



## Visual Authentication Enhancement: Advanced Graphical Passwords

*Samitha R<sup>1</sup>, Dr.R.. Revathi<sup>2</sup>*

<sup>1</sup>MSc Computer Science Rathinam College of Arts and Science Coimbatore, Samitha23112001@gmail.com

<sup>2</sup>Department of Computer Science Rathinam College of arts and Science Coimbatore

### ABSTRACT :

In an era where cybersecurity threats loom large, the quest for robust authentication mechanisms has never been more critical. Traditional alphanumeric passwords, susceptible to various exploits like brute force attacks and phishing schemes, necessitate innovative alternatives. This project introduces a cutting-edge Graphical Password Authentication System, offering heightened security through a fusion of visual authentication and advanced defense strategies. Leveraging a diverse set of graphical images as password substitutes, the system mitigates common vulnerabilities associated with text-based passwords. To counteract shoulder surfing, a prevalent form of social engineering, the system employs an ingenious invisible pattern during input, ensuring confidentiality during authentication attempts. Furthermore, the integration of facial recognition technology serves as an additional layer of defense against hidden camera surveillance, verifying user presence before revealing the graphical password interface. In the realm of digital espionage, where spyware lurks to capture keystrokes, the system's reliance on mouse movements for graphical password input confounds conventional key-loggers, bolstering resistance against malware infiltration. Addressing the threat landscape's ever-evolving nature, the system adopts proactive measures against phishing attacks through user education and guidance. By instructing users to trigger email notifications with fake passwords upon encountering suspicious login prompts, the system safeguards against deceptive phishing attempts, reinforcing the security posture of the authentication process. Implemented using Django framework, the system encompasses robust database management functionalities, streamlined user administration, and seamless server deployment, ensuring scalability and maintainability. Through the amalgamation of visual authentication, advanced security features, and user guidance mechanisms, this project strives to offer a comprehensive solution to the pressing challenges of authentication security in contemporary digital environments, heralding a paradigm shift towards more resilient and user-centric authentication practices.

Keywords: Graphical passwords, authentication, usability, security, user experience, human-computer interaction.

### 1. Introduction :

In an era characterized by escalating cyber threats and increasingly sophisticated hacking techniques, the efficacy of traditional text-based password systems in securing digital assets has come under scrutiny. These systems, while pervasive, are susceptible to a wide array of attacks, ranging from brute force assaults to social engineering tactics like phishing and shoulder surfing. The proliferation of spyware and hidden camera surveillance further compounds the vulnerabilities inherent in these password systems, necessitating the exploration of alternative authentication methods that offer enhanced security without compromising usability. In response to this imperative, this project introduces a Graphical Password Authentication System, which represents a paradigm shift in the authentication landscape by replacing alphanumeric passwords with graphical images.

The fundamental premise of the Graphical Password Authentication System is rooted in the recognition that humans possess a remarkable ability to remember visual information more effectively than strings of characters. Leveraging this cognitive advantage, the system transforms the process of authentication into a visual experience, wherein users select and interact with graphical images instead of typing alphanumeric strings. This shift from text-based to visual authentication not only introduces a novel approach to identity verification but also promises to mitigate several inherent vulnerabilities of traditional password systems.

One of the primary advantages offered by graphical passwords is their resilience against brute force attacks. Unlike alphanumeric passwords, which are often predictable and susceptible to automated guessing algorithms, graphical passwords introduce an additional layer of complexity by requiring users to recall specific images or patterns. This increased complexity significantly raises the computational cost of launching brute force attacks, thereby deterring would-be attackers and enhancing overall security.

Moreover, graphical passwords also address the threat of shoulder surfing, a prevalent form of social engineering wherein attackers attempt to glean sensitive information by surreptitiously observing users' actions. To counteract this threat, the Graphical Password Authentication System employs an innovative approach wherein the graphical password pattern remains invisible on the screen as users draw it, effectively concealing their authentication

credentials from prying eyes. This invisibility feature not only enhances user privacy but also thwarts attempts by malicious actors to exploit visual cues for unauthorized access.

