applied sciences

MDPI

Systematic Review

Systemic Literature Review of Recognition-Based Authentication Method Resistivity to Shoulder-Surfing Attacks

Lateef Adekunle Adebimpe [1,2], Ian Ouii Ng [1], Mohd Yamani Idna Idris [1], Mohammed Okmi [1,3], Chin Soon Ku [4,*], Tan Fong Ang [1] and Lip Yee Por [1,*]

[1] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia; dradebimpela@siswa.um.edu.my (L.A.A.); 22056562@siswa.um.edu.my (I.O.N.); yamani@um.edu.my (M.Y.I.I.); 17220556@siswa.um.edu.my (M.O.); angtf@um.edu.my (T.F.A.)
[2] Department of Computer Science, Emmanuel Alayande University of Education, Oyo 211225, Nigeria
[3] Department of Information Technology and Security, Jazan University, Jazan 45142, Saudi Arabia
[4] Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia
* Correspondence: kucs@utar.edu.my (C.S.K.); porlip@um.edu.my (L.Y.P.)

Abstract: The rapid advancement of information technology (IT) has given rise to a new era of efficient and fast communication and transactions. However, the increasing adoption of and reliance on IT has led to the exposure of personal and sensitive information online. Safeguarding this information against unauthorized access remains a persistent challenge, necessitating the implementation of improved computer security measures. The core objective of computer security is to ensure the confidentiality, availability, and integrity of data and services. Among the mechanisms developed to counter security threats, authentication stands out as a pivotal defense strategy. Graphical passwords have emerged as a popular authentication approach, yet they face vulnerability to shoulder-surfing attacks, wherein an attacker can clandestinely observe a victim's actions. Shoulder-surfing attacks present a significant security challenge within the realm of graphical password authentication. These attacks occur when an unauthorized individual covertly observes the authentication process of a legitimate user by shoulder surfing the user or capturing the interaction through a video recording. In response to this challenge, various methods have been proposed to thwart shoulder-surfing attacks, each with distinct advantages and limitations. This study thus centers on reviewing the resilience of existing recognition-based graphical password techniques against shoulder-surfing attacks by conducting a comprehensive examination and evaluation of their benefits, strengths, and weaknesses. The evaluation process entailed accessing pertinent academic resources through renowned search engines, including Web of Science, Science Direct, IEEE Xplore, ProQuest, Scopus, Springer, Wiley Online Library, and EBSCO. The selection criteria were carefully designed to prioritize studies that focused on recognition-based graphical password methods. Through this rigorous approach, 28 studies were identified and subjected to a thorough review. The results show that fourteen of them adopted registered objects as pass-objects, bolstering security through object recognition. Additionally, two methods employed decoy objects as pass-objects, enhancing obfuscation. Notably, one technique harnessed both registered and decoy objects, amplifying the security paradigm. The results also showed that recognition-based graphical password techniques varied in their resistance to different types of shoulder-surfing attacks. Some methods were effective in preventing direct observation attacks, while others were vulnerable to video-recorded and multiple-observation attacks. This vulnerability emerged due to attackers potentially extracting key information by analyzing user interaction patterns in each challenge set. Notably, one method stood out as an exception, demonstrating resilience against all three types of shoulder-surfing attacks. In conclusion, this study contributes to a comprehensive understanding of the efficacy of recognition-based graphical password methods in countering shoulder-surfing attacks by analyzing the diverse strategies employed by these methods and revealing their strengths and weaknesses.

Keywords: graphical password; authentication; recognition based; information security; shoulder surfing

check for updates

Citation: Adebimpe, L.A.; Ng, I.O.; Idris, M.Y.I.; Okmi, M.; Ku, C.S.; Ang, T.F.; Por, L.Y. Systemic Literature Review of Recognition-Based Authentication Method Resistivity to Shoulder-Surfing Attacks. *Appl. Sci.* **2023**, *13*, 10040. https://doi.org/10.3390/app131810040

Academic Editor: Jun Lee

Received: 10 August 2023
Revised: 31 August 2023
Accepted: 4 September 2023
Published: 6 September 2023

1. Introduction

The internet has significantly transformed our lives, bringing forth numerous benefits and advancements. However, growing reliance on the internet has also exposed various security flaws [1]. As a result, ensuring robust computer security is crucial to prevent unauthorized access and disruptions to services provided by computers and associated technologies [2]. Authentication serves as a fundamental method to mitigate unauthorized access [3–5], verifying the user's identity and allowing access only to authorized individuals, essentially demonstrating the principle of "you are who you say you are" [6]. Authentication plays a vital role in safeguarding sensitive data [7].

Authentication traditionally relies on three elements: something you know (knowledge elements), something you own (ownership factors), and something you are (inheritance elements) [7,8]. Knowledge factors, also known as knowledge-based authentication, involve elements such as passwords, personal identification numbers (PINs), challenge–response mechanisms, or security questions [6–10]. Ownership factors, known as token-based authentication, rely on possessions such as ID cards, ATM cards, cryptographic keys, security tokens, and more [6–10]. Inherence factors, or biometric-based authentication, leverage unique user characteristics or behaviors, including fingerprints, retinal patterns, DNA sequences, signatures, faces, voices, bio-electrical signals, and others [6–10].

Within the realm of authentication methods, alphanumeric passwords have long been prevalent [11]. However, the demand for complex passwords to ensure security poses challenges in terms of memorability for users. Complex passwords, while more secure, are often difficult to remember, leading users to compromise security by writing them down or reusing passwords across multiple accounts [12]. In response to these challenges, graphical passwords have been suggested as a replacement form of authentication [13–15].

Graphical passwords leverage visual objects in the authentication process, capitalizing on the human ability to remember images more easily than alphanumeric data [16,17]. Different methods have emerged, including recall-based methods, cued-recall-based methods, and recognition-based methods (RBMs) [8,14,18–20]. Recall-based methods involve reproducing a drawing, while cued-recall-based methods require selecting points on displayed images. RBMs necessitate distinguishing between registered and distractor objects and recognizing the pass-object [21]. Graphical passwords aim to address the challenge of memorability, surpassing alphanumeric passwords in terms of ease of remembering [17].

However, the convenience of graphical passwords also introduces risks, particularly from shoulder-surfing attacks (SSAs) [20]. Shoulder surfing (SS) involves unauthorized individuals observing and capturing authentication information while users enter their passwords, compromising the security of graphical passwords [22,23]. To counter these threats, researchers have dedicated efforts to developing resistance methods, with recognition-based graphical passwords (RBGPs) being widely used to avoid SS assaults [24]. Nonetheless, despite numerous proposed methods, challenges persist in effectively countering SSAs.

In light of the current related works on this topic, it is important to highlight the distinctive contributions and focus of this systematic literature review. While previous reviews [2,14,18,21] have touched upon the resistance of RBGP methods to SSAs, there is still a lack of research relating to advancing existing methods for countering SSAs. For example, the review conducted in [2] only focused on graphical passwords developed in Korea throughout the year 2017. The survey conducted in [14] reviewed nine recognition-based systems developed between 2000 and 2004. Islam et al. [18] evaluated and examined existing recognition-based systems up to 2016. Between 2009 and 2017, Jaffar and Zeki [21] reviewed the shoulder surfing resistivity of textual and graphical password schemes. Despite these assessments, adequate knowledge about the existing RBGP methods is still lacking.

The research problem addressed in this study is the evaluation of current recognition-based graphical password (RBGP) methods for resisting shoulder-surfing attacks (SSAs). While numerous RBGP schemes have been proposed, their effectiveness against SSAs, especially in real-world scenarios, remains uncertain. The research gap this work aims to fill is the absence of a comprehensive and up-to-date analysis of these methods in the context of SSAs. Through a systematic examination of the available literature, this review seeks to delineate the strengths, vulnerabilities, and potential improvements of existing RBGP methods in countering such attacks.

The paper's structure is arranged in the following manner: In the subsequent section, the research method is presented. The results of the systematic literature review and the answers to the research questions are presented in Section 3. The review discussion is presented in Section 4, and Section 5 concludes the review.

2. Method

Figure 1 depicts the systematic literature review methodology employed to evaluate the existing RBGP methods. To review the existing RBGP methods, a systematic literature review was conducted in accordance with the reporting guidelines outlined in the "Preferred Reporting Items for Systematic Reviews and Meta-Analyses" (PRISMA). The PRISMA guidelines aid to provide a clear and graphical representation of the article selection process by highlighting the number of articles identified, screened, and included in the systematic literature review.

