Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Graphical Authentication System Using Image Panels

[1]Y.Bhavani, [2]B.Kiran Kumar, [3]Swathy Vodithala, [4]V.Rachana, [5]P.Sravani

[1]Department of Information Technology
Kakatiya Institute of Technology and Sciences
Warangal,India
yerram.bh@gmail.com

[2]Deptment of Information Technology
Kakatiya Institute of Technology and Sciences
Warangal,India
kiran_b_kumar@yahoo.com

[3]Deptment of Computer Science and Engineering(N)
Kakatiya Institute of Technology and Sciences
Warangal,India
swathyvodithala@gmail.com

[4]Department of Information Technology
Kakatiya Institute of Technology and Sciences
Warangal,India
vannalarachana@gmail.com

[5]Department of Information Technology
Kakatiya Institute of Technology and Sciences
Warangal,India
sravanipasunuri18@gmail.com

Abstract— The use of alphanumeric usernames and passwords is the most widely used technique for authentication. It is found that this technique has serious drawbacks. For instance, users frequently select passwords that are simple to remember. On the other hand, it may be challenging to recollect a complicated password. The creation of an OTP is another option, but it can take some time and comes with a risk (losing it in the allotted time). These existing methodologies have some disadvantages. A graphical authentication is the best to remember and hard to guess. So, a graphical authentication technique is proposed to address the problems of low security, shoulder surfing, dictionary and brute force attacks. In this methodology, the user must register by providing the required information and by selecting a panel from 3-5 images. This methodology is tested using entropy and proved that this approach is efficient than the existing methods..

Keywords- Authentication; textual password; panels; graphical password; shoulder surfing; dictionary attacks; brute force

I. INTRODUCTION

The world is rapidly turning into digital, and everything is taking place online. Online transactions are just one aspect of daily life; other online activities include communication through email and messaging applications, document storage, and more. Everything moving online has increased the possibility of cybercrimes and privacy violations. Data is kept safe on both online and offline platforms thanks to authentication techniques.

Text passwords are naturally constrained by the amount of alphanumeric characters they may include and the absence of visual clues to aid with remembering password. In the future, because computing power is advancing, offline guess ability attacks will take less time to execute because of the short length of alphanumeric letters. Text passwords are additionally restricted by the human capacity for information memorization. Users typically utilize dictionary terms in their passwords since stronger complicated passwords are difficult to remember. These passwords are simple for dictionary attacks to crack.

Using graphic passwords is the practice of using pictures (or drawings) as passwords. Due to the fact that people remember images better than words, graphical passwords are simpler to remember[9][11][12]. They should also be more resistant to brute-force attacks because of the infinite search space. The two main types of graphical password strategies are recognition-based and recall-based graphical procedures. In recognition-based processes, a user must select one or more of the images they selected during registration in order to prove their identity.

Recall-based strategies rely on the user's memory of a registration-related action. There are several graphical password techniques that have been developed to increase the security of textual passwords. This user authentication method makes passwords visible when input is made, making many graphical password schemes vulnerable to attacks from shoulder surfers. There are different levels of graphic password security and usability; some are more secure while others are simpler to use. It takes a lot of thought and effort to create secure graphical password systems for authentication [13][14][15]. However, easy authentication techniques have security problems[10][16]. Usability and security have criteria that are incompatible, so a trade-off is required. For instance, inorder to speedup authentication, the password's length must be minimal. However, shorter passwords are now more sensitive to brute-force attacks.

The primary objective of our proposed methodology is to provide more security through graphical password. This approach is more effective when compared to the existing methodologies as we are dividing the image into panels. The entropy test is performed to prove the efficiency.

