Recognition Based Graphical Password Algorithms: A Survey

Jiya Gloria Kaka
School of Information and Communication Technology
Federal University of Technology
Minna, Nigeria
jiyakaka7@gmail.com

Ishaq Oyefolahan O.
School of Information and Communication Technology
Federal University of Technology
Minna, Nigeria
o.ishaq@futminna.edu.ng

Ojeniyi Joseph O.
School of Information and Communication Technology
Federal University of Technology
Minna, Nigeria
ojeniyija@futminna.edu.ng

***Abstract*- User Authentication is an important aspect of information security. Alphanumeric passwords are the most common and widely adopted means of user authentication. Nevertheless, there are several disadvantages attached to the alphanumeric forms of authentication for example, user choose passwords that are easy to guess (dates of births, their names, car plate number) in other to remember them, because difficult passwords are not easily remembered; this brought about the alternative of graphical passwords, research have been carried out to proof that humans find it easier to recall images. This paper reviews 10 recognition based graphical passwords algorithm; common usability and security threats of these systems where analyzed. This paper also suggests future research directions.**

Keywords- Graphical Passwords, recognition based, user interface.

I. INTRODUCTION

Researchers have come up with numerous graphical password algorithms to help users memorize their passwords, passwords should be easy to use and secured, therefore, ten (10) recognition based graphical password algorithms were analyzed in terms of common usability and security threats. Security threats arise with the evolving technology, important document files are stored on devices, most of the devices we use today have applications such as bank applications and private documents that need to be secured [1]. The most widely used authentication method is the text based authentication method, a user registers a username and text password then provides this information upon log in [2]. However users tend to choose passwords that are simple in order to remember them and that makes them easily guessable, they also tend to forget their passwords when strong, most times, they try to write them down thereby jeorpardising the security, or use same password across different platform [3] this brought about the alternative of graphical password to overcome the drawbacks of the tradional text passwords. According to [4] the fact that the human brain processes images easily makes graphical passwords superior to textual passwords. The Graphical password scheme is a form of authentication where users draw/click or select images as their pass images and are asked to redraw or reselect this image upon sign in [1]. Psychology research has been carried out to propose that humans recall pictures/images better than texts [5], similarly, [6], also established the fact that if users authentication tasks are personalized to their cognitive features it will assist the users to be efficient in processing details cognitively as well as task execution performance and in due course improve their experience and acceptance of such tasks [6]. This paper reviews Ten (10) recognition based graphical password algorithms, common usability and security threats were analyzed.

II RELATED WORK

Twenty five (25) recognition based graphical password systems was reviewed by [1], their study is aimed at providing countermeasures and suggestions to mitigate security threats, the security threats addressed in their research includees guessing attack, direct observation attack & frequency of occurrence, a comparison table was presented at the end of their study. Similarly five (5) graphical password authentication techniques was reviewed by [7] in terms of registration and log in time in seconds. Techniques from recognition based, recall based and cued recall based was studied, a general performance analysis was provided. In the same light, [8] discussed the advantages and limitations of graphical password authentication techniques, at the end of their study suggestions were made on enhancement of future graphical authentication scheme. The paper also proposed solutions to prevent shoulder surfing attacks, hidden camera and spyware attack [8]. An attempt to answer the question “are graphical passwords more secured than text passwords” was made by Jaffar and Ahmed in their study which was aimed at evaluating graphical password schemes in terms of attack resistance and usability [9].

However a comprehensive review in terms of usability and security threats involving recognitiion based graphical password is needed. This paper reviewed 10 recognition based graphical password algorithms from 2000 to 2020, a comprehensive survey on usability according to the ISO standard was carried out on the selected algorithm coupled with security threats (shoulder surfing attack, frequency of occurrence and social engineering), a comparison table is presented at the end of the study to guide future research study and researchers interested in coming up with new graphical password techniques.

