Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.082586

ARTICLE

A Graphical User Authentication with Compass Direction and Rotation-Based Dual-Derivation

Chin Soon Ku[1,*], Hui Yi Lim[2], Ana Nabilah Binti Sa'uadi[2], Siew Cheng Lai[1], Jit Theam Lim[3], Pei Xuan Ku[4], Zeng-Wei Hong[5] and Lip Yee Por[6]

[1]Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar, Perak, Malaysia
[2]Department of Information Systems, Universiti Tunku Abdul Rahman, Kampar, Perak, Malaysia
[3]Department of Digital Economy Technology, Universiti Tunku Abdul Rahman, Kampar, Perak, Malaysia
[4]School of Engineering, Faculty of Innovation and Technology, Taylor's University, Subang Jaya, Selangor, Malaysia
[5]Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan
[6]Center of Research for Cyber Security and Network (CSNET), Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, Wilayar Persekutuan, Malaysia

*Corresponding Author: Chin Soon Ku. Email: kucs@utar.edu.my

Received: 18 March 2026; Accepted: 01 June 2026; Published: 23 July 2026

ABSTRACT: In the expanding Internet of Things (IoT) ecosystem, billions of interconnected devices exchange sensitive data, making secure and usable authentication critical. IoT devices in public or shared environments are vulnerable to shoulder-surfing and video recorded observation attacks. Traditional passwords and static graphical schemes remain susceptible due to predictable patterns and direct credential entry. This study presents a novel recognition-based graphical authentication scheme that combines pass-image selection with compass direction substitution and rotation logic to resist observation-based attacks. A prototype was evaluated with 58 participants over three days. Usability metrics included registration time, login time, success rate, and error rate. Memorability and resistance to shoulder-surfing were also assessed. Results showed that login times decreased from 43.62 to 37.78 s, while success rates increased from 40% to 53%, indicating rapid adaptation. Memorability scores improved from 2.05 to 2.19 on a 3-point scale, with perfect recall for five-image passwords by Day 3. Shoulder-surfing tests recorded a 0% attacker success rate. The preliminary results suggest that the scheme offers a useful balance of usability, memorability, and resistance to single session observation attacks. Future work will explore adaptive complexity and accessibility features to further enhance secure authentication.

KEYWORDS: Graphical user authentication; compass direction; rotation pattern; dual-derivation; shoulder-surfing attack; video recording attack

1 Introduction

In an era of pervasive mobile and computing technologies, secure and reliable user authentication is essential for protecting sensitive information across personal, corporate, and public domains [1]. Although alphanumeric passwords remain the most widely used authentication method, they are increasingly vulnerable to observation-based attacks, particularly shoulder-surfing, in which attackers observe or record the authentication process to obtain users' credentials [2]. Such attacks are especially concerning in public or crowded environments, where attackers can remain undetected [3]. Graphical password schemes have been proposed as alternatives to conventional passwords because they leverage the human ability to recognize

and remember visual information more effectively [4]. These schemes generally improve usability and memorability. However, many still exhibit critical security weaknesses. Static image layouts, predictable click points, and repetitive interaction patterns make them vulnerable to shoulder-surfing, video recording, and replay attacks [5]. Even advanced recognition-based approaches may fail to conceal the actual password if an attacker observes the complete authentication sequence.

Many state-of-the-art schemes address only a subset of these threats and often rely on assumptions that limit their practical security. Some assume trusted environments, others require additional hardware, and still others depend on static secrets that remain vulnerable to repeated observation. In contrast, the proposed scheme is specifically designed to defend against observation-based attacks, such as shoulder-surfing and video recording attacks, without requiring auxiliary devices or substantially increasing interaction complexity. The scheme is intended to complement, rather than replace, existing authentication methods, and its security guarantees are defined within this specific threat model.

To address these limitations, this study introduces a recognition-based graphical authentication scheme that combines pass-image selection, compass direction substitution, and incremental rotation. Unlike conventional graphical password schemes, in which pass-images remain fixed or are selected directly, the proposed method derives the observable pass-images during each login session. It employs a session specific randomized grid, a user-defined initial direction, and a rotation rule. Unlike existing neighbor-based and rule-based graphical password approaches that rely on fixed substitution or adjacency rules, the proposed scheme integrates compass direction substitution with sequential direction updates. In the proposed approach, each password image undergoes two stages of derivation, producing session-dependent observable pass-images within a randomized grid. This design reduces the usefulness of video recorded login observations while preserving a simple interaction process suitable for mobile touch input. This study does not claim to introduce a new authentication paradigm. Rather, it presents a lightweight, transformation-based extension of graphical authentication that integrates indirect image selection, compass direction substitution, and sequential rotation logic in a mobile authentication setting. The main contributions of this paper are as follows:

- A transformation-based authentication design that separates visible user input from stored secrets through compass direction and rotation rules.
- A design rationale that targets casual and opportunistic observation attacks while maintaining low cognitive and interaction overhead.
- An initial controlled study evaluating the usability, memorability, and resistance of the proposed scheme to single session observation attacks.

The remainder of this paper is organized as follows. Section 2 reviews related work and existing graphical authentication mechanisms. Section 3 describes the proposed scheme, including its registration and authentication processes, as well as the compass direction substitution rules. Section 4 presents the user study methodology and results. Section 5 discusses the findings, limitations, and directions for future work. Finally, Section 6 concludes the paper.

2 Related Works

With growing concern over shoulder-surfing attacks in public environments, substantial research has focused on developing graphical password schemes capable of resisting observation-based threats. Traditional alphanumeric passwords, although widely used, are highly vulnerable to direct observation and video recording attacks. To address these limitations, researchers have explored graphical authentication mechanisms that leverage the human ability to recognize and recall visual information, thereby improving

both usability and security. Recognition-based graphical authentication systems have been central to these developments. EvoPass [6], for example, presents users with image-based selections within randomized grids and introduces two metrics which are Information Retention Rate (IRR) and Password Diversity Score (PDS), to evaluate memorability and uniqueness. Its dynamic mechanism improves resistance to shoulder-surfing without requiring frequent password changes. Similarly, PassMatrix [7] strengthens security through dynamic login pointers and randomized image positions, thereby disrupting repeated observation attempts.

Other approaches incorporate distinctive image-based input methods. SelfiePass [8] allows users to upload personal images and select password points, which are subsequently hashed and securely stored. This personalization improves memorability and makes credential replication more difficult. PassBYOP (Bring Your Own Picture) [9] extends this concept by combining graphical input with physical tokens in the form of printed image cards used alongside touchscreen devices. As a two-factor authentication scheme, it substantially reduces the risks of impersonation and replay attacks.

Several methods seek to conceal the authentication pattern itself. Pristine PixCaptcha [10] requires users to crop and reposition parts of an image according to specified instructions, while securely storing encrypted authentication data. This approach is designed to resist shoulder-surfing, dictionary, smudge, and brute-force attacks. Picture PassDoodle [11] uses free-form doodles drawn over background images, introducing variability in points of interest and stroke order to complicate unauthorized observation.