II. LITERATURE SURVEY

Takayuki kawamura et al., [1] introduced Estimated Encodable Distorted Pictures, a graphical authentication system that creates various optical illusions (EYEDi). In this Graphical authentication systems which have the benefit of becoming easier to remember than traditional credentials is proposed. Even though some picture deformation strategies to avoid over-the-shoulder assaults (OSAs) have been presented, these approaches can't stop camera recording attacks because the key images are the same each time. EYEDi produced distorted images by applying numerous image processing filters to the original photos. Furthermore, depending just on authentication and data, EYEDi calculated the necessary image analysis filtering intensity. 20 students used current methodologies plus EYEDi to execute 300 assaults on three main types of assaults (OSA, camera recording attack, and snapshot). Between both the valid user and hackers, EYEDi exhibited a reduced categorization failure rate in all three types of assaults. The most significant threat scenario, the picture assault, entirely bypassed the previous techniques, but attacks were stopped by EYEDi with a 10% classification error rate. Simply because of the difference in authentication times and an improved defensive strategy, EYEDi was able to defeat the image hacker.

Kapil Juneja [2] represented graphical picture using an XML-based structure. As soon as the user loads a password picture with a graphical pattern, based on the stroke length and drift, the server analyses the image and determines whether the pattern is real. By using the multiple transformations, several types of graphical patterns can be created from an input graphical pattern. These actions are used to save the gathered pixel values in an XML pattern database. The input picture was then modified by the server using LSB steganography before being returned to the user as a password image. Each password image that a user submits is obtained, and the password pattern is then mapped to an XML pattern database. There is a desktop and mobile application based on the described paradigm[10]. Comparative performance research shows that the approach out performs other image password feature maps. As a result of the query password pattern image returning extensive results, the password mapping is 100% accurate. The employed qualitative measures also attest to the proposed model's improved dependability and robustness against a variety of circumstances. But this methodology requires complicated calculations.

Alain Forget et.al., [3] have created Persuasive Text Passwords (PTP), a text password generating method. PTP increases security when users select a password during password formation by inserting randomly picked characters into the password at random points. Users can shuffle through a selection of characters that have been picked and placed at random to discover a grouping that strikes them as noteworthy. This approach provided an 83-participant user research assessing four PTP variants in this report. The results show that PTP versions significantly improved user password security. Additionally, authors noticed that people who intentionally chose weaker pre-improvement passwords to make up for the memory load were those who had a lot of unusual characters in their passwords. The rise in password security that PTP was able to attain was capped by this compensatory response

Chang-Chou Lin et.al., [4] suggested to use a new method for distributing encrypted images that is based on a (k,n)-threshold technique and includes authentication and steganography features. First, a secret image is converted into n shares, which are then cloaked in n manually chosen camouflage images. Using parity-bit checking, picture watermarking embeds delicate watermark signals into camouflaged images. A high secure and efficient mechanism for secret image sharing is provided by the entire suggested approach, which is not present in any other secret image sharing techniques.

Christina Katsini et al. [5] invented CogniPGA, a cued-recall graphical authentication method that uses gaze data to apply a cognition-based intervention. This study offers a longitudinal assessment of the proposed scheme's usability, memorability, and security from the viewpoint of cognitive style. The findings support the hypotheses that the creation of user-first authentication systems might be made possible by comprehending and utilizing the users' innate cognitive features where security cannot be compromised for the sake of usability or vice versa. There is proof that when people create graphical passwords, their visual behavior has an impact on the strength of the password. When interpreting the findings of recent investigations, a cognitive style approach showed that users create graphical passwords using multiple visual exploration pathways based on their cognitive style, which weakens the password.

Mohamed Khamis et al., [6] described a technique, which uses graphical filters to blur text passwords, is novel. Attackers find it challenging to decipher distorted passwords because they are unable to mentally undo the distortion. But because people can distinguish visually altered copies of material they have already seen, passwords can still be read by their owners. Using the results of such an internet survey and user study, it used Crystallize, Color-halftone Mosaic filters and Blurring with Plain Text and Asterisks to analyze one- word passwords, random character passwords, and passphrases when entering, editing, and shoulder surfing. A thorough analysis shows that when compared to current methods, these filters significantly increase editing speed, editing accuracy, and observation resistance.

Sonia Chiasson et al., [7] revealed the results of two studies on the usability of visual and click- based passwords. An early lab trial and preceding research both confirmed the usability of these passwords in terms of success rates and password entering times. The field study provided the first in- depth analysis of this form of password in a practical situation. Smaller tolerance squares might be acceptable because customers targeted their click-points more accurately than previously believed, according to the study.