III METHODOLOGY

This research is conducted by gathering information on present recognition based graphical password schemes. Information was gotten from different sources such as journals, conference proceedings, papers and legitimate websites such as google scholar. The selected recognition based graphical password scheme were evaluated to unveil the strength, weaknesses, usability and security aspect of the scheme. The results from the survey shows the present challenges and strengths of the recognition based graphical password scheme.

IV OVERVIEW OF THE GRAPHICAL PASSWORD AUTHENTICATION CATEGORIES

There are two categories of the graphical password authentication scheme which are both knowledge based authentication, these are:

- Recognition based graphical password scheme
- Recall based graphical password scheme

Recognition based graphical password scheme creates a platform for the user to select pictures from a variety of images provided, during authentication the user is asked to recognize the previously selected images to gain access hence, the name recognition based graphical scheme.

Recall based graphical password scheme gives the users an opportunity to recreate previously created passwords, users are either given hints or reminders (cued recall based) or asked to reproduce the passwords without reminders (pure recall based)

V. REVIEW OF SOME SELECTED RECOGNITION BASED GRAPHICAL PASSWORD SCHEMES

Some selected recognition based graphical passwords are reviewed in this section from 2000 to 2020

A. PassFace Sheme

This scheme was developed in the yeaar 2000 by a commercial company (Real user corporation) in an attempt to replace the traditional passwords with passface based on the argument that the mind can remember human faces easily making passfaces memorable [10], this scheme gives users an opportunity to select three (3) to seven (7) faces as their pass image, during the authentication process the users are given a trial version of authentication to get familiar with the process then requested to select each at a time their registered pass images from groups of nine faces each set of 9 contains random images [11]. This process is evidently time consuming, in a recent performance analysis conducted by [7], they stated that it takes 3 to 5minutes to register images.

Fig. 1. An example of PassFaces

In a research by [12] on user choice in graphical password scheme in 2004 advised against PassFaces stating that users select faces from the same race or most attractive, making the password easily guessable or predictable, they suggested that users should be educated on better password choice or forbid/limit the user choice of passwords.

It is easy for the attacker to attack the scheme using mouse clicks and keypad(keyboard) as it is notable for the attacker to see the pass images being selected by the user, although it has been argued that its difficult to describe faces, passfaces can be considered vulnerable to social engineering attack.

B. Déjà Vu

The Déjà vu scheme is one of the earliest proposed recognition based graphical password scheme, where users create image portfolio from a given set of images, during the authentication process the system presents the images from the user's portfolio and other decoy images, the images used are random art, the user must select correctly the images from her portfolio to gain access, after portfolio creation process users undergo the training process to help memorability. One of the shoulder surfing counter measures taken includes hiding the image selection, and making images unrecognizable to the attacker by altering them. Intersection counter measures were also taken such as making all challenge set the same, the distractor set are also the same throughout the challenge session. It was documented that the creation time for the Déjà vu system is 45seconds while login time after 1week is 36seconds [13]. The strength of the system includes the fact that about 90% of the users had a successful log in, but selecting a set of images to make a portforlio can be time consuming and tiring.

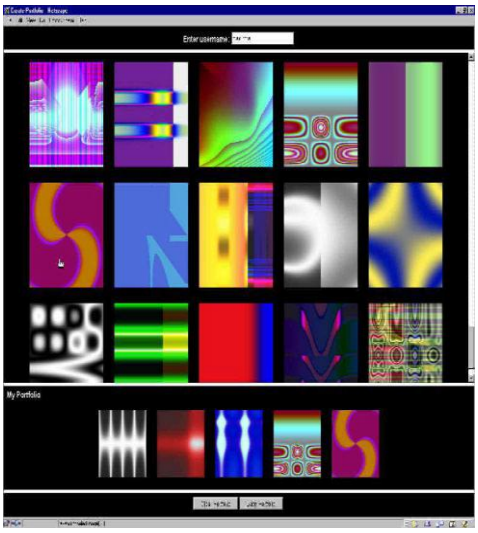

Fig. 2. Random Art used by Dhamija and Perrig.

