Graphical Password Scheme Based on Color Hint Approach

T. M Emmanuel[1] , S. U Suru[2], B. T Shehu[3]

[1]Sales and Distribution, MTN Nigeria

[2]Department of Computer Science, Kebbi State University of Science and Technology Aleiro.

[3]Department of Computer Science, Federal University Birnin Kebbi.

DOI: https://doi.org/10.51244/IJRSI.2024.1101011

Received: 24 December 2023; Accepted: 03 January 2024; Published: 29 January 2024

ABSTRACT

Generally, textual password is the most used kind of authentication technique. However, this authentication type is vulnerable to a lot of attacks. Users using this kind of authentication techniques are at the risk of exposing vital organizational data or even password to attacks such as phishing, shoulder surfing, brute force and dictionary attacks etc. This is the major reason why a new authentication type is required, in other to minimize these threats or attacks, graphical authentication techniques were developed. But this authentication also faces attacks such as shoulder surfing and guessing attacks etc. In this paper, a graphical password scheme based on color hint approach has been developed and analyzed. The scheme authenticates users in two different ways which are: using an image to select different password click points and using secret color hint and transparent shapes as a way for the user to know the position of the click points after it had been reshuffled on the selected image. The project will be limited to the reliability, efficiency, ease of use and friendliness of graphical user interface during the user authentication. The system has been able to minimize or reduce the problem of shoulder surfing and guessing attacks.

Keywords: Graphical, Password, Authentication, Schemes, Approach, Shoulder Surfing.

INTRODUCTION

There is a general problem faced by organizations and even individuals when it comes to user authentication to secure their computer system [10]. Most text-based passwords that are selected by users are predictable, insecure and the ability of individual to recall them are very slim. In most cases users have to retain password of different accounts for different use, making it difficult for them to recall all the passwords as a result of trying to make it easier to recall, they end up having weak password or similar password for different account which exposes the organization and individual system to attacks from hackers using virus, malware, brute force, dictionary attack, shoulder surfing, key logger attack and spywares [9]. Generally, these are the common authentication issues most of these schemes face, schemes like text based and user account schemes.

It is for this reason that authentication mechanism should be considered that will encourage a user to choose a very strong password that will combat the problem of shoulder surfing, guessing and dictionary attacks [14], which will also be easy to recall and remember. The developed Graphical Password Scheme Based Color Hint Approach makes it quite hard to select an easy or weak password that is guessable by hacker. This system gives the user hints or suggestion on how to create password that can easily be recalled using different techniques but yet strong.

Graphical Password Scheme Based Color Hint Approach brings into play the Idea of reshuffling click points randomly either clockwise or anti clockwise on the selected image this is done at each login the user can be able to remember the position of the through the assistance of the secret color hint chosen during registration which is known only by the user. The developed system allows the user to select a click points from the selected image, in which each click point is associated with a hint color. The number of colors and click points to be used all depends on the user's choice.

The next click point to be selected is done using the least significant bit algorithm which select new random click positions on the selected image. The new click points to be selected depends only on the color hint rather than the order in which they're stored in the database. The system will not show any message saying the click point selected is incorrect. The user can only login if all the selected click points during registration are selected in the order the hint color appears.

GRAPHICAL PASSWORD AUTHENTICATION SCHEMES

Authentication system had been very vital since the inception of information technology for protecting confidential data, information and statistics in all works of life. From time immemorial, textual based pass-wording systems had been the main authentication type that is used to secure data and information [17]. Authentication can be viewed as the act of verifying if a given information is correct by providing some required credential, after which access will be given if the credential is in harmony with what the system has [1].

Authentication generally gives answers to questions such as who is authorized to access this system, does such entity have all the necessary credentials required to access such system? This gives the reason why some organizations prefer some authentication systems over the others which is as a result of the level of security. Authentication can be classified into 3 different types which are knowledge based systems, token based systems and bio metric systems [4].

- **Token based authentication systems:**

This kind of authentication type are generally used in the banks and other commercial or financial institutions. They make use of ATM cards and smart cards. This kind of authentication is widely referred to as "what you have ". A lot of application makes use of this kind of authentication.

- **Bio metric based authentication:**

This kind of authentication systems are referred to as "what you are". These systems make use of finger prints, iris and palm scan for authentication. Even though this set of systems are very secured the major setback is that they are very expensive.

