International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Graphical Password Authentication: Strengthening Security in the Digital Age

Adithya Gopalakrishnan
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: agk58565@gmail.com

Anugraha K Anil
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: anugrahakanil55@gmail.com

Anu Thomas
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: anuthomas7781@gmail.com

Devika Vijayan
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: devikav757@gmail.com

Ms. Mafnitha KK
Assistant Professor
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:mafnitha@vjec.ac.in

***Abstract*—Authentication is vital for maintaining system security. Graphical password-based authentication systems provide a promising alternative to traditional authentication methods such as alphanumeric or text-based passwords. Conventional authentication systems are susceptible to brute force attacks, dictionary attacks, password guessing and user memory fatigue. Users create a personalized password by selecting a sequence of images or points in an image grid, which enhances security due to the complexity of graphical choices over traditional textual passwords.**

Graphical Password Based Authentication (GPA) incorporates a combination of image-based cues and persuasive elements which encourages a user to select a secure password. Our system addresses a major security concern, shoulder surfing, by creating and using hybrid images.

***Index Terms*—Password Space, Click-Point Distribution, Guessing Attacks, Recall Study, Shoulder Surfing Attacks, PCCP (Persuasive Cued Click Points), Hotspots, Hybrid Images, Cued Recall, False Accept Points, Deep Residual Networks (DRN), Edge Detection, Hybrid Textual-Graphical Authentication, Brute-force Attacks, Pattern Matching .**

I. Introduction

With an increasing reliance on digital systems, the security of user authentication methods has become a grave concern. Tradition alphanumeric passwords face significant challenges due to its vulnerability towards brute-force attacks, dictionary attacks, password guessing and how easily users forget them. As cyberattacks become more sophisticated the need for much secure systems have grown exponentially. Graphical password authentication systems offer a compelling alternative to traditional text-based methods by utilizing the brain's superior capacity for remembering visual information. These systems aim to address the limitations of tradition systems by replacing alphanumeric strings with images and click points. This paper explores the implementation and challenges of a graphical password-based authentication system. It employs techniques such as click points selection, image grids, persuasive cued click points, hybrid images and multi touch interaction. Additionally we evaluate the disadvantages such as shoulder surfing, dictionary attacks, etc and implement mechanisms that mitigates these threats while ensuring that the system remains user friendly. This study intends to highlight the benefits and drawbacks of this authentication mechanism, thereby helping to develop a more secure, scalable, and user-centric authentication framework for future digital systems.

II. Literature Survey

Sonia Chiasson [1] proposed a project that discusses a graphical password model that emphasizes its theoretical password space. The concepts discussed were about click-point distribution, theoretical password spaces and resistance against guessing attacks. A two-week recall study was conducted to gauge the users' long-term memorability. Usability assessments showed that the participants were able to recall their click-point selections effectively, with an inclination towards the interactive and visual aspects of PCCP when compared to the usual method of typing out passwords. Although the theoretical password space is huge, user behavior might limit the effective password space. Users frequently fail to remember passwords with several click-points after extended periods, especially when pushed to avoid patterns.

Harsh Kumar Sarohi [2] introduced a novel approach involving the use of images as passwords. This study examines current graphical authentication based systems and stratifies them into three categories: recognition, pure-recall and cued recall-based schemes. The Picture Superiority Effect posits that