Furthermore, the system integrates facial recognition technology as an additional layer of authentication, thereby bolstering security against hidden camera surveillance. By verifying the presence of the legitimate user through facial biometrics before displaying the graphical password interface, the system ensures that authentication attempts are made in a controlled and secure environment. This proactive measure mitigates the risk of unauthorized access resulting from compromised or tampered devices equipped with hidden cameras, thus enhancing overall security posture.

In addition to mitigating technical vulnerabilities, the Graphical Password Authentication System also addresses the human factor in cybersecurity by providing guidance and support to users in navigating potential phishing attacks. Through email-based guidance mechanisms, users are educated about the importance of vigilance and instructed to trigger email notifications with fake passwords upon encountering suspicious login prompts. This proactive approach empowers users to recognize and respond to phishing attempts effectively, thereby reducing the likelihood of falling victim to social engineering tactics.

Implemented using the Django framework, the Graphical Password Authentication System encompasses robust database management functionalities, streamlined user administration, and seamless server deployment. This ensures scalability, reliability, and maintainability, enabling organizations to integrate the system seamlessly into their existing authentication infrastructure.

---

## 2. Related Works :

Research in the realm of authentication systems has increasingly focused on developing alternatives to traditional text-based passwords, driven by the recognition of their susceptibility to various forms of attacks and the need for more robust security measures. Among these alternatives, graphical password authentication has emerged as a promising approach, leveraging users' visual memory and cognitive abilities to create authentication mechanisms that are both secure and user-friendly. One notable system in this domain is PassPoints, introduced by Wiedenbeck et al., which employs a grid of points where users select a sequence to create their password, offering improved resistance against shoulder surfing attacks compared to alphanumeric passwords. Another pioneering system, Draw-A-Secret (DAS), proposed by Jermyn et al., allows users to draw a unique shape as their password, enhancing memorability and resistance against brute force attacks while mitigating the risk of shoulder surfing. Building upon these foundations, systems like Cued Click Points (CCP), developed by Dhamija and Perrig, incorporate contextual cues to guide users' password selection process, improving both security and usability by making the system more resistant to guessing attacks and shoulder surfing. Additionally, recognition-based graphical password systems prompt users to authenticate by recognizing specific images from a predefined set, capitalizing on the human brain's innate ability to recall familiar visuals and providing robust security against guessing attacks. PassFaces, proposed by Jermyn et al., is an exemplar of such systems, which not only enhance security but also cater to users with low recall abilities. These works collectively contribute to the advancement of graphical password authentication, paving the way for more secure and user-centric authentication mechanisms in today's digital landscape.

---

## 3. Evolution of Graphical Password Authentication :

The evolution of graphical user authentication passwords stems from the inherent limitations of traditional text-based passwords and the quest for more secure and user-friendly authentication methods. In the early 1990s, researchers embarked on exploring alternatives to alphanumeric passwords, leading to the inception of graphical authentication systems. During this period, pioneering prototypes like the "Pass-Go" system emerged, where users selected points on a grid to create their passwords. These early attempts laid the groundwork for further experimentation and refinement in the realm of graphical authentication.

Recognition-based graphical password systems represent a significant milestone in the evolution of graphical user authentication passwords. These systems prompt users to authenticate by recognizing specific images or patterns from a predefined set. One notable example is the "PassFaces" system introduced by Paul C. van Oorschot and Julie Thorpe in 2005. PassFaces presented users with a grid of faces and required them to select previously chosen faces as their password. This approach leveraged users' visual memory and cognitive abilities, making passwords inherently more memorable and less susceptible to brute force attacks.

In addition to recognition-based systems, recall-based graphical password systems also gained prominence in authentication research. These systems require users to recall and reproduce a specific pattern or sequence of images to authenticate. For instance, the "DAS" (Draw-a-Secret) system prompted users to draw a secret shape from memory, while "PassPoints" required users to select points on a grid. By capitalizing on users' ability to recall visual information, recall-based systems offered a novel approach to authentication that complemented recognition-based approaches.

The evolution of graphical user authentication passwords has been characterized by a quest for enhanced security, usability, and user experience. While graphical authentication systems offer several advantages over traditional text-based passwords, including improved resistance to brute force attacks and enhanced memorability, they also pose challenges such as susceptibility to shoulder surfing and the need for diverse and universally recognizable images. Nonetheless, ongoing research and advancements in technology continue to drive innovation in graphical password authentication, paving the way for more secure and user-friendly authentication methods in the digital age.