- **Knowledge based authentication systems**

This kind of authentication systems make use of "what you know" type of password that is alphanumeric passwords. They involve the combination of both text based and picture based passwords. Picture based password or graphical passwords makes use of images or sometimes called drawing passwords. Research had proven that humans tends to remember images more easily than text and numbers. Graphical password provides resistance too many attacks, it also gives room for larger password space as compared to text based password.

RELATED WORKS

There are a lot of research work done which is as a result of how interesting this field of research is. A lot of people wants to find a better way to either improve the existing schemes or innovate another way of doing it better. Some of those works in the next few pages are going to be reviewed.

Al-risi & Al-bad proposed a System Child Friendly Authentication System [1] which provides an excellent electronic approach using graphic images to protect children from attackers since the educational system had adopted the use of electronics in studies. The report concentrated on creating a child friendly authentication system by using image-based authentication methods instead of the traditional text-based authentication method we know. The paper further gives a vivid description of the advantages of image-based authentications method over text-based authentication methods.

A paper on image-based password authentication system [17] tries to list the limitations of text based authentication scheme and the vulnerability of text based password authentication schemes. The researcher therefore proposed an image-based password authentication system which was able to overcome most of the challenges faced by the existing systems. Through the use of cryptographic algorithm, the username and key generated is encrypted to prevent attackers from hacking the database. It also makes use of a randomized image clickable grid in which the user clicks on some set of images from the grid after which the username and the generated key are inserted before access is given to the user. But still, this system is vulnerable to brute force attack. It also will be able to prevent most of the chances of shoulder surfing which is secure for any system. It also subdues most of the drawbacks of textual password system. The Shoulder surfing resistant password mechanism is unique. The randomization speed of image grid is good enough which makes the system high performing and shoulder surfing resistant. Moreover, percentage of database hacking is almost low. In case of hacking occur, the information (key number and username) will be safe as these are encrypted and then saved in database. User memorization skill is not a big concern here. User just need to memorize the user name and key number and nothing else. So, all these features altogether provide huge advantage.

Position-Based Multi-Layer graphical user authentication system [7]. The researchers developed a Position-Based Multi-Layer graphical user authentication system purposely to solve the problem of shoulder surfing attacks that most graphical password authentication systems faced, This system was able to achieve that through authenticating user in three different phases therefore making the system highly secured. But more work can be done in other to maintain high level of reliability and security.

A paper on Enhancing The User Authentication Process With Color Memory Cues [18] novel approach that utilizes color as a memory cue to increase password memorability and security is being introduced. A longitudinal study examined in total over 3000 passwords that were created, learnt and recalled (password process) over a period of five- weeks. By adding color to the password process, our results suggest that password memorability and security can be increased simultaneously. Through giving the user the option of choosing the colors (compared with colors being pre selected), encourages users to create more personal and meaningful memory cues when creating their passwords. Additionally, color also provided another security parameter by increasing password entropy. These unique results have practical implications for researchers and practitioners that could positively impact password security, and the financial losses suffered due to password security breaches.

In a review on recognition-based graphical password system [8], twenty-five recognition-based graphical authentication systems were intensively studied with respect to these security threats. Countermeasures were given on how to minimize these threats. Though the work only concentrated on security, but more can be done on usability, reliability and memorability.

A paper on Improving Memorability Using Emojis in a Shoulder Surfing Resistance Authentication Method [2] studies whether graphics such as emojis offer better memorability than numerics when implemented in a shoulder-surfing resistant authentication method. Thus, the proposed method aims to meet both needs of being shoulder-surfing resistant as well as being memorable.

Andriotis discussed on the paper Universal and Dynamic Graphical Password Schemes [3], android pattern unlock (APU) is a great example of a popular and usable graphical password scheme which can be easily compromised, by exploiting common and predominant human behavioristic traits. Despite its vulnerabilities, the scheme's popularity has led researchers to propose adjustments and variations that enhance security but maintain its familiar user interface. Nevertheless, prior work demonstrated that improving security while preserving usability remains frequently a hard task. In this paper a novel graphical password scheme built on the foundations of the well-accepted APU method, which is usable, inclusive, universal, and robust against shoulder surfing and smudge attacks was proposed. The scheme, named Bu-Dash, features a dynamic user interface that mutates every time a user swipes the screen. The pilot studies illustrate that Bu-Dash attracts positive user acceptance rates and maintains acceptable usability levels. Online surveys indicated that the scheme is comprehensive and easy to perceive because respondents ("Survey" Group), did not provide any invalid passwords when asked to create one after reading the basic instructions. By looking at the passwords provided by participants from groups "Pilot" and "Aux" (they actually interacted with Bu-Dash on their devices providing valuable, real world data) we can infer that the scheme provides the opportunity to diversify users' input compared to the APU. We did not find several repeating pass codes, but we recognize that our sample is not extended enough. However, we only saw a few trends in the sample that might be linked with human habits; e.g., the preference in using as a starting point, or the fact that seems to be the least favorite shape to use in general. Additionally, our analysis demonstrated that when participants were asked to form a Bu-Dash pass code on their devices, they chose shorter pass codes aiming probably to make them more memorable and usable. However, early indications show that while they were choosing short pass codes, they also aimed to add complexity to the pass code using at least three shapes.