TABLE I
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[1]	Graphical password model focuses on click-point distribution, theoretical password space and resistance to guessing attacks for improving usability and memorability.	- Users can recall click-points better than text-based passwords. - It resists guessing attacks.	- It may not work well for larger, more complex passwords. - Some might find it hard to use, especially those less familiar with visual systems.
[2]	Emphasizes the memorability and security of graphical authentication systems over text-based passwords, based on the Picture Superiority Effect.	- Image click sequence - hard to guess. - Cued recall - helps user recall next point.	- Registration and login are time consuming. - Difficulty in redrawing precisely.
[3]	Click-Based Graphical Password scheme using Django enhances security over Pass Points by increasing image-based authentication layers to resist guessing attacks.	- Visual cues - memorability. - Image combinations.	- Shoulder Surfing - Requires screen space
[4]	Graphical password model enhances usability and memorability through click-point distribution and resistance for guessing attacks.	- PCCP helps users create secure, memorable passwords. - Persuasive elements forces the users to create better passwords.	- The process could be slow - The complexity may prevent wide adoption.
[5]	Improved Cued-Click Point (CCP) method for graphical passwords, addressing errors with circular tolerance and reducing image requirements. .	- Circular tolerance reduces errors. - Easy recall.	- Limited no: of images. - Image hashing must be done properly.
[6]	Click-draw-based graphical password scheme enhances traditional graphical passwords by integrating multi-touch behaviors to improve user performance.	- Multi-touch features allow users to create more intuitive and engaging graphical passwords. - By allowing users to select multiple points simultaneously, multi-touch can reduce the risk of password patterns.	- Multi-touch gestures make the passwords easier to guess. - Multi touch doesn't support all mobile devices.
[7]	Graphical authentication system uses hybrid images to counter shoulder surfing attacks, that improve security and memorability	- Hybrid images reduce shoulder surfing risks. - Creating a story with selected images aids memorability.	- It remains vulnerable to attackers watching the password. - Some people may find the convergence of images and story method puzzling.
[8]	PassMatrix, a graphical password system uses a dynamic login indicator and scrolling bars to resist shoulder-surfing attacks.	- The horizontal and vertical bars prevent attackers from narrowing down the password space. - Changing login indicators stop attackers from figuring out passwords.	- Users may find it time-consuming compared to traditional passwords or PINs. - The security strength depends on the number of images and grid elements, which can limit the password space.
[9]	VerCube graphical password model combines cryptographic techniques and Visual Cryptography, using TDES encryption, image-based encoding and LSB retrieval to securely authenticate users.	- Increased cryptographic strength using TDES algorithm. - Data is embedded without loosing its visual quality using LSB.	- Issues with image loader unit could cause poor user experience. - Storing and transferring images requires extra bandwidth.
[10]	Recognition-based graphical password scheme with an intuitive GUI enhances usability and security by following ISO standards.	- One step registration and login. - Drag and Drop features.	- Image Quality - Space - Shoulder Surfing
[11]	Improved image-based password system using Persuasive Cued Click Points (PCCP) with vector images to enhance security, memorability and resistance to guessing issues like hot spots.	- Unique pattern points. - PCCP avoids hotspots.	- Incompatible with old devices. - Vulnerability due to image complexity.
[12]	DRN based GPA system enhances security by using edge detection and deep learning.	- Protects against shoulder-surfing attacks using edge detection and deep learning. - Graphical passwords are easier to remember than text-based ones.	- Managing and securing large set of images as system grows. - DRN edge detection may require significant computing power.

human cognition prioritizes image recognize and remember images over textual information, making graphical passwords more memorable. Graphical passwords have gained interest, with even Windows 8 adopting them for authentication. This paper explores various graphical authentication methods, highlighting their ease of recall and greater security compared to text-based passwords. In this paper users may choose images that are easy to guess over time and users may forget graphical passwords if they are not used frequently. This paper may not contain enough real-world examples to demonstrate the effectiveness of the method and may have difficulty selecting and setting up an image.

Dr V Kavitha proposed a new scheme called "Click Based Graphical Password" scheme [3] that focuses on providing an alternative to traditional text-based passwords. The paper goes through four main modules: Register Module, Login Module, Password Reset Module and Secure Account Block Module .In this Django framework is used for web development. System testing is carried out in three steps: Unit testing, Integration testing and Validation testing. The paper concludes that CCP is easier to use than Pass Points. They are preferred over pass point because maximum number of images can reduce the guessing attacks and confuses the hackers. Additionally paper explain the scope for future enhancement - system security can be increased by increasing the number of levels used and the number of tolerance squares used. This paper does not include comprehensive usability testing, nor does it compare with other graphical authentication methods in terms of usability,memorability, or ease of use.