Soon-Nyean et al., [8] suggested a method which offers complete security protection and improves users' digital lifestyles. To prevent unauthorized door entry, it may be connected with NFC-capable cell phones. The innovative design of a secure digital key for an NFC smart phone access control system may lead to aspects of NFC ESGP. It provides additional information to developers of NFC smart phone access control systems that they may use to concentrate on

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

creating systems that use security primitives like steganography, cryptography, and graphical passwords to secure the essential digital key from users. The smart phone NFC ESGP access control system may undoubtedly contribute to a high level of security.

III. Proposed System

User cannot remember numerous passwords from multiple different websites. A graphical password authentication system is provided that requires users to select graphical elements in a specific order rather than creating and maintaining a password in order to give them some degree of freedom. Dictionary attacks and brute force attacks cannot succeed against this type of authentication. Thus, the main aim of proposed system is to develop a graphical authentication scheme with higher security, memorability and usability to address this issue and boost flexibility.

The proposed system develops a graphical password authentication system that is immune to dictionary, brute force, and shoulder surfing attacks. User must first register by providing their information and selecting the number of images, after which the user may select an image from the available twenty images or user can also select the images from device, then the selected images will be split into 16 panels each as shown in fig.4, User have to select and remember one panel from each image.

The user details and images along with panel numbers are stored in the database. While logging in, user have to enter his username and select the images and panel numbers in the same order as in the registration process.

The Proposed method has two steps as shown in Fig.1 :

A. Registration

- While Registering, user is asked to enter details and number of images.
- 5*4 matrix of images will be displayed, user can also select images from their device.
- User clicks on an image and it will be divided into 16 panels (4*4).
- User should select any one panel from each image and he must remember it.

B. Login:

- User should login with his username and password.
- User can see the selected images in random order as in Fig.4.
- User should select the images and panels in correct order.
- If both of them match within three attempts, then user can login successfully.

In this proposed approach, division of image into panels is more advantageous because the more number of panels would increase the efficiency of approach. This approach is secured from the following attacks.

Shoulder surfing: A "shoulder surfing attack" occurs when an attacker manually inspects the device's keyboard and display to acquire personal information. This is one of the few attack methods that need physical proximity to the victim. In contrast to textual passwords, which are clicked on the keyboard, the user can click the panel numbers so quickly that anyone watching the user cannot remember them. Hence, Shoulder surfing attack is prevented.

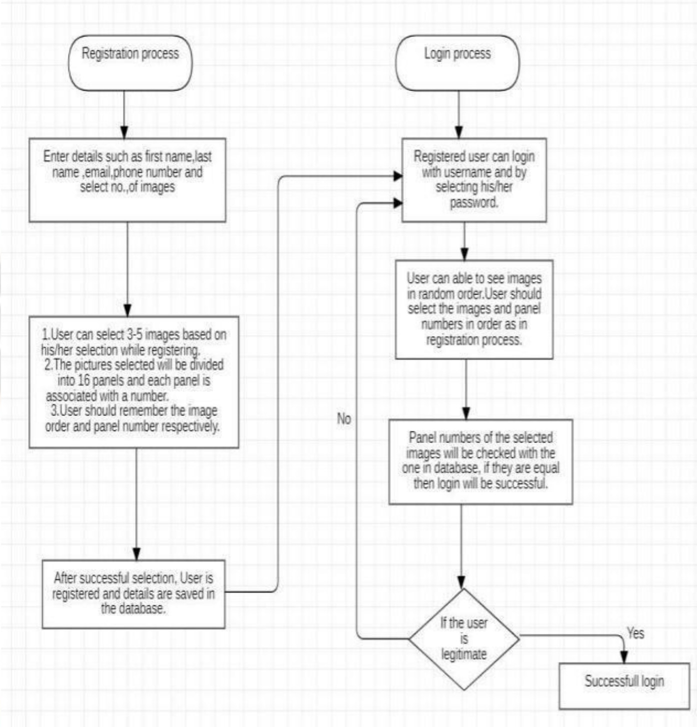

Registration process
Login process
Enter details such as first name,last name ,email,phone number and select no.,of images
1.User can select 3-5 images based on his/her selection while registering.
2.The pictures selected will be divided into 16 panels and each panel is associated with a number.
3.User should remember the image order and panel number respectively.
After successful selection, User is registered and details are saved in the database.
Registered user can login with username and by selecting his/her password.
User can able to see images in random order.User should select the images and panel numbers in order as in registration process.
Panel numbers of the selected images will be checked with the one in database, if they are equal then login will be successful.
No
If the user is legitimate
Yes
Successfull login