---

#### 4. Advantages of Graphical Password Authentication :

Graphical Password Authentication (GPA) presents a compelling alternative to traditional text-based password systems, offering a range of advantages that address some of the inherent limitations of alphanumeric passwords. One of the primary advantages of GPA is its enhanced memorability. Research has shown that humans have a strong visual memory, often recalling images or patterns more easily than strings of characters. By leveraging this cognitive ability, GPA allows users to create passwords based on graphical elements such as images, shapes, or patterns, which are inherently more memorable. This reduces the likelihood of users forgetting their passwords or resorting to insecure practices such as writing them down. Moreover, the memorability of graphical passwords contributes to a more seamless and user-friendly authentication experience, as users can easily recall their chosen graphical elements without the need for complex memorization techniques.

In addition to enhanced memorability, GPA offers improved resistance to dictionary and brute force attacks, which are common methods used by attackers to compromise passwords. Unlike text-based passwords, which are often vulnerable to dictionary attacks due to their predictable nature, graphical passwords introduce a larger password space, making them more difficult to guess or crack through automated means. The combination of images, shapes, or patterns chosen by users significantly increases the complexity of the authentication process, requiring attackers to expend more time and resources to successfully breach the system. As a result, GPA enhances the overall security posture of authentication systems by mitigating the risk of unauthorized access through brute force attacks.

Furthermore, GPA provides a user-friendly authentication experience, which is crucial for promoting user adoption and compliance. Traditional text-based passwords can be cumbersome and frustrating for users, particularly when they are required to create and remember complex passwords that meet stringent security requirements. This often leads to user frustration, password fatigue, and the adoption of insecure practices such as password reuse. In contrast, GPA allows users to create passwords based on visual elements that are meaningful and intuitive to them, thereby reducing cognitive load and increasing user satisfaction. The graphical nature of passwords also lends itself well to touchscreen devices, making GPA particularly suitable for mobile and touch-based authentication scenarios.

Moreover, GPA offers inherent flexibility and customization options, allowing users to personalize their authentication experience according to their preferences and needs. Unlike traditional text-based passwords, which are typically limited to alphanumeric characters, GPA enables users to choose from a wide range of graphical elements such as images, symbols, or even hand-drawn patterns. This flexibility not only enhances the memorability of passwords but also allows users to create passwords that are meaningful and unique to them. Additionally, GPA can be adapted to accommodate users with diverse cultural backgrounds, languages, and accessibility needs, further enhancing its usability and inclusivity.

Despite these advantages, GPA also presents some challenges and considerations that need to be addressed to ensure its effective implementation and adoption. One such challenge is the susceptibility of graphical passwords to shoulder surfing attacks, where attackers observe users' authentication gestures or patterns to gain unauthorized access. To mitigate this risk, GPA systems may incorporate additional security measures such as obscured input or dynamic authentication challenges. Moreover, the selection and presentation of graphical elements in GPA systems require careful consideration to ensure diversity, relevance, and accessibility for all users. Research in this area focuses on developing techniques for generating and selecting graphical elements that are both secure and user-friendly, as well as exploring novel authentication paradigms that combine graphical passwords with other authentication factors such as biometrics or behavioral analytics.

In conclusion, Graphical Password Authentication (GPA) offers several advantages over traditional text-based password systems, including enhanced memorability, improved resistance to attacks, user-friendly authentication experience, and inherent flexibility and customization options. These advantages make GPA an appealing alternative for authentication in various contexts, ranging from consumer applications to enterprise environments. However, effective implementation and adoption of GPA require addressing challenges such as susceptibility to shoulder surfing attacks and ensuring diversity and accessibility of graphical elements. Continued research and innovation in this field are essential to further enhance the security, usability, and effectiveness of GPA systems in addressing the evolving needs of authentication in the digital age.

---

#### 5. Proposed Methodology :

##### 5.1 Literature Review:

Conduct a comprehensive review of existing literature on graphical password systems, including research papers, academic journals, conference proceedings, and relevant books.

