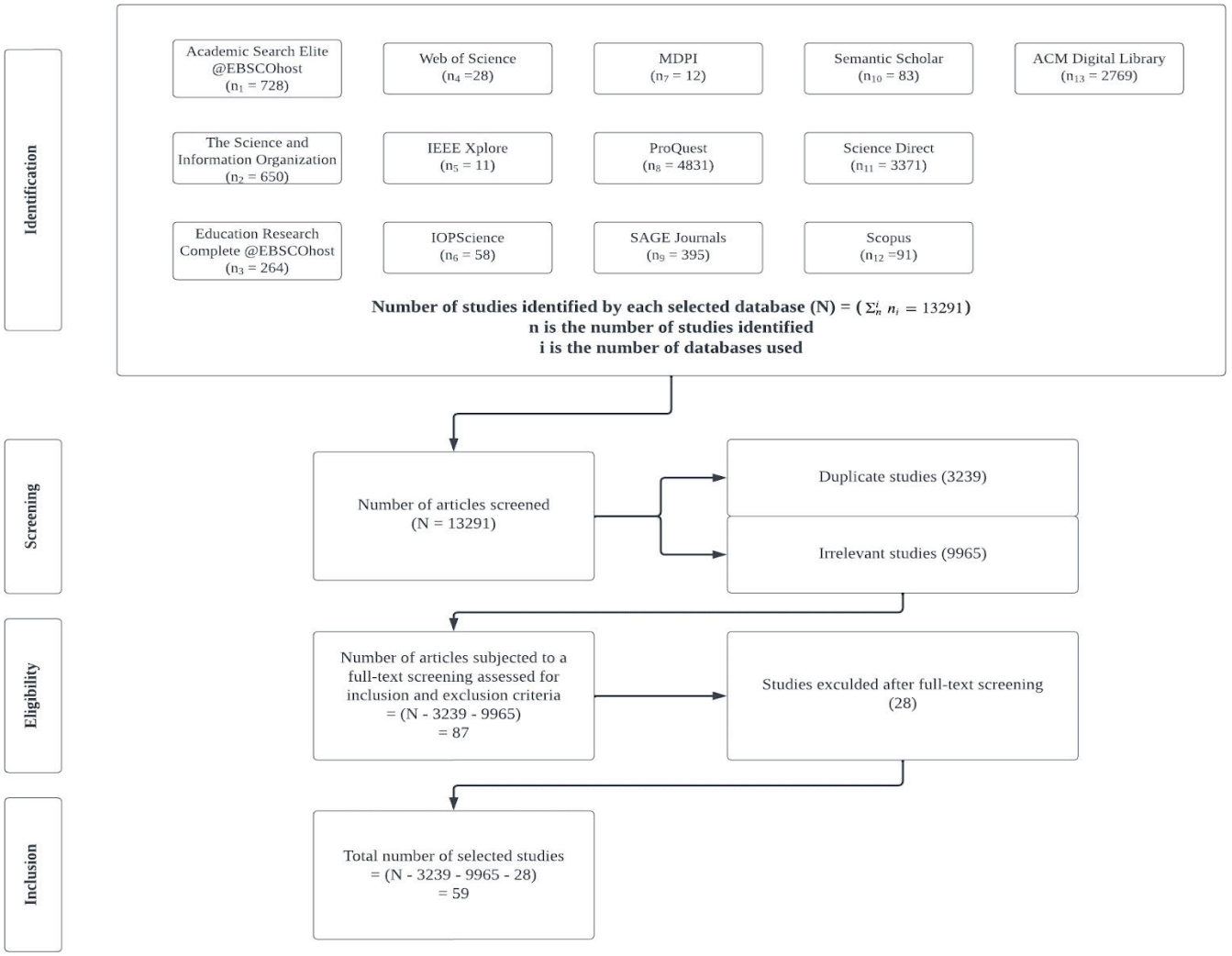

FIGURE 1. PRISMA flowchart for the study selection process.

graphical passwords and their corresponding countermeasures, with an emphasis on the security perspective.

I. IDENTIFY RESEARCH GAPS AND CONTRIBUTIONS

This review synthesizes the current state of knowledge concerning the security aspects of graphical passwords, providing a holistic view for future researchers to explore areas where further investigation is imperative. It contributes to the advancement of knowledge about securing graphical password systems. By reviewing the security threats revealed as well as the countermeasures proposed in the literature, we can identify gaps and limitations in existing strategies for mitigating security attacks. This includes identifying any emerging security challenges that may not have been sufficiently addressed, paving the way for future research endeavors.

Additionally, the insights gained from the review will support the design, development, and implementation of more robust and effective security measures within graphical password systems, thereby enhancing their overall security.

Through highlighting research gaps and contributing insights, this systematic literature review aims to foster the development of highly resilient graphical password systems, ultimately leading to password systems with heightened security.

This paper distinguishes itself by offering a comprehensive overview of the security landscape surrounding graphical password schemes. Through a meticulous examination of 13,291 articles retrieved from 13 databases and subsequent filtering, it identifies 14 prevalent security attacks, ranging from conventional threats like brute force attacks to more sophisticated challenges such as smudge attacks. Notably, the study also meticulously evaluates corresponding countermeasures proposed in previous research, with an emphasis on the widespread use of randomization to enhance security. However, the paper goes beyond mere enumeration of attacks and defenses; it critically assesses the limitations of existing

approaches and highlights gaps in the literature, setting a clear agenda for future research. Moreover, the emphasis on adopting a multidisciplinary approach underscores the paper's commitment to addressing not just technical vulnerabilities but also human factors and usability concerns.

III. RESULTS

A. STUDY SELECTION

Figure 1 illustrates the four stages of the PRISMA flowchart: identification, screening, eligibility, and inclusion, conducted in this systematic literature review. During the identification stage, we found a total of 13,291 studies across all selected databases by using the keywords (''graphic passwords'' OR ''picture-based passwords'' OR ''pattern-based authentication'') AND (''security attacks'' OR ''threats to graphical passwords'' OR ''authentication vulnerabilities'') AND (''countermeasures'' OR ''password security'' OR ''usability of graphical passwords'').

The number of studies identified in each of the selected databases was as follows:

- 728 in Academic Search Elite @EBSCOhost
- 650 in the Science and Information Organization
- 264 in Education Research Complete, @EBSCOhost
- 28 in the Web of Science
- 11 in IEEE Xplore
- 58 in IOPScience
- 12 in MDPI
- 4,831 in ProQuest
- 395 in SAGE Journals
- 83 in Semantic Scholar
- 3,371 in Science Direct
- 91 in Scopus
- 2,769 in the ACM Digital Library

We excluded a total of 3,239 duplicate studies and 9,965 irrelevant studies during the screening stage. After the screening stage, 87 of the remaining studies underwent full-text screening to assess their eligibility based on the inclusion and exclusion criteria. Following the full-text screening, 28 studies were excluded. In the final stage, 59 of the remaining studies that met all the inclusion and exclusion criteria were included in our systematic literature review.

B. QUALITY OF INCLUDED STUDIES

Among the 35 quantitative studies analyzed, 24 studies (68.57%) obtained MMAT scores of 100%, indicating high quality as they completely fulfilled the criteria. Eleven studies (31.43%) were of medium quality, with MMAT scores ranging from 60% to 80%, suggesting that these papers partially adhered to the criteria. Notably, there were no quantitative studies categorized as low quality. Some quantitative studies failed to satisfy criterion 1.2 (sample representativeness) due to the absence of the target group or demographic information of the participants. This may raise questions about whether the participants involved represent a valid sample of the entire target population. The quality assessment of the quantitative articles is reported in the Assessment of Study Quality (Appendix B).

