A Recommender-Based Graphical Authentication System

Elugbadebo Oladapo Joseph (PhD)
Department of Computer Science, Federal College of Education, Abeokuta
jossydayo72@gmail.com

Akinyele Sunday Akin
Department of Computer Science, Federal College of Education, Abeokuta
akinakinyelefce@gmail.com

Abstract
Graphical Authentication System (GAS), which requires the use of visual images or drawings as passwords, is now being adopted by many designers of information systems. However, most of the existing graphical authentication systems are not quite efficient because they do not consider operational and environmental factors. In addition, GAS is generally faced with the problems of shoulder surfing and visual dictionary attacks. In this study, an improved Recommendation technique for Graphical Authentication System (RGAS), which combines recognition and pure recall-based techniques, will be developed to address these problems. During authentication, Template matching analysis was used for representation and comparison of signs that are presented on a size GxG grid cells by the users. The design was implemented using JAVA scripts and WAMP client-server environment. The evaluation experiment was further conducted in the e-library unit of Federal College of Education, Abeokuta, with two hundred computer systems. The RGAS with other two existing schemes will be incorporated into the College library system and two hundred purposively selected participants were used and monitored for three months. The usability and security of RGAS were compared with A-Free Draw Graphical Password System (AFDGPS) and Hybrid Graphical Password Based System (HGPBS). The considered usability factors during evaluation are Efficiency (E), Learnability (L), Error rate (Er), Memorability (M) and Satisfaction (S). The performance of RGAS were evaluated using Accuracy Rate (ACR), Adaptation Rate (ADR), Success Rate (SR) and Mean Completion Time (MCT). Based on these usability and security evaluations, the result of the comparison of RGAS together with the existing AFDGPS and HGPBS are carried out to determine whether RGAS will yield better usability and security performance and that it will prevent all forms of common authentication attacks which could also be adopted by designers to enhance system security.

Keywords: Graphical password, recognition-based algorithm, cued recall-based algorithm, pure recall-based algorithm, RGAS, AFDGPS, HGPBS.
DOI: 10.7176/JIEA/14-2-01
Publication date: March 31st 2024

I.0 INTRODUCTION

Security plays some vital roles in our daily life and can be characterized as physical security, information security and our national border. In order words, computer system and the information associated to it should be protected. Computer system takes into consideration the human factors such as ease of use, ease to remember etc [32]. Most of the computer system protected with the use of textual password while some other systems are with biometrics [8]. But most commonly used is textual password. The way to provide the security to computer system or our important data is first, give the username and second, give the text password. In some program, user uses the encryption technique for storing password in database for security purpose. The problem in that process is if the user gives the weak password then it is easily identified through different type of attacks like dictionary attack and brute force attack. When the strong password is given that is, more combination of characters, symbols and numbers then the password is strong but hard to remember. This type of password is also useful in web application. The new type of password is graphical password. It is alternative to text password. The idea of graphical password was originally described by Greg Blonder in1996.

Blonder [5] further explained that graphical password is easy to remember as compared with text password because human brain process picture better than the text, they remember faces of people, place they visit and also process things they seen for the long duration [33]. Hence, graphical password provides the means for making more user-friendly passwords and thereby providing better security. However, it is noted also that though, graphical password is stronger than the text password, its disadvantages is the vulnerability to shoulder surfing attack [11, 31]. Shoulder surfing is one of the drawback of Graphical password because some people are standing around the user and many have the opportunity to capture the session and identify the password of the user. This way of observing password allows many people gaining access to the account of user without the user's authority to any person.

Due to recent events of thefts and terrorism, it has become more important for any organization to provide an accurate and reliable means of authentication. Currently the authentication methods can be broadly divided into three main areas [27]:

- Token based authentication (two factors)
- Biometric based authentication (three factors)
- Knowledge based authentication (single factor)

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example, Automated Teller machine (ATM) cards are generally used together with a Personal Identification Number (PIN) [11, 26].

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process though reliable but slow [17, 26].

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [7, 8, 32].

In this work, a new and more secure graphical password system called an improved Recommendation technique for Graphical Authentication System (RGAS) was designed to improve more on vulnerability to attacks such as shoulder surfing and hidden camera that are so paramount to all the existing graphical password because in the past, graphical password' users select the same number of images irrespective of their location and security complexity of application area. To overcome the vulnerabilities of the existing graphical password schemes, RGAS scheme was developed which allows users to select "n" images based on their location and the security complexity of the application area relatively to the recommendation of the Recommender system. The successful selection of "n" images by the users ends the first level check while in the second level check, the users are allowed to draw a sign on canvas comprises of GxG coordinates grid pairs as his/her password with a finger on a free-hand mouse.

1.1 Problem Statement

Computer security has traditionally focused on low-level, technical design and implementation details. Security experts often refer to human as the "weakest link". Sasse et al. [28] in their work on security chain, ascertains that the problem lies not with the security systems themselves, but security protocols. This approach of separating system design from user behaviour is band to fail because it ignores the larger content in which security systems are inevitably used.

The shift towards usable security and including human factors as part of system design is an important one that has a direct impact on the security of the system. Thus, data information security has grown from the use of textual passwords personal identification number (PIN), smart card and lately pictures or images known as graphical authentication system (GAS) [8, 18].