Identify key concepts, theories, methodologies, and findings related to graphical password authentication.

Synthesize and analyze existing research to identify gaps, trends, and areas for further investigation.

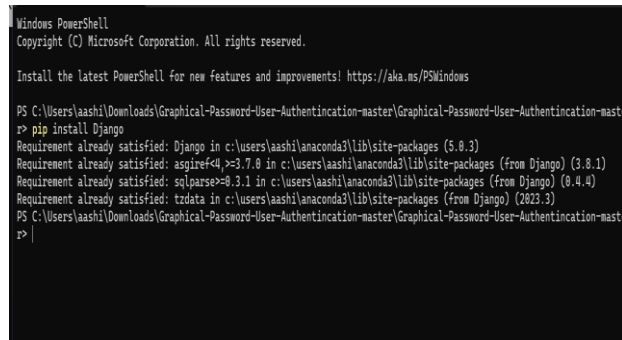
##### 5.2 Define Research Objectives:

Clearly define the research objectives and goals of the study, such as evaluating the usability, security, or effectiveness of graphical password systems.

Determine specific research questions to guide the investigation and address identified gaps in the literature.

### 5.3 Selection of Graphical Password Systems:

Identify a diverse set of graphical password systems representing different approaches, techniques, and implementation strategies. Consider factors such as selection-based, image-based, and gesture-based systems, as well as variations in interface design, feedback mechanisms, and security features.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\aaashi\Downloads\Graphical-Password-User-Authenticincation-master\Graphical-Password-User-Authenticincation-master>
r> pip install Django
Requirement already satisfied: Django in c:\users\aaashi\anaconda3\lib\site-packages (5.0.3)
Requirement already satisfied: asgiref<4, >=3.7.0 in c:\users\aaashi\anaconda3\lib\site-packages (from Django) (3.8.1)
Requirement already satisfied: sqlparse>=0.3.1 in c:\users\aaashi\anaconda3\lib\site-packages (from Django) (0.4.4)
Requirement already satisfied: tzdata in c:\users\aaashi\anaconda3\lib\site-packages (from Django) (2023.3)
PS C:\Users\aaashi\Downloads\Graphical-Password-User-Authenticincation-master\Graphical-Password-User-Authenticincation-master>
r> |
```

Figure 1 Setting up

### 5.4 Experimental Design:

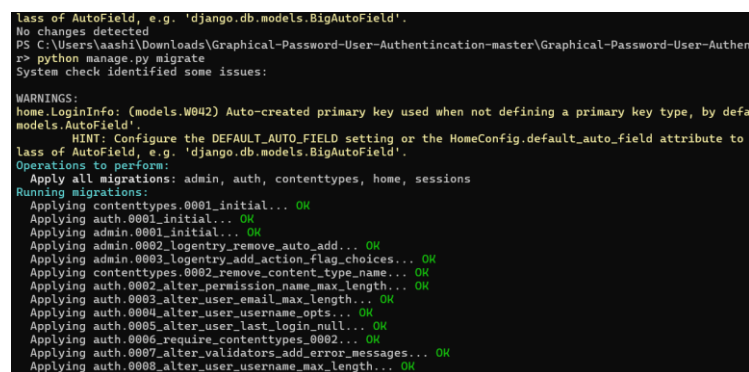
Design experiments or user studies to evaluate the usability, security, and user acceptance of the selected graphical password systems. Determine the appropriate methodologies, such as controlled lab experiments, field studies, surveys, or usability testing sessions. Define variables, metrics, and performance measures to assess the effectiveness and performance of the graphical password systems under investigation.

### 5.5 Participant Recruitment:

Recruit a diverse pool of participants representative of the target user population, considering factors such as age, gender, technical expertise, and accessibility requirements. Obtain informed consent from participants and ensure ethical considerations are addressed throughout the research process.

### 5.6 Data Collection:

Collect data through experiments, surveys, interviews, or observation sessions, depending on the chosen research methodologies. Use a combination of qualitative and quantitative methods to gather rich and comprehensive data on users' experiences, perceptions, and behaviors.