Multi-stage authentication systems have also been proposed to enhance protection. The Three-Step Authentication (TSA) model [12] integrates a one-time password (OTP), a textual password, and a graphical password, making it difficult for attackers to succeed using only a single captured credential. Easy-Auth [13] employs randomly generated panda image sequences within a three-layer architecture comprising presentation, logic, and storage layers. Meanwhile, the Directional-Based Graphical Authentication (DGA) method [14] uses cardinal direction gestures, such as up, down, left, and right, over a grid of images, requiring users to remember both the images and their associated directional relationships.

Spatial and neighbor-based schemes offer another line of defense. PassNeighbor [15] requires users to select images adjacent to a target image within a randomized grid, thereby obscuring the actual password image and reducing susceptibility to shoulder-surfing and video recording attacks. Similarly, LocPass [16] applies spatial navigation principles, requiring users to select a sequence of locations relative to a starting point. This approach is intended to improve memorability while maintaining resistance to observation-based attacks. Rule-based mapping, image substitution, and cipher-inspired techniques have also been explored. Digraph Substitution Rules with Pass-Image Output Feedback (DSR-PIOF) [17] employ grid-based logic and mental transformations, such as Playfair ciphers and Latin squares, to obscure password entry. PassNum [18] adopts a different approach by converting pass-image positions into numerical codes using predefined mapping rules. By varying displayed images and input mappings, PassNum makes it more difficult for attackers to reconstruct a password, even after multiple observations. Although many of these schemes improve resistance to shoulder-surfing, relatively few provide consistent protection against multiple attack vectors, including video recording, smudge, dictionary, and brute-force attacks. Table 1 presents a qualitative comparison of authentication schemes based on their reported resistance to common attack vectors.

Table 1: Comparative security features of selected graphical password schemes.

Scheme	Shoulder-Surfing	Video Recording	Smudge Attack	Dictionary Attack	Brute Force
EvoPass [6]	High	Medium	Medium	Low	Low
PassMatrix [7]	Medium	Medium	Low	Low	Low

(Continued)

Table 1 (continued)

Scheme	Shoulder-Surfing	Video Recording	Smudge Attack	Dictionary Attack	Brute Force
SelfiePass [8]	High	Medium	Medium	Medium	Medium
PassBYOP [9]	High	Medium	Medium	Medium	Medium
PixCaptcha [10]	High	Low	High	Medium	Medium
Picture PassDoodle [11]	Medium	Medium	Medium	Medium	Medium
TSA [12]	Medium	Low	Medium	Medium	Medium
Easy-Auth [13]	Medium	Low	Medium	Low	Low
DGA [14]	High	Medium	Medium	Medium	Medium
PassNeighbor [15]	High	High	Medium	Medium	Medium
LocPass [16]	High	High	High	Medium	Medium
DSR-PIOF [17]	High	High	High	Medium	Medium
PassNum [18]	High	High	Medium	Medium	Medium

Note: Low = little/no explicit protection; Medium = partial or conditional protection; High = explicitly designed and evaluated resistance under common threat models.

Although many existing graphical password schemes enhance resistance to shoulder-surfing attacks, most involve trade-offs that limit their practical adoption. Some methods strengthen security at the expense of usability by requiring complex gestures, multiple authentication stages, or external devices. Others prioritize ease of use but depend on static or predictable interaction patterns, leaving them vulnerable to repeated-session observation or video recording attacks. Furthermore, few schemes simultaneously address multiple attack dimensions while preserving memorability and minimizing cognitive load. To address this gap, the proposed scheme integrates randomized image grids with directional and rotational logic, with the aim of strengthening resistance to observation-based attacks without compromising usability or memorability.

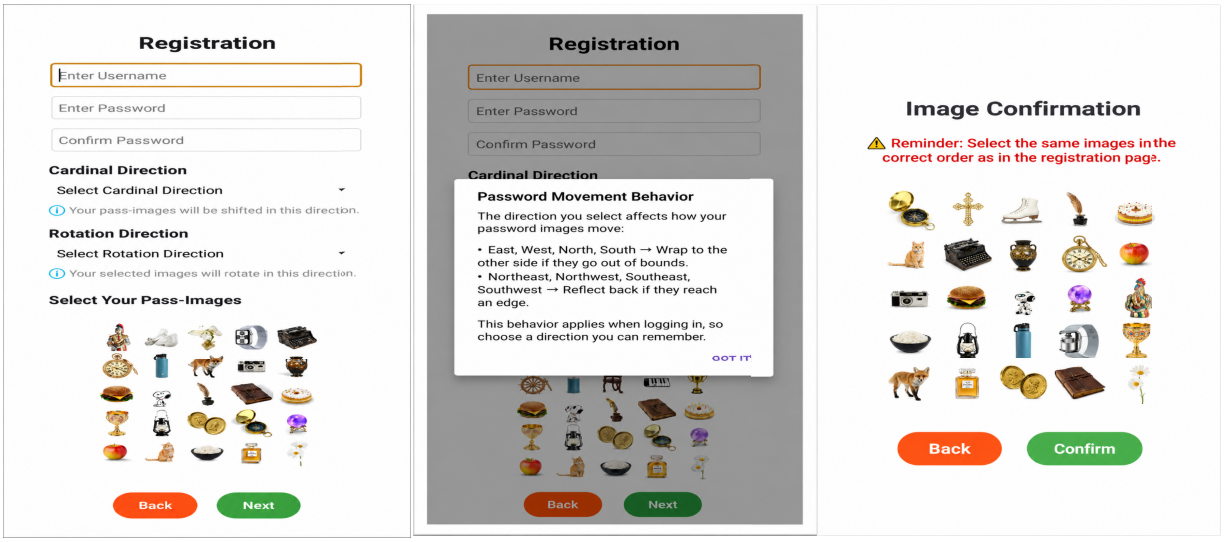
3 Methods

The proposed scheme consists of two phases: registration and authentication. It combines image selection with compass direction substitution and rotation-based input to resist shoulder-surfing and video recording attacks. The threat model assumes a passive adversary who can observe or record a login session but cannot access server-side secrets or internal system parameters. Within this threat model, the scheme is designed to conceal the actual password, ensure session specific authentication interactions, reduce the information that can be inferred from observation, and maintain usability. The proposed scheme is related to rule-based mapping, image substitution, and cipher-inspired techniques, such as DSR and PassNeighbor, but differs in its transformation mechanism. DSR uses rule-based substitutions to prevent users from directly entering their password images, whereas PassNeighbor conceals password images by requiring users to select neighboring images. However, these approaches generally rely on fixed rule structures or fixed neighboring relationships during a login attempt. In contrast, the proposed method applies a dual-derivation process with sequential rotation. The first transformation is determined by the compass direction selected during registration. The second transformation uses an active direction that changes from one password image to the next. Consequently, the mapping is sequence-dependent and varies according to both the position of each password image in the sequence and the randomized grid layout presented during the login session.