Similarly, a research was also conducted by [7]. The research work Pass Point Selection of Automatic Graphical Password Authentication Technique Based on Histogram Method the proposed system computes the password points using histogram arithmetic and encrypts the chosen password points using SHA 512. The envisioned system has been realized as an android application and evaluated with existing research considering multiple measurements such as required login time, password space, and entropy. The findings reveal that the new suggested system outperforms the reference work by more than 85% in terms of login latency and more than 72% in terms of entropy results..

Nawadkar[14] discussed on shoulder surfing resistant graphical authentication system mechanism which assure shoulder-surfing resistant authentication to user. It allows user to authenticate by entering password in graphical way at insecure places because user never have to click directly on password icons. Usability testing of this mechanism showed that novice users were able to enter their graphical password accurately and to remember it over time. However, the protection against shoulder-surfing comes at the price of longer time to carry out the authentication.

Furthermore a review was conducted on graphical password system from 1996 to 2019 by [16]. These researchers aim to fill in the gaps left by researchers as of the time of writing by reviewing existing Graphical Password Systems (GPSs), and they also addressed their contributions, limitations, the contexts in which they are used, and the relevant algorithms/techniques. To this end, a systematic literature review was conducted on empirical studies on a number of GPSs published from 1996 to 2019. This review identified a total of 1523 candidate papers. After applying a systematic study process and selection criteria, they selected a total of 56 papers. The main findings of this review in relation to the research questions are as follows: • There has been a great deal of research on GPSs. These schemes can be divided into four categories:

Recognition-based, Recall-based, Cued-recall-base and Hybrid. Among the 56 selected papers, 17 discussed recognition-based authentication schemes, 13 detailed recall-based schemes, 13 discuss cued-recall-based schemes and the remaining 13 papers dealt with hybrid authentication schemes. The analysis of the selected schemes showed that a wide variety of different algorithms/techniques are used by GPSs, like salt algorithm, hashing, encryption, and so on. They observed that, in the 56 selected studies, only 24 schemes used different algorithms. In the recognition-based category, we found that 6 schemes rely on algorithms. In the recall-based GPS category, 7 schemes use different algorithms. Among the 13 schemes in the cued-recall-based GPS category, 7 use either an algorithm or a technology. Finally, in the hybrid GPS category, only 3 schemes use an algorithm. This article also identifies the security threats that the reviewed schemes are resilient against. A number of schemes have been found to have greater resiliency against different attacks, but not a single scheme is completely resistant to all known attacks.

During registration, some intruders or attackers create harmful programmes that waste website resources by creating automated fraudulent enrolments known as bots. It is for this reason [5] worked a paper on ‘Adding A Timer To Captcha-Based Rgb Color Authentication’, the researchers discussed the necessity of web security and they examine current Captcha password schemes and demonstrate the importance of email authentication over cutting-edge Captcha advancements, where Captcha and its color(rgb) email authentication with respect to time can handle a wide range of security challenges. . CAPTCHA is performed by rearranging color code on the catches in an arbitrary order, and it is far from difficult to fool with simple key loggers. Client authentication is a significant challenge in data security across all frameworks. Furthermore, each framework relies on a password for authentication, whether it is a literary or color password. CAPTCHA is a computer-based test that only humans can pass. Computer programmes, on the other hand, cannot pass. The graphic representation of the thought process of incorporating to improve Email authentication is complete.

Pass-numbers graphical authentication password [9] authenticates users in two stage, first the make use of coordinate of a graphical grid cell-based numbers to enter password. The second stage is techniques that involve encrypting password based on the Image pixels. The proposed Pass numbers is considered as a new way to encrypt the password based on the image data that should be sent by the server during the authentication phase. It is depended on numbers which are difficult in guessing. The result of the analysis shows that the Pass numbers is an effective approach since the user interaction is easy and simple because the user only searches on the cell from the grid and clicks on it. Furthermore, the proposed approach can be applied in several applications including desktop systems, smart phones and ATMs. This system is highly resistant to shoulder surfing, and eavesdropping attacks.