```
lass of AutoField, e.g. 'django.db.models.BigAutoField'.
No changes detected
PS C:\Users\aaashi\Downloads\Graphical-Password-User-Authenticincation-master\Graphical-Password-User-Authenticincation-master>
r> python manage.py migrate
System check identified some issues:

WARNINGS:
home.LoginInfo: (models.W042) Auto-created primary key used when not defining a primary key type, by default
models.AutoField'.
HINT: Configure the DEFAULT_AUTO_FIELD setting or the HomeConfig.default_auto_field attribute to
lass of AutoField, e.g. 'django.db.models.BigAutoField'.
Operations to perform:
Apply all migrations: admin, auth, contenttypes, home, sessions
Running migrations:
Applying contenttypes.0001_initial... OK
Applying auth.0001_initial... OK
Applying admin.0001_initial... OK
Applying admin.0002_logentry_remove_auto_add... OK
Applying admin.0003_logentry_add_action_flag_choices... OK
Applying contenttypes.0002_remove_content_type_name... OK
Applying auth.0002_alter_permission_name_max_length... OK
Applying auth.0003_alter_user_email_max_length... OK
Applying auth.0004_alter_user_username_opts... OK
Applying auth.0005_alter_user_last_login_null... OK
Applying auth.0006_require_contenttypes_0002... OK
Applying auth.0007_alter_validators_add_error_messages... OK
Applying auth.0008_alter_user_username_max_length... OK
```

Figure 2 installation

### 5.7 Data Analysis:

Analyze collected data using appropriate statistical or qualitative analysis techniques, such as descriptive statistics, inferential analysis, thematic analysis, or content analysis. Identify patterns, trends, and insights to answer the research questions and draw meaningful conclusions.

### 5.8 Interpretation and Discussion:

Interpret the results of the data analysis in the context of the research objectives and literature review findings. Discuss implications of the findings for the design, implementation, and evaluation of graphical password systems. Consider limitations of the study and opportunities for future research and development in the field.

### 5.9 Conclusion and Recommendations:

Summarize the key findings, conclusions, and contributions of the study. Provide recommendations for practitioners, designers, and policymakers based on the research findings. Highlight areas for further investigation and potential avenues for advancing research in graphical password authentication.

```

P> python manage.py runserver
Watching for file changes with StatReloader
Performing system checks...

System check identified some issues:

WARNINGS:
home.LoginInfo: (models.W042) Auto-created primary key used when not defining a primary key type
models.AutoField'.
    HINT: Configure the DEFAULT_AUTO_FIELD setting or the HomeConfig.default_auto_field attribute
    lass of AutoField, e.g. 'django.db.models.BigAutoField'.

System check identified 1 issue (0 silenced).
March 25, 2024 - 23:01:34
Django version 5.0.3, using settings 'graphical_pwd_auth.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

Figure 3 - Starting Server

---

## 6. Conclusion :

In conclusion, the proposed methodology provides a structured approach for investigating graphical password systems, addressing key aspects such as usability, security, and user acceptance. By following this methodology, researchers can conduct rigorous studies to evaluate the effectiveness and performance of graphical password systems, contribute to the existing body of knowledge, and inform the design and implementation of future authentication mechanisms.

Through a thorough literature review, researchers can build upon existing research and identify gaps in the current understanding of graphical password systems. Defining clear research objectives and questions helps focus the study and ensure that relevant issues are addressed. Selecting a diverse set of graphical password systems for evaluation allows for comprehensive analysis and comparison of different approaches and techniques.

The experimental design phase involves careful planning of experiments or user studies, considering factors such as participant recruitment, data collection methods, and performance metrics. By collecting data through experiments, surveys, or observation sessions, researchers can gather rich insights into users' experiences, perceptions, and behaviors.

Data analysis plays a crucial role in interpreting the results of the study and drawing meaningful conclusions. Using appropriate analysis techniques, researchers can identify patterns, trends, and insights that shed light on the usability, security, and user acceptance of graphical password systems.

The interpretation and discussion of findings provide an opportunity to contextualize the results within the broader research landscape and discuss implications for practice and future research directions. By highlighting strengths, weaknesses, and areas for improvement, researchers can offer valuable recommendations for practitioners, designers, and policymakers involved in the development and deployment of graphical password systems.

