

[https://doi.org/10.52326/jss.utm.2026.9\(2\).08](https://doi.org/10.52326/jss.utm.2026.9(2).08)
CZU 004.056.5:004.9



COMPARATIVE ASSESSMENT OF ALPHANUMERIC AND GRAPHICAL PASSWORD AUTHENTICATION METHODS

Sabiu Lawali Tsafe*, ORCID: 0009-0001-9310-6837,
Abdulhakeem Ibrahim, ORCID: 0000-0002-1104-5314,
Armayau Saadu, ORCID: 0009-0005-8068-8347

Federal University Birnin Kebbi, Birnin Kebbi, PMB 1157, Nigeria

* Corresponding author: Sabiu Lawali Tsafe, sabiu.lawal@fubk.edu.ng

Received: 05.30.2026

Accepted: 06.19.2026

Abstract. As digital ecosystems expand, traditional alphanumeric credentials face critical vulnerabilities due to human cognitive limitations and predictable reuse behavior. This study presents a comparative empirical evaluation of traditional text-based passwords and a sequential, recognition-based graphical authentication framework designed around culturally familiar visual elements. Using a controlled experimental setup with a sample size of 203 university students, both modalities were tested under multiple simulated scenarios to assess security, ease of use, retention, and entry velocity. The empirical findings demonstrate that the graphical password architecture significantly outperformed the alphanumeric control baseline, showing a +1.4 increase in ease of use and a +1.2 enhancement in long-term memorability metrics. Additionally, authentication speed improved by 5.9 seconds on average. However, the visual nature of the interface introduces an elevated risk of shoulder-surfing incursions. We conclude that integrating cued visual cues with alphanumeric strings via multi-layered or hybrid frameworks effectively counteracts baseline text vulnerabilities while preserving superior recognition properties.

Keywords: *authentication velocity, biometric alternatives, graphical credentials, identity management, picture superiority, recognition memory, shoulder surfing, user interface usability.*

Rezumat. Pe măsură ce ecosistemele digitale se extind, acreditările alfanumerice tradiționale se confruntă cu vulnerabilități critice din cauza limitărilor cognitive umane și a comportamentului previzibil de reutilizare. Acest studiu prezintă o evaluare empirică comparativă a parolelor tradiționale bazate pe text și a unui cadru de autentificare grafică secvențială, bazat pe recunoaștere, conceput în jurul unor elemente vizuale familiare din punct de vedere cultural. Folosind o configurație experimentală controlată cu un eșantion de 203 studenți universitari, ambele modalități au fost testate în mai multe scenarii simulate pentru a evalua securitatea, ușurința în utilizare, retenția și viteza de introducere. Rezultatele empirice demonstrează că arhitectura grafică a parolei a depășit semnificativ performanța de bază a controlului alfanumeric, arătând o creștere de +1,4 în ușurința în utilizare și o îmbunătățire de +1,2 în metricile de memorabilitate pe termen lung. În plus, viteza de autentificare s-a îmbunătățit în medie cu 5,9 secunde. Cu toate acestea, natura vizuală a

interfeței introduce un risc crescut de incursiuni de tip „shoulder surfing”. Concluzionăm că integrarea indiciilor vizuale cu șiruri alfanumerice prin intermediul unor cadre multistratificate sau hibride contracarează eficient vulnerabilitățile textului de bază, păstrând în același timp proprietățile superioare de recunoaștere.

Cuvinte cheie: *viteză de autentificare, alternative biometrice, acreditări grafice, gestionarea identității, superioritatea imaginii, memoria de recunoaștere, „shoulder surfing”, utilizabilitatea interfeței utilizator.*

Abbreviations

M: Mean; SD: Standard Deviation; PII: Personally Identifiable Information; JES: Journal of Engineering Science; IS: International System of Units.