A graphical and pin-based hybrid authentication approaches for smart devices [10], a hybrid system was developed which integrated the attribute of both graphical and pin-based technique through the use of simple arithmetic operations such addition and subtraction which is used to generate random password for each login. To summarize the overall comparison of the proposed GRA-PIN authentication system with two alternate approaches, i.e., PIN lock and pattern lock, GRA-PIN performed well. The SUS score of GRA-PIN was considerably high, 94. At the same time, PIN lock had an SUS score of 69.5 and pattern lock of 60. As far as the findings of the T-test are concerned, GRA-PIN had a comparatively better average score of usability compared to pattern-based authentication, t (9.911) = 4.834, p = 0.001. Furthermore, GRA-PIN-based authentication results were also significantly better for usability compared to PIN-based authentication, t (18) = 8.092, p < 0.01. Moreover, all the attacks attempted on GRA-PIN took time and effort with no success ratio at all. This is what made the system to be highly resistant to shoulder surfing, guess attack therefore making this system highly secured and user friendly. The major challenge this system is facing is in trying to maintain a balance between usability and security.

Manzoor and colleagues[11] worked on a research paper titled Multi-Tier Authentication Schemes for Fog

Computing Architecture, Security Perspective and Challenges. The researcher's discussed the different multi-tier authentication schemes and how they were analyzed and evaluated based on three factors, ie, level of security, cost of deployment, and usability, after finding the limitations, improvement were made to make them more secured than single sign on. Evaluation of the authentication techniques reveal that the user preference, heterogeneous infrastructure, usability, and level of security are critical factors to consider in designing future authentication techniques. This work suggest that adaptive authentication techniques can be employed depending on user location and time stamp. But there is an issue in balancing between usability and security.

In Graphical User Authentication System an Overview [12] different techniques of graphical authentication systems such recall based, recognition based were discussed, their pros as well as the cons in terms of memorability, usability and security were also fully discussed. The paper also presented a brief description of graphical password authentication scheme. The three techniques related to graphical user authentication (GUA) namely, recognition based, recall based and hybrid based are discussed. The limitations and advantages of each method such as recall based, recognition based and hybrid based was also presented. The earlier work specifies the characteristics of authentication, memorability and possible attacks in terms of security issue, hybrid technique is more effective than the other two techniques such as recall based and recognition based. Hybrid technique provides protection against attacks such as shoulder surfing, dictionary attacks, etc.

Multi-Level Security System for Home Using Image Based Authentication And Automation Using Iot [13] three level security prototype was created to help reduce the theft incident faced in homes by notifying the admin if anyone comes close to the door of the house this is the first level in the second level notification is sent to the admin if movement are detected close to the door and the last level notifies the admin if the house look is broken. All this are done with the help of magnetic sensor, motion sensors etc. The objective of the Three Level Security System is to supply high security system for the admins and users. The user gets an alert message when the person tries to interrupt the door using vibration sensor, the message is distributed to the admin through the app. The image is distributed to admin or user as a notification. With this concept of level-oping a less complicated, multipurpose, cost- effective design to regulate the on-off mechanism of varied devices within the field via short message service or SMS. The project is more helpful just in case of crisis, things being the absence of the super- visor at the work place so he/she is unable to observe in the flesh for the aim of safety. The images of relatives and friends etc. details where trained in a model and if unknown faces detected in the main gate means the user can get that notification.

A Study on Priming Methods for Graphical Passwords [15] These nudges attempt to prime or non-intrusively bias user password choices (i.e., point selections) by gradually revealing a background image from a particular edge to another edge at password creation time. They researcher's conducted a large-scale user study (?? = 710) to develop further insights into the presence of this effect and to perform the first evaluations of its security impacts. They explore the usability impacts of this effect using the subset (?? = 100) of participants who returned for all three sessions. The usability analyses in this work indicate that these priming techniques do not harm usability. The security analyses reveal that the priming techniques can measurably enhance the security of graphical passwords; however, this effect is dependent on the combination of both the image and priming techniques used.