C. *Triangle scheme and moveable frame*

In 2002 Sobrado and Bridget proposed various graphical password technique to overcome the challenge of the shoulder surfing threat. The user choses a pass image from a set of predefined images, upon login an invisible triangle is formed using the three pass images the user has chosen, the user must click inside the convex hull space, sobrado and bridget suggested the use of 1000 images in the login phase to increase password space, but this will make the display of images crowded and users will find it hard to locate their pass images on time [14]

Fig.3. Triangle Scheme

Also, in 2002 Sobrado and Bridgte proposed the moveable Frame Scheme using the same idea as in triangular scheme, here the user selects three pass objects upon authentication the user moves the frame with the images by dragging the mouse around the frame till the other two pass images lines up. The process is repeated several times to avoid accidental or random log in.

D. *Picture Password*

Jansen et al proposed a recognition based graphical password scheme for handheld devices/mobile devices, the strength of their algorithm includes embedded salting. During the registration phase a user selects a theme (cat,sea etc), then 30 thumbnail images are presented to users for selection in a 5by6 matrix, images can be chosen individually or by pair selection, upon login users selects the images chosen in the correct sequence, each thumbnail image generates a numerical password, the major drawback of this is the numerical password generated is shorter than textual passwords length [15]

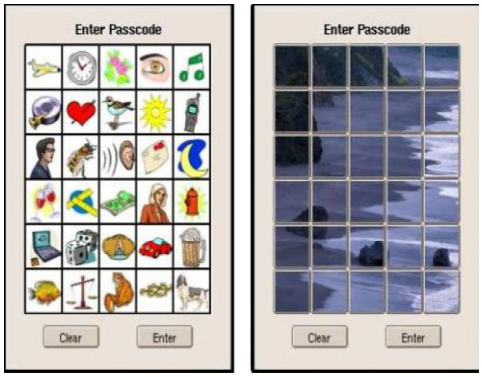

Fig. 4. An Example of the picture password on a PDA Screen

E. *A Secure Recognition based Graphical Password by Watermarking*

In 2011 [16] proposed a watermarking technique in an attempt to solve the challenge of image gallery attack and shoulder surfing. The users are presented with a 5by5 matrix

Fig. 5. Images with associated string

and select 3 images as their pass images the images selected generate a string and are stored in a server [16].

F. Select to Spawn: A novel Recognition based Scheme

In this scheme the users are presented with a set of images, they select an image from the predefined images. The image selected is divivded into 16 (4*4 grid) in a different window. This process is continuous and stops depending on the user. Then the images selected by the user from the different windows form the password. The drawback of this scheme involves prolonged registration and log in time, one of its strength includes a large password space which is about 270 million (approx.). [17]

G. A Hybrid Graphical User Authentication Scheme by Swaleha & Sarosh

This scheme was proposed mainly to build resistance against shoulder surfing attacks. The scheme combines recognition based scheme and dynamic graphics. During registration the user is provided with a 4*4 image grid and ask to select 5 images, the images has a code attached to them, the user enters this codes in order to select the images, upon log in a colored ball is displayed coupled with the image portfolio in login phase 2. The user is expected to remember the color of the ball associated with each image, the log in is in five sessions [18]. The log in process in this scheme is lengthy thereby increasing the log in time, the scheme is also not suitable for those with colour blindness.

H. Shoulder Surfing Resistant Graphical Passsword Technique

This technique was proposed in 2016 [4], it is an improvement on the previously proposed technique by [19] "A new graphical password: combination of recall and recognition based password". A user is presented with 25 images and a question set, he picks 3 questions from the question set and pass images as passwords. Upon login the user enters his username and pass images in the correct sequence, the order of questions will be random and the user clicks on the correct ROA's (Region Of Answers). In an attempt to combat the security challenges of recognition based graphical passwords researchers explored the option of hybrid recognition based systems such as the combination of recall and recognition, adding text to images, background questions as in this case. Although hybrid systems become more complicated and this have an adverse effect on the usability of the recognition based systems.