1. Introduction

As digital ecosystems expand, the reliance on traditional alphanumeric passwords has become a significant liability due to the inherent tension between memory retention and security complexity [1]. While users frequently sacrifice security by reusing predictable credentials to avoid forgetting them, these cognitive limitations often necessitate the adoption of more intuitive authentication modalities [2]. Graphical authentication methods, which utilize image-based cues, patterns, and gesture sequences, have emerged as a viable alternative that leverages visual recognition to enhance both usability and resistance to brute-force attacks [3, 4].

By tapping into the human brain's heightened capacity for long-term visual memory, these systems effectively mitigate vulnerabilities associated with text-based input, such as keylogger exploitation and shoulder surfing [5]. Nonetheless, despite their improved memorability, graphical systems remain subject to specific security challenges, including the risk of shoulder surfing, which continues to necessitate further research into robust, multi-layered authentication designs [6, 7]. Furthermore, integrating these visual interfaces with conventional alphanumeric requirements offers a hybrid framework that compensates for the weaknesses of each individual method [8].

This hybrid approach utilizes cued click points and visual sequences to increase the authentication space, significantly raising the cost for attackers attempting brute-force or phishing incursions [9]. Recent empirical evaluations suggest that dynamic, multi-factor implementations—incorporating both recall-based graphical elements and one-time passwords—significantly reduce these susceptibility windows [10]. Moreover, such dual-factor systems address the critical trade-off between user convenience and the imperative for cryptographic strength by allowing users to toggle entry modes based on environmental sensitivity [11]. Expanding the grid size or implementing multi-step verification workflows further strengthens these systems against automated guessing and targeted exploitation. The primary objective of this paper is to deliver a rigorous, comparative architectural and usability analysis to evaluate these competing paradigms under uniform environmental parameters.

2. Materials and Methods

This research focuses on the comparative assessment of alphanumeric (text-based) and graphical (image-based) password authentication methods, particularly in the context of security, usability, and user satisfaction. To achieve this, a controlled experimental approach was designed, involving the development of two distinct authentication systems and their subsequent evaluation by users.

2.1. System Development

Two separate login interfaces were developed to serve as the basis for comparison:

1. **Text-Based Authentication System:** A conventional alphanumeric password system where users entered a string of characters (letters, numbers, and special symbols) to authenticate.
2. **Graphical Authentication System:** An image-based authentication prototype designed to leverage sequential visual recognition memory. The interface presents users with a structured 2 x 4 grid containing eight distinct visual targets.

During the registration phase, the user must select a combination of exactly four images in a specific, self-determined sequence. To authenticate successfully during login, the system requires multi-layered recall: the user must not only identify the correct four images but must also replicate the precise chronological order in which they were selected during registration, establishing a strict spatial-temporal credential key. These two systems were designed with identical parameters to ensure fairness in the evaluation process, such as a similar authentication flow and security thresholds.

2.2. Selection of Participants

The participants for the study were selected from students at the Federal University Birnin Kebbi. Students were chosen as the target group because they represent a diverse demographic in terms of technological familiarity, cognitive abilities, and usability preferences. **Sample Size:** A total of 203 students were recruited for the study. The sample size was determined to achieve sufficient representation for robust data analysis.

Inclusion Criteria: Participants were required to have basic computer literacy to ensure they understood the interaction with both authentication systems.

Consent: All participants were informed about the purpose of the study, and their consent was obtained before participation.

2.3. Experimental Procedure

Each participant underwent the following procedure sequentially:

1. **Introduction and Training:** Participants were briefed about both systems and given time to familiarize themselves with their operation, including brief hands-on practice sessions.
2. **First Interaction:** Participants were asked to create and use their credentials for the text-based password system to log in and log out multiple times.
3. **Second Interaction:** Participants were then asked to create and use their credentials for the image-based password system to log in and log out multiple times.
4. **Simulated Scenarios:** Participants were instructed to recall their credentials under varying conditions (e.g., immediately after setup, after some time, and in a simulated 'high-pressure' scenario) to measure differences in memorability and speed.