Figure 1. Overview

Brute force: A cryptographic technique called a brute force attack, also known as an exhaustive search, makes use of guessing potential password choices until the right one is found. There will be many more permutations and combinations to check since the proposed system has 16 panels for each image and the user must choose 3-5 images, making it impossible to figure out the correct pattern in just three tries.

Dictionary Attack: In order to acquire access to a machine that stores login information, a network, or another IT service, Every word in a dictionary is used as a password in a dictionary attack. An encrypted message or document can also be cracked using a dictionary attack. There is no way for a dictionary attack to succeed and obtain the user's password with this method because it uses graphical images rather than text-based passwords.

IV. Experimentation and Results

Home page contains Registration and Login buttons, user can select either based on his/her status.

A. Registration

- New user should register by providing his/her details like first name, last name, email, phone number, username as shown in fig.2.
- User can select number of images i.e., 3-5.
- User is registered only if they use unique email, username and phone number.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

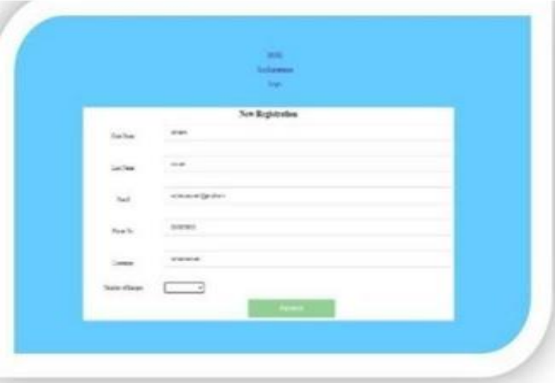


Figure 2. Registration page

- On Clicking password, user can able to see the screen with twenty images as in fig.3 and he/she can also choose images from his/her device.
- User can select 3-5 images based on his/her selection while registering.

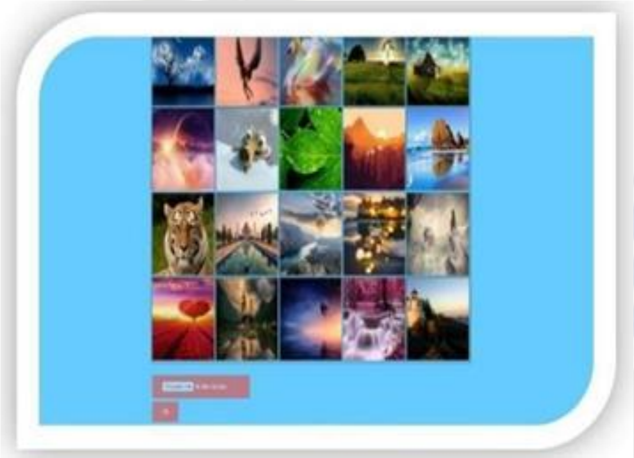


Figure 3. Selecting or uploading images

- The pictures selected will be divided into 16 panels and each panel associated with a number as shown in fig. 4.
- User should remember the image order and panel number respectively.