Among the 24 qualitative studies analyzed, 12 studies (50%) achieved high quality as they fulfilled all the criteria outlined by the CASP tool. The other half of the studies demonstrated medium quality due to a lack of description of the data collection and analysis processes. These studies primarily focused on the conceptual development and analysis of the proposed graphical password schemes. The CASP assessment for the qualitative studies is detailed in the Assessment of Study Quality (Appendix B).

TABLE 2. Types of security attacks and related articles.

Type of Security Attack	Related Articles
Shoulder Surfing Attack	[1], [2], [3], [4], [5], [6], [7], [9], 10], [12], [13], [15], [17], [18],[19], [20], [21], [22], [23], [24], [25], [26], [28], [29], [30], [32],[34], [35], [36], [37], [38], [39], [40], [42], [43], [44], [45], [46],[47], [48], [49], [50], [51], [53], [56], [57], [58]
Video Recording Attack	[1], [2], [3], [9], [23], [25], [27], [28], [30], [32], [35], [36], [47],[48], [50], [56], [57]
Smudge Attack	[2], [5], [8], [9], [10], [20], [31], [39], [43], [47], [48], [56], [58]
Spyware Attack	[4], [9], [12], [15], [16], [17], [20], [29], [38], [39], [49], [51], [52]
Brute Force Attack	[2], [5], [6], [9], [10], [15], [17], [19], [20], [21], [22], [26], [29], [31], [39], [46], [47], [49], [51], [52]
Computer Vision Attack	[54], [55]
Dictionary Attack	[4], [5], [6], [9], [10], [13], [15], [17], [19], [20], [26], [29], [32], [37], [38], [39], [41], [46], [49], [51], [56]
Eavesdropping Attack	[4], [6], [10], [13], [32]
Frequency of Occurrence Analysis (FOA) Attack	[4], [13], [14], [15], [17], [23], [33], [35], [42]
Guessing Attack	[1], [2], [6], [9], [10], [12], [13], [19], [20], [21], [26], [32], [34], [39], [47], [49], [50], [51], [56]
Social Engineering Attack	[2], [3], [4], [9], [10], [13], [15], [19], [29], [37], [38], [39], [56]
Image Gallery Attack	[29]
Sonar Attack	[11], [59]

C. RQ1: WHAT ARE THE EXISTING SECURITY ATTACKS ON GRAPHICAL PASSWORDS?

A total of 13 security attacks are reported in the articles. Table 2 displays the types of security attacks and the related articles discussing each attack.

Shoulder surfing involves the act of observing someone else using a computer or mobile device to enter a password with the intention of accessing their private or sensitive information [2]. This commonly occurs in crowded public places. There are several methods of shoulder surfing used to obtain user credentials or private information, such as direct visual observation or recording the entire login process [47].

In a video-recording attack, a hacker only requires a device with a camera to record the user while they enter their password [25]. The hacker can then replay the video to retrieve the password.

Smudge attacks, as described in [47], are another common form of attack on graphical passwords that is challenging to eliminate. These attacks occur when smudges are left on the screen after a user enters their password, allowing attackers to deduce the password by analyzing the smudges.

Spyware attacks involve the installation of malicious software on a user's device to record their information and actions [49]. One example of spyware is a screen scraper, which records all user activities on the screen.

As explained in [26], a brute-force attack entails attempting to guess a password by systematically trying every possible combination or passphrase until the correct one is found. Typically, brute force attacks target passwords with a limited character space. Additionally, a collection of forged fingerprint details can be used to launch a brute-force attack. In the case of captchas, a type of pictorial password, attackers may use optical character recognition (OCR) to perform a brute force attack.

A computer vision attack leverages artificial intelligence (AI) technology. It involves feeding a live feed or pre-recorded video into a system equipped with computer vision capabilities [55]. The system tracks the user's finger movements from the camera's perspective, generates the fingertip movements, transforms them into the user's perspective, infers several candidate patterns, and ranks them based on predefined criteria. This process ultimately provides the threat actor with the deduced graphical password [54].

In [4], a dictionary attack is defined as a password-cracking method where the attacker tries all possible passwords from a precompiled list (dictionary) based on user behavior. This attack uses a systematic key search approach, taking into account the most likely chances of success.

Eavesdropping, a man-in-the-middle attack, involves intercepting communication between the user and the server. The hacker can either intercept information sent by the user to the server and attempt to decrypt it or intercept the user's request and replay it to the server later to gain access to the user's account [13].

The frequency of occurrence analysis (FOA) attack analyzes the frequency of a specific pattern occurring during the login process [33]. Its aim is to identify and limit the number of possible keys used for authentication. FOA can analyze either image frequency or keypress location frequency, depending on the authentication scheme's design. By analyzing image frequency, hackers can make educated guesses about the password based on the most frequently occurring images [33]. Key press location frequency analysis aims to identify the most frequent location of the final image used for authentication by constructing a heatmap based on frequency [35].

Users often incorporate personal details into their graphical passwords for easier recall, increasing their vulnerability to guessing attacks [13]. While the success of such attacks depends on the accuracy of the estimate, they remain a serious concern.

Social engineering attacks involve manipulating users through trickery or exploitation of user information [15]. These attacks do not require technical knowledge but instead manipulate users into unknowingly disclosing their information. One common social engineering tactic is phishing, which can be executed by copying the original website or intercepting the server's response to the user's request and providing a maliciously altered version for the user to input their login details [13].

Image gallery attacks can occur when a threat actor gains physical access to the server or database [29]. With this access, the attacker can bypass any authentication requirements and modify the images used in the login and registration processes or during authentication. Additionally, direct server access may allow the threat actor to log in as any user.

Lastly, every mobile device is equipped with a microphone and speakers, which can be exploited in a sonar attack. A sonar attack involves using recorded acoustic signals to detect the user's gesture while unlocking the phone and deducing the pattern used. The application emits a frequency, often inaudible to most people, which is recorded by the device's microphone. The recorded audio undergoes processing, removing static noise, and is then used for calculations to measure relative movement and infer pattern lines. The inferred pattern lines are used to generate candidate patterns, which are ranked and provided to the attacker [11], [59].

D. RQ2: WHAT ARE THE COUNTERMEASURES INTRODUCED TO TACKLE THE EXISTING SECURITY ATTACKS ON GRAPHICAL PASSWORDS?

1) SHOULDER SURFING ATTACK

Obfuscation: Obfuscation is a technique that makes authentication information unclear to onlookers. It involves hiding or decoding the real input during authentication. For instance, graphical passwords can hide password components among decoy images, making it challenging for observers to identify the correct selections. Two methods for obfuscation are Secure Graphical One-Time Password (GOTPass) [4] and EvoPass [56].

- GOTPass: It uses the "Where You See is What You Enter" (WYSWYE) approach. Users don't directly select password images; instead, they mark positions on a response grid based on the images. Observers see random positions being clicked, making it hard to discern the actual password.
- EvoPass: This method modifies the selected password images to create decoy versions that evolve over time, gradually reducing recognizable information. Users can revert to a previous version if they have trouble recognizing evolved-pass sketches.

Randomization: Randomization introduces randomness in password elements' positions or arrangements, making it difficult for shoulder surfers to capture the actual password.

Two methods are the Coin Passcode Model [49] and the 2D Coordinates System [7].

- Coin Passcode Model: It combines colors, numerical values, and icons to form unique passcodes. Elements in the coin password are randomized every time, enhancing resistance against shoulder surfing and brute-force attacks. User interactions with the interface do not reveal the actual passcode.
- 2D Coordinates System: This approach uses randomized 2D coordinates to secure pictures and generate passwords. Images change randomly in x and y coordinates during login, making it challenging to identify the original picture and enhancing security against shoulder surfing attacks.