However, this study identifies major problems with the existing system GAS in that it allows for specified numbers of images or pictures to be selected by a user. The implications of these are:

i. The existing GAS system does not give room for security complexity of the application area;
ii. The majority of prior GAS systems give room for shoulder surfing attack;
iii. It is noted also that whenever the security of an authentication system such as GAS becomes more strict, the usability strength becomes lessened;
iv. The existing GAS does not take care of users preferences.

1.2 Motivation

This study is motivated by the quest to bridge the existing gap between Traditional textual password and GAS as stated below Elugbadebo et al. [15]:

i. The authentication system will give room for security complexity of the application area;
ii. The problem of shoulder surfing will be taken care of;
iii. The system will be secured and usable;
iv. The authentication system will provide preferences (choices) for system users.

1.3 Research Objectives

The objectives of this research work are to:

i. identify efficient design choices for implementing graphical passwords;
ii. design an improved draw-a-secret graphical authentication system;
iii. design of a Recommender-Based Graphical Authentication system (RGAS);
iv. implement and evaluate the designs.

2.0 Related work

2.1 Recognition Based Techniques

Dhamja and Perrig [11] proposed a graphical authentication scheme based on Hash visualization techniques. In this scheme, the author's idea is to allow user to select certain number of images from a set of random picture generated by a program. Later, user will be required to identify the pre-select images to determine the authenticity. The weakness of this systems is that the server needs to store the seeds of the portfolio images of each user in plain text [3]. Interface-wise, the process of selecting a picture from picture database can be tedious and time consuming for the user.

Dunphy et al. [14] proposed a recognition-based graphical password scheme, called PASSFACES. In the Passfaces scheme, the user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. This process will be repeated several times out of which user will be allowed to select four (4) images at four different times to login. The major limitation of this scheme is that the user's tendency to log in less frequently than users who had text passwords because the login process took too long (although no login times are reported) A user with sight impairment may be deprived the opportunity of using this scheme.

Davis et, al. [10] suggested a scheme that is similar to Passfaces called Story. In this scheme, user is required to choose four images from a panel that contains everyday objects, places or people upon which a story is constructed. In the authentication phase, the users will be granted an opportunity to select four images panel repeatedly to form their story in correct order as it was done in the registration phase to login. The drawback of this scheme was that users choices were more varied but still displayed exploitable patterns such as differences between male and female choices. Also, users had more difficulty remembering their Story passwords (≈ 85% success rate) and most frequently made ordering errors [10].

Anjum et al. [2] proposed a user authentication by secured graphical password implementation which is a graphical authentication scheme that involves recognition of portfolio images. During installation user creates a portfolio of 4 images or 4 characters or a 4-character word in combination with 2 numbers as password.

Jonathan [20] proposed a graphical password scheme that classify the randomly generated password into three group types- the first group use text-based passwords and the second group was given a static visual palette to enter the randomly assign password while the third group used the entry method that incorporates random synonym images to enter the randomly assigned password.

Shama and Ali [30] proposed an Image Based Password Authentication System using images and a unique key generated for each user. This method is also used to address some of the vulnerabilities associated with traditional password systems.

2.2 Recall Based Techniques

In this section we discuss two types picture password techniques: repeating a selection and reproducing a drawing.

2.2.1 Repeating a sequence of action

Blonder [5] designed a graphical password scheme in which a password is created by allowing the user to click on several locations on a single image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password).

Passlogix [24] has developed a graphical password system based on this idea. In their implementation , users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. A similar technique has been developed by sfr [30]. It was reported that Microsoft had also developed a similar graphical password technique where users are required to click on pre-selected areas of an image in a designated sequence [25,23].

The "PassPoint" system by Wiedenbeck et al. [35,36] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence [21]. This technique is based on the discretization method proposed by Birget et al. [4]. Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck et al. conducted a user study [37], in which one group of participants were asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

2.2.2 Reproduce a Drawing

Jermyn et al. [19] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

Goldberg *et al.* [16] did a user study in which they used a technique called "Passdoodle". This is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. Their study included that users were able to remember complete doodle images as accurately as alphanumeric passwords. The user studies also showed that people are less likely to recall the order in which they drew a DAS password. However, since the user study was done using a paper prototype instead of computer programs, with verifications done by a human rather than computer, the accuracy of this study is still uncertain.

Di *et al.* [12] present a scheme called qualitative Draw-A-Secret (QDAS) which is a pure recall graphical password authentication system similar to DAS in structure but different in the design of stroke encoding and monitoring the sequence of direction change in the stroke length of any drawing made by cell involved during registration and login phases. This model is implemented using dynamic grid transformation so as to conceal the process of creating the password. Although this method could be safer than the original DAS because it prevents shoulder surfing attacks, it has a lot more entropy than the previous DAS.

Dunphy *et al.* [13] proposed an algorithm called Background Draw-A-Secret (BDAS) which allow background images to be added to DAS to encourage users to create more complex passwords. In a comparison of BDAS to DAS, the result revealed that the background image reduced the amount of symmetry within password images and led users to choose longer passwords that were similarly memorable to the weaker DAS passwords. It is not known whether the background images introduced other types of predictable behaviour such as targeting similar areas of the images or image-specific patterns.