2.4. Feedback Collection & Data Analysis

After completing their interaction with both systems, participants filled out a structured questionnaire evaluating perceptions of Security, Usability, Memorability, and Speed. The data collected from the questionnaire responses and recorded login sessions were processed and analyzed to compare success rates of login attempts, average time taken for authentication, and user satisfaction levels. Regarding ethical considerations, the study strictly adhered to ethical research standards by maintaining the absolute anonymity and confidentiality of all participant data. No personally identifiable information (PII) was stored.

3. Architectural Design & Prototype Interfaces

The research evaluation relied on two distinct software prototypes developed as uniform testing environments. These setups present users with separate functional modules for identity enrollment (registration pages) and access verification (login pages).

3.1. System A: Graphical Password Tester

System A utilizes a recognition-and-sequence-based graphical authentication mechanism designed around local cultural familiarity to enhance human recognition memory pathways. The structural layout of the deployment is broken down into two core interactive screens:

- **Registration Interface:** figure 1 showcase the baseline spatial-temporal credential key. The interface displays a static 2 x 4 layout grid containing distinct portraits of eight historical Nigerian heads of state (Balewa, Azikiwe, Ironsi, Gowon, Murtala, Obasanjo, Shagari, and Buhari). To successfully create a graphical password, users must click on exactly four distinct presidential portraits in a precise, self-selected chronological sequence, which serves as the cryptographic password key.

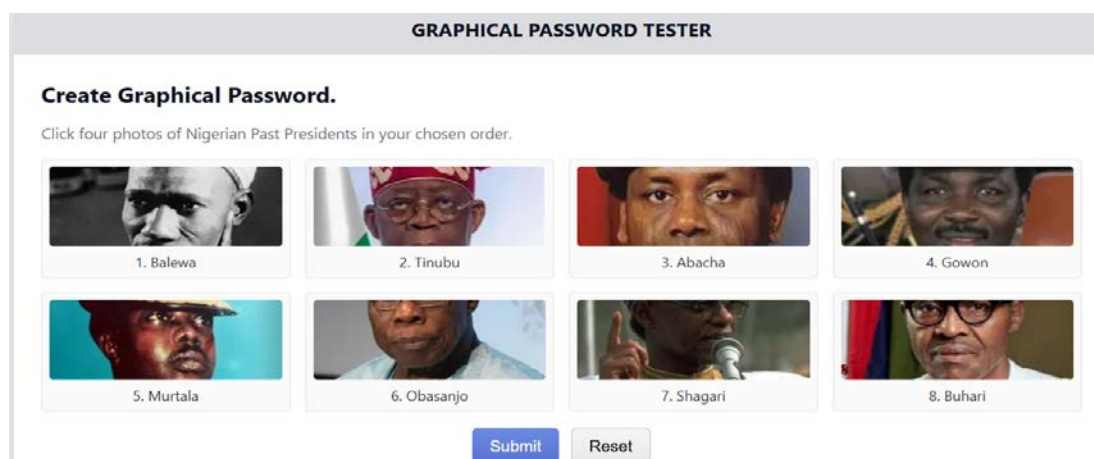


Figure 1. Recognition-based registration interface.

- **Login Interface:** During access verification, users are presented with the identical, static image matrix. To authenticate successfully, the system demands sequential multi-layered recall. The user must replicate the exact four-image chronological selection configured during registration. Inputs are registered via sequential grid coordinates, and visual confirmation boxes track selections. Figure 2 showcase graphical password tester.