2) VIDEO RECORDING ATTACK

Incorporating randomness or visual complexity to confuse potential attackers is a valuable strategy. As described in [27], a graphical password scheme called RiS (Rotating into Sector) was developed for this purpose. Additionally, they introduced another password scheme known as T-RiS (Rotating into Sector Based on Texts). Both RiS and T-RiS feature an LR1 login mode, which enhances security by introducing three concentric rings. This complexity adds a visual challenge for attackers attempting a video recording attack, as only the user can discern the location of the line or sector, and it changes randomly after each character entry. This approach effectively increases the difficulty of capturing the password through video recording.

3) SMUDGE ATTACK

The goal of the proposed countermeasures is to render the smudge marks left on the device screen devoid of useful information or to confuse potential attackers. These countermeasures can be categorized into two approaches:

- Randomizing the arrangement or position of authentication input elements.
- Introducing additional elements apart from patterns or graphical elements.

For instance, in [43], a system called SmudgeSafe was introduced as an authentication system designed to enhance the security of cue-recall graphical passwords. This concept involves applying random affine geometric transformations to the base password image. Since these transformations occur randomly during each login, smudge traces from a previous login become invalid for the current password image. This approach effectively mitigates the risks associated with smudge attacks and ensures that smudge marks do not reveal useful information to potential attackers.

4) SPYWARE ATTACK

Countermeasures against spyware attacks encompass various strategies, including randomization, conducting tests during authentication, employing different input methods, and incorporating additional elements during authentication. For instance:

- Randomization: A hybrid graphical-password mobile authentication scheme called Coin Passcode Graphical Password Authentication, proposed by [49], is an example of randomization. This scheme requires users to input the coin passcode in the correct sequence for authentication. The algorithm iterates six times to randomize the keypad elements for all six inputs. This randomization helps prevent unauthorized access to mobile devices through spying.
- Performing Tests During Authentication: CAPTCHA (Completely Automated Public Turing Tests to Tell Computers and Humans Apart), as proposed in various papers [15], [16], [26], [39], [52], involves conducting tests during authentication. Although there may be slight variations in implementations across different papers, the common goal is to generate problems that only humans can solve, surpassing the capabilities of current computer programs. This approach adds an additional layer of security to thwart spyware attacks.

5) BRUTE FORCE ATTACK

Countermeasures against brute force attacks encompass various strategies, including randomization, utilizing large password spaces, implementing additional authentication layers, and restricting login attempts. Here are some examples:

- Randomization: One example of randomization is the pass-matrix proposed by [51]. It offers a secure login interface featuring an 8×8 grid for selecting alphanumeric characters during the login phase. Each selected character undergoes a transpose operation on the columns during login sessions. This graphic (mutating) password scheme effectively thwarts brute-force attacks.
- Large Password Space: The vibration-and-pattern (VAP) code, introduced by [10], is an example of a large password space. It combines two distinct techniques, resulting in a password space that is influenced by the individual techniques' password spaces. This scheme offers a significantly larger number of potential patterns compared to Android-based PL, especially when $L \geq 4$. The expanded password space enhances security against brute-force attacks.

These countermeasures collectively aim to bolster security against brute force attacks by introducing complexity, randomness, and additional layers of authentication, making it exceedingly challenging for attackers to guess passwords through exhaustive trial-and-error methods.

6) COMPUTER VISION ATTACK

Countermeasures against computer vision attacks, as described in [54] and [55], involve various strategies to enhance security:

- Randomizing Pictures: One countermeasure involves randomizing the pictures, which shuffles the location of the touch point for each login. This randomization adds complexity to the authentication process and makes it challenging for attackers using computer vision techniques.
- Dynamic Screen Changes: Devices can prevent people from secretly recording videos by dynamically changing the screen's color and brightness. This alteration confuses the camera and prevents attackers from capturing a clear video for malicious purposes.
- User Education: Users should be educated about security best practices, including ensuring that their fingers are completely covered when drawing a pattern during authentication. This minimizes the chances of an attacker capturing usable information through video recording.
- Additional On-Screen Activities: Adding other on-screen activities to the pattern unlocking process can enhance security. For example, prompting the user to enter a sentence using a Swype-like method or sketching various graphical shapes before or after drawing the pattern can make the authentication process more complex for potential attackers.
- Skipping Dots: Users can also employ the strategy of skipping some dots in a vertical, horizontal, or diagonal line when drawing a pattern. This intentional skipping makes it challenging for tracking algorithms to identify which dots are intentionally skipped, further thwarting computer vision-based attacks.

These countermeasures collectively aim to increase the complexity and unpredictability of the authentication process, making it significantly more difficult for attackers to exploit computer vision techniques to compromise security.

7) DICTIONARY ATTACK

Countermeasures against dictionary attacks include various techniques that introduce randomness and complexity to the authentication process:

- Conundrum-Pass: This approach, proposed in [6], begins by asking users to select a desired image and choose a number, n. The chosen number is used to divide the selected image into a square matrix of n $\times$ n. Users can then create their desired patterns by selecting specific image chunks. During the login session, the concept of shuffling is introduced, where the image chunks are randomly arranged. To unlock the screen, users must select the previously chosen grids in the correct order. This method introduces randomness and complexity to the pattern selection process, making it resistant to dictionary attacks.
- Spin-Wheel-Based Authentication: Another countermeasure, suggested in [38], involves a spin-wheel-based graphical authentication mechanism. This approach offers a large password space, which makes it highly secure against dictionary attacks. Users are presented with a spin wheel consisting of four sub-wheels, each containing 36 slots filled with numbers from 1 to 36, arranged randomly. To set a password for authentication, users must select a number from each sub-wheel and arrange the four numbers in a row by rotating the wheel. This method introduces complexity and unpredictability into the password creation process, making it resistant to dictionary-based attacks.

These countermeasures aim to thwart dictionary attacks by making it challenging for attackers to guess passwords through systematic trial and error, even if they possess a predefined list of potential passwords.

8) EAVESDROPPING ATTACK

Countermeasures against eavesdropping attacks involve the use of secure authentication protocols and techniques that introduce randomness into authentication sessions to make it difficult for attackers to intercept and replicate authentication data. Here's how these countermeasures work:

- Authentication Protocol: Implementing a secure authentication protocol for data transmission between the server and client can effectively mitigate eavesdropping attacks. The key idea is to ensure that the values sent during each authentication session are randomized and unique. This prevents attackers from intercepting and replicating the same authentication data, even if they manage to eavesdrop on the communication.
- Hashing Timestamps and Pass-image Components: As proposed by English and Poet [13], one countermeasure involves applying hashing to various authentication components, including timestamps and pass-image-related data. By hashing these components, the authentication data becomes obfuscated and challenging for attackers to decipher. Hashing ensures that even if intercepted, the authentication data appears as random and unintelligible strings, making it resistant to eavesdropping.
- Random Location Assignment for Passphrase: Another security measure suggested by English and Poet [13] is to randomly assign the location of the passphrase for each authentication attempt. This means that the position of the passphrase is different for every session and is sent to the server for verification. This dynamic location assignment ensures that the data sent during authentication is always unique and distinct, reducing the risk of a replay attack.

By incorporating these countermeasures into the authentication process, organizations can enhance the security of their systems and protect against eavesdropping attacks by ensuring that intercepted data remains useless and non-reproducible for malicious actors.

9) FREQUENCY OF OCCURRENCE ANALYSIS (FOA) ATTACK

Countermeasures against Frequency of Occurrence Analysis (FOA) attacks can be implemented to enhance the security

of graphical password systems. These countermeasures target both FOA attacks based on image frequency and those based on the location where the pass-image appears. Here's how these countermeasures work:

Countermeasures Against FOA Attacks Based on Image Frequency:

- Use of Decoy Images: One effective countermeasure is to use decoy images that are the same for each pass-image. By employing this approach, both the decoy images and the actual pass-image occur at the same frequency, making it challenging for an attacker to identify the correct pass-image among the decoys.
- Display of ''Dummy Screens'' on Failed Attempts: In cases where users fail an authentication attempt, the subsequent session should display only distractor images, often referred to as ''dummy screens.'' This practice reduces the likelihood of an attacker observing the correct pass-image during repeated failed attempts.
- Limit on Failed Authentication Attempts: Implementing a limit on the number of failed authentications attempts a user can perform is another valuable countermeasure. This restriction aims to prevent attackers from repeatedly attempting to identify the pass-images through numerous incorrect guesses [14].