3.1 Registration Phase

Fig. 1 illustrates the registration interface. During registration, users first create a username and password. The system then presents a 5 × 5 grid containing 25 randomly arranged images.

Users select three to five memorable images as their pass-images, as shown in Fig. 1a. After selecting Next, the system displays an alert explaining the directional movement applied to the pass-images during authentication (Fig. 1b). Users are then required to reselect the same images in the same order to confirm both memorability and intentional selection (Fig. 1c). Next, users select an initial direction from eight possible options: North, Northeast, East, Southeast, South, Southwest, West, and Northwest. This initial direction determines the first directional transformation applied to each pass-image during authentication. Users subsequently select a rotation direction, either clockwise or counterclockwise, which determines how the active direction changes during the derivation process. The initial direction is applied first, while the selected rotation direction governs the subsequent update of the active direction. The registered pass-images, their order, the initial direction, the rotation direction, and relevant timestamps are securely stored in the database for subsequent authentication and verification.



(a) **(b)** **(c)**

Figure 1: Graphical user interface design for the proposed method's registration process: (**a**) username and password creation; (**b**) alert message explaining password movement behavior; (**c**) pass-image confirmation.

3.2 Authentication Phase

The authentication phase employs an indirect password-entry mechanism. During login, users do not select their actual pass-images directly. Instead, they select derived images generated through spatial transformations applied to a dynamically randomized image grid. For each authentication session, the system presents a randomized 5 × 5 grid of images. Because the arrangement changes between sessions, attackers cannot readily reuse previously observed input patterns. Compared with static graphical password schemes, this dynamic challenge response approach improves resistance to shoulder-surfing, replay, and video recording attacks [19]. Users begin with their registered sequence of pass-images, which constitutes the underlying graphical password. They then generate session specific observable pass-images by applying the registered compass direction rule together with the rotation mechanism. These transformations map each actual pass-image to a visible selectable image in the current grid. Consequently, the observable input

sequence changes across login sessions, even though the underlying password remains unchanged. This separation between the visible authentication actions and the actual password reduces the information exposed through observation-based attacks while preserving usability through intuitive spatial reasoning.

3.2.1 Compass Direction Substitution Rules

The proposed technique combines compass direction substitution and rotation principles to resist shoulder-surfing and video recording attacks. It employs eight directions: North, Northeast, East, Southeast, South, Southwest, West, and Northwest. During registration, users select a sequence of images and an initial direction. During authentication, this direction is used to locate derived pass-images relative to the actual password images. Directional movement and rotational substitution rules are then applied to determine the final pass-images. Fig. 2 illustrates the representation of the directional marker.

Figure 2: Marker's representation indicates: (**a**) the password image (blue), (**b**) the derived pass-image located outside the challenge set grid (purple), and (**c**) the finalized pass-image used as the password.

Fig. 3 presents the complete set of compass direction substitution rules used to derive the final pass-images. For the North and South rules, a pass-image is normally located one step vertically above or below the corresponding password image. If the password image lies on the top or bottom boundary, respectively, the position wraps around to the opposite row within the same column (Fig. 3a–d). For the East and West rules, a pass-image is normally located one step horizontally to the right or left of the password image. If the password image lies on the rightmost or leftmost boundary, respectively, the position wraps around to the opposite column within the same row (Fig. 3e–h).

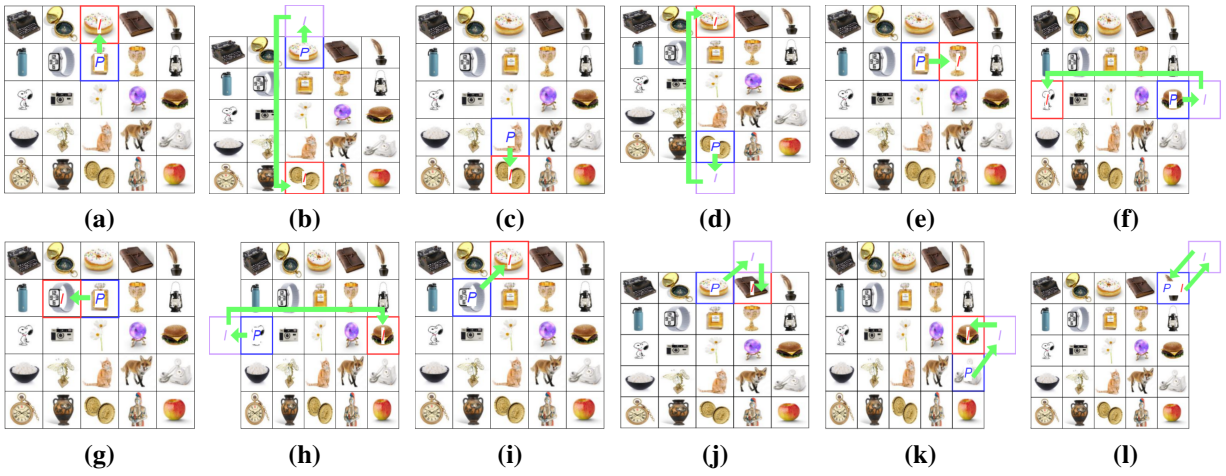


Figure 3: (Continued)