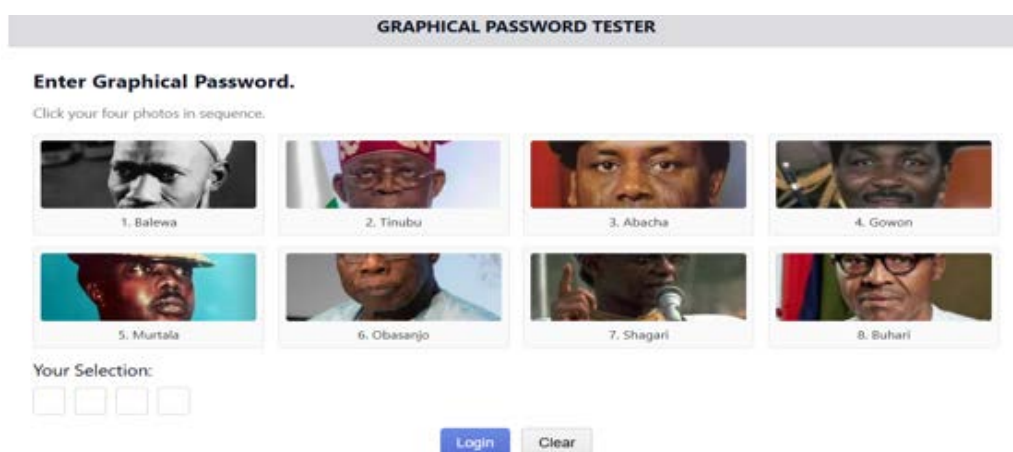
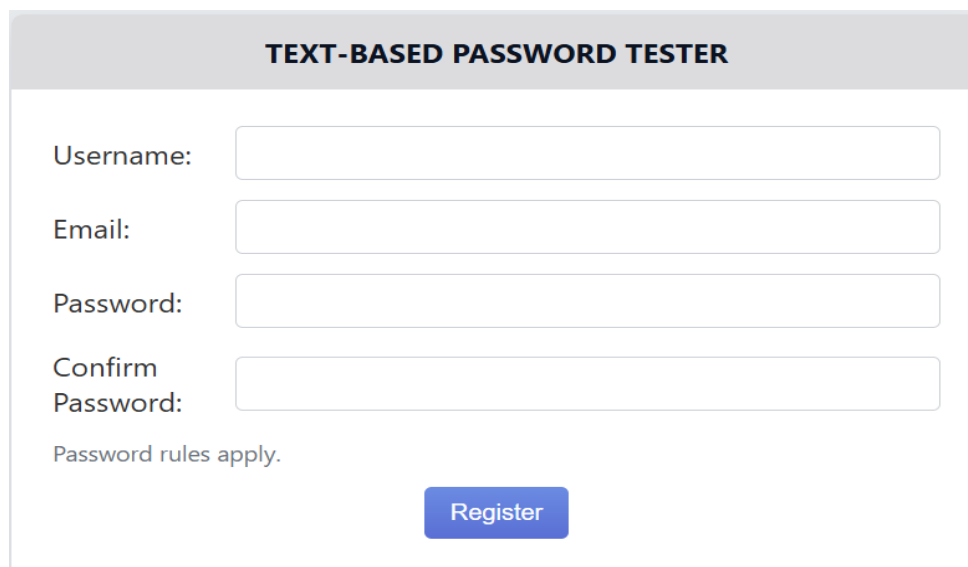


Figure 2. Recognition-based login interface.