Atish Nayak described a graphical password authentication solution called Persuasive Cued Click Points (PCCP). [4]. Conventionally users choose passwords that are easily memorable and susceptible to attacks, while strong system generated passwords were difficult to recall due to its complexity. The PCCP system aims to strike a balance between both by encouraging users to select a secure password through persuasive elements. This approach tries to mitigate the issue of "hotspots", which are areas of the image that are commonly chosen, making the password much more predictable and vulnerable to dictionary attacks. The images are slightly shaded excluding certain view-ports forcing users to select their click points within this view-port, making it more tedious and time consuming to select a weak password. It also reduces the generation of new hotspots amongst users by distributing click-points randomly. While PCCP minimizes hotspots, it does not completely eradicate them, allowing for sophisticated dictionary or automated attacks. The "shuffle" feature for avoiding hotspots might slow down password formation, irritating users. Karmajit Patra proposed a method for Cued-Click Point on Graphical Password by introducing CCP and Pass Point [5]. The CCP algorithm uses a 2D discretization method to match the click points entered by the user during the login stage to those recorded during the registration stage. Main goal of this research is to address a small error in the current CCP method by introducing circular tolerance and reducing the number of images needed for password creation. The Pass Point method allows users to select a particular number of points within a single image. Both CCP and Pass Point offer similar password space, the memory consumption is far greater in CCP due to the larger number of images required. The system relies on a tolerance value. If the segment identifier for a login click matches the registration click, then the login is successful. However, sometimes the algorithm incorrectly accepts points that should be outside the tolerance range. These are called "false accept points," which can cause authentication errors or false acceptances, potentially affecting security. The implementation of the system was effectively carried out utilizing both NETBIN IDE and ECLIPSE IDE. A range of parameters, including tolerance size, image size, password space, and false acceptance points, were assessed under various conditions. This paper does not provide any method prevent attackers from watching and stealing passwords. Also there is no real-world study on how easy or difficult it is for users. There is no discussion on how secure it is against repeated guessing.

Weizhi Meng [6] proposed a novel approach for click-draw-based graphical passwords (CD-GPs). This plan focuses on one potential way to get beyond the limitations of text-based Authentication via password. The purpose of this approach is to clarify how multi-touch interactions affect users graphical password creation behaviors, specifically with regard to click-draw based graphical passwords. . Through the integration of the input methods like clicking, selecting, and sketching, this CD-GPS was created to enhance conventional graphical passwords. This work's primary goal is to examine how multi-touch actions affect password strength, user performance while creating a password. The improvement of CD-GPS via multi-touch behavior is the main emphasis of this paper. We carried out two significant experiments as part of an in-lab user research to assess the performance of the multi-touch enabled CD-GPS with 90 people in all who agreed to participate in our study. This paper provide the best-case password space, but the actual password space changes with user behavior which reduces the accuracy of the security estimates. In this paper we analyze common attacks like dictionary attacks but we do not simulate real-world attacks, which limits our security evaluation.

Basak Bilgi proposed a graphical authentication system [7] that tackles the issue of shoulder surfing, by implementing hybrid images. This system leverages the human ability to retain images or visual objects better than text. The major drawback of this system was its vulnerability towards shoulder surfing attacks where an attacker could eavesdrop and remember the password selection. The suggested method utilizes hybrid images, which combines the low and high spatial frequencies of two images. This causes the image to appear differently depending on viewing distance, making it harder for the attacker to notice and recall the user's password selection. The registration procedure entails the user selecting six photos from a specified group of photographs and writing a story that matches to the chosen images, which aids in memorability. The paper compares the proposed method to other graphical and text-based authentication methods in terms of security

and usability. The hybrid image-based method is confined to systems that can successfully process visual inputs. It may not perform effectively on platforms with limited bandwidth or image sharpness.