RESEARCH METHODOLOGY

A research method refers to the systematic approach or procedure used to conduct research, gather data, and answer research questions or investigate a specific topic. It provides a framework for collecting, analyzing, and interpreting data in a structured and reliable manner. The research method used can be categorized as "experimental research" or "user study." Where the program allows users to interact with a graphical interface by clicking on points and observing the visual changes.

In this paper qualitative approach was used. This approach is made up of three data collection methods; which are the interview, observation, and survey. But our sole focus is the survey, reason been that it has an advantage over interview and observation in the area of user convenience and time, it gives the users the opportunity to respond to questionnaires without been supervised or observed it can be either printed or the user can just fill the questionnaire online. The program can be used to collect data on user interactions and behavior, such as the clicked points, the order of clicks, and the colors selected. By analyzing this data, researchers can gain insights into user preferences, behavior patterns, and the effectiveness of the interface design. This research method is often used in usability studies, user experience research, and human-computer interaction studies. In addition to the experimental research, surveys with questionnaires are used to collect qualitative data.

This qualitative approach emphasizes on open-ended questions and allows for detailed narratives and rich descriptions, its analyses data through interpretation and categorizing data into themes, patterns, or codes. It aims to uncover underlying meanings and generate theories. In this research, because of the sample size, 60 participants are used to experiment on 3 systems, and a within user studies is adopted to reduce the biases of the experiment, this is achieved through the use of a Latin square, which is an arrangement of letters or symbols such that each occur n times, in a square array of n 2 compartments so that no letter appears twice in the same row or column.

During this experiment, the 60 participants are allowed to experiment on the systems labeled A, B, and C. These participants experiment on all the 3 systems in the morning hours, afternoons, and evenings after which the result is collated and analyzed using ANOVA in R analysis, ANOVA refers to analysis of variance, in this analysis the variance of the average mean of each system is collated using the login time and registration time as parameters for each system to be analyzed and compared to ascertain if there are any significant difference in the performance based on the compared mean of each system.

RESULTS AND DISCUSSION

To assess the performance of the system, a recognition-based graphical user authentication system and text-based password system was selected as a benchmark for comparison with the newly developed Graphical Password Scheme Based on color Hint Approach. The evaluation focused on the following performance metrics:

1. Security: The ability of the system to ensure the confidentiality and integrity of user data and prevent unauthorized access or impersonation.
2. Reliability: The system’s ability to perform consistently and accurately under different conditions, without unexpected failures or errors.
3. Individual Preference: User satisfaction and preference towards the system, considering factors such as usability, intuitiveness, and overall user experience.
4. User friendliness: The ability of users to complete a given task, such as login and navigating through the system with ease and within a limited time will determine how user friendly the system is. The clarity of the system interface and feed back gotten from each participant ` also determine the measure of how user friendly the system is.
5. Efficiency: they systems ability to measure the time the participant take to complete key tasks such as registration and login as compared with the bench mark system will determine how efficient this system is.
6. Ease of use: they ability of each participant using the system to learn how to navigate through the system and perform key tasks with minimal errors in a short time is a key indicator of how easy to use the system is.

5.1 Experimental Approach:

Three experiments is being carried out here 60 participants are used to experiment on 3 systems these participant are a combination of both MTN staffs and contract staffs who are computer literates, During this experiment, the 60 participants are allowed to experiment on the systems labeled A, B, and C. These participants experiment on all the 3 systems in the morning hours, afternoons, and evenings after which the result is collated and analyzed using ANOVA in R analysis,. During the experiment, participants registered and logged in using all the systems. The registration and login time for each user were recorded. Additionally, participants were asked to provide their comments and feedback on all the systems through questionnaire. The collected data was analyzed using ANOVA to derive meaningful insights and draw conclusions.

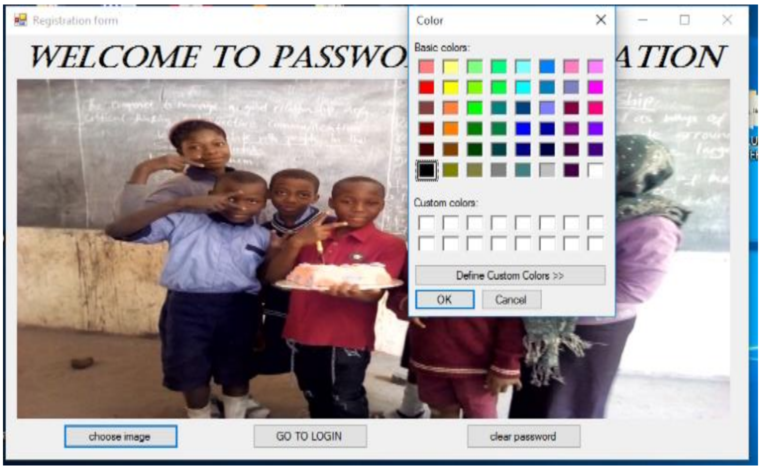

Figure 1: Registration Screen Diagram

Table I: Registration Time Of Users (Gpsucha)