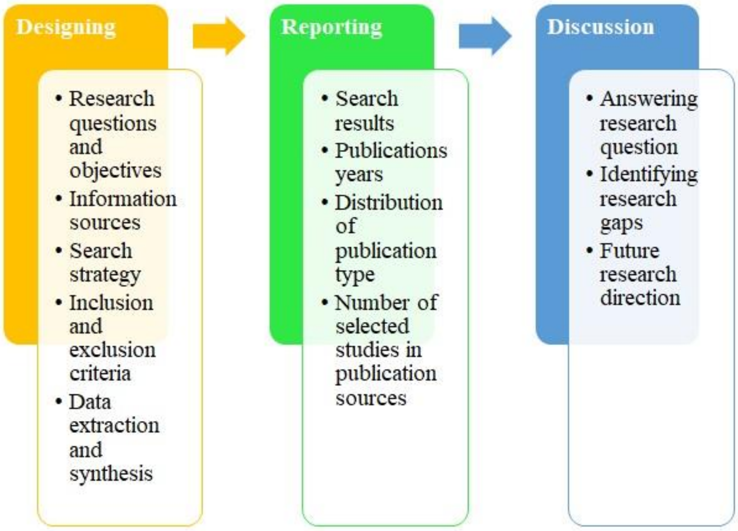
Designing
• Research questions and objectives
• Information sources
• Search strategy
• Inclusion and exclusion criteria
• Data extraction and synthesis
Reporting
• Search results
• Publications years
• Distribution of publication type
• Number of selected studies in publication sources
Discussion
• Answering research question
• Identifying research gaps
• Future research direction

Figure 1. Systematic literature review methodology.

The systematic literature review methodology used consists of three phases: the designing phase, the reporting phase, and the discussion phase. The designing phase entails defining and developing the following steps: research questions and objectives, a search strategy, and inclusion and exclusion criteria.

2.1. Defining Research Questions and Objectives

The primary aim of this systematic literature review is unequivocally to assess the resistance of existing RBGP methods to SSAs. Specifically, the study endeavors to:

- Comprehensively categorize and describe the current RBGP methods.
- Critically evaluate the susceptibility or robustness of these methods to SSAs.
- Explore the nuances of pass-objects utilized within these methods, emphasizing their role in either fortifying or undermining security against SSAs.
- Synthesize the findings to determine the overall efficacy of the RBGP methods in terms of both security against SSAs and user friendliness.

Table 1 presents the research objectives and questions of this systematic literature review.

Table 1. Research questions and objectives.

Research Questions (RQ)	Research Objectives (RO)
RQ1: What are the existing recognition-based methods?	RO1: To identify the existing recognition-based methods.
RQ2: What pass-objects are used for authentication in these methods?	RO2: To determine the pass-objects used for authentication in these methods.
RQ3: What are the strengths and weaknesses of the selected recognition-based methods?	RO3: To examine the strengths and weaknesses of the selected recognition-based methods.
RQ4: How effective are the selected recognition-based methods in terms of usability and security?	RO4: To evaluate the effectiveness of the selected recognition-based methods in terms of security and usability.

2.2. Identifying Information Sources

A comprehensive search was conducted using various databases, including Web-of-Science, Science Direct, IEEE Xplore, ProQuest, Springer, Scopus, Wiley Online Library, and Ebsco. These sources were searched to obtain relevant journal articles and conference papers.

2.3. Developing the Search Strategy

A search strategy was developed using a combination of keywords and controlled vocabulary terms related to graphical passwords, recognition-based authentication, shoulder surfing, and shoulder-surfing attacks. Boolean operators (AND, OR) were used to combine and refine search terms. The search strategy was tailored to the syntax and capabilities of each database. The following search string was thus applied for this study:

((Graphical Password) OR (Graphical Authentication)) AND ((Shoulder Surfing) OR (Shoulder-Surfing)) AND (Recognition).

2.4. Inclusion and Exclusion Criteria

The establishment of inclusion and exclusion criteria was undertaken in order to ascertain the studies that should be incorporated into the review and those that should be excluded. Table 2 outlines the criteria for inclusion and exclusion that were employed in this review.

Table 2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Research studies that were published between 2016 and 2023	Papers that do not focus on RBGP methods
Papers that propose or deal with only RBGP schemes	Non-peer-reviewed papers
Papers published in the English language	Papers published in languages other than English
Peer-reviewed articles and conference papers	

2.5. Selecting Relevant Papers

The selection process involved a two-stage screening process. Initially, the papers were evaluated and assessed for relevance and eligibility based on their title and abstract to determine their relevance to the RQ and eligibility criteria. Papers that were assessed as inconsistent with the established inclusion criteria were eliminated from the review process. Subsequently, a full-text assessment was conducted on the remaining papers to determine their suitability for inclusion in the review. The full-text assessment is a crucial step in the systematic review process, ensuring that each article selected for final inclusion aligns well with the study's objectives. During this full-text assessment, we dug deeper into each paper, beyond just the abstract, to gain a comprehensive understanding of its content. Here are some specific points or criteria that were typically considered during this assessment:

Relevance to the Research Objective: The primary aim was to confirm if the paper directly addressed the research objective; in this case, assessing the resistance of recognition-based graphical password methods to shoulder-surfing attacks.

Study Design and Methodology: We looked at the design of the study, whether it was experimental, observational, or another type, to ensure the methods used were rigorous and could yield reliable results.

Outcomes and Measurements: The outcomes that the study measured and how these were measured (i.e., the metrics and tools used) were evaluated to ensure they were relevant and would contribute meaningfully to the review.

Consistency with Other Studies: While not a strict criterion, understanding how the findings of a paper align with or differ from other studies in the field can offer insights into the broader context and the robustness of the findings.

Contribution to the Field: The potential contribution of the study to the existing body of knowledge was assessed. This could be in terms of novel methodologies, unique findings, or a new perspective on an existing challenge.

Potential Biases: Any apparent biases, either in terms of the study's funding sources, the authors' affiliations, or the methodology used, were taken into account to ensure the review's integrity.

Clear Conclusions: The study needed to have clear, well-defined conclusions that could be extracted and synthesized into the systematic review.

Any disagreements during the selection process were resolved through discussion and consensus among the reviewers.

2.6. Extracting Data

A standardized data extraction form was developed to systematically retrieve relevant information from the chosen publications. The extraction form included data fields such as authorship details, year of publication, research design, participant characteristics, graphical password methods used, evaluation methods, and key findings related to the strengths, weaknesses, security, and usability of the RBM. Data extraction was conducted by one reviewer, and a subset of papers was independently reviewed by a second reviewer to ensure accuracy and consistency.

2.7. Synthesizing the Data

The findings from the selected papers underwent a comprehensive synthesis using a content analysis and narrative synthesis approach. Key themes, pass-objects, strengths, weaknesses, security aspects, and usability aspects related to the RBGP methods were identified and summarized. Through this process, we carefully analyzed the variations and inconsistencies in the findings and thoroughly explored potential explanations to offer a comprehensive understanding of the existing RBGP methods. In addition, we conducted a rigorous analysis using content and descriptive analyses to provide valuable insights into patterns and relationships among the existing RBGP methods for SSAs.

2.8. Identifying Research Gaps and Contributions

The primary aim of this review is to discover alternate strategies that future researchers might employ to effectively counter SSAs while also mitigating other potential security vulnerabilities. The study's findings will provide insight into the current state of research regarding the resistance of RBGP methods to SSAs. Through the identification of gaps and limits in the current body of literature, this review aims to offer significant insights that may inform and guide future research endeavors. In addition, these gaps will serve as a foundation for further investigations to develop more robust and secure authentication mechanisms against SSAs.

By following these steps, this systematic literature review contributes to the existing knowledge and understanding of the resistance of RBGP methods to SSAs. It provides insights for further research and supports the development of more effective security measures and enhanced user authentication in digital systems.

3. Results

This section provides a concise overview of the findings derived from the process of selecting studies, discusses the results of each research question, and presents the proposed taxonomy of the graphical password schemes.

3.1. Study Selection

Figure 2 shows the PRISMA flowchart, which outlines the stages involved in the systematic literature review conducted for this paper: identification, screening, eligibility, and inclusion. During the identification stage, a comprehensive search was performed using keywords ((Graphical Password) OR (Graphical Authentication)) AND ((Shoulder Surfing) OR (Shoulder-Surfing)) AND (Recognition) in multiple databases, resulting in a total of 1075 studies. These studies were distributed across different databases as follows: 18 in Web-of-Science, 15 in IEEE Xplore, 61 in Science Direct, 143 in ProQuest, 547 in Springer, 21 in Scopus, 55 in Wiley Online Library, and 215 in Ebsco.