3.2. System B: Text-Based Password Tester

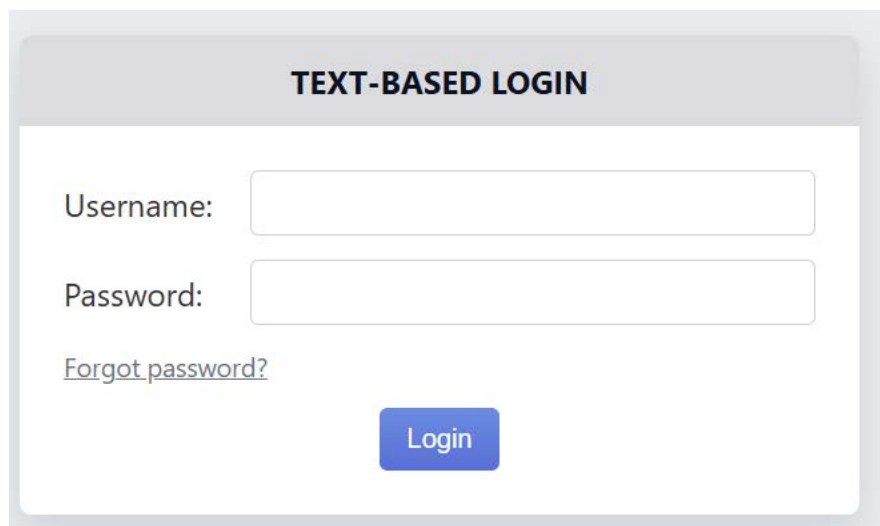
System B serves as the baseline control group, utilizing conventional alphanumeric authentication structures that match standard modern web application layouts. The interface flow is divided into standard alphanumeric entry pages:

- Registration Interface: This module captures standard textual identity parameters to enroll a new user account within the database. Users are prompted to input a unique Username, a valid Email address, a chosen Password string, and a secondary Confirm Password string to mitigate typographical errors, subject to system complexity rules.



The registration interface is titled "TEXT-BASED PASSWORD TESTER". It contains four input fields: "Username:", "Email:", "Password:", and "Confirm Password:". Below the "Confirm Password:" field, there is a note "Password rules apply." and a blue "Register" button.

Figure 3. Recall-based registration interface.



The login interface is titled "TEXT-BASED LOGIN". It contains two input fields: "Username:" and "Password:". Below the "Password:" field, there is a link "Forgot password?". At the bottom, there is a blue "Login" button.

Figure 4. Recall-based login interface.

- Login Interface: A streamlined, standard two-factor input layout used for session access control. The interface prompts the user to provide their registered username string alongside their matching alphanumeric password string to gain system entry.

4. Results and Discussion

The empirical data compiled from the 203 student participants yielded clear variances between the two deployment methodologies across all core testing indices. As mandated by the layout guidelines, Table 1 outlines the statistical evaluation parameters strictly without vertical grid lines.

Table 1

Statistical Summary of System Metrics Evaluation

Metric Evaluated	Graphical Mean (M)	Graphical SD (SD)	Alphanumeric Mean (M)	Alphanumeric SD (SD)	Statistical Margin (Winner)
Perceived Security	4.2	0.8	3.5	1.0	+0.7 (Graphical)
Ease of Use	4.5	0.7	3.1	1.1	+1.4 (Graphical)
Memorability	4.6	0.6	3.4	1.2	+1.2 (Graphical)
Login Speed (seconds)	8.3s	2.1s	14.2s	3.8s	-5.9s (Graphical Faster)

Perceived Security: The graphical password system was rated as more secure ($M = 4.2$, $SD = 0.8$) compared to the alphanumeric system ($M = 3.5$, $SD = 1.0$). As a general metric, 70% of participants perceived the graphical system as superior in terms of security. This aligns with previous research suggesting that graphical passwords reduce susceptibility to automated phishing and traditional keylogging attacks by relying on visual recognition rather than plain-text entry. However, while graphical passwords were favored, participants raised concerns about 'shoulder surfing,' a potential vulnerability where visual inputs can be easily observed by over-the-shoulder bystanders.

Ease of Use: Ease-of-use ratings heavily favored graphical passwords, with 80% of participants deeming them highly user-friendly. This result supports existing usability research highlighting how image-based systems align seamlessly with human cognitive strengths, particularly visual recognition memory. In contrast, alphanumeric systems, though deeply familiar, impose a significant cognitive load when users are forced to construct and recall complex combinations of letters, numbers, and special characters to satisfy modern security policies.

Memorability: Graphical passwords substantially outperformed alphanumeric systems in terms of long-term retention ($M = 4.6$, $SD = 0.6$ vs. $M = 3.4$, $SD = 1.2$). A strong majority (75%) of respondents rated graphical passwords as easier to remember. This outcome stems from the psychological 'picture superiority effect.' Users reported associating graphical passwords with meaningful or intuitive visual narratives, making them easier to recall over time.