Users	Registration Time	Percentage (%)
19 users	1- 60 seconds	32%
25 users	60-120 seconds	42%
16 users	120-200 seconds	26%

Table II: Calculation of Mean for Registration Time of Users (for GPSUCHA)

Registration Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	19 users	570
60-120 seconds	60 seconds	25 users	1500
120-200 seconds	90 seconds	16 users	1,440
		∑f=60	*∑fx: 3,510*

$$Mean = \frac{\sum fx}{\sum f} = \frac{3510}{60} = 58.2 \text{ seconds}$$

Table III: Registration Time of Users (Text Based Password)

Users	Registration Time	Percentage (%)
12 users	1- 60 seconds	20%

20 users	60-120 seconds	33%
28 users	120-200 seconds	47%

Table IV: Calculation of Mean for Registration Time of Users (Text Based Password)

Registration Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	10 users	300
60-120 seconds	60 seconds	20 users	1200
120-200 seconds	90 seconds	30`users	2700
		$\sum f=60$	$\sum fx$: 4200

$$\mathbf{Mean} = \frac{\sum f x}{\sum f} = \frac{4200}{60} = 70 \text{ seconds}$$

Table V: Registration Time of Users (Picture Login)

Users	Registration Time	Percentage (%)
12 users	1- 60 seconds	24%
21 users	60-120 seconds	42%
27 users	120-200 seconds	54%

Table VI: Calculation of Mean for Registration Time of Users (Picture Login)

Registration Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	15 users	459
60-120 seconds	60 seconds	25 users	1,500
120-200 seconds	90 seconds	20 users	1800
		$\sum f=60$	$\sum fx= 4050$

Mean = ∑fx= 4050/∑f=60 *= 62.5 seconds*

From the mean gotten from table II, the average registration time of users for the (graphical password scheme based on color hint approach) is 58.2 seconds. But, from the mean gotten from table 4.4 and 4.6, the average registration time for (picture login system) and text-based password are 67.5 seconds and 1min 10 seconds. Hence, Graphical password scheme based on color hint approach takes shorter time to register.

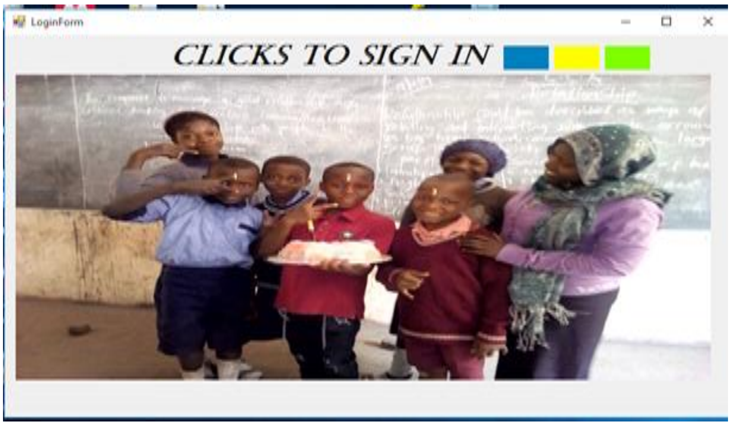

Figure II: Login Screen

Table VII: Login Time of Users (GPSUCHA)

Users	Login Time	Percentage (%)
38users	1- 60 seconds	63%
17 users	60-120 seconds	28%
5 users	120-200 seconds	8%

Table VIII: Calculation of Mean for Login Time of Users GPSUCHA)

Login Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	38 users	1140
60-120 seconds	60 seconds	17 users	1020
120-200 seconds	90 seconds	5 users	300
		∑f=60	*∑fx=2460*

Mean = ∑fx=2460/∑f=60 *= 41 seconds*

Table IX: Login Time of Users

Users	Login Time	Percentage (%)
15 users	1- 60 seconds	25%
20 users	60-120 seconds	33%
25 users	120-200 seconds	42%