Countermeasures Against FOA Attack Based on Pass-image Location:

- Dynamic Generation of Target Images: To thwart FOA attacks based on the location of the pass-image, a method is proposed where users select a sequence of unique images during the registration phase. These selected images are used to identify the final ''target'' image within the grid during the authentication phase [23].
- Algorithmic Determination of Target Images: Initially, the first and second password images are used as the starting picture and cue picture, respectively. An algorithm is applied to determine the first ''target'' image. This ''target'' image becomes the starting picture for the next step, while the next registered password image serves as the cue picture. This process continues until users identify the final ''target'' image [23].
- Random Distribution of Target Images: The effectiveness of this method lies in the generation of random and evenly distributed ''target'' images across all grid locations. This randomization makes it challenging for attackers to predict the location of the pass-image [23].

By implementing these countermeasures, organizations can enhance the security of their graphical password systems and mitigate the risks associated with FOA attacks, whether they are based on image frequency or pass-image location.

10) GUESSING ATTACK

Countermeasures Against Guessing Attacks:

- Randomization Technique: A key strategy to thwart guessing attacks is the use of the randomization technique. One notable example is the ''Click-based Captcha as a Graphical Password (CaRP)'' [26] system, which effectively minimizes the risk of guessing attacks by generating random challenge images that contain password letters for each authentication session.
- ClickText Scheme: Within the CaRP system, the ''ClickText'' scheme is employed, which involves the random arrangement of alphanumeric and special characters within a challenge image. This randomization adds a layer of complexity and unpredictability to the authentication process, making it difficult for attackers to guess the correct password [26].
- AnimalGrid Scheme: Another approach within the CaRP system is the ''AnimalGrid'' scheme, which utilizes 2D animal images as part of the authentication process. Similar to the ClickText scheme, the AnimalGrid scheme introduces randomness and variability in the arrangement of these images, further enhancing security against guessing attacks [26].

By incorporating these randomization techniques and schemes, organizations can effectively mitigate the risk of guessing attacks in their graphical password systems, thereby enhancing overall security.

11) SOCIAL ENGINEERING ATTACK

Countermeasures Against Social Engineering Attacks:

- User Awareness: Preventing social engineering attacks heavily relies on user awareness and vigilance. Users should be educated and trained to recognize potential threats and tactics employed by attackers. One common social engineering tactic is phishing.
- HTTPS Verification: Users can protect themselves from phishing attacks by verifying the presence of an HTTPS prefix before entering their password on a website. HTTPS indicates that the website employs Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, providing a secure and encrypted connection. This visual indicator helps users identify legitimate and secure websites [15].
- Certificate Verification: Additionally, the system should verify the website's digital certificate, which is a public key paired with a digital signature and identity information. When a browser encounters an unsigned certificate from an untrusted Certificate Authority (CA), it should promptly alert the user. This alert serves as a warning, preventing users from entering their passwords on potentially malicious websites [15].

By combining user education, HTTPS verification, and certificate validation, organizations can significantly reduce the risk of falling victim to social engineering attacks, such as phishing, thereby enhancing overall security.

12) IMAGE GALLERY ATTACK

Countermeasures Against Image Gallery Attacks:

- Watermarking Techniques: To protect against image gallery attacks and unauthorized modifications to images in the gallery, watermarking techniques can be employed (Citation: [29]). Watermarking involves the process of embedding a unique watermark into each digital image. A secret key is utilized to determine the watermark's specific location within the image.
- Verification Using Secret Key: When users or the system need to verify the integrity and authenticity of images within the gallery, the secret key can be employed. By extracting the watermark from an image and comparing it to the embedded watermark using the secret key, one can determine whether the image has been tampered with or remains unaltered.

Implementing watermarking techniques and secret key verification enhances the security of the image gallery, helping to detect any unauthorized changes or abuses of functionality in the stored images.

13) SONAR ATTACK

Countermeasures Against Sonar Attacks:

- Restricting Microphone Usage: One approach to mitigating sonar attacks is to restrict microphone usage in the background during pattern drawing [59]. By limiting access to the microphone, acoustic signals cannot be captured, preventing attackers from determining fingertip motions on the screen.
- Randomization of Pattern Grid Layouts: Randomizing the layout of pattern grids, including their position and spacing between rows and columns, adds complexity to the attack [59]. This randomization makes it difficult for attackers to construct a valid database matching movement features with password patterns. However, it's important to consider the potential impact on the user experience.
- Restricting Frequency Range: Another countermeasure is to restrict the device's supported frequency range to avoid the transmission of inaudible signals [11]. Additionally, pop-up notifications can be implemented to alert users when a high-frequency sound signal is detected, making them aware of the potential presence of a side-channel attack.
- Acoustic Jamming: Enabling jamming in the acoustic channel is another option to thwart sonar attacks. By introducing interference, attackers are prevented from successfully launching the attack.

These countermeasures aim to enhance security against sonar attacks while considering the impact on the user experience and providing users with awareness of potential attacks.

Table 3 shows the summary of countermeasures proposed for each security attack.

IV. STUDY TAXONOMY

Figure 2a presents a taxonomy of security attacks and corresponding countermeasures within the domain of graphical passwords. This taxonomy is developed based on the findings from research questions 1 and 2, which explore the landscape of security attacks on graphical passwords and the strategies employed to mitigate these threats.

In this study, we categorize security attacks into several types:

- Physical observation attacks: shoulder-surfing attacks and smudge attacks.
- Technical observation attacks: sonar attacks, video recording attacks, eavesdropping attacks, image gallery attacks, and computer vision attacks.
- Malware attacks: spyware attacks.
- Human manipulation attacks: social engineering attacks.
- Password attacks: brute-force attacks, guessing attacks, and dictionary attacks.
- Statistical analysis attacks: frequency-of-occurrence analysis attacks.

The first category, the physical observation attack, encompasses threats such as shoulder surfing attacks and smudge attacks (see Figure 2e). Countermeasures against these attacks focus on techniques like obfuscation, randomization, and the utilization of different input methods to obscure the user's password input.

Moving on, the Technical Observation Attack category involves attacks like video recording, image galleries, sonar, eavesdropping, and computer vision attacks (see Figure 2b). These attacks exploit various technical means to compromise graphical passwords. Countermeasures here include strategies like randomization, vision complexity, watermarking, and pass-image location randomization to thwart these attacks.

Malware attacks are the third category, where spyware attacks fall. Countermeasures against spyware attacks involve randomization, tests during authentication, and alternative input methods to combat malicious software attempting to record user information (see Figure 2g).

The Human Manipulation Attack category encompasses social engineering attacks, which rely on manipulating human psychology to acquire sensitive information (see Figure 2d). Countermeasures emphasize user awareness, particularly regarding secure HTTPS connections and certificate verification, to prevent phishing attacks.

Password attacks, the fifth category, comprise brute force, guessing, and dictionary attacks (see Figure 2c). Countermeasures for brute force attacks involve large password spaces, additional authentication layers, and login attempt limitations. Guessing attacks are mitigated through the randomization of challenge images, while dictionary attacks employ randomization of pass-image locations and larger password spaces as safeguards.