Ziran *et al.* [38] generated an idea for a scheme that will produce a map from shape to text with stroke of the shape and a grid with text. In the registration stage, the user is allow to choose a letter from his name and draw the shape on a grid cell, the order of the drawing will be mastered by the system and store in the database. During login phrase, the user has to produce the shape of letter drawn in the registration phase in the same order to determine the authenticity of the user.

Wazir et al. [34] proposed a scheme which allows the user to select the user name and a textual password in a conventional manner and then chooses the objects as password during registration. The minimum length for textual password is L=6. Textual password can be a mixture of digits, lowercase and uppercase letter. After this the system shows objects on the screen of a PDA to select as a graphical password. After choosing the objects, the user draws those objects on a screen with a stylus or a mouse. Objects drawn by the user are stored in the database which will later produce back during Login phase in the same order.

Alice and Fuhua [1] proposed a scheme which allows users to create combinations of the collected sample drawings in the form of a banded signature/picture called a *prediction interval*. If the signature/picture lies inside the prediction interval, the drawing is accepted.

Elugbadebo et al. [15] proposed a scheme which allows users to select the username and textual password followed by the animal type in an encrypted format, after which three images will be selected from a panel of nine images (one at a time) as a recognition-based method and later draw pattern on each of the images for the pure recall-based type.

Lapin and Šiurkus [23] proposed a Balancing Usability and Security of Graphical Passwords which involves the selection of images and drawing of lines which makes the scheme an interesting alternative to traditional textual passwords. This approach can indeed enhance security while maintaining usability

Carrillo-Torres et al. [6] proposed a Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations which is a two-factor authentication mechanism that explore image identification and establishing a self-pre-configured relation between two given images adds an additional layer of security to the authentication process. This approach is used to leverages both something the user knows (the pre-configured relation) and something the user has (the ability to identify specific images)

3.0 Methodology

3.1 Proposed System

The complete architecture of an improved Recommendation technique for Graphical Authentication System (RGAS) is divided into three phases. In phase 1, the user interact with Multi-image based graphical authentication system (MIGAS) sub-sever which is a recognition-based graphical password system that allow users to select and memorize portfolio of images during password creation at registration phase (one image at a time depending on the number specified by the Recommender system) and then must recognize their images from "n" decoys in pre-defined order to login as first level authentication. In phase 2, a pure re-call graphical system named SGAS is incorporated into the system as second level authentication. This SGAS allows the user to draw a simple sign with finger on a free-hand mouse on the screen. The user is able to identify square grid of size GXG coordinate pairs of grid cells containing several numbers of pixels. The sign is drawn on the pixels of grid cells as password. The total and dimension of location of pixels are of great importance during registration and login phase. In phase 3, the two sub-severs are managed by a chief controller and coordinator system which serves as additional backup and broking system. The controller engine sever is also a server that mediate between the two components of RGAS in an effort to provide a robust authentication graphical environment. The controller provides the following:

i. Ability to reconfigure and update between components of the system without a restart.
ii. Transparent broking services for data transfer between components.
iii. Tight system security with advanced user, resource, data and memory protection.
iv. Provides backup services.

Complete architecture of RGAS is shown in Figure 1.

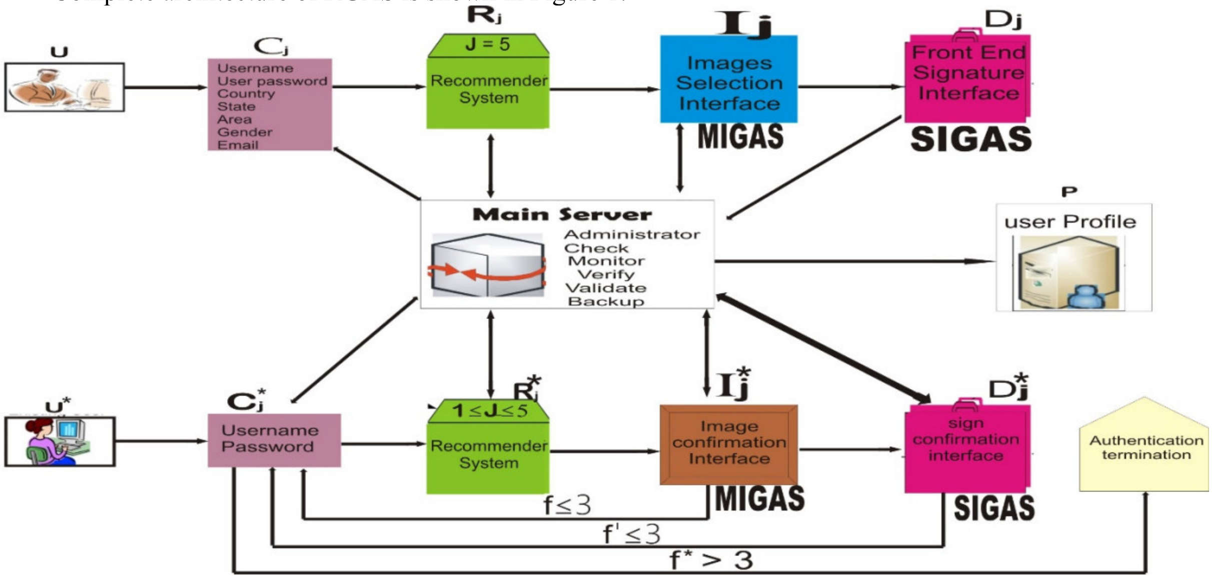

Figure 1: Architecture of an improved Recommendation technique for Graphical Authentication System (RGAS)