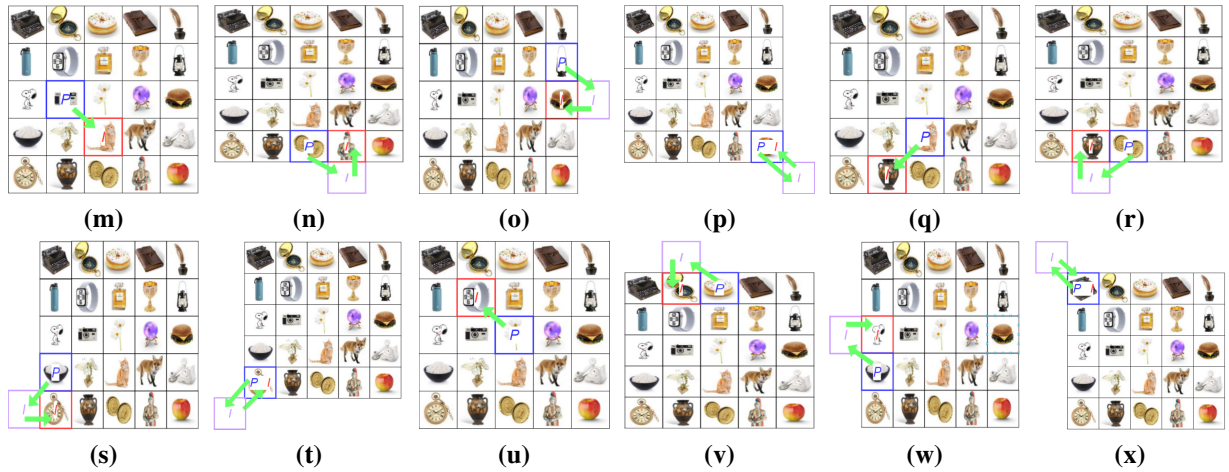


Figure 3: Compass direction substitution rules: (**a**) North (Normal), (**b**) North (Special), (**c**) South (Normal), (**d**) South (Special), (**e**) East (Normal), (**f**) East (Special), (**g**) West (Normal), (**h**) West (Special), (**i**) Northeast (Normal), (**j**) Northeast (Special 1), (**k**) Northeast (Special 2), (**l**) Northeast (Special 3), (**m**) Southeast (Normal), (**n**) Southeast (Special 1), (**o**) Southeast (Special 2), (**p**) Southeast (Special 3), (**q**) Southwest (Normal), (**r**) Southwest (Special 1), (**s**) Southwest (Special 2), (**t**) Southwest (Special 3), (**u**) Northwest (Normal), (**v**) Northwest (Special 1), (**w**) Northwest (Special 2), and (**x**) Northwest (Special 3).

For the diagonal rules which are Northeast, Southeast, Southwest, and Northwest, the pass-image is normally obtained by moving one step along both relevant axes. If one component of the movement falls outside the grid boundary, only the valid component is applied. Thus, when a password image lies on a single boundary, the diagonal movement is reduced to either a horizontal or vertical step. If both movement components are invalid, as occurs when the password image occupies the relevant corner position, the pass-image remains unchanged. This condition applies to Northeast at the top-right corner (Fig. 3i–l), Southeast at the bottom-right corner (Fig. 3m–p), Southwest at the bottom-left corner (Fig. 3q–t), and Northwest at the top-left corner (Fig. 3u–x).

3.2.2 Rotation-Based Dual-Derivation

In the proposed scheme, pass-images are derived by combining a registered compass direction with a rotation pattern. This dual-derivation process causes the observable input to vary across both authentication steps and login sessions, even though the user's actual password remains unchanged. Its primary objective is to separate the hidden password from the visible input sequence. Users do not enter their password directly; instead, they enter a derived sequence determined by hidden spatial transformation rules. Consequently, observing a complete login process does not directly reveal the underlying password. Each login session uses a newly randomized 5 × 5 image grid, making every observable input sequence session specific and difficult to reuse. The first layer of indirection is provided by compass direction substitution, through which users select images positioned relative to their actual password images rather than selecting the password images themselves. The second layer is introduced through direction rotation, which changes the mapping rule throughout the login sequence.

For the first pass-image, the system derives a temporary image from the corresponding password image using the registered initial direction. For example, if the registered direction is North, the temporary image is the cell located directly above the password image, subject to the applicable boundary rule. The final pass-image is then obtained by applying the current active direction to the temporary image. For the first

pass-image, the active direction is identical to the registered initial direction. For each subsequent pass-image, the same two-stage derivation procedure is repeated. First, a temporary image is derived from the corresponding password image using the registered initial direction. Next, the active direction is rotated by one step according to the user's selected rotation pattern. For example, under clockwise rotation, an initial direction of North becomes Northeast for the second image, East for the third image, and so forth. The updated active direction is then applied to the temporary image to obtain the final pass-image. This sequential rotation mechanism causes the mapping rule to change throughout the authentication sequence. A fixed directional rule alone may allow attackers to infer patterns after repeated observations. By contrast, the rotation mechanism reduces this risk by making the transformation path non-static. As a result, visible authentication behaviour depends on both the position of the password image in the sequence and the randomized grid presented during the session.

From a security perspective, this layered transformation functions as a lightweight, human-computable cipher: the password is never entered directly, the transformation rules are user specific, and the visible input is dependent on the current session. From a usability perspective, compass directions and rotational movements are intuitive and require relatively limited mental effort. By combining a fixed registered direction with a rotating update rule, the scheme generates pass-images that are difficult for an observer to predict. If a user selects an incorrect pass-image, the challenge grid is immediately reshuffled to discourage iterative guessing. After three consecutive failed attempts, the system activates a lockout mechanism. Formally, the challenge set is represented as a randomized 5 × 5 image grid G, where each cell $G_{i,j}$contains a unique image. The user's registered password is defined as an ordered sequence of images $P = \{p_1, p_2, \ldots, p_k\}$, where $3 \le k \le 6$. Each user also registers an initial compass direction $d_0 \in D$, where $D = \{N, NE, E, SE, S, SW, W, NW\}$, and a rotation direction $r \in \{\text{clockwise, anti-clockwise}\}$. The complete compass direction and rotation-based dual-derivation procedure is summarized in Algorithm 1.

Algorithm 1: Compass direction and rotation-based dual-derivation pseudocodes

Input:
G: randomized 5 × 5 image grid
$P = \{p_1, p_2, \ldots, p_k\}$: registered password images
d_0: registered initial compass direction
r: registered rotation pattern, where r ∈ {clockwise, counterclockwise}
Output:
$PI = \{PI_1, PI_2, \ldots, PI_k\}$: determined pass-images sequence
Begin:
Shuffle challenge set in grid G
For $i = 1$ **to** k **do**:
Locate p_i in grid G
// Update the current direction using the registered rotation pattern
If $i == 1$ **then**
$d_i \leftarrow d_0$
Else
$d_i \leftarrow$ RotateDirection(d_i, r)
End If
$T_i \leftarrow$ ApplyCompassDirectionSubstitutionRule(p_i, d_0, G) //First derivation with registered initial direction
$PI_i \leftarrow$ ApplyCompassDirectionSubstitutionRule(T_i, d_i, G) //Second derivation uses the current direction

(Continued)

Algorithm 1 (continued)

End For
Return *PI*
End

Fig. 4a shows a sample password set (P1–P6) registered by the user, with East as the compass direction and clockwise as the rotation pattern. During login, the system presents a randomized challenge set (Fig. 4b). Temporary images are labeled T1–T6. The final pass-images are labeled PI1–PI6. The derivation process is as follows:

- P1: Apply East (normal case) to get T1. Since T1 is not in the rightmost column, apply East (normal case) again to get PI1 (Fig. 4c).
- P2: Apply East (normal case) to get T2. Rotate the direction from East to Southeast. Since T2 is in the rightmost column, apply Southeast (special case 2) to get PI2 (Fig. 4d).
- P3: Apply East (normal case) to get T3. Rotate the direction from Southeast to South. Since T3 is in the bottom row, apply South (special case) to get PI3 (Fig. 4e).
- P4: Apply East (special case) to get T4. Rotate the direction from South to Southwest. Since T4 is at the bottom-left corner, apply Southwest (special case 3) to get PI4 (Fig. 4f).
- P5: Apply East (normal case) to get T5. Rotate the direction from Southwest to West. Since T5 is not in the leftmost column, apply West (normal case) to get PI5 (Fig. 4g).
- P6: Apply East (normal case) to get T6. Rotate the direction from West to Northwest. Since T6 is in the top row, apply Northwest (special case 1) to get PI6 (Fig. 4h).