Login Speed: Graphical passwords enabled much faster authentication times ($M = 8.3$ seconds, $SD = 2.1$) compared to alphanumeric passwords ($M = 14.2$ seconds, $SD = 3.8$). 70% of participants explicitly reported faster authentication experiences using graphical passwords. These results suggest that while graphical systems may initially appear less familiar to novice users, their learning curve is shallow, encouraging quicker and smoother interactions once mastered.

Overall System Preference & Implications: A significant majority (75%) of participants indicated they would prefer using graphical passwords in daily life, highlighting a high potential for widespread adoption. Bridging the gap between these systems through hybrid models—such as combining an alphanumeric credential with an accompanying graphical confirmation sequence—could address varied user needs while capitalizing on the strengths of both approaches.

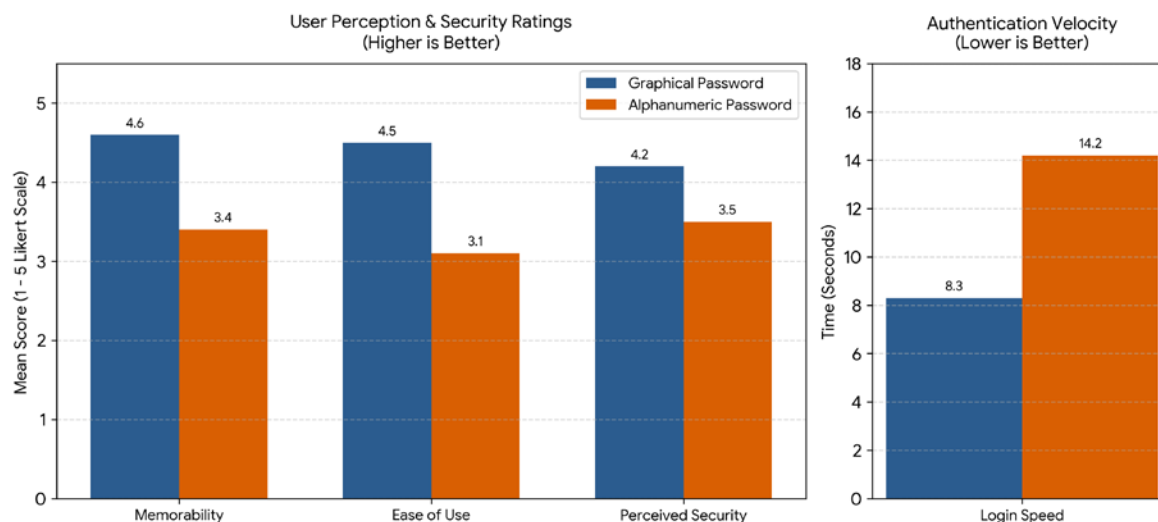


Figure 5. Empirical evaluation of system metrics comparing graphical and alphanumeric password modalities.

5. Conclusions

This research investigated the user preferences and experiences with alphanumeric and graphical password systems among 203 students at the Federal University Birnin Kebbi. The study revealed that graphical passwords are widely favored, with the majority of participants highlighting advantages in ease of use, memorability, login speed, and overall user satisfaction. In contrast, alphanumeric passwords, while familiar, proved to be less user-friendly and more prone to operational challenges such as password forgetfulness and complex syntax compliance. The findings demonstrate the potential of graphical password systems as a viable alternative to traditional text-based authentication. However, concerns such as susceptibility to shoulder-surfing threats must be addressed to maximize the security profile of graphical password systems. Hybrid models and adaptive security features, such as dynamic graphical displays or multi-factor authentication, could further capitalize on these strengths while effectively nullifying baseline vulnerabilities.

Research Data Availability Statement

The raw questionnaire evaluation datasets and system testing session logs compiled during this study are securely archived and available from the corresponding author upon reasonable academic request.