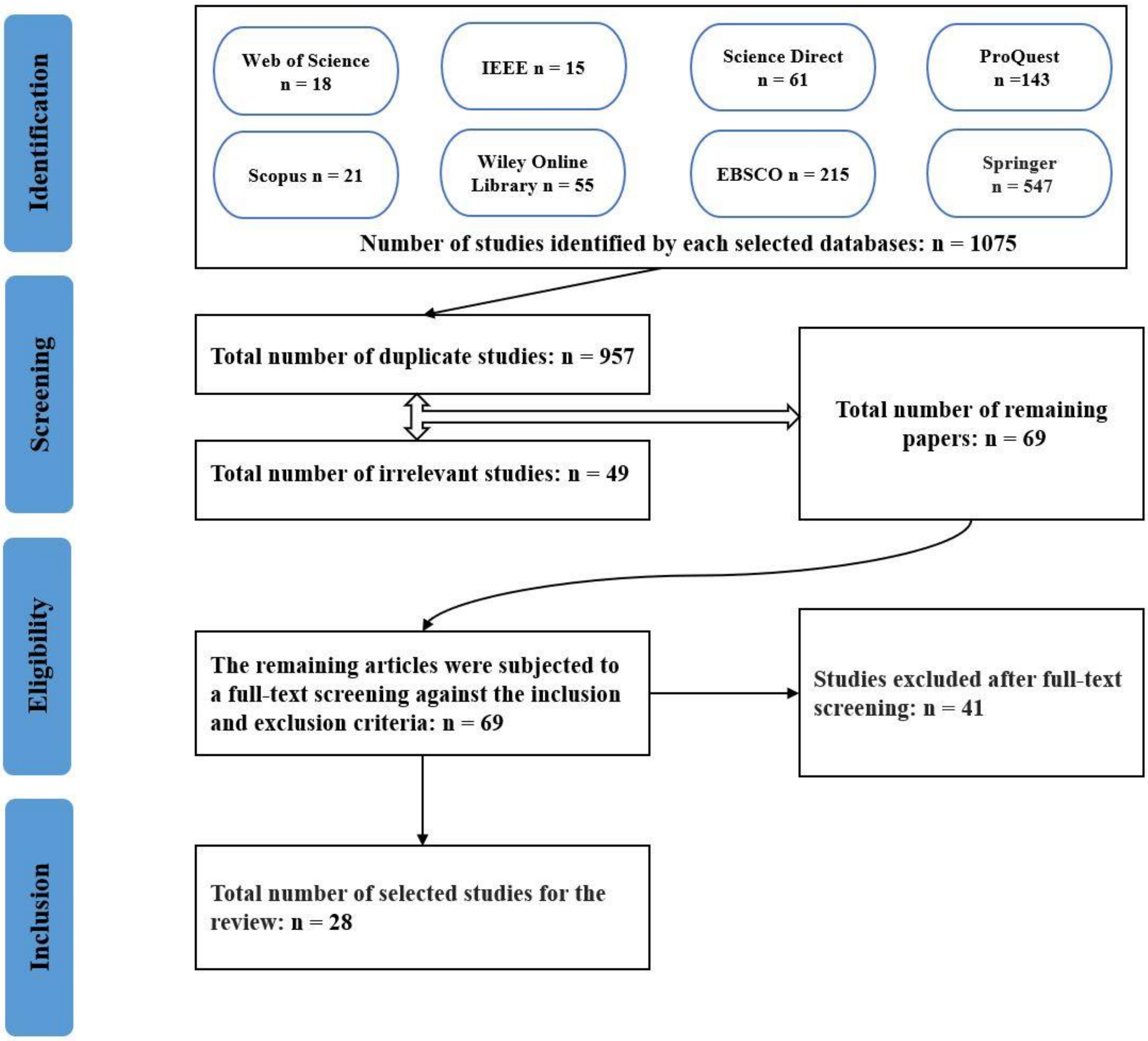
Identification
Screening
Eligibility
Inclusion
Web of Science n = 18
IEEE n = 15
Science Direct n = 61
ProQuest n =143
Scopus n = 21
Wiley Online Library n = 55
EBSCO n = 215
Springer n = 547
Number of studies identified by each selected databases: n = 1075
Total number of duplicate studies: n = 957
Total number of irrelevant studies: n = 49
Total number of remaining papers: n = 69
The remaining articles were subjected to a full-text screening against the inclusion and exclusion criteria: n = 69
Studies excluded after full-text screening: n = 41
Total number of selected studies for the review: n = 28

Figure 2. The PRISMA flowchart [25] for the study selection process.

Following the identification stage, the screening process began. Duplicate studies were removed, resulting in the exclusion of 957 papers. Additionally, 49 papers were deemed irrelevant or not focused on recognition-based approaches and were subsequently removed from consideration.

Subsequently, the eligibility stage encompassed an in-depth assessment of the remaining 69 studies through a full text screening procedure, adhering to the predefined inclusion and exclusion criteria outlined in Table 2. During this stage, a total of 41 articles were excluded from the study based on the predetermined exclusion criteria.

Finally, the inclusion stage included the remaining 28 studies that met all the inclusion and exclusion criteria and were deemed relevant to the systematic literature review. These 28 studies formed the basis for the analysis and synthesis of the research findings.

3.2. *RQ1: What Are the Existing Recognition-Based Methods?*

A total of 28 RBGP schemes have been developed and reported in the literature. Figures 3–5 depict the analysis of publishing channels and the years associated with the largest and lowest quantities of studies pertaining to RBGPs.

3.2.1. Publications Years

Figure 3 illustrates the distribution of chosen research papers according to their respective years of publication. According to the data presented in the figure, it is evident that the year 2021 had the highest volume of published studies, with a total of 10 publications. Subsequently, the papers published in the year 2022 totaled eight, while the years 2018 and 2019 each yielded three publications. In the years 2016, 2017, 2020, and 2023, there was a single article published in each respective year.

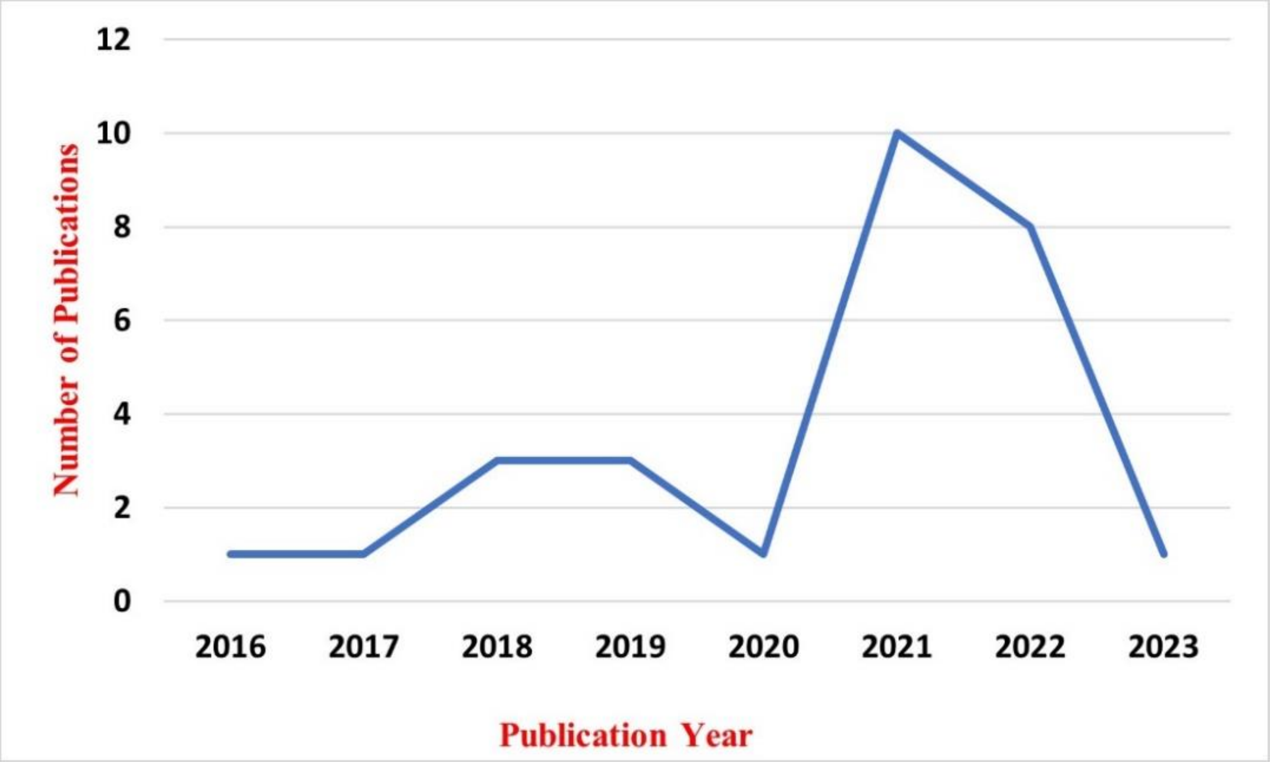

Figure 3. The distribution of the chosen publications is categorized based on the year of publication.

3.2.2. Publication Sources

Out of the selected 28 primary studies, 15 (54%) were published in scholarly journals, while 13 (46%) were presented at conferences. Figure 4 indicates a comparable level of active publications in RBGP authentication schemes across journals and conferences.

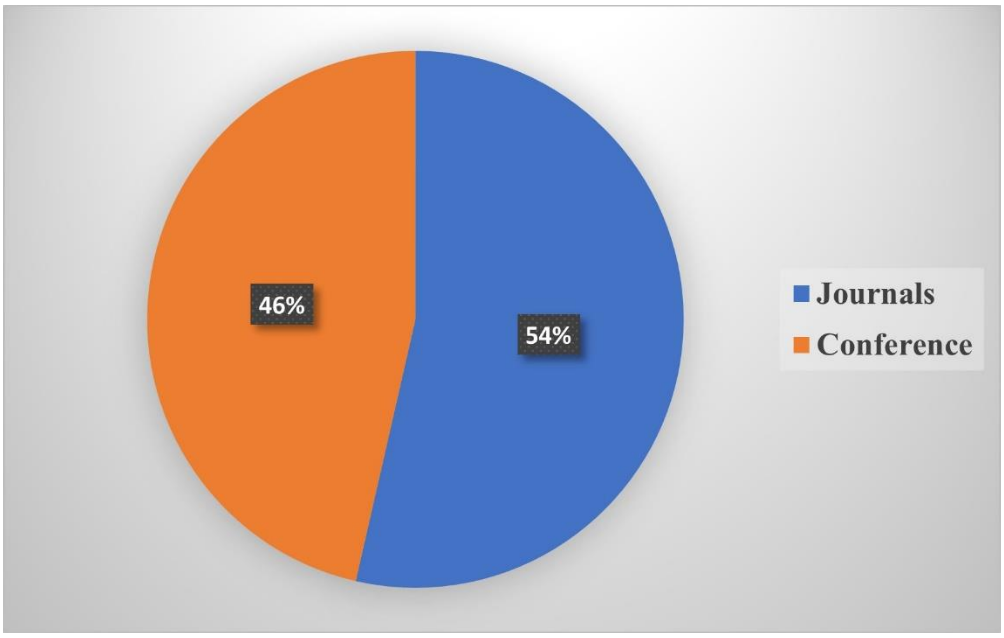

Figure 4. Distribution of publication type.