Fig.6. Step I Registration Phase

Fig. 7. Step II Registration Phase

The registration phase I & II from the images above shows the region of answers by the left and the images to be selected

Fig. 8. Step I Login Phase

appear by the right, the user first creates a profile, selects images and then three question set.

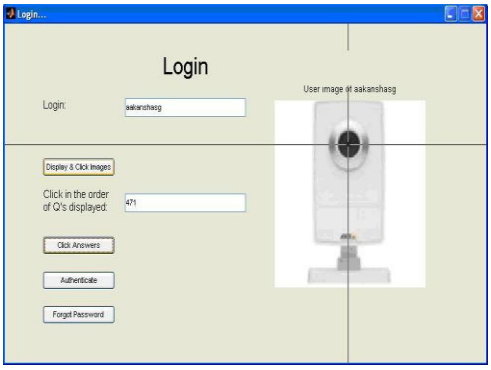

Fig. 9. Step II Login Phase

The login phases I and II provides the user with the 25 set of images and question set, the users are expected to choose accurately the images selected during registration in a sequential manner. To be authenticated the user has to enter a correct username, for step II login the order of questions are randomized.

In the proposed system by Akansha users are to select pass images not less than 6. A session password is then generated based on the pass images. The pass images selected are put in a panel below the grid which disappears after 5 seconds so it can be remembered easily. This is the improvement made to make the previous system more secured. The other additions to their system include email id, mobile number. The system can be considered as secured but not usable as it takes longer to log in.

I. A Novel Hybrid Password Authentication Scheme Based on Text and Image by Mackie and Yildrim

The proposed system is of texts and images combined aimed at reducing phising attack, if a user is deceived to release his text password it will be difficult to release his image password. This scheme is also aimed at reducing the log in and registration time. During registration the user is expected to memorize the key characters provided. The key characters are associated with their images. Upon logging the user can decide to make the images invisible and just enter the key characters. The drawback of this system includes shoulder surfing, its strength includes resistant against brute force attack. [20]

J. Graphical Passwords: Behind the Attainment of Goals

The proposed approach is a combination of recognition based technique, distorted images, an email-id for recovery and visual cryptography. The registration phase has three sessions, the first session secures the details of users, in the second phase user id is transformed into two images through visual cryptography, one image is stored in the database and the order is sent to the user. The login comprises of four sessions. The user submit the image sent, a distorted 5by5 image grid is displayed, the user selects the pass images. [21] . The strength of this approach includes: no image is highlighted when a user selects images, this aimed at preventing shoulder surfing attack. Its major drawback is its lengthy login process.

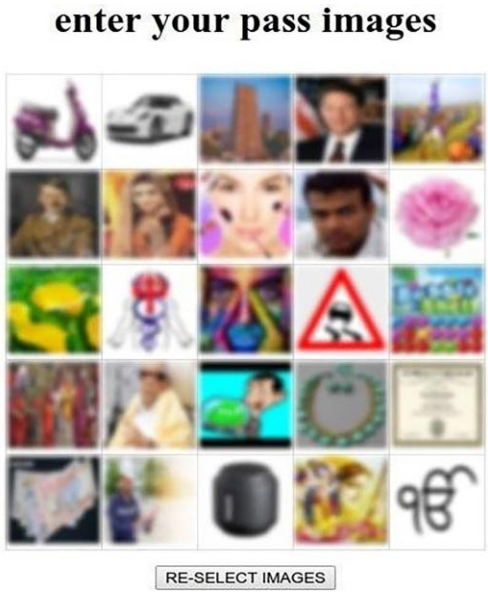

Fig. 10. blurred images presented

VI. *Attacks Common to recognition based graphical Passwords*

This section presents some common attacks and security threats that are common to recognition based graphical passwords.

A. The shoulder surfing attacks

The shoulder surfing attack is also known as the peeping attack, this attack enables an attacker or observer look over the shoulder of an authorized user to gain their password combination, the shoulder surfing attack is one of the major security threat on graphical passwords most especially recognition based graphical passwords. Researchers have tried to come up with approaches to prevent this attack. Randomization algorithms has been one of the best approaches

to prevent this attack, although uniform randomization also leads to frequency of occurrence attack.