Lastly, statistical analysis attacks encompass frequency of occurrence analysis (FOA) attacks (see Figure 2f). Countermeasures here involve the use of similar decoy images, limiting login attempts, displaying dummy screens upon failure, and employing algorithms to determine the final

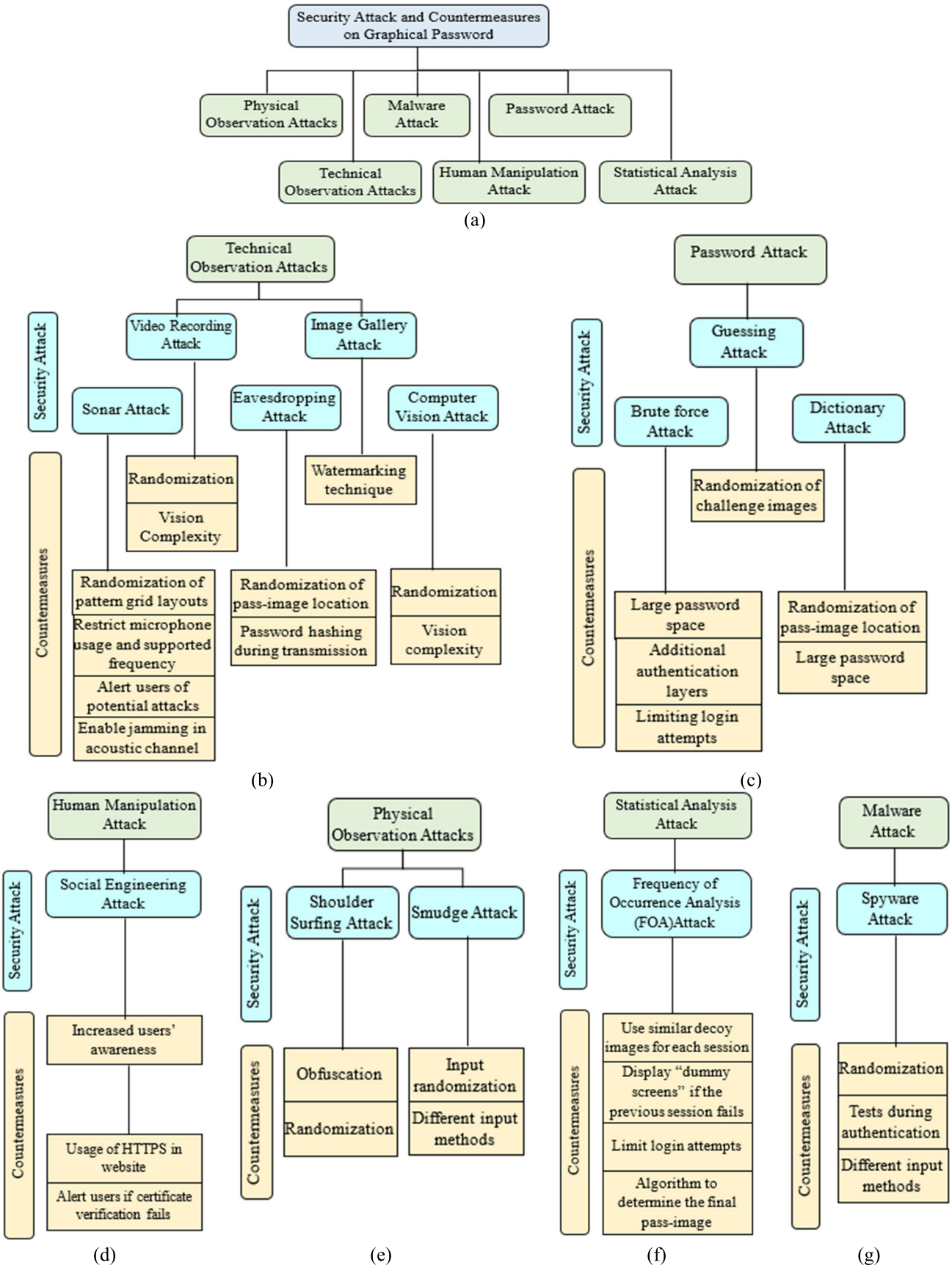

FIGURE 2. Taxonomy of security attacks and countermeasures on graphical passwords (a) Overview; (b) Technical observation attack; (c) Password attack; (d) Human manipulation attack; (e) Physical observation attack; (f) Statistical analysis attack; (g) Malware attack.

TABLE 3. Security attacks and their countermeasures.

Type of Security Attack	Countermeasures
Shoulder Surfing Attack	• Obfuscation • Randomization
Video Recording Attack	• Randomization • Vision complexity
Smudge Attack	• Input randomization • Different input methods
Spyware Attack	• Randomization • Tests during authentication • Different input methods
Brute Force Attack	• Large password space • Additional authentication layers • Limiting login attempts
Computer Vision Attack	• Randomization • Vision complexity
Dictionary Attack	• Randomization of pass-image locations • Large password space
Eavesdropping Attack	• Randomization of pass-image locations • Password hashing during transmission
Frequency of Occurrence Analysis (FOA) Attack	• Use similar decoy images for each session • Display "dummy screens" if the previous session fails • Limit login attempts • Algorithm to determine the final pass-image
Guessing Attack	• Randomization of challenge images
Social Engineering Attack	• Increased users' awareness a) Usage of HTTPS on the website b) Alert users if certificate verification fails
Image Gallery Attack	• Watermarking technique
Sonar Attack	• Randomization of pattern grid layouts • Restrict microphone usage and the supported frequency range of a device • Alert users of potential attacks • Enable jamming in the acoustic channel

pass-image, all aimed at thwarting statistical analysis-based threats.

This taxonomy offers a structured framework to understand the diverse array of security attacks facing graphical passwords and the measures employed to safeguard against them. By categorizing these threats and countermeasures, it provides valuable insights for researchers, practitioners, and developers working on enhancing the security of graphical password systems.

V. DISCUSSION

A physical observation attack refers to a method of obtaining sensitive information or violating security by physically observing a target or its surroundings. In this type of attack, individuals or groups may employ direct observation to gain unauthorized access to data or physical systems. This category encompasses two security attacks: shoulder surfing attacks and smudge attacks.

On the other hand, a technical observation attack involves the use of various tools, techniques, and technologies to collect data without direct physical interaction. It entails monitoring or gathering information about a target system, network, or data through technical means. Attacks falling under this category encompass video recording attacks, image gallery attacks, sonar attacks, eavesdropping attacks, and computer vision attacks.

Malware attacks entail deploying harmful software with the aim of compromising or disrupting a computer system, network, or device, often to steal sensitive information. Among malware attacks, spyware attacks are a prominent category. Meanwhile, human manipulation attacks involve manipulating individuals into revealing private information by leveraging psychology, emotions, and behaviors. Notably, social engineering attacks serve as an example of human manipulation attacks.

In the context of a password attack, unauthorized individuals attempt to gain access to someone else's account or system by guessing or obtaining the password. This category comprises brute-force attacks, guessing attacks, and dictionary attacks.

Furthermore, statistical analysis attacks employ analytical techniques such as pattern analysis, anomaly detection, and prediction to compromise systems or data. An example of a statistical analysis attack is the Frequency of Occurrence Analysis (FOA) attack.

Randomization stands out as a common and effective countermeasure against various attacks, except for social engineering attacks, image gallery attacks, and FOA attacks. Meanwhile, large password spaces serve as a countermeasure by increasing the variability of potential combinations, making them useful against brute force and dictionary attacks.

Complexity, as a countermeasure, enhances the unpredictability of passwords, making it challenging for attackers to visually decipher or automate the recognition of complex password patterns. This complexity is particularly useful in tackling video recording and computer vision attacks.

Different input methods prove effective in countering smudge attacks and spyware attacks. These methods introduce variability in how users interact with devices, disrupting the consistency that attackers may rely on.

Additionally, specific countermeasures tailored for each attack include advanced encryption, behavioral analysis, and more.

Our research has faced certain challenges, including the lack of standardization in graphical password systems, which can complicate comparisons among studies and findings. Different implementations and variations of graphical passwords may hinder the establishment of universal conclusions.