In Figure 1 above, three authentication phases were explored viz, registration phase, login phase, and the authentication phase. The registration phase of the architecture is as follows. For every new user **U** that does not belong to server M, register user's credentials C_j and send it to the Recommender system R. There exists user's image I such that J = 5. Then transfer user's details to front end signature interface D where the user will draw a sign and save them in the main server for future use. During the login phase, the existing user U^* enter his/her credentials C_j^* and then send it to the recommender system R^*. Then, there exist user's image I^* on the image confirmation interface such that I≤J≤5. The user's details are then transferred to the sign confirmation interface D^* where the user's drawing of a sign is made. During the Authentication process, the user's original password U_O is compared with user's current password U_c^* to determine the authenticity of a user. For every user's image selection failure (f ≤ 3), go back to U_j^* to re-enter username and password, likewise for user's sign drawn failure ($f^{|} \leq 3)$, follow through the same process for a maximum number of three (3) attempts. If the user's failure rate for both image selected and a sign drawn is greater than three ($f^* > 3)$, terminate user's authentication process until after twenty-four hours (24Hrs). This authentication process can best be explained by verification and validation processes as follows.

3.2 An improved Recommendation technique for Graphical Authentication System (RGAS) Model

The recommender based graphical authentication system model for the existing users and new users is as follow:

For each j $\ni$ i ≤ j ≤ n
Set

$$R = \sum_{j=1}^{n} \left(\sum_{i=1}^{7} Cji + \sum_{i=1}^{5} I_{ji} + D_j\right) \quad (12)$$

$$R^* = \sum_{j=1}^{n}\left(\sum_{i=1}^{2} Cji + \sum_{i=1}^{5} I_{ji} + D_j\right) \quad (13)$$

Where i = $\begin{cases} 1 & \textit{if image i is recommended} \\ 0 & \textit{if image i is not recommended} \end{cases}$

For each I_{ji} *selected*

3.3 Criteria for implementing an improved Recommendation filtering technique for Graphical Authentication System algorithm

Authentication system is a way through which an authenticity of a user is determined. This is established by generating template for each user's authentication system. The purpose of this template is to create a model of what is normal behaviour for a particular user. The distance of this template against data from an authentication attempt is then calculated using a selected Coordinate pairs distance metric. To be able to decide if this authentication attempt is genuine or an impostor attempt, the threshold and percentage accuracy criteria are considered.

3.4 Method of data collection

A total of two hundred (200) respondents will be randomly selected from five (5) schools viz: schools of Arts and social sciences, Education, Languages, Sciences and Vocational Education. Forty respondents will be selected from each school comprising of both male and female for gender balance.

In this study, each of the respondents will be engaged for three (3) sessions in a week to allow for an assessment of each scheme in a week and this will be done for a period of six (6) weeks. A twenty five (25) item questionnaire in-built in the scheme will be addressed by the users at the end of each session for each of the scheme at a time for the period of six weeks.

The questionnaire items addressed five usability components viz: efficiency, learnability, errors, memorability and satisfaction. The items were given face validity by expert. A five (5) likert scale option was used to obtain data from the respondents, measuring strongly agree, agree, not sure, disagree and strongly disagree responses.

For the security comparative analysis of the schemes, the two hundred (200) users will be grouped into five (5) to make use of the forty systems in the computer laboratory of Federal College of Education, Abeokuta will be used. Using the Close-Circuit Television (CCTV) camera, placed at strategic places of the Computer laboratory, the login process of the users will be monitored in the television placed in the server room. The monitor (human) in the server room will be used to hack the login details of the users without the prior knowledge of the users.

In another form, Five (5) attackers (human) will also be positioned strategically in the Computer Laboratory hall where the users are to login their details, the purpose of the attackers is to lunch shoulder surfing attack and get the login details of the users' systems without their prior knowledge.

The result of the total number of the systems hacked into by both the CCTV attackers in the server room and that of the shoulder surfers in the computer laboratory hall will be presented and compared in order to determine whether the new scheme will prevent all forms of common authentication attacks. .