The user must select all pass-images (PI1–PI6) in the correct order to gain access (Fig. 4i).

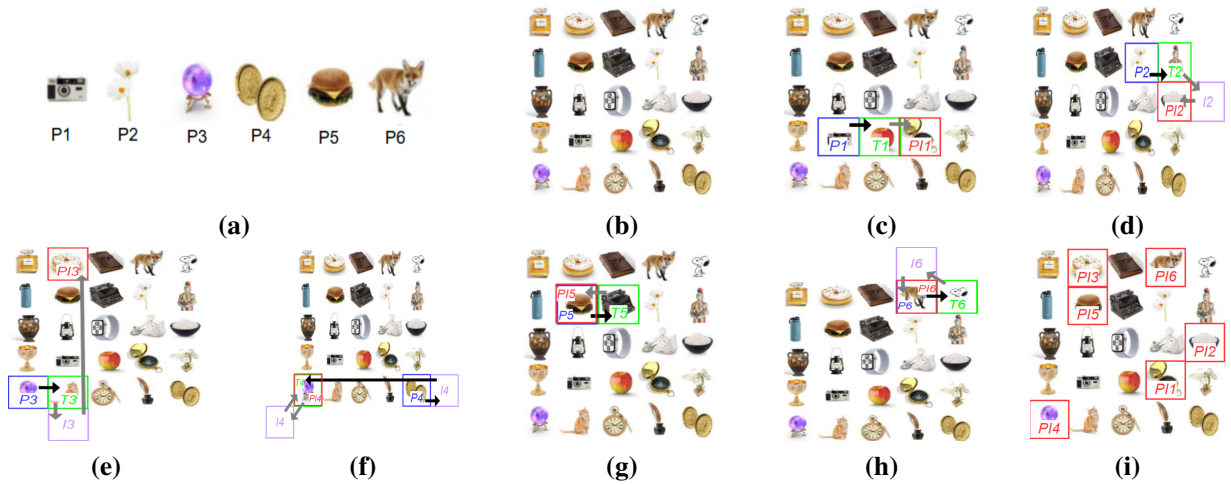


Figure 4: Example of the login process using the proposed method: (**a**) Example of user's password, (**b**) randomized challenge set for a login session, (**c**) determining the first pass-image (PI1), (**d**) determining the second pass-image (PI2), (**e**) determining the third pass-image (PI3), (**f**) determining the fourth pass-image (PI4), (**g**) determining the fifth pass-image (PI5), (**h**) determining the sixth pass-image (PI6), and (**i**) finalized pass-images for login.

4 User Study Results

4.1 User Study Procedure

The present evaluation should be regarded as an initial controlled user study rather than a final large scale deployment study. Its purpose was to examine whether users could understand and apply the proposed

direction-rotation authentication logic and whether the scheme demonstrated resistance to passive single session video recording attacks under controlled conditions.

Three user studies were conducted to evaluate the proposed authentication system in terms of usability, memorability, and resistance to shoulder-surfing attacks. Together, these studies provide an overall assessment of the system under a controlled threat model. The study focused on the proposed scheme and was not intended as a direct comparison with other authentication methods. A fair comparison with PINs, text passwords, or other graphical schemes would require the same task design, threat model, participant conditions, and evaluation metrics. Such a comparison was beyond the scope of the present study and is suggested as future work in Section 6. A total of 58 participants took part in the evaluation. The study was conducted over three consecutive days using a structured testing process: Session 1 was held on Day 1, Session 2 on Day 2, and Session 3 on Day 3. Penetration testing was also performed to examine resistance to unauthorized access and identify potential weaknesses. The evaluation included registration and login tasks. During these tasks, the system automatically recorded registration time, login time, login success rate, and error frequency. This automated process reduced manual error and ensured accurate real-time data collection. Participants also completed questionnaires through Google Forms to report their views on ease of use, understanding, memorability, and perceived security.

Usability was examined by asking participants to complete both registration and login tasks. Each participant was guided through the process to ensure familiarity with the system. During registration, users created an account by selecting an image-based password together with cardinal and rotational directions. The recorded measures were then used to assess how easily participants could understand and use the system without excessive cognitive or operational effort.

The current study was limited to video recording attacks and did not evaluate malware-assisted attacks. Malware keyloggers, touch event loggers, screen capture tools, and spyware represent a stronger threat model because they can access internal device events rather than only external visual information. Therefore, protection against compromised device attacks is outside the scope of this work and should be examined in future studies. Resistance to shoulder-surfing was evaluated using a video recorded observation scenario in which participants acted as attackers. Each participant was shown a video recording of a successful login session using the proposed authentication method. The recording provided a clear view of the login interface and the user's interaction with the system; thus, the attacker was assumed to have captured all visible information from the login process. Participants were also informed about the general operation of the proposed method, including its use of image selection, compass direction substitution, and rotation-based derivation. However, they were not given the legitimate user's secret pass-images, initial compass direction, or rotation rule. After observing the video, participants attempted to reproduce the login sequence based only on the visible input and their knowledge of the method. Attack success rates and participant feedback were used to evaluate the system's resistance to visual observation and replay-based attacks.

Memorability was examined by asking participants to log in again after a delay, without hints or reminders. Login times, attempts, and success rates from the delayed session were recorded and compared with the initial results. Follow-up tests were conducted weekly until the fourth week to observe longer-term recall. These results were used to assess how well users could remember and apply their picture-based passwords over time.

The proposed authentication scheme was implemented as a mobile application prototype that can be installed and run on different smartphone models. The application presents users with a 5×5 graphical challenge grids during registration and login. The mobile prototype supports touch-based image selection and implements the proposed compass direction substitution and rotation-based pass-image derivation logic.

4.2 Registration and Login Time Result

The average registration time across all participants was 22.78 s, indicating that the registration process was relatively quick. Login times decreased across the three sessions, suggesting increased familiarity with the authentication procedure. The average login time was 43.62 s on Day 1, decreasing to 39.38 s on Day 2 and 37.78 s on Day 3.

4.3 Login Success Rate Result

The login success rate improved across the three sessions. On Day 1, 23 of 58 login attempts were successful, resulting in a success rate of 40%. This increased to 43% on Day 2, with 25 successful logins, and to 53% on Day 3, with 31 successful logins. This trend suggests that participants became more familiar with and confident in the authentication process over time.