Moreover, our systematic literature review (SLR) only includes articles published until September 6, 2023, potentially excluding more recent research. Furthermore, our focus exclusively on security attacks and countermeasures for graphical passwords overlooks other password types, such as PIN passwords.

Given the rapid evolution of technology and security threats, it is crucial to acknowledge the time frame covered by our SLR, as the identified countermeasures may become outdated. The diverse methodologies employed in the studies

included in this review to attack graphical passwords may also pose challenges to comparability.

Despite these limitations, our review offers a valuable overview of the current research landscape in this area and identifies opportunities for future research to address the identified limitations.

Moving forward, it is imperative to emphasize that security attacks are evolving in increasingly advanced ways, warranting more attention and investigation to safeguard our privacy and information security effectively.

A. LIMITATIONS OF PREVIOUS STUDIES AND CONTRIBUTIONS OF THIS STUDY

While previous studies have significantly contributed to understanding security attacks and countermeasures in graphical password systems, several limitations have been observed. Two such limitations are highlighted below:

1) NARROW SCOPE AND FOCUS

Some previous studies have suffered from a narrow scope, focusing either on specific types of attacks or limited timeframes. For example, the study by Asmat and Qasim [6] presented a new graphical password approach called Conundrum-Pass, but its evaluation was confined to a specific set of parameters and did not consider a comprehensive range of security threats. Similarly, Higashikawa et al. [22] proposed a shoulder-surfing-resistant authentication method using a pass pattern of pattern lock, but it primarily focused on one particular type of attack and did not explore the broader landscape of security vulnerabilities.

2) LACK OF DEPTH IN COUNTERMEASURE EVALUATION

Another limitation observed in previous studies is the lack of depth in evaluating countermeasures. While many studies have identified potential countermeasures against specific attacks, their effectiveness and practicality may not have been thoroughly assessed. For instance, Cheng et al. [11] introduced SonarSnoop, an active acoustic side-channel attack, but did not provide a comprehensive evaluation of existing countermeasures against such attacks. Similarly, Nizamani et al. [32] proposed a divide and conquer approach for solving security and usability conflicts in user authentication but did not extensively analyze the efficacy of this approach in real-world scenarios.

3) CONTRIBUTIONS OF THE STUDY

In contrast to previous studies, this study offers several improvements and contributions:

- Comprehensive Analysis: This study conducts a systematic literature review covering a wide range of databases and sources to gather a comprehensive collection of security attacks and countermeasures in graphical password systems. By synthesizing findings from diverse studies, it provides a holistic view of the security landscape, encompassing both traditional and emerging threats.
- Evaluation of Countermeasures: Unlike some previous studies that lack depth in evaluating countermeasures, this study critically assesses the effectiveness of various mitigation strategies. Through rigorous analysis, it identifies gaps in existing approaches and proposes novel strategies to enhance graphical password security. This approach enables the study to offer practical insights and recommendations for researchers and practitioners in the field.

VI. CONCLUSION

The systematic literature review conducted here delves into the current landscape of security attacks and threats against graphical password schemes, along with their corresponding countermeasures. The review encompassed a comprehensive search across 13 databases, resulting in the retrieval of a total of 13,291 articles using specific keywords. Following a rigorous filtering and screening process, 59 studies were identified as meeting all the inclusion and exclusion criteria for this systematic literature review.

Within this study, we have meticulously identified a total of 14 security attacks targeting graphical password schemes. Notably, among these identified attacks, shoulder surfing, spyware, and brute force attacks emerge as the most prevalent. Although various countermeasures have been proposed in the studies, they often exhibit limitations in fully mitigating all types of attacks. Furthermore, several prior studies exhibit narrow scopes, focusing exclusively on specific attack types or specific timeframes. Despite the existence of more sophisticated and evolving attacks, we have endeavored to compile a comprehensive collection of attacks and countermeasures gleaned from our extensive research.

While previous studies have provided valuable insights into graphical password security, they often suffer from limitations. One common constraint is their narrow scope, focusing on specific attack types or limited timeframes. This narrow focus may overlook emerging threats, resulting in an incomplete understanding of the security landscape.

Furthermore, some studies lack depth in evaluating countermeasures, prioritizing attack identification over mitigation strategies. This deficiency can impede the development of effective defenses against evolving threats, leaving systems vulnerable to exploitation.

In contrast, our study addresses these limitations by offering a broader perspective on graphical password security. We meticulously compiled a comprehensive collection of attacks and countermeasures, encompassing a wide range of threats and mitigation strategies. By synthesizing findings from diverse sources, we provide a holistic view of the security landscape, covering both traditional and emerging threats.

Moreover, our study goes beyond merely identifying attacks by critically evaluating the effectiveness of countermeasures. Through rigorous analysis, we identify gaps in

existing approaches and propose novel strategies to enhance graphical password security. This approach enables us to offer practical insights and recommendations for researchers and practitioners in the field.

This review offers two distinct contributions to the field. Firstly, it consolidates existing knowledge by furnishing a well-structured overview of the current state of research in this domain. Secondly, it underscores gaps and limitations in the literature, thereby charting a course for future research and innovation.

Our in-depth examination of these articles has revealed a broad spectrum of security risks that graphical password systems must confront. These vulnerabilities range from intricate challenges like smudge attacks to more conventional concerns such as brute force attacks and shoulder surfing. This spectrum of vulnerabilities underscores the pressing need for ongoing research and the development of novel approaches in the realm of graphical password security.

Turning our attention to the defensive aspect, out of the 14 attacks mentioned earlier, we have ascertained that 13 of these attacks have corresponding countermeasures proposed in previous studies. The use of randomization emerges as the most prevalent and widely applied technique to enhance the security of graphical password schemes. Randomization facilitates the fragmentation and reshuffling of password images, introducing complexity and making it significantly more challenging for attackers to remember, guess, or capture the correct pass image, even when aided by computer vision.

However, despite the advancements in countermeasures, certain limitations persist in mitigating security attacks, particularly in light of evolving and increasingly sophisticated technologies. The amalgamation of findings from numerous studies underscores the importance of adopting a comprehensive approach to graphical password security. As we advance, it is imperative to address not only technical vulnerabilities but also human aspects, usability, and the overall user experience. Achieving effective countermeasures necessitates a multidisciplinary strategy that involves security specialists, psychologists, and designers, acknowledging the interplay of various facets in safeguarding graphical password systems.

REFERENCES

[1] N. A. A. Othman, M. A. A. Rahman, A. S. A. Sani, and F. H. M. Ali, "Directional based graphical authentication method with shoulder surfing resistant," in *Proc. IEEE Conf. Syst., Process Control (ICSPC)*, Dec. 2018, pp. 198–202, doi: 10.1109/SPC.2018.8704157.

[2] I. A. M. Abass, L. F. Hussein, T. Kallel, and A. B. Aissa, "New textual authentication method to resistant shoulder-surfing attack," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 1, pp. 490–496, 2022, doi: 10.14569/ijacsa.2022.0130161.

[3] B. M. AlBaradi, A. M. AlTowayan, M. M. AlAnazi, S. Ambreen, and D. M. Ibrahim, "PathGazePIN: Gaze and path-based authentication entry method," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 264–270, 2019, doi: 10.14569/ijacsa.2019.0101136.

[4] H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Secure graphical one time password (GOTPass): An empirical study," *Inf. Secur. J. A Global Perspective*, vol. 24, nos. 4–6, pp. 207–220, Dec. 2015, doi: 10.1080/19393555.2015.1115927.

[5] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A pilot study on the security of pattern screen-lock methods and soft side channel attacks," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw.* NY, USA: ACM, Apr. 2013, pp. 1–6, doi: 10.1145/2462096.2462098.