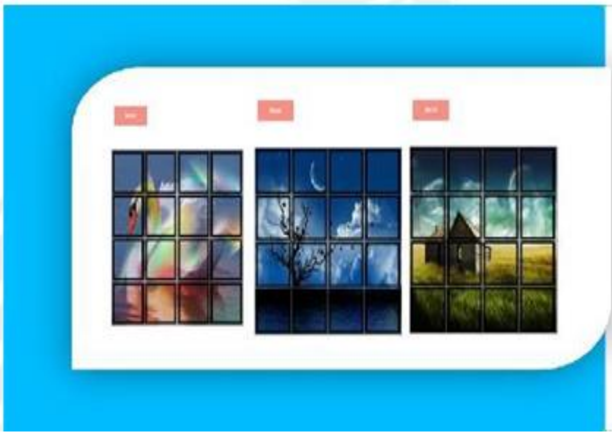
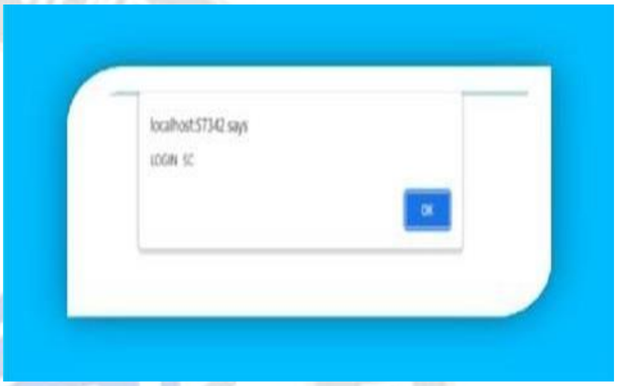


Figure 4. Selecting Panels

B. *Authentication*

- Panel numbers of the selected images will be stored in the database.
- After successful selection, User is registered and details are saved in the database and alert is raised.
- Registered user can login with username and by selecting his/her password.
- User can able to see images in random order
- User should select the images and panel numbers in order as in registration process.
- Panel numbers of the selected images *will* be checked with the one in database, if they are equal then login will be successful and alert is raised as in Fig.5.


localhost:57342 says

LOGIN SC

Figure 5. Login Success alert

V. Analysis of Security for proposed approach

Resistance to Guessing: Our proposed method can provide high resistance to guessing attacks. The user can select the panels within milliseconds of time. so the attacker cannot guess the user's choices.

Entropy and Complexity: The number of possible combinations or patterns in graphical passwords contributes to high entropy and complexity, making brute force attacks more difficult. The formulae for calculating entropy for graphical passwords can be derived using the principles of information theory. Entropy (H) for a discrete system with n choices (e.g., graphical elements) and probabilities p1, p2, ..., pn for each choice is calculated using (1)

$$\mathrm{H} = -\sum_{i=1}^{m} (p_i \, log_2 \, (p_i)) \qquad (1)$$

- H represents the entropy of the system, which measures the average uncertainty or randomness in the graphical password.
- pi represents the probability of choosing the ith choice (graphical element)
- log2(pi) is the logarithm base 2 of the probability of the ith choice

In our proposed method each image is split into 16 panels. From that we select 4 panels for successful login, so (1) can be represented as shown in (2)

$$\mathrm{H}= -(\mathrm{p}_1 \log_2 (\mathrm{p}_1)+\mathrm{p}_2 \log_2 (\mathrm{p}_2)+\ldots+ \mathrm{p}_4 \log_2 (\mathrm{p}_4)) \qquad (2)$$

From the experimentation it is found that the probabilities of selecting the graphical elements are 0.2, 0.15, 0.6, 0.82. So

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

the entropy complexity is more when compared with the existing methods. The greater the entropy, indicates increased security as shown in fig. 6

Shoulder surfing Analysis: In our proposed method the shoulder surfing risk is very low as each image is divided into more panels and viewing the correct panels is impossible.

Pattern analysis: .Analyzing the diversity of patterns to ensure the correct password there are no common or easily guessable choices.

From the above analysis we can say that our proposed method is stronger to the existing methods.