Hung-Min Sun [8] introduced a Pass Matrix which presents a new graphical password system designed to resist advanced shoulder-surfing threats. Shoulder-surfing attacks involve direct observation or recording of password entry in public settings, exposing users credentials to potential attackers. Studies have shown that while alphanumeric passwords provide reasonable security, their reliance on user behavior, such as choosing simple or reused passwords, weakens their effectiveness. To overcome these challenges, several graphical password methods have been developed. These use visual cues, which are easier for people to remember compared to text-based passwords. PassMatrix presents a new graphical password system designed to resist advanced shoulder-surfing attacks. Unlike earlier methods, it uses a dynamic login indicator that allows users to input their passwords without directly clicking on them. This approach effectively balances security and ease of use, as shown through testing on an Android prototype.

PassMatrix is vulnerable to hotspot analysis, which often identifies points chosen by attackers to guess passwords. One of the disadvantage is that users take longer to sign in compared to other methods.The authentication process requires additional work which impacts user experience.

S. Sivagama Sundari proposed [9] a graphical password authentication scheme VerCube model. This model combines a cryptographic approach with a Visual Cryptography scheme. This model encrypts and decrypts the data using TDES algorithm. The model verifies the user through three internal stages: Encryption Stage ,Portion Division, Encoding Stage. It generates a random secret code which is encrypted by using the above algorithm. After encrypting this code each section in this code will be encoded in every image. Using VerCube model user authenticity is verified by implementing certain verifier unit. The model loads and verifies the data availability. The LSB approach is used to extract the encrypted secret code from the pixels. The obtained secret code is decoded and then validated using image pairings. Actual and decrypted data are verified, if similar authentication success otherwise failed. This paper focuses primarily on usability, but does not provide an in-depth analysis of how well the method resists advanced attacks Although improved usability is claimed, no direct comparison with other graphical password authentication methods has been made. One of the disadvantage is that the study does not focus on how effective the method is against different type of attack.

Faranak Rabiei [10] explains a novel recognition based graphical user interface with enhanced usability features. This method is proposed as a way to overcome the weaknesses and vulnerabilities of alphanumeric passwords by evaluating the usefulness of graphical passwords based recognition,taking into account usability factors and considering ISO standards. The two phases of the scheme are authentication and registration. Three primary usability characteristics from ISO standards are explained in the document 9241, 9126, 13407. Here GUI is made for the system's client side, enabling users to communicate with the server, specifically the database administration system.

Pathik Nandi proposed a method for enhancement of password authentication system using vector (graphical) images [11]. This method includes multiple layers of security, making it more resilient to shoulder surfing and other potential attacks. The objective is to facilitate system access for authenticated users while restricting unauthorized entities. Graphical password techniques are generally divided into two types: recognition-based, where users select images they registered earlier, and recall-based, where users must remember their selected images during registration. The brain processes visual stimuli more efficiently than text, enhancing the secure and easier to recall. They are also resistant to attacks like dictionary attacks, key loggers, and social engineering. There are two common methods: color-based and image-based authentication. The article focuses primarily on usability, but does not provide a detailed security analysis against attacks such as brute force, phishing, or replay attacks and also no information is provided about how well the system works for thousands of users. There is no integration with multi-factor authentication. One of the disadvantage is the usability issues that is if a user forgets a color or image-based password sequence, it may be difficult to recover.

Norman Ignatius Dias introduced a model called Deep Residual Network-based Graphical Password, designed to protect against shoulder-surfing threats. In the registration phase, users choose a confidential pass image, after which a challenge set is created utilizing edge detection techniques. This edge detection is facilitated by a classifier based on deep residual networks. Shoulder-surfing attacks occur through two methods: direct observation or using camera devices to record the user's password entry. This model outperforms existing graphical password methods in terms of Information Retention Rate and Password Diversity Score. Graphical passwords tend to be more memorable for users while simultaneously presenting greater challenges for potential attackers to decipher. They categorized into recall, cued-recall, and recognition-based models. Challenge set is used in authentication phase. It consists of pass and decoy images that are generated after applying edge detection. The use of deep learning, particularly DRN for edge detection, significantly enhances the overall security of the system. From this paper we came to know that deep learning can slow down the login process as compared to methods. There is no multi-factor authentication also we cannot make sure that there is no evidence that it works well for many users. One of the disadvantage is deep learning requires powerful hardware and it is more complex.

