http://www.casestudiesjournal.com/
Impact Factor: 4.428

Color Hints Method for Graphical Authentications: A Review

Author's Details:
T.M Emmanuel[1], S.U Suru[2,] B.T Shehu[3]
[1] Sales and distribution MTN Nigeria.
Etimothy324@gmail.com
[2]Department of Computer Science, Kebbi State University of Science and Technology Aliero.
surusalihu@yahoo.com
[3]Department of Computer Science, Federal University Birnin Kebbi.
bashartukurshehu@gmail.com

Abstract:
Humans easily memorize and recall images better than text; for this reason, the concept of graphical authentication schemes was introduced as a possible alternative to text-based password systems. Most of these authentication systems widely rely on what the user knows or what they have to generate the password, and recalling the generated password is usually a challenge. In some other authentication systems, what the user is, used to generate their password, but these authentication systems are generally expensive and are affected by the aging factor in humans. Some of this limitation led to further research to develop systems that can be used in generating graphical passwords with hints in relation to this research, such as color hints that can assist the user in recalling the selected clicks or images during password creation. The main objective of this review paper is to study recent works done on graphical authentication schemes using colors or hints to enhance the memorability and usability of the schemes.
Keywords: *Authentication, Schemes, Hint, Graphical.*

1. Introduction

The increase in threats to our computer systems and personal data has led to an increasing demand for securing our systems, thus giving room for the development of various authentication systems, including graphical authentication systems. Graphical passwords are authentication systems that usually work with graphical user interfaces (GUIs) that permit the user to select specific images or click points in a specific order. Graphical passwords are an alternative to alphanumeric passwords, just as authentication schemes using color hints are enhancements to the existing graphical password schemes [21]. The introduction of graphic authentication schemes using color hints helped to increase the password space when selecting images or click points, therefore helping to reduce shoulder surfing attacks.

In an overview of password using color, text, and images techniques, discussion, implementation, and comparison, the use of colors, images, and text was introduced to help reduce the problem of shoulder surfing, though this password was entered in sessions that were not repeated.

Why that picture? [22], research that further explains why people prefer a graphical authentication approach as compared to the usual alphanumeric password system, this study investigates user choices in password selection for recognition-based graphical authentication. The analysis is based on a total of 302 participants continuously using a graphical authentication system during a 6-week-long study. The results show pronounced preference effects for image properties such as color, shape, and category. Additionally, there is a significant difference between genders in the selected images based on the same properties.

Much work had been done on graphical passwords, but in addition to this, authentication systems had been enhanced to aid memorability and usability of this password, either by clicking points on images or by selecting one or two images from a set of images. What makes it easier for users to recall is the use of hints, which are either colors or shapes, which can easily help the user recall the password.

2.GRAPHICAL PASSWORD AUTHENTICATION SCHEMES

Graphical password are categories into 3 which are:

i. Recognition based
ii. Recall based
iii. Hybrid based

i. **RECOGNITION BASED:** this kind of password method involve the selection of image in the order to which they were select during registration. The moment the user is able to recognize these images in the order to which the where selected during registration phase he is granted access into the system. Examples of this system include pass face [12] and Déjà vu [3].

ii. **RECALL BASED**: this type graphical authentication system requires the user to recollect the password base on memory without the aid of clues from the system. The method is further divided into 2 categories that's pure recall that is without any form of hint and cued recall based which make use of some kind of hint. Example of pure recall are grid selection [4], DAS [2] while example of cued recall are blonder [10] and pass point [18].

ii. **Hybrid technique:** this type of system combines the properties of both recall and recognition based in order to bring about usability and applicability example include multifactor authentication system [13].

3. RELATED WORKS

Researchers [8] proposed captcha based graphical password with strong password space and usability [8]. This paper presents a model of the Graphical password scheme under the impact of security and ease of use for user authentication. The researcher integrated the concept of recognition with re-called and cued-recall based schemes to offer superior security compared to existing schemes.

Click Symbols (CS) Alphabet combine into one entity: Alphanumeric (A) and Visual (V) symbols. (CS-AV) is Captcha-based password scheme, the researcher integrated it with recall-based n times n grid points, where a user can draw the shape or pattern by the intersection of the grid points as a way to enter a graphical password. Next scheme, the combination of CS-AV with grid cells allows very large password space (2.4 times 10^4 bits of entropy) and provides reasonable usability results by determining an empirical study of memorable password space. The drawback of this system is that it vulnerable to spoofing attack.