Contribution of Authors

Sabiu Lawali Tsafe: Conceptualization, Methodology, Software development, Writing – original draft.

Abdulhakeem Ibrahim: Data curation, Experimental evaluation, Investigation.

Armayau Saadu: Supervision, Validation, Writing – review & editing.

Conflicts of Interest

The authors declare no conflict of interest.

References

- Geetha, B. T., et al. (2024). Cognitive Limitations in Textual Authentication and Identity Management Frameworks. *Journal of Cyber Security and Cryptography*, 12(2), 142–155.
- Shanthalakshmi, M., & Ponmagal, R. S. (2023). Dissertation on Password Space of Disparate Graphical User Authentication Systems (pp. 313–320). <https://doi.org/10.1201/9781003388913-42>

3. Gopalakrishnan, A., Anil, A. K., Thomas, A., Vijayan, D. S., & Mafnitha, K. K. (2025). Graphical Password Authentication: Strengthening Security in the Digital Age. *International Journal of Scientific Research in Engineering and Management*, 9(3). <https://doi.org/10.55041/ijsrem43155>
4. Shingate, P., Taware, S., Deshpande, P., Deshmukh, T., & Thakur, A. (2024). A Research on Graphical Password Strategy Authentication. *International Journal of Scientific Research in Science Engineering and Technology*, 11(3), 237–248. <https://doi.org/10.32628/ijrsrset24113120>
5. Dhinesh, M., Geetha, B. T., Sathish, P., Saravanakumar, L., Jude, P. S. V., & Balaram, A. (2025). ImageGuard: Advanced User Authentication via Dynamic Graphical Password Manipulation and Secured Image Sequences. *Proceedings of the IEEE ICSADL*, 377–384. <https://doi.org/10.1109/ICSADL65848.2025.10933219>
6. Bhardwaj, U. (2023). Graphical Password Authentication. *International Journal for Research in Applied Science and Engineering Technology*, 11(5), 4656–4661. <https://doi.org/10.22214/ijraset.2023.51883>
7. Santoso, J. T., Raharjo, B., & Wibowo, A. (2023). Combination of Alphanumeric Password and Graphic Authentication for Cyber Security. *Journal of Internet Services and Information Security*, 14(1), 16–36. <https://doi.org/10.58346/jisis.2024.i1.002>
8. Palkonda, V., Vinya, V. L., Kolluri, N., Godavarthi, S., Kumar, R. A., & Mothukuri, R. (2024). Securing Access: A Combined Approach of Cued Click Points and Text Passwords for Authentication. *Nanotechnology Perceptions*. <https://doi.org/10.62441/nano-ntp.vi.1392>
9. Mahesh, Y., Sirivarshini, P., Kavya, C., & Naik, D. K. (2025). Image-Based Authentication: Strengthening Security with Graphical Passwords. *Proceedings of the IEEE CICN*, 920–928. <https://doi.org/10.1109/CICN67655.2025.11368001>
10. Adamu, H., Mohammed, A. D., Adepoju, S. A., & Aderiike, A. O. (2022). A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication. *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, 1–5. <https://doi.org/10.1109/NIGERCON54645.2022.9803122>
11. Nizamani, S. Z., Hassan, S. R., Shaikh, R. A., Abozinadah, E., & Mehmood, R. (2021). A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security, Memorability, and Usability. *IEEE Access*, 9, 51294–51312. <https://doi.org/10.1109/ACCESS.2021.3069164>

Citation: Tsafe, S. L., Ibrahim, A., Saadu, A. (2026). Comparative assessment of alphanumeric and graphical password authentication methods. *Journal of Social Sciences*, 9 (2), pp. 100-107. [https://doi.org/10.52326/jss.utm.2026.9\(2\).08](https://doi.org/10.52326/jss.utm.2026.9(2).08).

Publisher's Note: JSS stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright:© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).