[6] N. Asmat and H. S. A. Qasim, "Conundrum-pass: A new graphical password approach," in *Proc. 2nd Int. Conf. Commun., Comput. Digit. Syst.*, Mar. 2019, pp. 282–287, doi: 10.1109/C-CODE.2019.8680989.

[7] P. J. Assudani, "Graphical password using 2D coordinates," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 467–469, Feb. 2018, doi: 10.26483/ijarcs.v9i2.5761.

[8] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf. Offensive Technol.*, 2010, pp. 1–7.

[9] K. A. Awan, I. U. Din, A. Almogren, N. Kumar, and A. Almogren, "A taxonomy of multimedia-based graphical user authentication for green Internet of Things," *ACM Trans. Internet Technol.*, vol. 22, no. 2, pp. 1–28, May 2022, doi: 10.1145/3433544.

[10] S. Azad, M. Rahman, M. S. A. N. Ranak, B. M. F. K. Ruhee, N. N. Nisa, N. Kabir, A. Rahman, and J. M. Zain, "VAP code: A secure graphical password for smart devices," *Comput. Electr. Eng.*, vol. 59, pp. 99–109, Apr. 2017, doi: 10.1016/j.compeleceng.2016.12.007.

[11] P. Cheng, I. E. Bagci, U. Roedig, and J. Yan, "SonarSnoop: Active acoustic side-channel attacks," *Int. J. Inf. Secur.*, vol. 19, no. 2, pp. 213–228, Apr. 2020, doi: 10.1007/s10207-019-00449-8.

[12] E. Darbanian and G. D. Fard, "A graphical password against spyware and shoulder-surfing attacks," in *Proc. Int. Symp. Comput. Sci. Softw. Eng. (CSSE)*, Aug. 2015, pp. 1–6, doi: 10.1109/CSICSSE.2015.7369239.

[13] R. English and R. Poet, "Towards a metric for recognition-based graphical password security," in *Proc. 5th Int. Conf. Netw. Syst. Secur.*, Sep. 2011, pp. 239–243, doi: 10.1109/ICNSS.2011.6060007.

[14] R. English and R. Poet, "The effectiveness of intersection attack countermeasures for graphical passwords," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1–8, doi: 10.1109/TRUSTCOM.2012.271.

[15] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," *J. Softw.*, vol. 8, no. 7, pp. 1678–1698, Jul. 2013, doi: 10.4304/jsw.8.7.1678-1698.

[16] H. Gao and X. Liu, "A new graphical password scheme against spyware by using CAPTCHA," in *Proc. 5th Symp. Usable Privacy Secur.* NY, USA: ACM, Jul. 2009, Art. no. 21, doi: 10.1145/1572532.1572560.

[17] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," in *Proc. 4th Int. Conf. Innov. Comput., Inf. Control (ICICIC)*, Dec. 2009, pp. 675–678, doi: 10.1109/ICICIC.2009.158.

[18] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *Proc. Int. Conf. Cyberworlds*, Oct. 2010, pp. 194–199, doi: 10.1109/CW.2010.34.

[19] M. A. S. Gokhale and V. S. Waghmare, "The shoulder surfing resistant graphical password authentication technique," *Proc. Comput. Sci.*, vol. 79, pp. 490–498, 2016, doi: 10.1016/j.procs.2016.03.063.

[20] M. Guerar, A. Merlo, and M. Migliardi, "Clickpattern: A pattern lock system resilient to smudge and side-channel attacks," *J. Wireless Mob. Netw. Ubiquitous Comput. Dependable Appl.*, vol. 8, no. 2, pp. 64–78, 2017.

[21] S. Hanif, F. Sohail, S.-A. Tariq, and M. Imran, "A new shoulder surfing and mobile key-logging resistant graphical password scheme for smart-held devices," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 432–437, 2019, doi: 10.14569/ijacsa.2019.0100957.

[22] S. Higashikawa, T. Kosugi, S. Kitajima, and M. Mambo, "Shoulder-surfing resistant authentication using pass pattern of pattern lock," *IEICE Trans. Inf. Syst.*, vol. E101, no. 1, pp. 45–52, 2018, doi: 10.1587/transinf.2017mup0012.

[23] P. F. Ho, Y. H.-S. Kam, M. C. Wee, Y. N. Chong, and L. Y. Por, "Preventing shoulder-surfing attack with the concept of concealing the password objects' information," *Sci. World J.*, vol. 2014, pp. 1–12, 2014, doi: 10.1155/2014/838623.

[24] R. Kaur and A. Kaur, "Enhancing authentication schemes for multi-level graphical password in cloud environment," *Commun. Appl. Electron.*, vol. 5, no. 8, pp. 12–18, Aug. 2016, doi: 10.5120/cae2016652340.

[25] T. Kawamura, T. Ebihara, N. Wakatsuki, and K. Zempo, "EYEDi: Graphical authentication scheme of estimating your encodable distorted images to prevent screenshot attacks," *IEEE Access*, vol. 10, pp. 2256–2268, 2022, doi: 10.1109/ACCESS.2021.3138093.

[26] V. K. Kolekar and M. B. Vaidya, "Click and session based—Captcha as graphical password authentication schemes for smart phone and web," in *Proc. Int. Conf. Inf. Process. (ICIP)*, Dec. 2015, pp. 669–674, doi: 10.1109/INFOP.2015.7489467.

[27] W.-C. Ku, B.-R. Cheng, Y.-C. Yeh, and C.-J. Chang, "A simple sector-based textual-graphical password scheme with resistance to login-recording attacks," *IEICE Trans. Inf. Syst.*, vol. E99, no. 2, pp. 529–532, 2016, doi: 10.1587/transinf.2015edl8080.

[28] W.-C. Ku, Y.-C. Yeh, B.-R. Cheng, and C.-J. Chang, "A sector-based graphical password scheme with resistance to login-recording attacks," *IEICE Trans. Inf. Syst.*, vol. E98, no. 4, pp. 894–901, 2015, doi: 10.1587/transinf.2014edp7302.

[29] A. H. Lashkari, A. A. Manaf, and M. Masrom, "A secure recognition based graphical password by watermarking," in *Proc. IEEE 11th Int. Conf. Comput. Inf. Technol.*, Aug. 2011, pp. 164–170, doi: 10.1109/CIT.2011.29.

[30] L. A. Adebimpe, I. O. Ng, M. Y. I. Idris, M. Okmi, C. S. Ku, T. F. Ang, and L. Y. Por, "Systemic literature review of recognition-based authentication method resistivity to shoulder-surfing attacks," *Appl. Sci.*, vol. 13, no. 18, p. 10040, Sep. 2023, doi: 10.3390/app131810040.

[31] W. Meng, W. Li, D. S. Wong, and J. Zhou, "TMGuard: A touch movement-based security mechanism for screen unlock patterns on smartphones," *Lecture Notes Comput. Sci.*, vol. 9696, pp. 629–647, 2016, doi: 10.1007/978-3-319-39555-5_34.

[32] S. Z. Nizamani, W. Ali, and S. Awan, "Divide and conquer approach for solving security and usability conflict in user authentication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 5, pp. 489–495, 2018, doi: 10.14569/ijacsa.2018.090564.

[33] L. Y. Por, "Frequency of occurrence analysis attack and its countermeasure," *Int. Arab J. Inf. Technol.*, vol. 10, no. 1, pp. 189–197, 2013.

[34] P. L. Yee and M. L. Mat Kiah, "Shoulder surfing resistance using PENUP event and neighboring connectivity manipulation," *Malaysian J. Comput. Sci.*, vol. 23, no. 2, pp. 121–140, Sep. 2010, doi: 10.22452/mjcs.vol23no2.5.

[35] L. Y. Por, C. S. Ku, and T. F. Ang, "Preventing shoulder-surfing attacks using digraph substitution rules and pass-image output feedback," *Symmetry*, vol. 11, no. 9, p. 1087, Aug. 2019, doi: 10.3390/sym11091087.