Web based graphical password authentication system [19]. In this paper, another incorporated arrangement of token and video-based confirmation has been proposed in which two-level of authentication is done. In the first phase, the digital image displayed on any token like mobile is used for authentication. In the second phase, frames of some random video are chosen as passwords. The information was tried for 50 clients which are attempting to figure out the password of another client. The chance of guessing the correct video and correct frame is almost negligible. However, there may be a chance that the selected token picture is available at any social networking site so, guessing possibility of picture is becomes 2 out of 50 users. At last, the chance of guessing both correct videos as well as correct token image is zero.

Authentication scheme for password using color and text [11]. Most of the graphical schemes are helpless to shoulder surfing as well as it has higher storage and computational complexity. To address this problem, text can be combined with colors to generate passwords for authentication. The combination of color and text password with efficient matching between the two provides authentication as well as security to the user. Hence using the technique of integration with color and textual password is proposed to generate passwords which are resistant to shoulder surfing.

Increase the remembrance of the password using graphical password with a support of sound signature [9]. In this proposed work a Select based graphical password scheme called Phonemes Select Points (PSP) is presented. In this system a password consists of collection of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. We propose to extend our existing work for supporting sound signature process for higher authentications in integrating security of data for accessing service. Our experimental results show

efficient data security in login process authenticated by the other users.

Shoulder surfing resistant text based graphical password schemes using color [16]. This system consist of two phase the first which is the login phase the user types his or her user ID. Then he or she must choose one image (can be from system or personal). The image will be divided into six images, and the user will be shown the result of the division. After registration, the user will get the sequence of passcolor from number telephone or email. This will help to make the session password. In the second phase the user enters user ID. Furthermore, the user must remember the image part of the image that has been selected. Password consists of 8 characters. The eight characters are divided into two parts, the four characters at the beginning and at the end that have the same color sequence. Four characters consist of three sequence characters passcolor and one character of non-passcolor or detractors color. The detractors color is raised from the position and color of the selected image. For example, the image in position 3rd and the color is red. So, the detractors are in third place by selecting characters on the red grid. The systems use both graphical password and text password. The use of text is to eliminate the problem of shoulder surfing 1]. In addition, it is beneficial to keep the image password. Each login, the part of image will be randomized so that it will be different every login. Login screen is divided into two, there are part of image with abbreviation of colors and QWERTY keyboard characters to make session password. Firstly, part of image is taken from one image that is selected previously. Before dividing it into six parts, the image is changed to grey for the prevention of social engineering by verbal communication. The six parts of images are randomized on every login. The means of R, G, B, and so on are abbreviation of colors like R for Red, G for Green, B for Blue, and so forth. Secondly, QWERTY keyboard characters consist of 26 uppercase, 26 lowercase, 10 digit, and 28 symbol.

Wheel Authentication based on Multi-level Scalable Color-Textual Graphical Password System [5]. In this paper, we have introduced an improved scheme based on alphanumeric text to defense against shoulder surfing. The scheme based on random number generation that provide a better choice for the users. In addition, provision of color scheme strengthens the proposed password scheme. Moreover, placement of all data in multi circular randomized wheel pattern make it more secure, reliable, and usable.

Improving children's authentication practices with respect to graphical authentication mechanism [6]. A variety of authentication mechanisms are used for online applications to protect user's data. Prior literature identifies that adults and children often utilize weak authentication practices and our own initial research corroborates that children often create weak usernames and passwords. One reason children adopt weak authentication practices is due to difficulties in remembering their usernames and passwords. Existing literature suggests that people are better at remembering graphical information than text and words. In this dissertation, my research goal is to improve the usability and security of children's authentication mechanisms. My research includes designing, developing, and evaluating a new graphical user authentication mechanism for children where children choose a sequence of pictures as their password. In our studies, this mechanism, named KidsPic, allowed children (ages 6-11) to create and remember their passwords better than an alphanumeric password. Usability studies identified areas needing further investigation with regards to usability and security. With regards to usability: we investigated whether resolution influences picture selection, the influence of category order on memorability, if the number of objects in a picture influences its selection, and if picture features like dominant colors influences picture selection. With regards to security: we designed and implemented mechanisms to mitigate brute-force and shoulder surfing attacks. For guessing attacks, we conducted a usability study with child dyads. The results and analysis from these additional usability research objectives revealed no influence of picture resolution, order of picture categories, number of objects in each picture, and dominant colors on children choosing pictures for their password. The security research objectives resulted in design enhancements of KidsPic that mitigate brute- force, shoulder surfing, and guessing attacks.