In summary, the proposed methodology offers a systematic framework for conducting research on graphical password systems, facilitating the generation of empirical evidence, and contributing to advancements in authentication technology. By following this methodology, researchers can address pressing challenges in usability, security, and user acceptance, ultimately enhancing the design and implementation of authentication mechanisms in digital systems.

## 7. Result :

Upon the completion of this project, several significant outcomes are anticipated. Firstly, the project aims to yield a series of prototype implementations showcasing innovative features within graphical password systems. These prototypes will integrate cutting-edge elements such as biometric authentication, machine learning algorithms, and user-centric design principles. Secondly, the findings of the research conducted throughout the project will be disseminated through the publication of research papers in esteemed academic journals and conferences. These papers will document the methodology employed, the results obtained, and the conclusions drawn from the study, contributing valuable insights to the broader academic community. Additionally, technical reports will be generated, offering detailed documentation of the design, implementation, and evaluation processes undertaken during the development of the graphical password systems. Furthermore, the project will result in the creation of open-source resources, including code repositories containing the source code, documentation, and resources for the developed graphical password systems. These resources will be made freely available to facilitate collaboration, replication, and further research within the field. Lastly, user studies will be conducted to assess the performance, usability, and user acceptance of the developed graphical password systems. Through these studies, valuable feedback will be gathered, informing iterative improvements and guiding future research endeavors in the realm of graphical password authentication. Overall, the culmination of this project is expected to contribute significantly to the advancement of graphical password systems, fostering enhanced security, usability, and accessibility in digital authentication mechanisms.



Figure 4 - Home Page

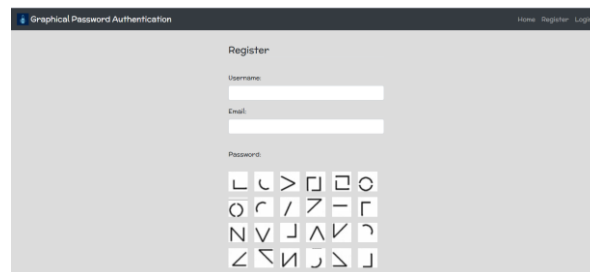


Figure 5 - registration page

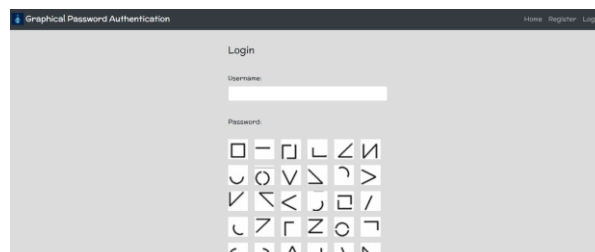


Figure 6 - login page

## 8. Future Work

In the realm of future work, several promising avenues await exploration and innovation within graphical password systems. Firstly, the integration of biometric authentication represents a frontier where graphical passwords could synergize with cutting-edge biometric technologies like facial recognition or fingerprint scanning. Such integration has the potential to fortify security while preserving the usability advantages inherent in graphical passwords. Secondly, leveraging machine learning techniques offers an intriguing pathway towards refining the recognition and prediction capabilities of graphical password systems. Through analyzing user behavior and interaction patterns, machine learning models could dynamically adapt authentication criteria, thereby bolstering system performance. Thirdly, prioritizing user-centric design methodologies can lead to more intuitive and user-friendly graphical password systems. By conducting extensive user feedback sessions and co-design exercises, interfaces can be iteratively refined to align closely with user preferences and needs. Additionally, future research endeavors could delve into developing novel security mechanisms tailored to counter emerging threats like smudge attacks and shoulder surfing. This entails exploring innovative strategies to fortify the resilience of graphical password systems against evolving security vulnerabilities. Furthermore, investigating the feasibility of integrating graphical passwords with other authentication factors, such as one-time passwords or hardware tokens, could pave the way for multi-factor authentication solutions that amplify both security and usability. As digital ecosystems diversify across various platforms and devices, ensuring cross-platform compatibility becomes paramount. Hence, efforts should be directed towards crafting adaptive user interfaces that seamlessly transition across different contexts and form factors. Longitudinal studies are essential for understanding the long-term memorability and sustainability of graphical passwords. By tracking factors influencing password retention and recall rates over extended periods, researchers can glean insights into user behavior and satisfaction trends. Moreover, enhancing accessibility features is crucial for fostering inclusivity within graphical password systems. Collaborating with industry partners to conduct real-world deployment studies can provide invaluable insights into system performance and user acceptance across diverse organizational settings and user demographics. Through these concerted efforts, the future of graphical password systems holds the promise of heightened security, enhanced usability, and broader inclusivity in the digital landscape.