4.0 Usability Evaluation Results of RGAS, AFDGPS and HGPBS

The usability evaluation results of RGAS, AFDGPS and HGPBS showed that majority of the users found the design systems very good in the area of efficiency, learnability, error prone, memorability and satisfaction. The chart for each component is shown in Figure 2 to Figure 6 as follows:

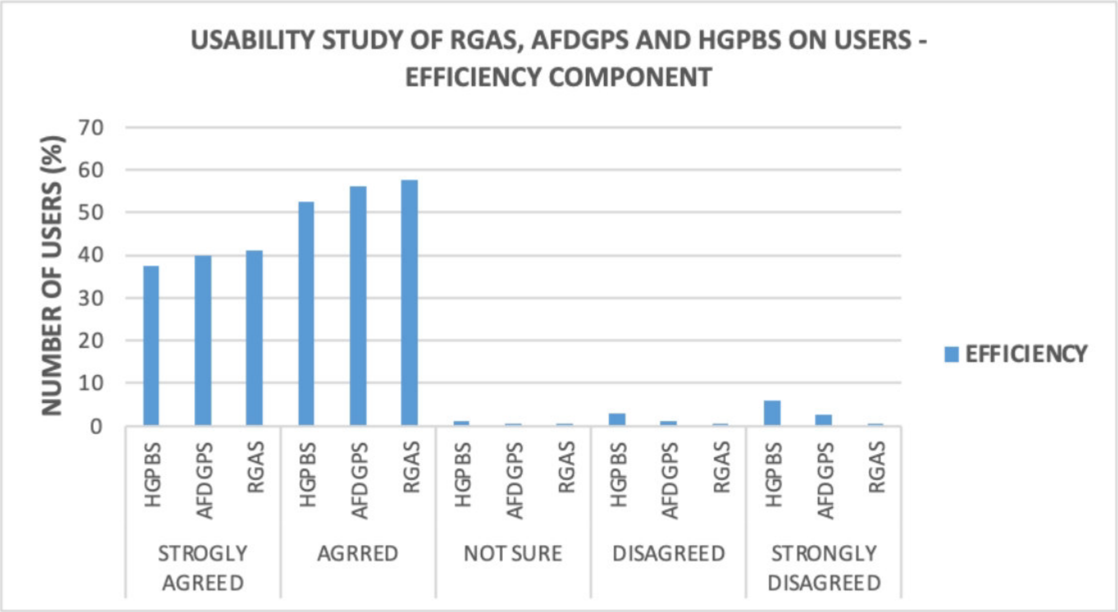

Figure 2: User's Responses on RGAS, AFDGPS and HGPBS Efficiency

Testing the efficiency of the three schemes in Figure 50, 197 (98.5%), 192 (96%) and 180 (90%) of the participants agreed on the efficiency of the RGAS, AFDGPS and HGPBS respectively. The result shows that though all schemes are efficient but RGAS is more efficient.

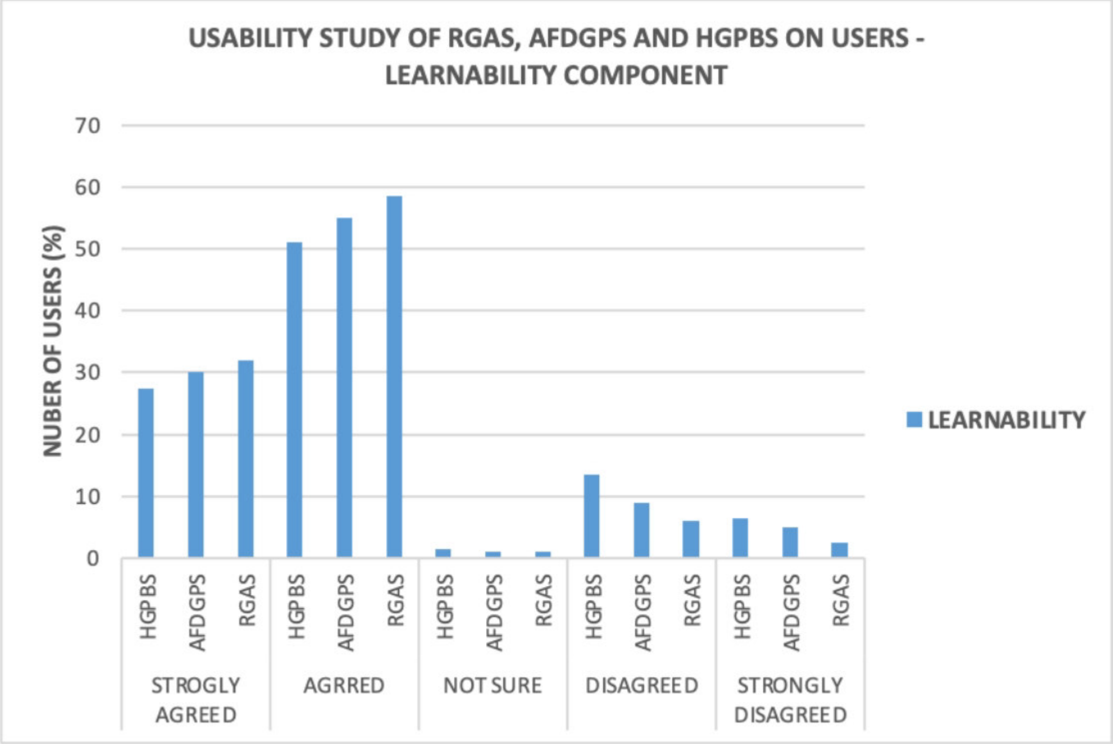

Figure 3: User's Responses on RGAS, AFDGPS and HGPBS Learnability

The result in Figure 3 shows that 181 (90.5%) of the users agreed that the RGAS is easier to learn than AFDGPS (85%) and HGPBS (78.5%). The study also shows that HGPBS is the most difficult to learn among the three schemes with (20%) users not agreeing to its learnability.