Digital invisible ink writing: imperceptibility & security enhancement technique [14]. The authors refined the meaning of stenography which is the craft and science of apparent communication which is also referred to as the art of digital invisible ink communication. This implies that hiding of information from raising a suspicion can be achieved by concealing secret message behind objects e.g.,

images or pictures to dissuade an intruder's attention from the stego image, during a communication session. As stated by [18], hiding of information is not sufficient, in other to guarantee information confidentiality, integrity and availability, it is very important to conceal the existence of the secret message by using steganography. The objects can be any of the following: image, audio, or video. Steganography is but a termed that is extracted from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" and by combining both words, we now attain what is called "covered writing". However, when we talk about image steganography the information hidden is limited to images. The author is of the opinion that steganography is the digital art of invisible writing ever invented by man. That can be used to conceal the existence of secret message.

Adding a timer to captcha-based rgb color authentication [1]. This paper discusses the necessity of web security and we 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.

Design of authentication system using multimedia for better security [1] this novel authentication system Pass Matrix is based on graphical password to resist shoulder surfing attacks. With a onetime valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hints for attackers to figure out or narrow down the password even they conduct multiple camera based attacks. We also implemented a Pass Matrix prototype on android and carried out real user experiments to evaluate this memorability and usability. From the experimental result the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack [15]. This research presents a security scheme with the help of Graphical Password which uses images. The primary objective of this algorithm is to support the users in selecting better and safe passwords. The user will click on already selected Click point at the time of registration of the image to confirm the authentication. The persuasive cued clicked points will provide a series of images so that security increases as it will give a workload for the intruders. The user will select multiple images along with selecting the at least 3-4 click points on every image. The psychological study reveals that except remembering alpha-numeric characters, a person can easily remembers a visual image. So remembering the points on the images for a user will be easy and will be difficult for an intruder to get access. The persuasive cued clicks help the users to choose more random positions for the increase of security. The major advantage of this Graphical Authentication Algorithm is to provide the easy usability and greater security to the user in authentication process.

Khan in graphical password authentication scheme [7] authentication based password is very common in computer security and privacy. Most of the traditional passwords are numbers, numbers with alphabets and numbers with alphabets and symbols. That can be easily broken by the attacks such as eves dropping, dictionary attacks, social engineering and shoulder surfing attacks. However, human factors such as choosing bad passwords and keeping passwords in an insecure place are also big problems. In order to address these challenges, several graphical authentication schemes have been proposed, but still shoulder surfing attack increasing. This study proposed multiplication matrix for graphical authentication scheme to reduce shoulder surfing attack. The system attained high degree of accuracy to restrict unauthorized users.

Providing security using CAPTCHA: CAPTCHA as a graphical password [17]. Various security primitives uses hard mathematical problems. Use of hard AI problems for security is emerging and exciting new pattern, but has not yet been explored. In our task, we present another security crude dependent on hard AI issues, this framework is named as Captcha as graphical passwords (CaRP). CaRP is Captcha just as graphical secret key plan. CaRP symbolize various security issues together, for

example, web-based speculating assaults, transfer assaults, and shoulder-surfing assaults. By and large, a CaRP secret phrase can be discovered just probabilistically via programmed web based speculating assaults regardless of whether the secret key is in the hunt set CaRP likewise offers well way to deal with address the notable picture hotspot issue in mainstream graphical secret phrase frameworks, as PassPoints, that by and large prompts decisions of feeble secret word.