Table X: Calculation of Mean for Login Time of Textbased Password

Login Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	15 users	450
60-120 seconds	60 seconds	20 users	1200
120-200 seconds	90 seconds	25 users	2250
		∑f=60	*∑fx=3900*

Mean = ∑fx=3900/ ∑f=60 *= 65 seconds*

Table XI: Login Time of Users Picture Login)

Users	Login Time	Percentage (%)
35 users	1- 60 seconds	70%
19 users	60-120 seconds	38%
6 users	120-200 seconds	12%

Table XII: Calculation of Mean for Login Time of Users (Picture Login)

Login Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	35 users	1050
60-120 seconds	60 seconds	19 users	1140

120-200 seconds	90 seconds	6 users	540
		∑f=60	*∑fx=2730*

Mean = *∑fx=2730/∑f=60* = 45.5 seconds

The result of the mean gotten from table viii, the average login time of users for Graphical password scheme using color hint approach is 41 seconds. But, from the mean gotten from table x, the average registration time for (Text-based password) is 65 seconds. And the average registration time for (picture Login) is 45.5 seconds, with the graphical password scheme based on color hint approach having lesser login time than the other two system, it becomes slightly effective in terms of login time than the others.

Registration and Login Time:

The registration and login times were measured to assess the efficiency and speed of the systems. The following table summarizes the average registration and login times for both systems:

Systems	Average registration time (seconds)	Average login time(seconds)
Picture login	62.5 Seconds	45.5 Seconds
Text=Based password	70 seconds	65 seconds
Minimised graphical password scheme based on color hint approach	58. 2 Seconds	41 Second

ANOVA RESULT AND DISCUSSION

Interpretation:

There is a highly significant main effect of ‘time_spent’, There is a highly significant main effect of ‘num_users’, but the variability is practically zero (Sum Sq = 0)..

The interaction between ‘time_spent’ and ‘num_users’ is highly significant, but again, the variability is practically zero (Sum Sq = 0). The residuals show no unexplained variability in this specific output. The small p-values suggest that the effects are statistically significant, but it’s crucial to assess the practical significance and consider the context of your study**!.**

Based on the above analysis interpretation it had been observed that there is a significant difference in the login time of the 3 system within which GPSBCHA having an age over the other systems , this is achieved through the use of the 2 way anova matrics.

a) System Security

The primary objective of this research work is to minimize the problem of shoulder surfing attack, hence this led to the development and implementation of Graphical password scheme based on color hint approach system. We evaluated the system to see if it Minimizes shoulder surfing attack, this is done by allowing the first group of participants to create there password after which the get to the login phase. In this phase we called some participant from other groups who didn’t know much about the system to come and watch them as the login after the first login process we ask the participant that were observing to try and login using the details they observed but it was un successful, this was repeated for 4 occasion but the observe were not able to successfully login this is a result of the randomization algorithm we used called fisher yate algorithm, these algorithm takes a list of all the element in the shuffled sequence and continually determines the next element in the shuffled sequence by randomly drawing an element from the list until no elements remain. This makes it difficult for the other participant observing to guess the right position of the click points.

b) System Reliability

After giving room to 60 participants to test the two systems, they were asked to make recommendation and individually chose the system that they feel is more reliable 28 individually which is 47% chose to use Graphical password scheme based on color hint approach while 20 participant which is 33.3% chose to use windows login and 12 which represent 20% of the participant chose text based password this show that Graphical password scheme based on color hint approach is more reliable than picture login or text based password system

c) Individual Preference

Furthermore, the 60 participants were asked to choose the system that is best for them between the 3 systems, based on personal preference. The choices they made shows that 57% i.e 34 participant chose MGPS while 23% which represent 14 participant chose picture login frame work and the remaining 20% represent 12 participant sticked with the text based password system.

d) Ease Of Use

When navigating and experimenting the system 32 participant preferred the system to the text based and picture login reason being that it was easy to navigate around and given task where done with minimal errors. Further the system instruction and guidelines where clearly understood by the participant.

e) User Friendly

The graphical interface of the system is user friendly because the instruction given by the system are easily understood and the ease in navigating around the system is also an indication of how user friendly the system is as indicated by the samples during the survey.

CONCLUSION

In conclusion, the review provides a comprehensive overview of graphical authentication schemes using color hints, covering different types, related works, and innovative approaches. It emphasizes the importance of balancing usability and security while addressing the limitations of traditional authentication methods.