B. Frequency of Occurrence Attack

The frequency of occurrence attack(FOA) is most common to recognition based graphical passwords with invariable and consistent randomization algorithm. Graphical password approaches with large amount of decoy is exposed to the FOA, the pass images will have to appear at every login with just a limited number of decoy set in every challenge.

C. Social Engineering

In this type of attack an attacker interacts with an authorized user to gain access to their pass images, this form of attack may be particular difficult for some graphical password approach as it is difficult to describe images, but easy on other graphical password schemes such as recognition based, for example PassFaces that uses facial expressions or a people of a particular race.

VII. Usability

Usability according to the ISO standard(ISO 9241-110) is the usage of a system to achieve a specific purpose through effectiveness, efficiency and satisfaction [22]. Usability features from the ISO is shown in table 1 below

Table 1. usability features from the ISO standards

Usability features	Attributes	Attributes for GUA	Abbreviation
Effectiveness	Reliability & accuracy	Reliability & accuracy	R&A
Efficiency	The utilization in real word	Applicable	Applicable
Satisfaction	Easy to use	Use the mouse easily	Mouse usage
	Easy to create	Select simple way to create the password	Create simply
	Easyto memorize	Meaningful	Meaningful
		Memorability	Memorability
	Easy to execute	Select simple steps of registration & login	Simple steps
	Good view	Select good interface	Nice interface
	Easy to understand	Simple training session	Training simply
	Pleasant	Pleasant picture	Pleasant picture

VIII. Comparison on security and usability of the selected recognition based algorithms

Algorithms	Shoulder surfing attack	Frequency of occurrence attack	Social engineering attack	Usability features								
				Satisfaction							effectiveness	efficiency
				Easy to use	Easy to create	Memorability	Easy to execute	Good interface	Easy to understand	Meaningful pictures	Reliability & Accuracy	Applicability
PassFaces (2000)	×	×	√	√		√		×	√	√	√	√
Déjà vu (2000)	×	×	×	√	×	√	√	×	√	×	√	√
Triangule scheme (2002)	√	×	√	×	×	×	×	×	×	√	√	√
Picture password (2004)	×	×	√	√	×	×	√	√	×	√	√	√
watermarking (2011)	×	×	×	×	√	-	×	√	--	√	×	√
Select to spawn (2012)	×	√	√	√	√	√	√	×	×	-	√	√
Swaleha & Sarosh (2015)	√	√	√	×	×	×	×	×	×	-	√	×
Aakansha et al (2016)	×	×	√	×	×	×	×	√	×	√	√	√
Mackie and Yildrim (2018)	√	√	-	√	×	×	√	√	×	-	√	√
Ankitha, et al. (2020)	×	√	-	×	×	√	×	√	×	×	×	√

X: vulnerable √: not vulnerable - : not researched

VIII. CONCLUSION

In this paper, ten (10) recognition based graphical password algorithms are reviewed including hybrid passwords involving text and images. From the comparison table above shoulder surfing attack remains a challenge for graphical password authentication, although researchers have come up with algorithms to combat this challenge, users find it hard to easily create and understand recognition based graphical password scheme. Another aspect researchers should look into is the tradeoff between the usability and security of graphical passwords and find a balance between them. A naturalistic experimental evaluation on graphical password system was carried out and the results showed a trade-off between usability and security [23].After the survey carried out on the ten recognition based graphical password algorithms the ISO standard for usability was used to make a comparison table for the chosen algorithms, together with a survey on some attacks. Although there is no general security measures for examining the security of recognition based graphical passwords, some researchers such as [24] came up with metrics towards the security of recognition based graphical passwords.

REFERENCE

[1] I. Amanul, P. Lip, O. Fazidah and C. ku, "A review on Recognition Based Graphical Password Techniques," *Computational Science and Technology,* pp. 503-512, 2019.