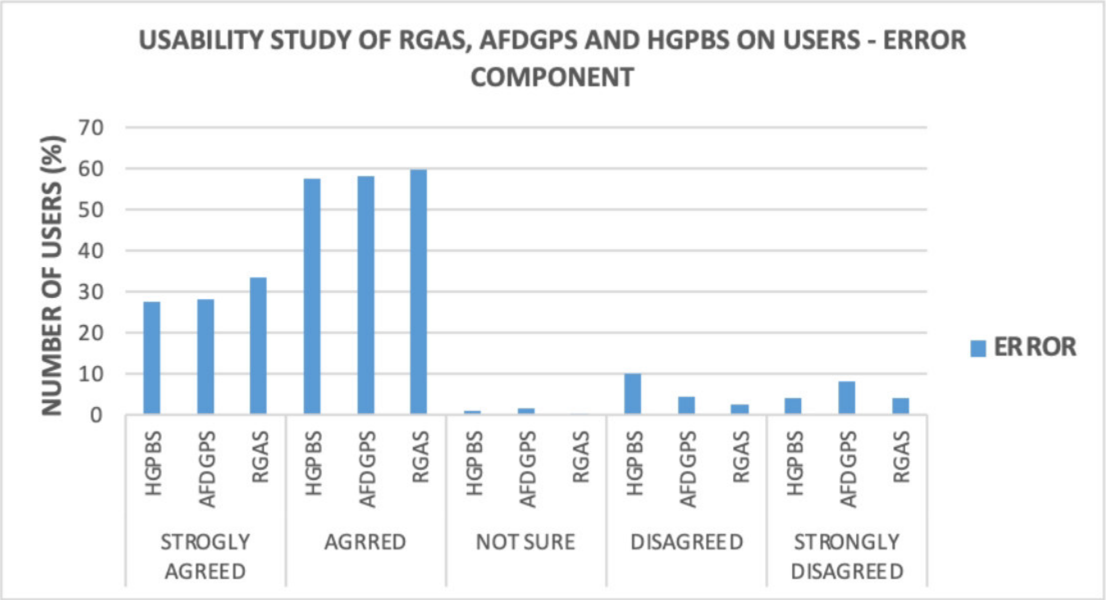

Figure 4: User's Responses on RGAS, AFDGPS and HGPBS Error

The result in Figure 4 revealed that on the accuracy of the three schemes, the error –free component was tested with questionnaire items such as, accuracy, entry of password and easy login. The result shows that RGAS is the most error-free with 186 (93%) of the users agreeing to its error-free status. The other two existing schemes was tested for AFDGPS 172 (86%) and HGPBS 170 (85%) error-free results.

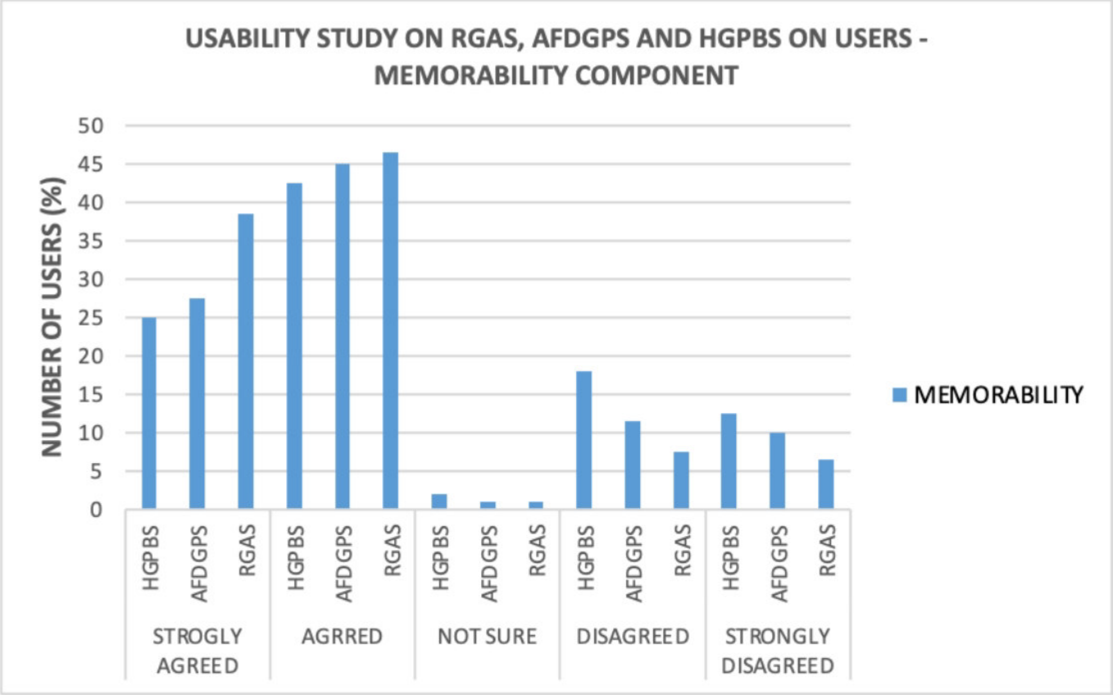

Figure 5: User's Responses on RGAS, AFDGPS and HGPBS Memorability

The result in Figure 5 indicates as to the fact that whether or not the choice of passwords was easy to memorize. Among the three schemes, the result of the passwords used in RGAS reveals that it was very much easy to memorize and reproduce with 170 (85%) user in agreement compared with the memorability of the existing AFDGPS 140 (70%) and HGPBS 135 (67.5%).