Cybering private footage video securing towards unpredictable imaging patterns [20]. Securing the video footages of the high authenticated confidential places is very important at present in the market. Authentication is an obligatory factors of technological world concerned with security. Multifactor authentication becomes familiar due to two way authentication process which is proposed by google .In this research we will have the two step verification in the pc itself instead of depending on the external devices. Text based Password and Picturing Location based hotspot. In the existing methodology, an authentication by means of user security input in the form of text is utilized. This can be replaced with confusion picture matrix in which the user will be redirected to some other pictures which results in blocking of the user itself. The successive selection of the exact hot spots in the splitter image will enable the user to move to the next successful images. This hotspot will be another prominent way of authentication.

4. DISCUSSION ON GRAPHICAL AUTHENTICATION SYSTEMS USING HINTS

i. . Graphical Authentication Systems Overview:

The review provides a comprehensive understanding of graphical authentication systems, highlighting their significance in the face of increasing threats to computer systems and personal data. Graphical passwords are presented as an alternative to traditional alphanumeric passwords, leveraging the human ability to memorize images more effectively than text.

ii. Types of Graphical Passwords:

The categorization of graphical passwords into recognition-based, recall-based, and hybrid-based systems is well-explained. Each type has its advantages and limitations, and the hybrid approach seems promising for combining the strengths of recognition and recall.

iii. Color Hint as an Enhancement:

The main focus of the review is on the integration of color hints to improve the memorability and usability of graphical passwords. The rationale behind this enhancement is to aid users in recalling their selected clicks or images during password creation, thereby addressing some of the limitations of traditional graphical password systems.

iv. Recognition vs. Recall vs. Hybrid Techniques:

The review discusses recognition-based, recall-based, and hybrid techniques in graphical password authentication. The inclusion of color hints in these techniques is explored in various works. For instance, the combination of recognition with recall-based schemes is presented as offering superior security.

v. The related work:

This section covers a range of graphical authentication schemes that incorporate color hints, such as Captcha-based schemes, web-based authentication systems, and schemes combining color with text. Each scheme is analyzed in terms of its strengths, weaknesses, and usability.

vi. Usability and Security Considerations:

Several works in the review emphasize the importance of improving both usability and security. For example, the KidsPic mechanism aims to enhance children's authentication practices by leveraging graphical user authentication. Additionally, there's a discussion on mitigating brute-force, shoulder surfing, and guessing attacks.

vii. Innovative Approaches:

The review introduces innovative approaches like the Phonemes Select Points (PSP) system, which combines graphical elements with sound signatures to enhance password recall. The Wheel Authentication based on Multi-level Scalable Color-Textual Graphical Password System proposes an improved scheme based on alphanumeric text to resist shoulder surfing.

viii. Challenges and Limitations:

While the review highlights the advancements and benefits of graphical authentication with color hints, it's essential to acknowledge potential challenges,

such as vulnerability to spoofing attacks, usability concerns, and the need for ongoing research to address emerging threats.

ix. Future Directions:

The review could further discuss potential future directions for graphical authentication schemes, considering emerging technologies, user preferences, and evolving security threats. Exploring the integration of machine learning or biometrics into graphical authentication could be an interesting avenue for future research.

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.

REFERENCE

i. Bk, A. (2022). *ADDING A TIMER TO CAPTCHA-BASED RGB COLOR AUTHENTICATION*. 1–11.

ii. Chalkias, K., Alexiadis, A., & Stephanides, G. (2006). A multi-grid graphical password scheme. *Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, Thessaloniki, Greece*, 1–11. http://www.researchgate.net/publication/27380592_A_Multi-Grid_Graphical_Password_Scheme/file/d912f5108fffc41fde.pdf

iii. Dhamija, R., & Perrig, A. (2000). Déjà Vu: A user study using images for authentication. *Proceedings of the 9th USENIX Security Symposium*, *102590*.

iv. Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). YAGP: Yet Another Graphical Password strategy. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 121–129. https://doi.org/10.1109/ACSAC.2008.19

v. Ilyas, M., & Ahmed, W. (2020). Wheel Authentication based Multi-level Scalable Color-Textual Graphical Password System. *International Conference on Computational Sciences and Technologies, August 2022*, 101–108.

vi. *IMPROVING CHILDREN ' S AUTHENTICATION PRACTICES WITH RESPECT TO GRAPHICAL*. (2022). *August*.