3.2.3. Publication Sources

Figure 5 displays the quantity of chosen studies, categorized by their respective publishing channels. According to the data presented in the figure, it can be observed that IEEE has the biggest quantity of papers, namely 12, while Springer follows with a count of 7 studies. Additionally, MDPI is revealed to have a total of three papers. Elsevier, ACM, academia, Hindawi, arXiv, and ResearchGate each have one publication.

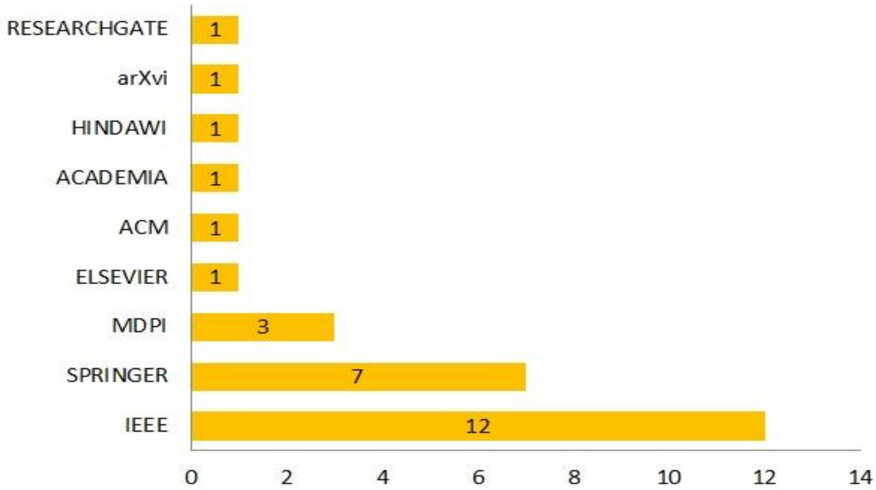

Figure 5. Distribution of publisher channels.

3.3. *RQ2: What Pass-Objects Are Used for Authentication in These Methods?*

The object(s) that a user clicks on during authentication may inadvertently make it possible for the attackers to obtain information that is helpful to log into a secured system. Hence, we examine the types of objects used for authentication. As shown in Figure 6, 14 (50.0%) of the selected schemes allowed the use of registered objects as pass-objects; 2 (7.14%) schemes used decoy objects as pass-objects; 1 (3.57%) scheme used both registered and decoy objects as pass-objects; and 11 (39.29%) schemes used none of the registered and decoy objects as pass-objects.

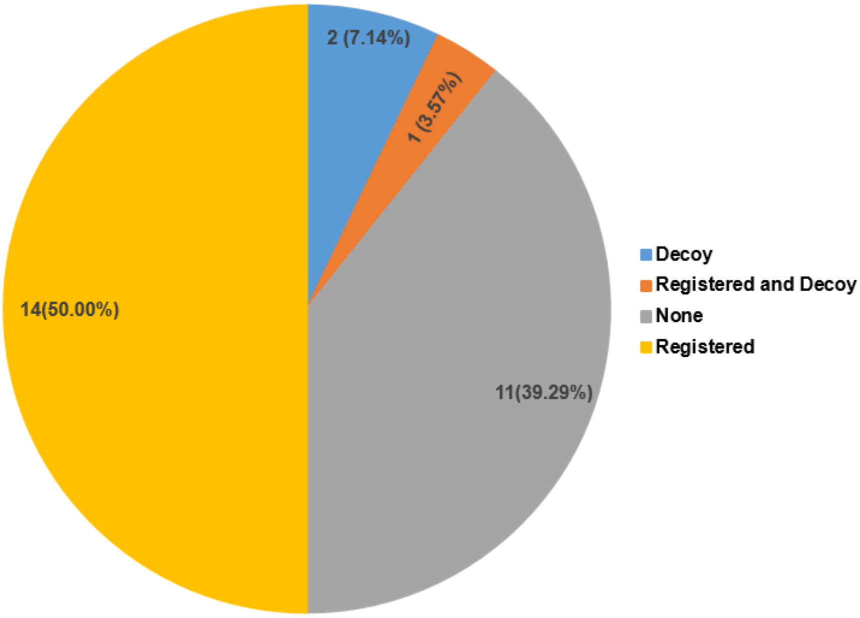

Figure 6. Distribution of selected schemes based on pass-object used.

An overview of the pass-objects used in the selected schemes is presented in Table 3 below.

Table 3. Overview of the pass-objects used in recognition-based systems.

Method	**Pass-Objects**			
	Registered Object	**Decoy Object**	**Registered and Decoy Objects**	**None**
Gokhale and Waghmare scheme [26]			√	
Por et al. scheme [27]		√		
3DGUA [28]	√			
PassMatrix [29]	√			
Othman et al. scheme [30]		√		
PRGUARSS [31]	√			
Salman et al. scheme [32]				√
LocPass [33]				√
PassPage [34]	√			
Nizamani et al. scheme [35]				√
MFAS [36]				√
HyPA [37]				√
PinWheel [38]	√			
EYEDi [39]	√			
Khodadadi et al. scheme [40]	√			
SelfiePass [41]	√			
AlignPIN [42]	√			
EASY-AUTH [43]	√			
Alfard et al. scheme [44]				√
GRA-PIN [45]				√
Hasan et al. scheme [46]				√
VGMSGP [47]	√			
Sharna and Ali scheme [48]				√
Adamu et al. scheme [49]	√			
Lapin and Šiurkus scheme [50]	√			
Sani et al. scheme [51]	√			
Kaur et al. scheme [52]				√
RPP [53]				√

Note: √ denotes yes.

As indicated in Table 4, the authentication schemes proposed in [28,29,31,34,38–43,47,49–51] require the users to login with only the registered objects as the pass-objects during the authentication process. The schemes developed by Por et al. [27] and Othman et al. [30] are the two methods that permit the use of only decoy objects. The pass-object that [26] used could be either the decoy images or the registered images. As a result of this, the attackers are unable to determine whether the image that was clicked was the decoy image or the registered image. In the cases of [32,33,35–37,44–46,48,52,53], the registered icons and the decoy icons are not clicked. Consequently, it would be difficult for the attackers to make any intelligent analysis to distinguish which icons are the registered icons and which are the decoys.

Table 4. Overview of the contributions and limitations of the selected recognition-based systems.

ID	Method	Author	Strengths	Weaknesses
S1	Gokhale and Waghmare scheme	Gokhale and Waghmare [26]	It is simple to implement and has the potential to defend against shoulder-surfing attacks.	Vulnerable to multiple observations of shoulder-surfing attacks (MOSSAs).
S2	Por et al. scheme	Por et al. [27]	Capable of mitigating SSAs without weakening password strength.	Weak against observational attacks involving multiple sessions.
S3	3DGUA	Katsini et al. [28]	Simple to operate.	Susceptible to direct observation attacks on account that the images that a user clicks on are the images that are registered.
S4	PassMatrix	Sun et al. [29]	Use the login indicator to mitigate the direct observation attack.	Open to potential compromises involving video recording and multiple observations.
S5	Othman et al. scheme	Othman et al. [30]	Capable of mitigating direct observation attacks using decoy images.	Vulnerable to MOSSAs and video-recorded shoulder-surfing attacks (VRSSAs).
S6	PRGUARSS	Osunade et al. [31]	Capable of mitigating direct observation attacks.	Susceptible to MOSSAs and VRSSAs because registered images are fixed and always connected with a line.
S7	Salman et al. scheme	Salman et al. [32]	Potential to protect against direct observation attacks.	Vulnerable to MOSSAs and VRSSAs.
S8	LocPass	Por et al. [33]	Potential to thwart SSAs.	The authentication time may be high due to the navigation involved.
S9	PassPage	Chu et al. [34]	Easy and convenient to use.	Susceptible to direct observation attacks on account that a user logs in with only the registered images.
S10	Nizamani et al. scheme	Nizamani et al. [35]	Use a pass-string to mitigate direct observation attacks.	Vulnerable to MOSSAs and VRSSAs because the system always selects and displays registered images.
S11	MFAS	Alsaleem and Alshoshan [36]	Potential to protect against keyloggers.	Susceptible to SSAs because an adversary can easily observe the code entered by the user and associate it with registered images.
S12	HyPA	Gopali et al. [37]	Easy and convenient to use with an alphanumeric password.	Susceptible to direct observation attacks on account that the images that a user clicks on are the images that are registered.
S13	PinWheel	Li et al. [38]	Capable of mitigating direct observation attacks.	Susceptible to SSAs if multiple authentication sessions are video recorded.
S14	EYEDi	Kawamura et al. [39]	Potential to prevent shoulder-surfing attacks using deformed images.	Vulnerable to SSAs because registered images would always appear in the same fixed locations.