4.4 Degree of Correctness Result

This metric measures how accurately users recalled and selected their pass-images, including in unsuccessful login attempts. Table 2 presents the average correctness scores for different password lengths across the three test days. On Day 1, the average correctness scores for password lengths of 3, 4, and 5 were 0.80, 0.66, and 0.80, respectively. By Day 3, these scores were 0.76, 0.82, and 1.00, respectively. Overall, the results suggest improved recall accuracy over time, particularly for longer passwords. This may indicate that repeated exposure strengthened participants' memory of both the selected images and their associated directional rules.

Table 2: Average degree of correctness for different password lengths across the three test days.

Password Length	Avg. Correctness		
	Day 1	Day 2	Day 3
3	0.80	0.81	0.76
4	0.66	0.70	0.82
5	0.80	0.83	1.00

4.5 User Feedback (Ease of Use and Understanding) Result

Questionnaire responses showed steady improvement in perceived ease of use and understanding across the three test days. Using a 3-point Likert scale (1 = low, 2 = moderate, 3 = high), the average usability score increased from 2.17 on Day 1 to 2.48 on Day 3. Similarly, the average ease-of-understanding score increased from 2.17 to 2.40. These findings suggest that repeated use increased user confidence and reduced the perceived complexity of the authentication process.

4.6 Shoulder-Surfing Attack Testing Result

A pre-recorded login video was used to simulate attacker observation during authentication. Participants acted as attackers and were asked to reproduce the login sequence based only on their observations. Across all three test days, no participant successfully replicated the password, resulting in a 0% attack success rate in every session. These results suggest that the proposed authentication scheme resists shoulder-surfing and video recorded attacks under the controlled conditions examined. Participant feedback supported these quantitative findings. Most participants rated the system's security positively and agreed that it was effective against observation-based attacks. Several participants reported that the combination of randomized image

grids and direction-based movement rules made the login process difficult to reconstruct. A small number noted a minor learning curve during the first session, particularly when recalling directional and rotational patterns. However, this difficulty decreased with brief practice. The security evaluation in this study was based on a threat model focused on passive observation attacks. Under this model, an adversary can observe or record authentication sessions but does not interact directly with the system. The main evaluation scenario assumes limited observation opportunities, such as one or a small number of login sessions, reflecting common real-world situations in public or shared settings. More capable adversaries who collect and analyze multiple recordings across sessions are beyond the main scope of this study and are discussed as a limitation.

4.7 Memorability Testing Result

Memorability was evaluated by asking participants to log in again after a time gap, without hints or assistance. Using a 3-point Likert scale (1 = low, 2 = moderate, 3 = high), the average memorability score increased from 2.05 on Day 1 to 2.19 on Day 3. This upward trend suggests increasing familiarity with the system and improved recall of password components, including pass-images, directions, and rotation patterns.

5 Discussion

5.1 Usability Analysis

Compared with systems such as PassMatrix [7] and EvoPass [6], which rely heavily on grid navigation and indicator cues, the proposed method combines direct image selection with spatial movement logic. Although the initial login success rate was modest, at 40% on Day 1, it increased steadily to 53% by Day 3. This may compare favourably with schemes such as Draw-A-Secret (DAS) [20] and Picture PassDoodle [11], which can exhibit low reproducibility because they rely on free-form input. Unlike systems such as SelfiePass [8], which require precise click points on personal images, the proposed method reduces dependence on fine motor precision and may therefore be more accessible. The average registration time was 22.78 s, while the average login time decreased from 43.62 to 37.78 s across the three sessions. These results suggest that users can become familiar with the system after limited exposure. However, the login success rate increased only from 40% to 53%, which remains modest for practical deployment. Therefore, the findings should be interpreted as evidence of early learnability rather than proof of deployment readiness. Future versions should incorporate clearer instructions, guided practice, visual feedback, and adaptive difficulty.

5.2 Security Analysis

The proposed system demonstrated resistance to observation-based attacks under the tested conditions. Unlike static graphical schemes such as PassPositions [21] or Click Points, in which repeated observation may reveal consistent input patterns, the proposed method uses dynamic positional derivation based on cardinal directions and rotation. This increases input uncertainty and makes visible actions less directly related to the underlying password. In the controlled video recording attack test, no participant successfully reproduced the correct authentication sequence, resulting in a 0% attack success rate under the evaluated condition. The method also avoids some limitations of hybrid schemes such as PassBYOP [9] and TSA [12], which may require external devices or multiple credentials. In addition, the movement-based logic makes video analysis more difficult because repeated playback does not directly reveal the hidden directional and rotational rules without prior knowledge. For the analytical model, an adversary is assumed to be capable of fully observing or recording the authentication interface across login sessions, as in shoulder-surfing or video recording attacks. However, the adversary does not know the user specific secret parameters, namely the registered starting compass direction and rotation rule.

Let the challenge set be a randomly permuted 5 × 5 grid containing 25 distinct images. A user password consists of an ordered sequence of k images, where $3 \leq k \leq 6$. In each login session, the mapping between password images and observable pass-images is determined by: (i) session specific randomness from grid permutation, and (ii) user specific transformation rules based on directional substitution and rotation. As a result, the observable input sequence is a one-time transformation of the actual password rather than a direct encoding. Although each actual password image can be transformed using one of eight compass directions, this does not produce 8 × 25 unique valid pass-images within the grid. The value 8 × 25 represents the number of possible actual-image and direction-mapping pairs, not the number of unique pass-image cells. Since every determined pass-image must still lie within the same 5 × 5 grid, the maximum number of valid observable pass-image cells at each authentication step is 25. Multiple actual image and direction pairs may also map to the same pass-image cell, especially under boundary conditions and compass direction substitution rules. Therefore, the direction and rotation mechanisms increase the number of possible derivation paths and obscure the relationship between actual password images and observed pass-images. However, they do not increase the number of observable pass-image cells beyond the 25 valid grid positions at each step. The password entropy of the proposed system is $k \log_2 25$.

Observation-based attacks are further constrained by the randomized challenge grid. Even if an adversary records a complete login session, the observed pass-image sequence is associated with that session's grid arrangement and cannot be directly reused in a later login session. Without knowledge of the directional and rotational rules, a recorded observation does not directly disclose the registered password images. Thus, the scheme exhibits a challenge-response characteristic that reduces the effectiveness of simple replay attacks. This analytical reasoning is consistent with the empirical findings, particularly the 0% success rate observed in the shoulder-surfing and video recording simulations. Together, the analysis and experimental results suggest that the proposed scheme provides resistance to common observation-based attacks within the evaluated threat model.

Smudge attacks were not experimentally simulated in this study. Because the proposed method uses indirect pass-image selection, touch traces left on the screen may correspond to derived pass-images rather than the actual registered password images. This may reduce the direct usefulness of smudge traces compared with schemes in which users touch their actual password positions. Furthermore, the same screen locations are likely to contain different images in subsequent login sessions because the grid is reshuffled.