[36] L. Y. Por, L. A. Adebimpe, M. Y. I. Idris, C. S. Khaw, and C. S. Ku, "LocPass: A graphical password method to prevent shoulder-surfing," *Symmetry*, vol. 11, no. 10, p. 1252, Oct. 2019, doi: 10.3390/sym11101252.

[37] P. Kavitha Rani, R. Sai Krishna, U. S. Siddarth, and E. Vidya Sagar, "A novel session password security technique using textual color and images," *J. Phys. Conf. Ser.*, vol. 1916, no. 1, May 2021, Art. no. 012176, doi: 10.1088/1742-6596/1916/1/012176.

[38] M. Kameswara Rao, D. S. G. Santhi, and D. Md. Ali Hussain, "Spin wheel based graphical password authentication resistant to peeping attack," *Int. J. Eng. Technol.*, vol. 7, no. 2.7, p. 984, Mar. 2018, doi: 10.14419/ijet.v7i2.7.11607.

[39] G. Shivaprasad, "Research and development of user authentication using graphical passwords: A prospective methodology," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 9S3, pp. 385–390, Aug. 2019, doi: 10.35940/ijitee.I3071.0789S319.

[40] R. Düzgün, P. Mayer, and M. Volkamer, "Shoulder-surfing resistant authentication for augmented reality," in *Proc. Nordic Hum.-Comput. Interact. Conf.*, NY, USA: ACM, Oct. 2022, pp. 1–13, doi: 10.1145/3546155.3546663.

[41] A. Sadovnik and T. Chen, "A visual dictionary attack on picture passwords," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2013, pp. 4447–4451, doi: 10.1109/ICIP.2013.6738916.

[42] P. Saranya, S. Sharavanan, R. Vijai, and R. Balajee, "Authentication scheme for session passwords using color and image," *Int. J. Smart Sens. Intell. Syst.*, vol. 10, no. 5, pp. 590–603, Jan. 2017, doi: 10.21307/ijssis-2017-272.

[43] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "SmudgeSafe," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, NY, USA: ACM, Sep. 2014, pp. 775–786, doi: 10.1145/2632048.2636090.

[44] A. Shah, P. Ved, A. Deora, A. Jaiswal, and M. D'silva, "Shoulder-surfing resistant graphical password system," *Proc. Comput. Sci.*, vol. 45, pp. 477–484, 2015, doi: 10.1016/j.procs.2015.03.084.

[45] S. Akter Sharna and S. Ashraf Ali, "Image based password authentication system," 2022, *arXiv:2205.12352*.

[46] N. K. Sreelaja and N. K. Sreeja, "An image edge based approach for image password encryption," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5733–5745, Dec. 2016, doi: 10.1002/sec.1732.

[47] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 2, pp. 180–193, Mar. 2018, doi: 10.1109/TDSC.2016.2539942.

[48] S. Tabrez and D. J. Sai, "Pass-matrix authentication a solution to shoulder surfing attacks with the assistance of graphical password authentication system," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Jun. 2017, pp. 776–781, doi: 10.1109/ICCONS.2017.8250568.

[49] T. J. Fong, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 302–308, 2019, doi: 10.14569/ijacsa.2019.0100140.

[50] D. S. Thosar and M. Singh, "A review on advanced graphical authentication to resist shoulder surfing attack," in *Proc. Int. Conf. Adv. Comput. Telecommun. (ICACAT)*, Dec. 2018, pp. 1–3, doi: 10.1109/ICACAT.2018.8933699.

[51] P. R. Thumma, "Password authentication using pass matrix to avoid shoulder surfing," *Int. Res. J. Eng. Technol.*, vol. 7, no. 7, pp. 5851–5853, Jul. 2020.

[52] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2010, pp. 760–767, doi: 10.1109/AINA.2010.46.

[53] Z. Wang, L. Liao, R. Meng, C.-N. Yang, Z. Zhou, and H. Yang, "Verification grid and map slipping based graphical password against shoulder-surfing attacks," *Secur. Commun. Netw.*, vol. 2022, pp. 1–9, Apr. 2022, doi: 10.1155/2022/6778755.

[54] G. Ye, Z. Tang, D. Fang, X. Chen, K. I. Kim, B. Taylor, and Z. Wang, "Cracking Android pattern lock in five attempts," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15, doi: 10.14722/ndss.2017.23130.

[55] G. Ye, Z. Tang, D. Fang, X. Chen, W. Wolff, A. J. Aviv, and Z. Wang, "A video-based attack for Android pattern lock," *ACM Trans. Privacy Secur.*, vol. 21, no. 4, pp. 1–31, Nov. 2018, doi: 10.1145/3230740.

[56] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: Evolvable graphical password against shoulder-surfing attacks," *Comput. Secur.*, vol. 70, pp. 179–198, Sep. 2017, doi: 10.1016/j.cose.2017.05.006.

[57] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in *Proc. 7th Symp. Usable Privacy Secur.*, NY, USA: ACM, Jul. 2011, pp. 1–12, doi: 10.1145/2078827.2078835.

[58] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proc. Int. Conf. Intell. User Interface* NY, USA: ACM, Mar. 2013, pp. 277–286, doi: 10.1145/2449396.2449432.

[59] M. Zhou, Q. Wang, J. Yang, Q. Li, F. Xiao, Z. Wang, and X. Chen, "PatternListener," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, NY, USA: ACM, Oct. 2018, pp. 1775–1787, doi: 10.1145/3243734.3243777.

LIP YEE POR (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from Universiti Malaya, Malaysia. He is currently an Associate Professor with the Faculty of Computer Science and Information Technology, Universiti Malaya. His research interests include neural networks (such as supervised and unsupervised learning methods, such as support vector machines and extreme learning machines), bioinformatics (such as biosensors and pain research), computer security [such as information security, steganography, and authentication (graphical password)], grid computing, and e-learning framework.

IAN OUII NG received the B.Sc. degree from Universiti Malaya, Malaysia, where he is currently pursuing the master's degree in computer science. He is currently the Chief Executive Officer with Original Intelligence Sdn. Bhd. He is a seasoned professional with a strong background in software development and IT solutions. With two decades of experience in the field, he has successfully implemented numerous IT solutions for well-known local companies, including Maybank, CIIMB, RHB, AIA, and Prudential. In addition to his professional achievements, he is also dedicated to furthering his education. His expertise and commitment to continuous learning make him a valuable asset in the world of technology and innovation.

YEN-LIN CHEN (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical and control engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2000 and 2006, respectively. From February 2007 to July 2009, he was an Assistant Professor with the Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan. From August 2009 to January 2012, he was an Assistant Professor with the Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei, Taiwan, where he was an Associate Professor, from February 2012 to July 2015, and has been a Full Professor, since August 2015. His research interests include artificial intelligence, intelligent image analytics, embedded systems, pattern recognition, intelligent vehicles, and intelligent transportation systems. His research results have been published in over 100 journals and conference papers. He is a fellow of IET and a member of ACM, IAPR, and IEICE.

JING YANG (Graduate Student Member, IEEE) received the Bachelor of Engineering degree in navigation technology from Shandong Jiaotong University, in 2022. He is currently pursuing the master's degree in data science with Universiti Malaya. His research interests include medical image processing and deep learning.

CHIN SOON KU received the Ph.D. degree from Universiti Malaya, Malaysia, in 2019. He is currently an Assistant Professor with the Department of Computer Science, Universiti Tunku Abdul Rahman, Malaysia. His research interests include AI techniques (such as genetic algorithms), computer vision, decision support tools, graphical authentication (authentication, picture-based password, and graphical password), machine learning, deep learning, speech processing, natural language processing, and unmanned logistics fleets.