Table 4. *Cont.*

ID	Method	Author	Strengths	Weaknesses
S15	Khodadadi et al. scheme	Khodadadi et al. [40]	Straightforward to operate.	Extremely susceptible to SSAs on account that the images that a user clicks on are the registered images.
S16	SelfiePass	Rajarajan and Priyadarsini [41]	Use a secret token to thwart SSAs.	The user's device may be in the possession of an adversary.
S17	AlignPIN	Jain et al. [42]	Thwart direct observation attacks.	Vulnerable to MOSSAs and VRSSAs.
S18	EASY-AUTH	Harshini et al. [43]	Easy and convenient to use.	Susceptible to direct observation attacks on account that the images that a user clicks on are the images that are registered.
S19	Alfard et al. scheme	Alfard et al. [44]	Employs eye gazing rather than direct clicking.	Vulnerable to MOSSAs and VRSSAs.
S20	GRA-PIN	Kausar et al. [45]	Capable of mitigating direct observation SSAs.	Vulnerable to MOSSAs and VRSSAs because the images used in a challenge set are always the same.
S21	Hasan et al. scheme	Hasan et al. scheme [46]	Potential to mitigate shoulder-surfing attacks.	Vulnerable to MOSSAs and VRSSAs.
S22	VGMSGP	Wang et al. [47]	It is difficult for potential adversaries to determine the registered points and the verification grid.	Vulnerable to MOSSAs and VRSSAs because a user would always map the same set of registered points into a specific verification grid.
S23	Sharna and Ali scheme	Sharna and Ali [48]	It is difficult for potential attackers to determine the key number required to login.	Susceptible to SSAs because an attacker can record the entire authentication process and then examine the images that are clicked in order to determine what number they correspond to.
S24	Adamu et al. scheme	Adamu et al. [49]	Uses an OTP for authentication.	Susceptible to direct observation attacks on account that the images that a user clicks on are the images that are registered.
S25	Lapin and Šiurkus scheme	Lapin and Šiurkus [50]	Potential to protect against brute force.	Susceptible to direct observation attacks on accounts that users login with only the registered images.
S26	Sani et al. scheme	Sani et al. [51]	It is difficult for the attackers to perfectly capture the clicked points.	Vulnerable to MOSSAs and VRSSAs.
S27	Kaur et al. scheme	Kaur et al. [52]	Capable of mitigating direct observation attacks.	Susceptible to MOSSAs and VRSSAs.
S28	RPP	Bostan and Bostan [53]	Potential to protect against SSAs.	Vulnerable to MOSSAs and VRSSAs.

3.4. RQ3: What Are the Strengths and Weaknesses of the Selected Recognition-Based Methods?

Several graphical password methods have been presented in order to address the challenges presented by SSAs and other security threats. Table 4 presents a detailed analysis of the strengths and weaknesses associated with the RBGP systems that have been documented in the literature. In our research, we specifically chose to focus on three primary forms of shoulder surfing attacks: direct observation attacks, multi-observation SSAs, and video-recorded SSAs. These types were selected based on their prevalence, feasibility, and the potential threat they pose in real-world scenarios. Here is a brief explanation of each:

Direct Observation Attacks: This is the most straightforward form of SSA, where an attacker merely observes the authentication process of the user directly. Given its simplicity and immediate nature, this type of attack is considered to be among the most common in everyday scenarios, such as using devices in public places.

Multi-Observation SSAs: Here, the attacker observes the authentication process multiple times, either in immediate succession or over extended periods. This form can be especially challenging for RBGP schemes where the graphical elements or patterns remain consistent across multiple authentications.

Video-Recorded SSAs: Modern technology has made it feasible for attackers to surreptitiously record individuals as they input their graphical passwords. This kind of attack allows attackers to replay, review, and even zoom into recorded sessions, making it potentially more potent than direct observation.

The selection of these forms for our research was driven by several factors:

- Prevalence: To the best of our knowledge, the three mentioned forms of SSA are among the most frequently reported and executed in real-life scenarios.
- Impact: These forms can significantly compromise the security of RBGP schemes if not adequately addressed.
- Feasibility for Attackers: The simplicity and ease with which these attacks can be carried out make them more probable compared to more complex or niche methods.

However, we recognize the ever-evolving nature of cybersecurity threats, and it is possible that new or different forms of SSA might emerge or gain prominence in the future. As a result, subsequent research might need to delve into these newer forms to ensure the continued resilience of RBGP schemes against all potential threats.

3.5. RQ4: How Effective Are the Selected Recognition-Based Methods in Terms of Security and Usability?

A good method must strike a good balance between usability and security, making it easier for users to have a better experience and finish the authentication process quickly and correctly. In this question, the usability and security of the selected RBMs were evaluated and analyzed. The results of the analysis of the selected scheme are presented in Table 5.

Table 5. Security and usability of the selected RBMs.

Method	**Shoulder Surfing**			**Password Space Estimation**		**Login Time Comparison**		
	DO [1]	**VR [2]**	**MO [3]**	**Password Length (n)**	**Password Space in (r) Rounds**	**Min Login Time (Seconds)**	**Max Login Time (Seconds)**	**Mean Login Time (Seconds)**
Gokhale and Waghmare scheme [26]	Resist	×	×	n	$25!/(25-n)!$	×	×	×
Por et al. scheme [27]	Resist	×	×	2	$(25!/(25-n)!)\ x\ r$	3.0	28.0	9.67
3DGUA [28]	×	×	×	5	$150!/(150-n)!\ x\ r$	×	×	×
PassMatrix [29]	Resist	×	×	1	$77^n\ x\ r$	×	×	31.31
Othman et al. scheme [30]	Resist	×	×	4	$9^n\ x\ r$	×	×	×
PRGUARSS [31]	Resist	×	×	5	$70!/(70-n)!$	×	×	×
Salman et al. scheme [32]	Resist	×	×	1	$40!/(40-n)!$	22.0	29.75	22.33
LocPass [33]	Resist	Resist	Resist	n	25^r	4.0	20.0	6.55
PassPage [34]	×	×	×	n	$k!/(k-n)!$	20.0	×	27.12
Nizamani et al. scheme [35]	Resist	×	×	n	$118!/(118-n)!$	13.14	40.16	20.84
MFAS [36]	×	×	×	3	$9!/(9-n)!$	×	×	×
HyPA [37]	×	×	×	n	$9!/(9-n)!$	2.7	3.5	×
PinWheel [38]	Resist	×	×	2	$36!/(36-n)!$	8.0	17.0	14.0
EYEDi [39]	Resist	×	×	n	$25!/(25-n)!$	34.7	110.0	×
Khodadadi et al. scheme [40]	×	×	×	8	$32!/(32-n)!$	×	×	×
SelfiePass [41]	×	×	×	2	$k!/(k-n)!$	×	×	×
AlignPIN [42]	Resist	×	×	1	$40!/(40-n)!$	19.74	79.55	19.66
EASY-AUTH [43]	×	×	×	3	$9!/(9-n)!$	×	×	×
Alfard et al. scheme [44]	Resist	×	×	1	$9!/(9-n)!$	×	×	×
GRA-PIN [45]	Resist	×	×	n	$k!/(k-n)!$	×	×	×

Table 5. *Cont.*

Method	Shoulder Surfing			Password Space Estimation		Login Time Comparison		
	DO [1]	VR [2]	MO [3]	Password Length (n)	Password Space in (r) Rounds	Min Login Time (Seconds)	Max Login Time (Seconds)	Mean Login Time (Seconds)
Hasan et al. scheme [46]	Resist	×	×	2	$10!/(10-n)!$	5.8	12.37	8.23
VGMSGP [47]	Resist	×	×	n	$k!/(k-n)!$	5.2	9.0	×
Sharna and Ali scheme [48]	×	×	×	4	$k!/(k-n)!$	×	×	×
Adamu et al. scheme [49]	×	×	×	n	$k!/(k-n)!\ x\ r$	46.0	82.0	×
Lapin and Šiurkus scheme [50]	×	×	×	3	$k!/(k-n)!$	×	×	×
Sani et al. scheme [51]	Resist	×	×	3	$9!/(9-n)!$	×	×	×
Kaur et al. scheme [52]	Resist	×	×	2	$16!/(16-n)!$	×	×	11.0
RPP [53]	Resist	×	×	n	$k!/(k-n)!$	×	×	×

Abbreviations: DO [1]: direct observation SSA; VR [2]: VRSSA; MO [3]: MOSSA; k: denotes the total number of icons used in each challenge set; × denotes not resist.

Based on the findings shown in Table 5, it is evident that every one of the reviewed methods, except for references [28,34,36,37,40,41,43,48,50], is capable of resisting direct observation SSAs. All of the methods that were examined, with the exception of [33], were unable to withstand video-recorded and multiple-observation SSAs. The reason why other methods that were examined are susceptible to MOSSAs is because the objects that a user clicks on within each challenge set may inadvertently make it possible for the attackers to obtain information that is helpful in determining the pass-objects.