5.3 Memorability Analysis

Graphical password systems such as Hybrid Images and Picture PassDoodle [11] aim to improve memorability by encouraging users to create visual stories or doodles. However, such approaches may result in inconsistent recall because users can reproduce patterns differently over time. In contrast, the proposed system combines spatial memory with fixed directional and rotational logic. In the user study, memorability scores increased from 2.05 on Day 1 to 2.19 on Day 3, indicating improved recall of password components over the three sessions. Participants also showed strong correctness for longer passwords, with five-image passwords achieving a correctness score of 1.00 by Day 3. This performance may be comparable to schemes such as LocPass [16] and CMAPS [22], which also employ structured movement cues. Unlike simpler or more static approaches, however, the proposed system uses changing visible inputs, which may reduce vulnerability to direct replay attacks.

5.4 Strengths, Limitations and Future Work of This Study

The proposed authentication scheme seeks to balance usability, memorability, and resistance to observation-based attacks. It does not aim to eliminate dictionary or brute-force attacks on the underlying

password. Instead, it increases the difficulty of observation-based inference and may reduce attack feasibility under practical constraints such as lockout policies and limited observation opportunities. By combining image selection, compass direction substitution, and rotation-based direction updates, the scheme creates a layered defense while remaining learnable. Each component contributes differently to security. Static image selection, as used in many conventional graphical password schemes, is vulnerable to shoulder-surfing and video recording attacks because observed input may be directly reused. Compass direction substitution improves security by separating the visible input from the actual password image, requiring attackers to infer hidden spatial relationships rather than merely copy observed selections. Rotation-based direction updates strengthen this separation by changing the effective direction for each pass-image. Together, these mechanisms reduce the stability of visible input patterns and make the authentication sequence more difficult to reproduce.

The user study results provide initial support for this design. Login success rates increased across the three sessions, while average login times decreased, suggesting that participants became more familiar with the directional and rotational logic. Longer password sequences also showed improved correctness, possibly because structured spatial sequences provide stronger procedural cues and help users maintain a consistent mental model across steps. Resistance to shoulder-surfing was especially notable under the tested condition: no participant successfully reproduced a password after observing a recorded login session. This suggests that the layered design can conceal direct password entry in a passive observation scenario.

Other than these strengths, several limitations remain. Initial login performance was relatively low, particularly among users unfamiliar with directional and rotational logic. Although performance improved with practice, onboarding support such as visual cues, tutorials, and guided instructions may help reduce the initial learning curve. The mental effort required for spatial transformation represents a deliberate trade-off between usability and security. Rather than memorizing long or arbitrary secrets, users must remember a small set of consistent spatial rules, with performance expected to improve as procedural familiarity develops.

The study is also limited by its relatively small and homogeneous participant sample. Although 58 participants were sufficient for an initial controlled evaluation, most were drawn from a university environment. This may have resulted in similarities in age, education level, and technical familiarity. Therefore, the reported login time, success rate, memorability, and perceived usability findings should be interpreted as preliminary indicators rather than fully generalizable outcomes. Future studies should recruit a larger and more diverse sample, including at least 100 participants across a wider age range, such as 18–65 years, with balanced representation of technical and non-technical users. This would allow the scheme's usability and accessibility to be assessed across different levels of digital literacy, cognitive ability, and authentication experience.

The study also has threat-model limitations. The evaluation considered passive video recording attacks under limited observation conditions and did not formally test multi-session attackers. Repeated observations across multiple randomized grids may allow attackers to reduce uncertainty by comparing observed pass-image sequences and reverse-mapping candidate password images. Future work should therefore extend the threat model to include multi-session attacks. Such evaluations should measure full recovery rate, partial recovery rate, candidate-space reduction, and the number of observed sessions required to infer the secret. Future studies should also examine stronger threats, including malware keyloggers, touch event loggers, screen capture tools, and spyware.

Another limitation concerns the duration of the memorability evaluation. The present results mainly demonstrate early learnability and short-term adaptation, rather than long-term memorability. Since real authentication systems may be used intermittently, future evaluations should include delayed recall tests after one week and four weeks, as well as longer intervals such as two or three months. These tests should measure login success rate, login time, number of failed attempts, degree of correctness, and subjective memorability.

Such evaluations would help determine whether users retain both the selected images and the associated direction-rotation rules over time.

The present study did not conduct a head-to-head comparison between the proposed method and baseline authentication schemes such as PIN, Android Pattern, EvoPass, or DSR under identical experimental conditions. Therefore, comparisons with related work should be interpreted only as high-level contextual observations based on previously reported findings, not as controlled performance comparisons. Since prior studies differ in participant characteristics, task procedures, devices, threat models, and success-rate definitions, direct numerical comparisons may be misleading. Future work should conduct a within-subjects or between-subjects comparative study in which participants use the proposed scheme and select baseline methods under the same conditions. Metrics should include registration time, login time, login success rate, error rate, memorability, subjective usability, and resistance to shoulder-surfing and video recording attacks.

Finally, the proposed scheme may be improved in three directions. First, adaptive security could be explored by varying password length according to application risk level. High security contexts may require longer image password sequences, whereas lower risk contexts may use shorter sequences to improve usability. Second, accessibility features such as voice-over guidance, high contrast display, adjustable grid cell size, and haptic feedback could be added to support users with visual or motor limitations and older adults. Third, the scheme could be integrated with multi-factor authentication, such as biometrics or one-time passwords, to strengthen protection in high-risk applications.

6 Conclusion

This paper presented a graphical authentication scheme designed to resist observation-based attacks through indirect input and spatial transformation rules. Rather than prioritizing security at the expense of usability, the proposed method applies directional and rotational logic to increase attack difficulty while remaining learnable for users. The scheme may be suitable for security-sensitive applications, such as automated teller machines, digital identity wallets, healthcare systems, and corporate platforms, where privacy and confidentiality are important. By shifting authentication from direct password entry to structured spatial procedures, the scheme reduces the risk of credential disclosure through casual shoulder-surfing and simple replay attacks. Although the proposed method does not eliminate all guessing or observation-based attacks, the preliminary findings indicate meaningful security benefits without requiring complex gestures, additional hardware, or excessive login time. Participants showed improvements in login time, success rate, and memorability across sessions. In addition, no successful attack was recorded in the controlled shoulder-surfing simulation. Overall, the results suggest that shifting part of the cognitive effort from memorizing static secrets to applying structured spatial transformations may provide a practical authentication alternative in environments where conventional passwords and PINs remain vulnerable to observation-based attacks. Further evaluation with larger and more diverse samples, longer memorability intervals, comparative baselines, and stronger threat models are required before deployment readiness can be established.

Acknowledgement: Not applicable.