III. Conclusion

Our research demonstrated that while the integration of image grids, click-point selection and persuasive cues encourages the users to create a more secure password, it also discourages the user from creating an unsafe password by making the task

more tedious. These safeguards serve to reduce threats such as brute force, dictionary attacks, and password guessing. The usage of hybrid images helps to completely mitigate the issue of shoulder surfing. It combines the spatial frequencies of one image with the high spatial frequencies of another image, allowing it to be viewed differently depending on the distance of observation. Despite its promising potential there are several challenges that remain. While the system performs well in terms of security, user engagement and retention there is scope for improvement in areas such as adaptation to different devices or minimization of error rates during login. As cyber security threats evolve, graphical password systems present a viable solution to safeguarding sensitive information, offering both enhanced security and a more intuitive user experience

REFERENCES

[1] S. Chiasson, E. Stobert, A. Forget, R. Biddle and P. C. Van Oorschot, "Persuasive Cued Click-Points: Design, Implementation and Evaluation of a Knowledge-Based Authentication Mechanism," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2 (2012), pp. 222-235.

[2] Sarohi, Harsh Kumar and Farhat Ullah Khan. "Graphical password authentication schemes: current status and key issues." International Journal of Computer Science Issues (IJCSI) 10, no. 2 Part 1 (2013): 437.

[3] Harini, M., Kavitha, Dr. and Hindusthan College of Arts and Science. (2022). GRAPHICAL PASSWORD AUTHENTICATION SYSTEM. In Journal of Emerging Technologies and Innovative Research (Vol. 9, Issue 5)(2014) [Journal-article]. https://www.jetir.org.

[4] Nayak, Atish and Rajesh Bansode. "Analysis of knowledge based authentication system using persuasive cued click points." Procedia Computer Science 79 (2016): 553-560.

[5] Patra, Karmajit, Nemade, Bhushankumar, Mishra, Deb, Satapathy, Prajnya. (2016). Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features. Procedia Computer Science. 79. 561-568.

[6] Weizhi Meng, Wenjuan Li, Lam-For Kwok, Kim-Kwang Raymond Choo, Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones, Computers and Security, Volume 65, 2017, Pages 213-229.

[7] Bilgi, B. and Tugrul, B., 2018, September. A shoulder-surfing resistant graphical authentication method. In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP) (pp. 1-4). IEEE.

[8] H. -M. Sun, S. -T. Chen, J. -H. Yeh and C. -Y. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 2, pp. 180-193, 1 March-April (2018).

[9] Sundari, S. Sivagama and K. Kuppusamy. "Graphical User Authentication Using Hybrid Visual Cryptographic Technique." (2020).

[10] Khodadadi, Touraj, Yashar Javadianasl, Faranak Rabiei, Mojtaba Alizadeh, Mazdak Zamani and Saman Shojae Chaeikar. "A novel graphical password authentication scheme with improved usability." In 2021 4th International symposium on advanced electrical and communication technologies (ISAECT), pp. 01-04. IEEE, 2021.

[11] Nandi, Pathik and Dr Preeti Savant. "Graphical password authentication system." Int J Res Appl Sci Eng Technol 10, no. 4 (2022): 1759-1765.

[12] Dias, Norman Ignatius, Mouleeswaran Singanallur Kumaresan and Reeja Sundaran Rajakumari. "Deep learning based graphical password authentication approach against shoulder-surfing attacks." Multiagent and Grid Systems 19.1 (2023): 99-115.