In addition, Table 5 shows the comparative analysis of the selected schemes for password space estimation. Research has shown that estimating the password space is a major issue in recognition-based systems. Most of the RBGP methods have small password spaces. Hence, they are vulnerable to brute force and guessing attacks [27]. Increasing the password entropy is a countermeasure against an attacker who intends to guess the registered location. Research has shown that in recognition-based systems, the only method that is used to expand the password space involves increasing the number of objects (such as icons and images) that are included in a challenge set. However, having too many objects in a challenge set may burden the users with identifying their pass-objects.

Finally, the login time for graphical password methods is a crucial metric for assessing the ease of use of any authentication system. The time it takes to log in can significantly impact user satisfaction and may influence their willingness to use the method repeatedly. Recording the login time provides essential insights into a method's usability. A faster login time indicates better usability, making it a critical metric for assessing the method's effectiveness. This measurement is indicative of the ease and speed with which users can navigate the authentication process. By tracking login time, we can identify any potential bottlenecks in the process and make appropriate adjustments to improve usability. Table 3 presents a comparative analysis of the selected RBMs' login times. Among these, [37] had the fastest login time, followed by [27], whereas the method in [49] had the slowest login time. The method in [39] had the longest maximum login time. Regarding the mean login time, [33] outperformed most of the other methods. This is because other methods use either a password, a passphrase, or both, which makes the authentication process more time consuming. In [33], users only need to remember their registered locations, which are unique to each person, and how they log in. This method makes the user's job a lot easier and does not add any more things to remember.

3.6. Study Taxonomy

In RBMs, a user is required to identify objects that are presented in the form of a challenge. The users need to go through an authentication process using specific methods or algorithms, including clicking a pass-object, entering a pass-string, shifting or aligning certain icons, or connecting or highlighting icons with a line or color. As shown in Figure 7, eight schemes (S28, S34, S39, S40, S43, S49, S50, and S51) required users to directly click on the registered objects to login. In the rest of the selected schemes, registered objects are only used to determine what to use for authentication. Out of the five schemes that allow authentication by clicking objects, two schemes (S27 and S30) allow the use of decoy objects, one scheme (S26) allows the use of both registered and decoy objects, and two schemes (S33 and S48) require users to click other objects other than registered and decoy objects. Seven schemes (S29, S35, S36, S37, S44, S45, and S52) require users to enter a pass-string to perform authentication. Five other methods (S32, S38, S41, S42, and S47) demand shifting or alignment of icons for authentication. Finally, to login in the following three schemes (S31, S46, and S53), users need to use lines to connect objects or highlight icons with color.

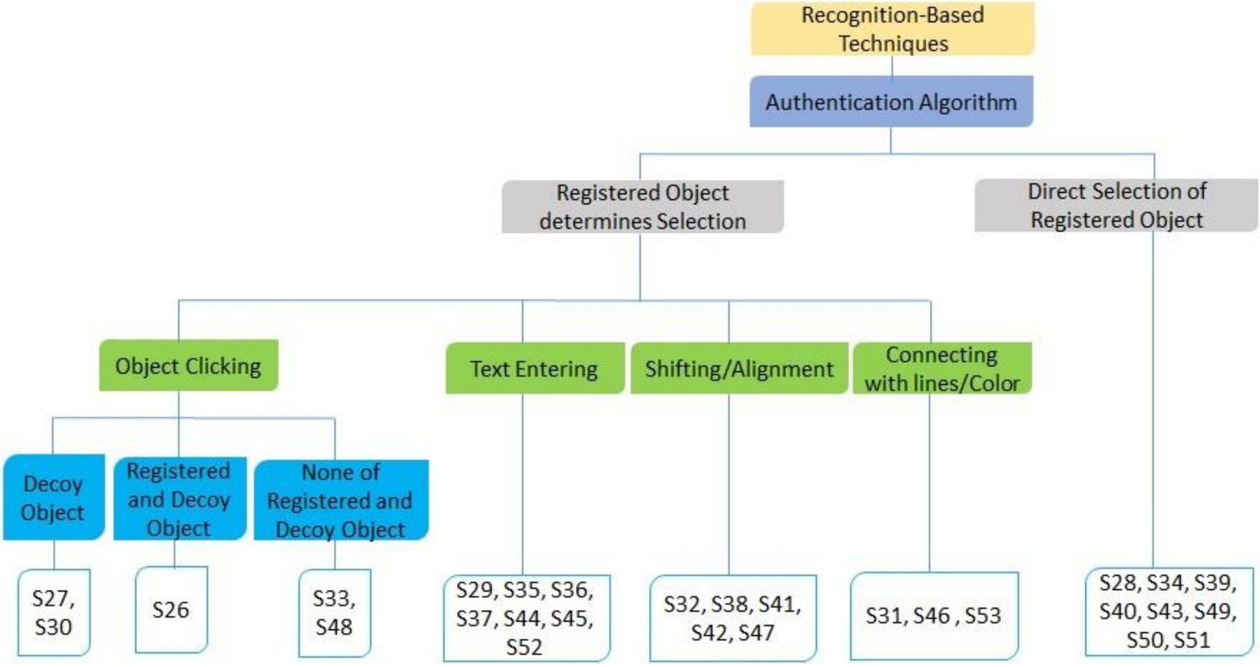
Recognition-Based Techniques
Authentication Algorithm
Registered Object determines Selection
Direct Selection of Registered Object
Object Clicking
Text Entering
Shifting/Alignment
Connecting with lines/Color
Decoy Object
Registered and Decoy Object
None of Registered and Decoy Object
S27, S30
S26
S33, S48
S29, S35, S36, S37, S44, S45, S52
S32, S38, S41, S42, S47
S31, S46 , S53
S28, S34, S39, S40, S43, S49, S50, S51

Figure 7. Taxonomy of RBM resistivity to shoulder-surfing methods.

4. Discussion

The evolution of recognition-based graphic passwords (RBGPs) stands as a testament to the ever-evolving nature of digital security. As authentication measures become more sophisticated, so do the methods by which they are exploited. The primary goal of our review was to shine a light on the vulnerability of current RBGP methods to shoulder-surfing attacks (SSAs).

The contemporary literature starkly reveals the persistent challenge of effectively combating SSAs within RBGP systems. While previous research ventures have explored RBGPs' vulnerabilities against SSAs, what has been notably missing is a comprehensive examination that encapsulates the entirety of available data. Often, the lens of research has been limited, either zeroing in on specific RBGP subsets or being confined by certain temporal and regional parameters. This observation fueled our journey into an exhaustive systematic literature review. Our net was cast wide, drawing from an array of articles, journals, and conference papers that revolved around the central theme of RBGPs' susceptibility to SSAs.

Our ambition was not merely to echo known conclusions but to amalgamate insights, providing a holistic overview of RBGP techniques' strengths and pitfalls. This was done with an eye on uncovering innovative methodologies or previously unaddressed vulnerabilities. A recurring motif from our deep dive into the literature is the security challenge SSAs pose. When users engage with their graphical passwords in public or semi-public domains, they unknowingly become potential prey to malicious observers. These prying eyes, either through direct observation or covert means like camera recordings, can discern and duplicate the user's interaction sequence with graphical elements, potentially granting them unauthorized access.

Graphical passwords, with their inherent reliance on visual patterns, sequences, or image selections, unfortunately play into human strengths in recalling visual sequences, rendering them particularly susceptible to SSAs. This not only challenges the foundational security promise of RBGPs but also threatens to compromise their envisioned role as user-friendly alternatives to traditional text-based passwords.

Pooling from an expansive source range, our aspiration was to bridge the knowledge gaps in existing research. More than a scholarly exercise, we hoped our findings would illuminate the path for future endeavors in the realm of secure, effective, and user-friendly graphical password mechanisms. Our meticulous approach was steered by the PRISMA framework, ensuring that our findings were rooted in relevance and precision. From the plethora of data, 28 articles stood out, becoming the cornerstone of our analysis. Our scrutiny extended to the specific elements a user interacts with during authentication. An emerging observation was the inadvertent risk posed by clicking within a challenge set during the authentication process.

When one grasps the gravity of the vulnerabilities SSAs present, the ripple effects become palpable. From an individual's perspective, this could translate into compromised personal data, a veritable Pandora's box opening up to financial loss, identity theft, and infringed privacy. For organizations, it is a deeper chasm; a breached employee account can be a Trojan Horse, allowing unauthorized access to sensitive company intel. The resulting fallout can range from severe economic setbacks and reputational damage to potential legal entanglements.

Moreover, as graphical passwords are poised as the avant-garde alternative to traditional passwords, their susceptibility can shake users trust in their efficacy. It is a domino effect, leading to escalated security expenditure; hurdles in digital transformation, especially in sectors managing sensitive data; and a potential shift in the trajectory of design and innovation, emphasizing the equilibrium between user experience and stringent security.

To distill our observations, the crux of the challenge SSAs pose to RBGP methods transcends mere technical complications. It underscores the pivotal role of robust authentication measures in our digital era. Our exploration did have some silver linings. For instance, one reviewed method [33] showcased resistance against direct observation, multi-faceted observation, and VRSSAs. However, perfection remains elusive, as the method's elongated login time, especially when juxtaposed against others like [37], remains a challenge.