This paper focused on the development of a Graphical password scheme based on color hint Approach that authenticate user by clicking on the right position of the reshuffled click point based the color hint displayed, before the user will be granted access into the system or next phase. The implemented system was able to minimize the problem of shoulder surfing attacks.

This research will be beneficial to the society in general and help different sectors and industries to secure their data against intruders. At the end of this research, a Graphical password scheme based on color hint was developed, which reduces the effect of shoulder surfing attack and guarantees the safety of user data. Research can still be carried out in this area especially with the application of artificial intelligence, in other to come up with a more efficient model that will have a higher level of security and reliability. During the ANOVA analysis it been observed that the results f-value was Extremely large, which may indicate that the sample size is influencing the results. It’s essential to interpret the results cautiously and consider the practical significance. To resove this more work can be done by increasing the sample so as to avoid the scenerio where the sample is influencing the account of the analysis.

REFERENCES

1. Al-risi, N. H. M., & Al-badi, F. K. M. (2022). Child Friendly Authentication (CFA). 1(1), 58–86.
2. Amer, M. M. M., Kam, Y. H.-S., & Elkhedrawi, A. H. (2022). Improving memorability using Emojis in a shoulder surfing resistant authentication method. F1000Research, 11, 362. https://doi.org/10.12688/f1000research.73691.1
3. Andriotis, P., Kirby, M., & Takasu, A. (2022). Bu-Dash: A Universal and Dynamic Graphical Password Scheme. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13333 LNCS, 209–227. https://doi.org/10.1007/978-3-031-05563-8_14
4. Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of Graphical Password Authentication Techniques. International Journal of Computer Applications, 116(1), 11–14. https://doi.org/10.5120/20299-2332
5. Bk, A. (2022). ADDING A TIMER TO CAPTCHA-BASED RGB COLOR AUTHENTICATION. 1–11.
6. Edward, A. L., Suru, H. U., & Okudo, J. (2022). Position-Based Multi-Layer Graphical User Authentication System. 11(1), 1–11. https://doi.org/10.11648/j.ajsea.20221101.11
7. F. Abbas, S., & Jawad, L. M. (2023). Pass Point Selection of Automatic Graphical Password Authentication Technique Based on Histogram Method. Iraqi Journal of Information and Communication Technology, 6(1), 28–39. https://doi.org/10.31987/ijict.6.1.212
8. Islam, A., Por, L. Y., Othman, F., & Ku, C. S. (2019). A review on recognition-based graphical password techniques. Lecture Notes in Electrical Engineering, 481, 503–512. https://doi.org/10.1007/978-981-13-2622-6_49
9. Jirjees, S. W., Mahmood, A. M., & Nasser, A. R. (2022). Passnumbers: An Approach of Graphical Password Authentication Based on Grid Selection. International Journal of Safety and Security Engineering, 12(1), 21–29. https://doi.org/10.18280/ijsse.120103
10. Kausar, N., Din, I. U., Khan, M. A., Almogren, A., & Kim, B. S. (2022). GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. Sensors, 22(4), 1–17. https://doi.org/10.3390/s22041349
11. Manzoor, A., Shah, M. A., Khattak, H. A., Din, I. U., & Khan, M. K. (2022). Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. International Journal of Communication Systems, 35(12). https://doi.org/10.1002/dac.4033
12. Maruthi, P. B., & Rani, K. S. (2016). Graphical User Authentication System – An Overview. 1, 44–48.
13. MULTI LEVEL SECURITY SYSTEM FOR HOME USING IMAGE BASED. (2021). 14, 158–163.
14. Nawadkar, P. A. (2022). Shoulder surfing resistant graphical authentication system. 05, 3944–3946.
15. Parish, Z., & Thorpe, J. (n.d.). A Study on Priming Methods for Graphical Passwords (Vol. 1, Issue 1). Association for Computing Machinery.
16. Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020). A Systematic Literature Review of Graphical Password Schemes. Journal of Computing Science and Engineering, 16(4), 163–185. https://doi.org/10.5626/JCSE.2020.14.4.163
17. Sukanya, S., & Saravanan, M. (2017). Image based password authentication system for banks. 2017 International Conference on Information Communication and Embedded Systems, ICICES 2017, 1–5. https://doi.org/10.1109/ICICES.2017.8070764
18. Woods, N., & Silvennoinen, J. (2023). Enhancing the user authentication process with colour memory cues. Behaviour and Information Technology, 42(10), 1548–1567. https://doi.org/10.1080/0144929X.2022.2091474