Funding Statement: The research was supported by the Ministry of Higher Education (MoHE), Malaysia through the Fundamental Research Grant Scheme (FRGS/1/2023/ICT03/UTAR/02/1). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Chin Soon Ku and Hui Yi Lim; methodology, Chin Soon Ku, Hui Yi Lim and Ana Nabilah Binti Sa'uadi; software, Hui Yi Lim; validation, Ana Nabilah Binti Sa'uadi, Pei Xuan Ku, Zeng-Wei Hong and Lip Yee Por; formal analysis, Hui Yi Lim, Jit

Theam Lim and Zeng-Wei Hong; resources, Hui Yi Lim and Chin Soon Ku; data curation, Siew Cheng Lai; writing—original draft preparation, Chin Soon Ku; writing—review and editing, Chin Soon Ku and Lip Yee Por; visualization, Hui Yi Lim; supervision, Chin Soon Ku; project administration, Chin Soon Ku; funding acquisition, Chin Soon Ku. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the Corresponding Author, Chin Soon Ku, upon reasonable request.

Ethics Approval: All participants provided informed consent prior to taking part in the user study. No personal, sensitive, or identifiable data were collected, and all responses were recorded anonymously. The research involved only voluntary participation and posed no physical, psychological, or social risk to the participants.

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

References

1. Asmat N, Qasim HSA. Conundrum-pass: a new graphical password approach. In: 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE); 2019 Mar 6–7; Islamabad, Pakistan. p. 282–7. doi:10.1109/C-CODE.2019.8680989.
2. Eiband M, Khamis M, von Zezschwitz E, Hussmann H, Alt F. Understanding shoulder surfing in the wild: stories from users and observers. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM; 2017. p. 4254–65. doi:10.1145/3025453.3025636.
3. Ahmad Awan K, Ud Din I, Almogren A, Kumar N, Almogren A. A taxonomy of multimedia-based graphical user authentication for green Internet of Things. ACM Trans Internet Technol. 2022;22(2):1–28. doi:10.1145/3433544.
4. Zhou Z, Yang CN, Yang Y, Sun X. Polynomial-based google map graphical password system against shoulder-surfing attacks in cloud environment. Complexity. 2019;2019(1):2875676. doi:10.1155/2019/2875676.
5. Ku WC, Cheng BR, Yeh YC, Chang CJ. A simple sector-based textual-graphical password scheme with resistance to login-recording attacks. IEICE Trans Inf Syst. 2016;E99.D(2):529–32. doi:10.1587/transinf.2015edl8080.
6. Yu X, Wang Z, Li Y, Li L, Zhu WT, Song L. EvoPass: evolvable graphical password against shoulder-surfing attacks. Comput Secur. 2017;70(1):179–98. doi:10.1016/j.cose.2017.05.006.
7. Sun HM, Chen ST, Yeh JH, Cheng CY. A shoulder surfing resistant graphical authentication system. IEEE Trans Dependable Secure Comput. 2018;15(2):180–93. doi:10.1109/TDSC.2016.2539942.
8. Rajarajan S, Priyadarsini P. SelfiePass: a shoulder surfing resistant graphical password scheme. In: 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT); 2021 Aug 27–28; Bangalore, India. p. 563–7. doi:10.1109/rteict52294.2021.9573972.
9. Bianchi A, Oakley I, Kim H. PassBYOP: bring your own picture for securing graphical passwords. IEEE Trans Hum Mach Syst. 2016;46(3):380–9. doi:10.1109/THMS.2015.2487511.
10. Chithra P, Sathya K. Pristine PixCaptcha as graphical password for secure eBanking using Gaussian elimination and cleaves algorithm. In: 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP); 2018 Feb 22–23; Chennai, India. p. 1–6. doi:10.1109/ICCCSP.2018.8452829.
11. Schwab D, ALharbi L, Nichols O, Yang L. Picture PassDoodle: usability study. In: 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService); 2018 Mar 26–29; Bamberg, Germany. p. 293–8. doi:10.1109/BigDataService.2018.00052.
12. Adamu H, Mohammed AD, Adepoju SA, Aderiike AO. A three-step one-time password, textual and recall-based graphical password for an online authentication. In: 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON); 2022 Apr 5–7; Lagos, Nigeria. p. 1–5. doi:10.1109/NIGERCON54645.2022.9803122.
13. Harshini M, Sai PL, Chennamma S, Thanuja, Reddy AG, Kim HS. Easy-auth: graphical password authentication using a randomization method. In: 2021 IEEE Latin-American Conference on Communications (LATINCOM); 2021 Nov 17–19; Santo Domingo, Dominican Republic. p. 1–6. doi:10.1109/latincom53176.2021.9647825.

14. Abu Othman NA, Rahman MAA, Sani ASA, Ali FHM. Directional based graphical authentication method with shoulder surfing resistant. In: 2018 IEEE Conference on Systems, Process and Control (ICSPC); 2018 Dec 14–15; Melaka, Malaysia. p. 198–202. doi:10.1109/SPC.2018.8704157.
15. Saeed S, Umar MS. PassNeighbor: a shoulder surfing resistant scheme. In: 2016 2nd International Conference on Next Generation Computing Technologies (NGCT); 2016 Oct 14–16; Dehradun, India. p. 797–802. doi:10.1109/NGCT.2016.7877519.
16. Por LY, Adebimpe LA, Idris MYI, Khaw CS, Ku CS. LocPass: a graphical password method to prevent shoulder-surfing. Symmetry. 2019;11(10):1252. doi:10.3390/sym11101252.
17. Por LY, Ku CS, Ang TF. Preventing shoulder-surfing attacks using digraph substitution rules and pass-image output feedback. Symmetry. 2019;11(9):1087. doi:10.3390/sym11091087.
18. Ahmad A, Asif M, Hamid I, Aljuaid H. PassNum: a usable and secure method against repeated shoulder surfing. Behav Inf Technol. 2025;44(17):4220–46. doi:10.1080/0144929X.2025.2469665.
19. Shen SS, Kang TH, Lin SH, Wei C. Random graphic user password authentication scheme in mobile devices. In: 2017 International Conference on Applied System Innovation (ICASI); 2017 May 13–17; Sapporo, Japan. p. 1251–4. doi:10.1109/ICASI.2017.7988123.
20. Patkar UC, Bhardwaj S, Patil US, Khope N, Ovhal SN, Mahalpure PV, et al. A secure authentication-graphical password authentication system. Int J Intell Syst Appl Eng. 2024;12(3s):209–17. doi:10.53555/kuey.v29i2.8404.
21. Yang GC. PassPositions: a secure and user-friendly graphical password scheme. In: 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT); 2017 Aug 8–10; Kuta Bali, Indonesia. p. 1–5. doi:10.1109/CAIPT.2017.8320723.
22. Zhu Y, Gurary J, Corser G, Oluoch J, Alnahash N, Fu H, et al. CMAPS: a chess-based multi-facet password scheme for mobile devices. IEEE Access. 2018;6:54795–810. doi:10.1109/ACCESS.2018.2872772.