Our journey through this domain paints a vivid picture of the balance that needs to be struck: a security framework that thwarts potential breaches while ensuring an efficient user experience. The horizon beckons with challenges, but with challenges come opportunities for innovation and advancement.

5. Conclusions

This study examined current RBGP methods through a systematic review of the relevant literature. The search across eight databases yielded a total of 1075 articles. A total of 28 schemes were selected for review based on the application of the inclusion and exclusion criteria. The twenty-eight (28) schemes were classified into four categories based on the pass-objects selected by users during the authentication process.

The contemporary literature reveals a persistent challenge in effectively countering SSAs within RBGP methods. Although past research has ventured into the realm of RBGP vulnerabilities against SSAs, a comprehensive and up-to-date examination that aggregates the entirety of available data remains absent. Previous studies have either been limited in scope, focusing on particular RBGP subsets, or constrained by specific time frames and regions.

In light of this observed research void, our study embarked on an extensive systematic literature review, encompassing a broad spectrum of articles, journals, and conference papers related to RBGP methods and their susceptibility to SSAs. Our endeavor is not just to reiterate known findings but to present a consolidated view of the strengths and weaknesses of RBGP techniques, bringing to light any novel methodologies or overlooked vulnerabilities.

From the literature, the specific security challenge posed by SSAs in the context of graphical password authentication is the unauthorized observation and potential capture of a user's graphical password. When users input their graphical passwords on devices in public or semi-public spaces, malicious observers (either directly or through covert means such as using cameras) can watch and memorize or record the sequence in which the user interacts with the graphical elements. This observed sequence can then be replicated by the attacker to gain unauthorized access. Given that graphical passwords often rely on pattern recognition, sequences, or the selection of images, they can be particularly vulnerable to SSAs, as humans are generally adept at recalling visual patterns. This vulnerability undermines the security premise of graphical passwords, which is to provide an alternative to text-based passwords that is both secure and more user friendly.

By synthesizing information from a diverse range of sources, we have filled the gap in existing research, hoping to provide a panoramic view of RBGP methods and their battle against SSAs. This contribution is not merely academic; our findings intend to serve as a guiding beacon for future research initiatives, paving the way for advancements in crafting secure, efficient, and user-friendly graphical password mechanisms.

The vulnerability introduced by SSAs in RBGP methods has profound real-world implications, affecting both individuals and organizations. Here is a deeper look into its consequences:

Compromised Personal Data: For individuals, the susceptibility of RBGP methods to SSAs means that their personal information, including financial data, contact details, and private communications, can be easily accessed by malicious entities. This not only jeopardizes their privacy but can also lead to financial loss and identity theft.

Organizational Security Breach: For organizations, an employee's compromised account can provide a gateway for attackers to access sensitive company information. Intellectual property, strategic plans, financial records, employee data, and customer details could be at risk. This can lead to significant economic losses, damage to reputation, and potential legal repercussions.

Decreased Trust in Graphical Passwords: As graphical passwords are introduced as an alternative to traditional textual passwords, aiming for enhanced memorability and security, their vulnerability to SSAs can erode users' trust in this authentication method. Perception of insecurity could deter users from adopting graphical passwords, negating the progress made in this area.

Increased Costs: Organizations might find themselves incurring extra costs in response to these vulnerabilities. This could involve implementing additional security measures, training employees on security best practices, managing public relations after a breach, or dealing with the aftermath of data theft.

Barrier to Digital Transformation: In a world that is increasingly becoming digital, the promise of secure and user-friendly authentication methods is crucial for the seamless transition and acceptance of new technologies. Vulnerabilities like those in SSAs can slow down the pace of digital adoption, especially in sectors that deal with highly sensitive data, like healthcare, finance, and defense.

Influence on Design and Innovation: Recognizing the vulnerability of RBGP methods to SSAs can shape the direction of future research and product development. It underscores the need for a balanced approach that prioritizes both user experience and robust security in authentication mechanisms.

In conclusion, the challenge posed by SSAs to RBGP methods extends beyond just a technical hiccup. It touches upon the very fabric of our digital society, emphasizing the need for secure yet user-friendly authentication solutions that can safeguard our personal and collective digital realms.

This study's findings indicate that although RBMs have significant potential, there is room for improvement. Future research should explore alternative methods to counter

SSAs and mitigate additional security risks. Furthermore, it is crucial to discover additional methods that can effectively counter SSAs and minimize the login time. This is essential for striking a balance between preventing security breaches and accelerating the login process.

Graphical Password Vulnerabilities: The study revealed that while recognition-based graphical password (RBGP) methods hold promise, they are susceptible to shoulder-surfing attacks (SSAs). This vulnerability can compromise the very security benefits these methods were designed to offer.

Authentication Process Variances: Among the selected schemes analyzed, there were variations in authentication processes, such as clicking on registered objects, entering a pass-string, or connecting icons. Each of these methods displayed distinct strengths and weaknesses in resisting SSAs.

Balancing Act: A critical observation was the challenge of striking a balance between security and usability. While some methods demonstrated strong resistance to various types of observation attacks, they often did so at the expense of longer login times, potentially affecting the user experience.

Implications for Design: The study underscores the need for a holistic approach in designing RBGP methods. Designers and developers must consider not just the innate security of the method but also external vulnerabilities, user experience, and the real-world contexts in which these methods will be used.

Areas for Future Research:

- Decoy and Registered Objects: Exploring the utility and effectiveness of decoy objects alongside registered ones in deterring SSAs.
- Reducing Login Time: Innovating methods that resist SSAs while also optimizing the speed of the login process.
- Adaptive Authentication: Investigating adaptive RBGP schemes that modify their challenge based on the perceived risk level of the authentication attempt.
- User Experience: Delving deeper into user perceptions and experiences with various RBGP methods to ensure that enhanced security does not detract from usability.

Implications for Implementation: Organizations and developers looking to implement RBGP methods should not only evaluate their intrinsic security features but also consider their resistance to real-world threats like SSAs. Additionally, user training and awareness regarding the risks of SSAs can be an auxiliary line of defense.

In essence, this study sheds light on the intricate landscape of RBGP methods, emphasizing that while they bring a fresh perspective to authentication, they are not without their challenges. Addressing these challenges requires an amalgamation of design innovation, technological prowess, and a deep understanding of user behavior.