### References :

1. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. "Graphical Password Authentication Using Cued Click Points." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07), pp. 139-148. ACM, 2007.
2. Zeynep Tufekci, and George Danezis. "Social authentication: harder than it looks." In Proceedings of the 2nd USENIX conference on Web Application Development, pp. 1-1. 2011.
3. Sonia Chiasson, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. "A Usability Study and Critique of Two Password Managers." In Proceedings of the 15th International Conference on Human-Computer Interaction (INTERACT '15), pp. 19-36. Springer, 2015.
4. H. T. Li, and Z. L. Zhou. "Research on Application of Improved Graphical Password Scheme Based on Multi-Step Recognition Technology." Journal of Theoretical & Applied Information Technology, 96(19), 6518-6529. 2018.
5. F. Monrose, and A. Rubin. "Authentication via Graphical Passwords: Effects of Tolerance and Image Choice." In Proceedings of the 13th USENIX Security Symposium, pp. 1-1. USENIX Association, 2004.
6. Sonia Chiasson, Elizabeth Stobert, and P.C. van Oorschot. "The Usability of Password Managers: A Security and Privacy Perspective." Proceedings of the 15th International Conference on Human-Computer Interaction (INTERACT '15), Springer, 2015.
7. L. Hong, and S. W. Cho. "Graphical Passwords: A Survey." Smart Computing Review, 3(3), 189-204. 2013.
8. Saeed Samet, and Mohsen Ramezani. "A new graphical password authentication scheme based on matrices." In 2012 International Symposium on Computer Networks and Distributed Systems (CNDIS), pp. 1-5. IEEE, 2012.
9. G. E. Blonder, K. Promislow, and E. Schwartz. "Recognition and Reproduction of Visual Shapes." Memory & Cognition, 2(1), 81-87. 1974.
10. Sonia Chiasson, Elizabeth Stobert, and Robert Biddle. "Graphical passwords: Learning from the first twelve years." ACM Computing Surveys (CSUR), 45(4), 44. 2013.
11. Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys (CSUR), 45(4), 44.
12. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. In Proceedings of the 8th USENIX Security Symposium (Vol. 8, pp. 1-14).
13. Forget, A., & Chiasson, S. (2008). User Choice in Graphical Passwords. In Security and Usability (pp. 55-72). Springer, Berlin, Heidelberg.
14. Thorpe, J., & van Oorschot, P. C. (2008). Human-seeded attacks and exploiting hot fields. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 48-57).
15. Hayashi, E., Hong, J., & Bhamidipati, S. (2008). Empirical studies on the memorability of system-generated graphical passwords. In Symposium on Usable Privacy and Security (SOUPS), July.
16. Thorpe, J., Patrick, A., & van Oorschot, P. C. (2007). Secure, Usable and Deployable Graphical Password Authentication. In Proceedings of the 15th USENIX Security Symposium (pp. 51-66).
17. Tari, F., & Ozok, A. A. (2007). Recognition-based graphical passwords: A comparative study. Interacting with Computers, 19(2), 292-303.
18. Sobrado, L., & Birget, J. C. (2004). Graphical passwords: A survey. Revista de Informática Teórica e Aplicada, 11(2), 63-89.
19. Dhamija, R., & Perrig, A. (2000). Déjà Vu: A User Study Using Images for Authentication. In Proceedings of the 9th conference on USENIX Security Symposium (Vol. 9, pp. 45-45).
20. Dunphy, P., & Yan, J. (2014). Understanding user perceptions of password security and authentication. International Journal of Human-Computer Studies, 72(6), 783-797.