vii. Informatic, S., Science, C., Polytechnic, F., Polytechnic, F., State, O., & Mudasiru, H. (2020). *P r e v e n t i n g s h o u l d e r s u r f i n g a t t a c k i n g r a p h i c a l p a s s w o r d a u t h e n t i c a t i o n s c h e m e. XVIII*.

viii. Khan, A., & Chefranov, A. G. (2020). A Captcha-Based Graphical Password with Strong Password Space and Usability Study. *2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, August*. https://doi.org/10.1109/ICECCE49384.2020.9179265

ix. Kumar, A. (n.d.). *Ncst239 INCREASE THE REMEMBRANCE OF THE PASSWORD USING GRAPHICAL PASSWORD*. *Ijspt M*.

x. Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. *Scientific Research and Essays*, *5*(24), 3865–3875.

xi. O, V. B. (2015). *Authentication Scheme for Passwords using Color and Text*. *3*(3), 316–323.

xii. *Passface authentication system*. (n.d.).

xiii. Suru, H. U., Muslim, A. A., Suru, S. U., & Suru, H. U. (2019). *A Review of Graphical, Hybrid and Multifactor Authentication Systems*. *10*(1), 1447–1475.

xiv. Sylvester, A. (2023). *Digital Invisible Ink Writing : Imperceptibility & Security Enhancement Technique Department of Software Development and Entrepreneurship Digital Invisible Ink Writing : Imperceptibility & Security Enhancement Technique Supervisor*. *January 2022*.

xv. Thosar, D. S., & Verma, D. (2021). *A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack*. *18*(4), 2559–2566.

xvi. Ulya, N. K., Nugroho, L. E., Adhipta, D., Mada, U. G., & Technology, I. (2015). *SHOULDER SURFING RESISTANT TEXT BASED GRAPHICAL PASSWORD SCHEMES USING COLOR*. 109–114.

xvii. Vasudha, V. (2020). Providing security using CAPTCHA: CAPTCHA as a graphical password. *International Journal of Computing and Artificial Intelligence*, *1*(2), 01–04.

https://doi.org/10.33545/27076571.2020.v1.i2a.9

xviii. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). *PassPoints : Design and longitudinal evaluation of a graphical password system*. *63*, 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010

xix. Yadav, B., Singh, K., & Saxena, A. (2022). Video Based Graphical Password Authentication System. *Lecture Notes in Networks and Systems*, *481 LNNS*(7), 78–90. https://doi.org/10.1007/978-981-19-3182-6_7

xx. Yuvalakshmi, K., & Usha, S. (2021). *CYBERING PRIVATE FOOTAGE VIDEO SECURING TOWARDS UNPREDICTABLE IMAGING PATTERNS*. *4*(1), 1–6.

xxi. Khodadadi, T., Javadianasl, Y., Rabiei, F., Alizadeh, M., Zamani, M., & Chaeikar, S. S. (2021). A Novel Graphical Password Authentication Scheme with Improved Usability. *2021 4th International Symposium on Advanced Electrical and Communication Technologies, ISAECT 2021, March 2022*. https://doi.org/10.1109/ISAECT53699.2021.9668599

xxii. Mihajlov, M., Jerman-Blažič, B., & Ciunova Shuleska, A. (2016). Why That Picture? Discovering Password Properties in Recognition-Based Graphical Authentication. *International Journal of Human-Computer Interaction*, *32*(12), 975–988. https://doi.org/10.1080/10447318.2016.1220103

AUTHOR PROFILE

T.M Emmanuel received his B.Sc. and M.Sc. degrees in Computer Science from Usmanu Danfodiyo University Sokoto and Kebbi State University of Science & Technology Aleiro, respectively. He is currently working as a sales representative with MTN Nigeria. His area of research interests includes Human-Computer Interaction, Privacy and Information Security.

S.U Suru is a lecturer in the Department of Computer Science and was the Director of ICT in Kebbi State University of Science and Technology Aleiro from 2014 to early 2018. His area of research interest is Usability and Security of Graphical Authentication Systems.

B.T Shehu received his B.Sc. and M.Sc. degrees in Computer Science from Usmanu Danfodiyo University Sokoto and Kebbi State University of Science & Technology Aleiro, respectively. He is currently working as a lecturer in the department of Computer Science, Federal University Birnin Kebbi. His area of research interests includes Human-Computer Interaction, Privacy and Information Security