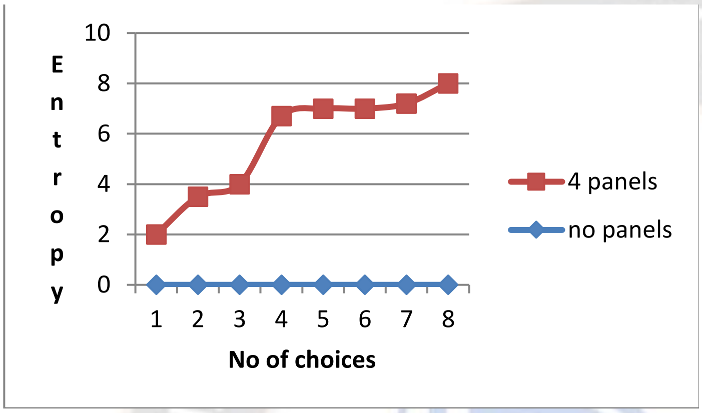


Figure 6. Entrophy calculation for the given number of panels

VI. Conclusion

Text-based password methods have been used for user authentication till now despite security issues. Several graphical password schemes have been developed, although the use of text-based passwords has not totally been superseded. Trivial-to-remember passwords are simple to crack using both textual and graphical password schemes, whereas safe or robust passwords are more challenging to remember. Both of the two distinct categories of authentication methods are open to multiple recording attacks. Since they take longer to log in and require more effort during authentication, graphic password systems that are just moderately secure also have usability difficulties. Over the years, a variety of hybrid password systems have been created to address the problems with graphical and textual authentication. However, these strategies are open to a number of attacks, such as repetitive recording attacks and hybrid tactics that require additional devices for password entry, which limits their usefulness. Our proposed method overcome all the above problems and has best user interface and less memory usage. It uses complex password strategy. So, an attacker who chooses shoulder surfing, brute force and dictionary attacks etc., cannot crack the password.

REFERENCES

[1] Kawamura,Takayuki, et al. "EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to PreventScreenshot Attacks." IEEE Access 10 (2021): 2256-2268.

[2] Juneja, Kapil. "An XML transformed method to improve effectiveness of graphical password authentication." Journal of King Saud University-Computer and Information Sciences 32.1 (2020):11-23.

[3] Forget, Alain, et al. "Improving text passwords through persuasion." Proceedings of the 4thSymposiumon Usable Privacy and Security. 2008.

[4] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography andauthentication." Journal of Systems and software73.3 (2004): 405-414.

[5] Katsini, Christina, Nikolaos Avouris, and Christos Fidas. "CogniPGA: Longitudinal evaluation ofpicturegesture authentication with cognition-based intervention." i-com 18.3 (2019): 237-257.

[6] Khamis, Mohamed, et al. "Passquerade: Improving error correction of text passwords on mobile devices by using graphic filters for password masking." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019.

[7] Chiasson, Sonia, Robert Biddle, and Paul C. Van Oorschot. "A second look at the usability of click- based graphical passwords." Proceedings of the 3rd symposium on Usable privacyand security. 2007.

[8] Cheong, Soon-Nyean, Huo-Chong Ling, and Pei-Lee Teh. "Secure encrypted steganography graphicalpassword scheme for near field communication smartphone access control system." Expert Systems with Applications 41.7 (2014): 3561-3568.

[9] Nizamani, Shah Zaman, et al. "A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability." IEEE Access 9 (2021): 51294-51312.

[10] Chang, Ting-Yi, Cheng-Jung Tsai, and Jyun-Hao Lin. "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices." Journal of Systems and Software 85.5 (2012): 1157-1165.

[11] Sarohi, Harsh Kumar, and Farhat Ullah Khan. "Graphical password authentication schemes: current status and key issues." International Journal of Computer Science Issues (IJCSI) 10.2 Part1 (2013): 437.

[12] Luo, Xiang-Yang, et al. "A review on blind detection for image steganography." Signal Processing 88.9 (2008): 2138- 2157.

[13] Bilgi, Basak, and Bulent Tugrul. "A shoulder-surfing resistant graphical authentication method." 2018International Conference on Artificial Intelligence and Data Processing (IDAP). IEEE, 2018.

[14] Othman, Noor Ashitah Abu, et al. "Directional Based Graphical Authentication Method with ShoulderSurfing Resistant." 2018 IEEE Conference on Systems, Process and Control (ICSPC). IEEE, 2018.

[15] Shen, Sung-Shiou, et al. "Random graphic user password authentication scheme in mobile devices." 2017 International conference on applied system innovation (ICASI). IEEE, 2017.

[16] K. Sharmila Reddy, Dr. V. Janaki, K. Shilpa, 2014, An Alternative Authentication Methodology in Case of Biometric Authentication Failure : AAP Protocol, International Journal Of Engineering Research & Technology (Ijert) Volume 03, Issue 01 (January 2014),