[2] S. Xiaoyuan, Z. Ying and O. Scott, "Graphical Passwords: A Survey," *IEEE,* 2005.

[3] A. Hussain, P. Maria, D. Paul and F. Steven, "Graphical One-Time Password GOTPass: A usability evaluation," *Information Security Journal: A global Perspective,* pp. 94-108, 2016.

[4] G. Aakansha and W. Vijaya, "The Shoulder Surfing Resistant Graphical PasSword Authentication Technique," in *Procedia Computer Science*, 2016.

[5] S. Lionel, "Learning 10,000 Pictures," *Quarterly Journal of Experimental Psychology,* pp. 207-222, 1973.

[6] B. Marios, C. F. P. G. and G. S. , "The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective," *Computers in Human Behavior,* 2017.

[7] M. Hemamalini, A. Nahomiyal and S. R, "Performance Analysis of Graphical Password Authentication Techniques," *Our Heritage, UCG care listed journal,* vol. 68, no. 4, pp. 271-278, 2020.

[8] P. Shikhar, J. Akarsh, A. Yash and S. Bharti, "Survey on Graphical Password Authentication System," in *Springer*, 2021.

[9] J. Jaffar and Z. Ahmed, "Ev aluation of graphical password schemes in terms of attack resistance and usability," in *IEEE*, 2020.

[10] B. Sacha and S. Angela, "Are PassFacess more usable than Passwords?," *Springer,* 2000.

[11] "About Passfaces," 2005. [Online]. Available: http://www.realuser.com.

[12] E. Hadyn, S. John and D. Graham, "identification of familiar and unfamiliar faces from internal and external features: some implications for theories of face recognition," *ResearchGate,* vol. 8, pp. 431-439, 2004.

[13] D. Rachna and P. Adrian, "Deja Vu: A User Study Using Images for Authentication," in *Prooceedings of the 9th USENIX Security Synposium*, Denver, 2000.

[14] L. Sobrado and J.-C. Bridget, "Graphical passwords," in *The Rutgers Scholar:An Electronic Bulletin of Undergraduate Research*, Camden, 2002.

[15] W. Jasen, "Authenticating mobile device users through image selection," *The Internet Society: Advances in Learning, Commerce and Security,* pp. 184-192, 2004.

[16] L. Arash, M. Azizah and M. Maslin, "A Secure Recognition based Graphical Password by Watermaking," in *11th IEEE International Conference on Computer and Information Technology*, Malaysia, 2011.

[17] U. Mohammad and R. Mohammad, "Select-to-Spawn: A Novel Recognition-based Graphical User Authentication Scheme," *IEEE,* 2012.

[18] S. Swaleha and U. Sarosh, "A Hybrid Graphical User Authentication Sheme," in *2015 international conference on communication, control and intelligent system*, 2015.

[19] H. Asraful and I. Babbar, "A new graphical password:combination of recall and recognition based approach," *World academy of science engineering and technology international*

journal of computer, information, systems and control engineering, 2014.

[20] I. Mackie and M. Yildrim, "A Novel Hybrid Password Authentication Scheme Based on Text and Images," in *IFIP Annual conference on data and application*, 2018.

[21] V. Ankitha, V. Deepthi, P. Vineetha, P. Raveendra, S. Ji Sun and A. Goutham, "Graphical passwords: Behind the attachment of goals," *Security and Privacy,* pp. 1-10, 2020.

[22] ISO, "Ergonomics of human-system interaction-part110: Interaction principles," 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en.

[23] Z. Moustapha and S. Pascal, "Security and Usability: A Naturalistic Experimental Evaluation of a Graphical Authentication System," in *Congress of the international Ergonomics Association*, 2018.

[24] R. English and R. Poet, "Towards a metric for recognition-based graphical password security," in *5th International Conference on Network and System Security*, Milan, 2011.

[25] G. Aakansha and W. Vijaya, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," in *7th International Conference on Communication, Computing and Virtualization*, India, 2016.