Author Contributions: Conceptualization, L.Y.P., L.A.A. and I.O.N.; methodology, L.A.A., I.O.N. and T.F.A.; software, L.A.A.; validation, M.Y.I.I., M.O. and C.S.K.; formal analysis, L.A.A. and M.O.; investigation, M.Y.I.I., L.Y.P. and C.S.K.; resources, L.Y.P. and M.Y.I.I.; data curation, T.F.A.; writing—original draft preparation, L.A.A.; writing—review and editing, L.Y.P., M.O. and C.S.K.; visualization, L.A.A. and I.O.N.; supervision, L.Y.P. and M.Y.I.I.; project administration, L.Y.P.; funding acquisition, C.S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universiti of Tunku Abdul Rahman in Malaysia under grant number IPSR/RMC/UTARRF/2023-C1/K01.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Faircloth, C.; Hartzell, G.; Callahan, N.; Bhunia, S. A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 501–507.
2. Yang, G.C. Development Status and Prospects of Graphical Password Authentication System in Korea. *KSII Trans. Internet Inf. Syst.* **2019**, *13*, 5755–5772.
3. Siddiqui, M.U.; Umar, M.S.; Siddiqui, M. A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; pp. 1–5.
4. Gupta, S.; Sahni, S.; Sabbu, P.; Varma, S.; Gangashetty, S.V. Passblot: A highly scalable graphical one time password system. *Int. J. Netw. Secur. Appl.* **2012**, *4*, 201. [CrossRef]
5. Wajid, A.; Ahmad, T.; Rafique, M. A Face Recognition and Graphical Password Based Hybrid Technique of Information Security. *Pak. J. Sci.* **2018**, *70*, 304.
6. Authentication: Wikipedia. Available online: https://en.wikipedia.org/wiki/Authentication (accessed on 14 June 2023).
7. Still, J.D.; Cain, A.A. Over-the-Shoulder Attack Resistant Graphical Authentication Schemes Impact on Working Memory. *Adv. Intell. Syst. Comput.* **2020**, *960*, 79–86.
8. Addobea, A.A.; Li, Q.; Obiri, I.A., Jr.; Hou, J. Secure multi-factor access control mechanism for pairing blockchains. *J. Inf. Secur. Appl.* **2023**, *74*, 103477. [CrossRef]
9. Authentication in an Internet Banking Environment: Federal Financial Institutions Examination Council. Available online: https://www.ffiec.gov/pdf/authentication_guidance.pdf (accessed on 17 June 2023).
10. Binbeshr, F.; Kiah, M.M.; Por, L.Y.; Zaidan, A.A. A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. *Comput. Secur.* **2021**, *101*, 102116. [CrossRef]
11. Sinha, A.; Shrivastava, G.; Kumar, P.A. Pattern-Based Multi-Factor Authentication System. *Scalable Comput. Pract. Exp.* **2019**, *20*, 101–112.
12. Alsaiari, H.; Papadaki, M.; Dowland, P.; Furnell, S. Graphical one-time password (GOTPass): A usability evaluation. *Inf. Secur. J. A Global Perspective* **2016**, *25*, 94–108. [CrossRef]
13. Wang, H.; Xu, J.; Ma, M.; Zhang, H. A New Type of Graphical Passwords Based on Odd-Elegant Labelled Graphs. *Secur. Commun. Netw.* **2018**, *2018*, 9482345. [CrossRef]
14. Suo, X.; Zhu, Y.; Owen, G.S. Graphical passwords: A survey. In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05), Tucson, AZ, USA, 5–9 December 2005.
15. Jirjees, S.W.; Mahmood, A.M.; Nasser, A.R. Passnumbers: An approach of graphical password authentication based on grid selection. *Int. J. Saf. Secur. Eng.* **2022**, *12*, 21–29. [CrossRef]
16. Carrillo-Torres, D.; Pérez-Díaz, J.A.; Cantoral-Ceballos, J.A.; Vargas-Rosales, C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. *Appl. Sci.* **2023**, *13*, 1374. [CrossRef]
17. Al-Ameen, M.N.; Wright, M.; Scielzo, S. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing System, Seoul, Republic of Korea, 18–23 April 2015.
18. Islam, A.; Por, L.Y.; Othman, F.; Ku, C.S. A Review on Recognition-Based Graphical Password Techniques. In *Computational Science and Technology, Lecture Notes in Electrical Engineering*; Alfred, R., Lim, Y., Ibrahim, A., Anthony, P., Eds.; Springer: Singapore, 2019.
19. Por, L.Y.; Lim, X.T. Issues, threats and future trend for GSP. In Proceedings of the 7th WSEAS International Conference on Applied Computer & Applied Computational Science, Hangzhou, China, 6–8 April 2008.
20. Dagvatur, Z.; Mohaisen, A.; Lee, K.; Nyang, D. Secure Human Authentication with Graphical Passwords. *J. Internet Technol.* **2019**, *20*, 1247–1259.
21. Jaffar, J.A.; Zeki, A.M. Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability. In Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 20–21 December 2020; pp. 1–5.
22. Por, L.Y.; Kiah, M.L.M. Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. *Malays. J. Comput. Sci.* **2010**, *23*, 121–140.
23. Bošnjak, L.; Brumen, B. Shoulder surfing: From an experimental study to a comparative framework. *Int. J. Hum.-Comput. St.* **2019**, *130*, 1–20. [CrossRef]
24. Khot, R.A.; Srinathan, K.; Kumaraguru, P. Marasim: A novel jigsaw based authentication scheme using tagging. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, 7–12 May 2011; pp. 2605–2614.
25. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Rev. Panam. Salud Publica-Pan Am. J. Public Health* **2022**, *46*, e112.
26. Gokhale, M.A.S.; Waghmare, V.S. The shoulder surfing resistant graphical password authentication technique. *Procedia Comput. Sci.* **2016**, *79*, 490–498. [CrossRef]
27. Por, L.Y.; Ku, C.S.; Islam, A.; Ang, T.F. Graphical password: Prevent shoulder-surfing attack using digraph substitution rules. *Front. Comput. Sci.* **2017**, *11*, 1098–1108. [CrossRef]

28. Katsini, C.; Raptis, G.E.; Fidas, C.; Avouris, N. Does image grid visualization affect password strength and creation time in graphical authentication? In Proceedings of the 2018 International Conference on Advanced Visual Interfaces, Castiglione della Pescaia, Grosseto, Italy, 29 May–1 June 2018; p. 33.
29. Sun, H.M.; Chen, S.T.; Yeh, J.H.; Cheng, C.Y. A shoulder surfing resistant graphical authentication system. *IEEE Trans. Depend. Secur.* **2018**, *15*, 180–193. [CrossRef]
30. Othman, N.A.A.; Rahman, M.A.A.; Sani, A.S.A.; Ali, F.H.M. Directional Based Graphical Authentication Method with Shoulder Surfing Resistant. In Proceedings of the 2018 IEEE Conference on Systems, Process and Control (ICSPC), Melaka, Malaysia, 14–15 December 2018.
31. Osunade, O.; Oloyede, I.A.; Azeez, T.O. Graphical User Authentication System Resistant to Shoulder Surfing Attack. *Adv. Res.* **2019**, *19*, 1–8. [CrossRef]
32. Salman, M.; Li, Y.; Wang, J. A Graphical PIN Entry System with Shoulder Surfing Resistance. In Proceedings of the 2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP), Wuxi, China, 19–21 July 2019.
33. Por, L.Y.; Adebimpe, L.A.; Idris, M.Y.I.; Khaw, C.S.; Ku, C.S. LocPass: A graphical password method to prevent shoulder-surfing. *Symmetry* **2019**, *11*, 1252. [CrossRef]
34. Chu, X.; Sun, H.; Chen, Z. PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 14 February 2020; pp. 166–176.
35. Nizamani, S.Z.; Hassan, S.R.; Shaikh, R.A.; Abozinadah, E.A.; Mehmood, R. A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability. *IEEE Access* **2021**, *9*, 51294–51312. [CrossRef]
36. ALSaleem, B.O.; Alshoshan, A.I. Multi-Factor Authentication to Systems Login. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021.
37. Gopali, S.; Sharma, P.; Khethavath, P.K.; Pal, D. HyPA: A Hybrid Password-Based Authentication Mechanism. In Proceedings of the Future of Information and Communication Conference, Vancouver, BC, Canada, 29–30 April 2022; pp. 651–665.
38. Li, Y.; Yun, X.; Fang, L.; Ge, C. An Efficient Login Authentication System against Multiple Attacks in Mobile Devices. *Symmetry* **2021**, *13*, 125. [CrossRef]
39. Kawamura, T.; Ebihara, T.; Wakatsuki, N.; Zempo, K. EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to Prevent Screenshot Attacks. *IEEE Access* **2021**, *10*, 2256–2268. [CrossRef]
40. Khodadadi, T.; Javadianasl, Y.; Rabiei, F.; Alizadeh, M.; Zamani, M.; Chaeikar, S.S. A Novel Graphical Password Authentication Scheme with Improved Usability. In Proceedings of the 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Alkhobar, Saudi Arabia, 6–8 December 2021.
41. Rajarajan, S.; Priyadarsini, P.L.K. SelfiePass: A Shoulder Surfing Resistant Graphical Password Scheme. In Proceedings of the 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 27–28 August 2021.
42. Jain, S.; Dabola, S.; Binjola, S.; Jindal, R. AlignPIN: Indirect PIN Selection for Protection Against Repeated Shoulder Surfing. In Proceedings of the 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 28–29 January 2021; pp. 594–599.
43. Harshini, M.; Sai, P.L.; Chennamma, S.; Reddy, A.G.; Kim, H.S. Easy-Auth: Graphical Password Authentication using a Randomization Method. In Proceedings of the 2021 IEEE Latin-American Conference on Communications (LATINCOM), Santo Domingo, Dominican Republic, 17–19 November 2021.
44. Alfard, F.M.; Keshlaf, A.A.; Bouzid, O.M. IoTGazePass: A New Password Scheme for IoT Applications. In Proceedings of the 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, Tripoli, Libya, 25–27 May 2021; pp. 299–304.
45. Kausar, N.; Din, I.U.; Khan, M.A.; Almogren, A.; Kim, B.S. GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. *Sensors* **2022**, *22*, 1349. [CrossRef] [PubMed]
46. Hasan, S.S.U.; Ghani, A.; Din, I.U.; Almogren, A.; Altameem, A. IoT devices authentication using artificial neural network. *Comput. Mater. Contin.* **2022**, *70*, 3701–3716.
47. Wang, Z.; Liao, L.; Meng, R.; Yang, C.N.; Zhou, Z.; Yang, H. Verification Grid and Map Slipping Based Graphical Password against Shoulder-Surfing Attacks. *Secur. Commun. Netw.* **2022**, *2022*, 6778755. [CrossRef]
48. Sharna, S.A.; Ali, S.A. Image Based Password Authentication System. *arXiv* **2022**, arXiv:2205.12352. [CrossRef]
49. Adamu, H.; Mohammed, A.D.; Adepoju, S.A.; Aderiike, A.O. A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication. In Proceeding of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 5–7 April 2022; pp. 1–5.
50. Lapin, K.; Šiurkus, M. Balancing Usability and Security of Graphical Passwords. In Proceeding of the 9th Machine Intelligence and Digital Interaction Conference, Warsaw, Poland, 9–10 December 2021; pp. 153–160.
51. Sani, S.I.A.; Alhassan, J.K.; Mohammed, A.S. Graphical Based Authentication Method Combined with City Block Distance for Electronic Payment System. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics*; Misra, S., Arumugam, C., Eds.; Springer: Cham, Switzerland, 2022; pp. 289–323.

52. Kaur, A.; Mustafa, K. Preference-Oriented Password-Based Authentication. In Proceeding of the Information and Communication Technology for Competitive Strategies (ICTCS 2020), Jaipur, India, 11–12 December 2022; pp. 953–965.
53. Bostan, H.; Bostan, A. Shoulder surfing resistant graphical password schema: Randomized Pass Points (RPP). *Multimed. Tools Appl.* **2023**, 1–25. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.