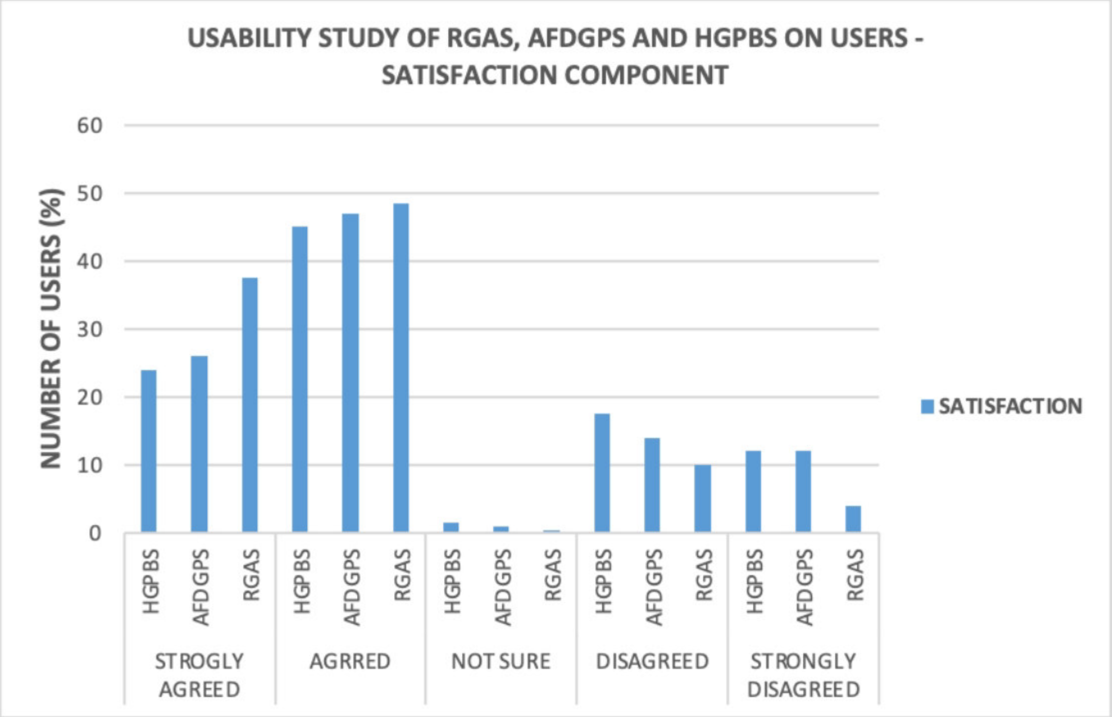

Figure 6: User's Responses on RGAS, AFDGPS and HGPBS Satisfaction

In Figure 6, the satisfactions of the users after using the three schemes were tested and it is noteworthy that most of the participants were very much pleased with the RGAS scheme. This is confirmed by the result, where 172 (86%) of the users agreed to full satisfaction compared with 146 (73%) of AFDGPS and 138 (69%) of HGPBS.

4.1 Security Evaluation Results of RGAS, AFDGPS and HGPBS

The security experiment conducted in Federal College of Education E-Library with two hundred participants on one system to a user. They were thoroughly monitored by twenty professional password crackers from Information Technology System and Security Professionals for the period of six weeks to monitor the Login details of the users. Analysis of the security test as shown in Table 11 revealed 0, 2 and 3 malicious logins in RGAS, AFDGPS and HGPBS respectively throughout the period of the experiment.

Table 1: Comparative security analysis of the proposed system

SCHEME	WEEK 1	WEEK 2	WEEK 3	WEEK 4	WEEK 5	WEEK 6	TOTAL. HACKED
HGPBS	-	-	-	1	1	1	3
AFDGPS	-	-	-	-	1	1	2
RGAS	-	-	-	-	-	-	-

4.2 Systems' performance Evaluation Results of RGAS, AFDGPS and HGPBS

The Systems' performance evaluation results of HGPBS, AFDGPS and RGAS showed that majority of the users found the design systems very good in the area of Accuracy Rate, Adaptation Rate, Mean completion Time and Success Rate in terms of password creation, password confirmation and password login. The chart for each performance study is shown in Figure 7 to Figure 10 as follws:

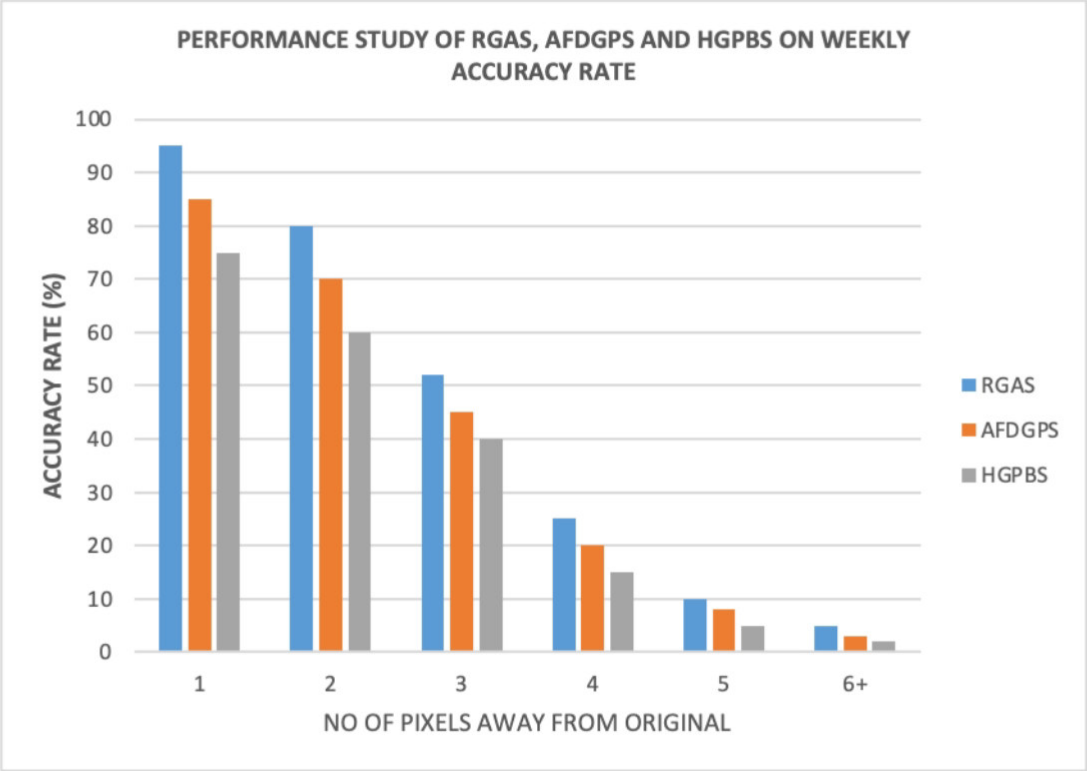

Figure 7: Weekly Accuracy Rate of RGAS, AFDGPS and HGPBS on Pixels' number away from Original

The result of the first experiment conducted on FCES datasets comprised of data with percentage accuracy that varied between 0% and 100% of the total pixels, with a fixed degree of tolerance of 15mm.

In Figure 7, the effect of weekly accuracy rate on number of pixels away from original test was carried out and the result from the experiment showed that the accuracy rate of RGAS was better than that of AFDGPS and GHPBS algorithms. It was also noted that the pixels' number away from original is inversely proportional to the accuracy rate of RGAS, AFDGPS and HGPBS algorithms. That is, as the number of pixels away from original increased, the accuracy rate per participants on weekly basis decreased.

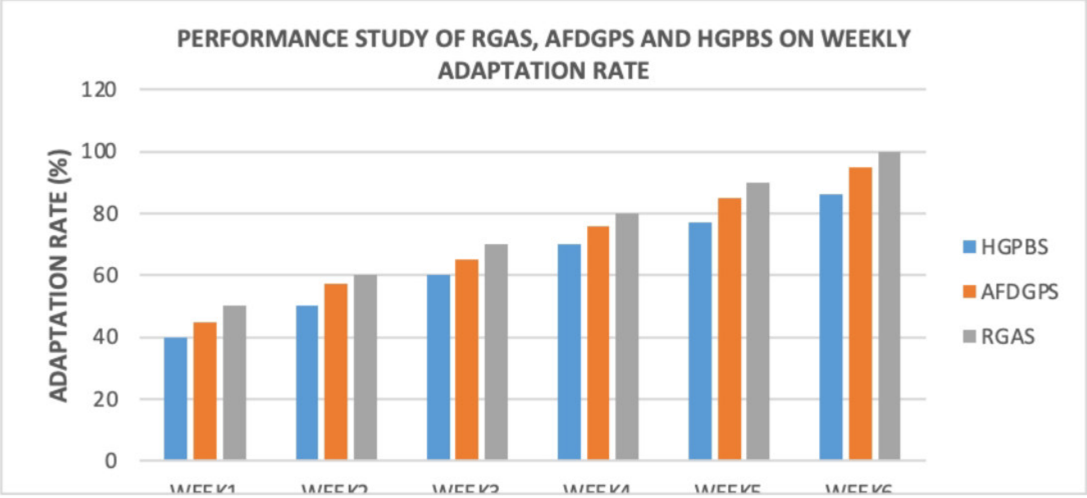

Figure 8: Weekly Adaptation Rate of RGAS, AFDGPS and HGPBS

The result of the second experiment conducted on FCES datasets comprised of percentage' number of adaptation rate varied between 0% and 100% of the successful number of participant trials.

In Figure 8, the participants' weekly performance based on their percentage number of adaptation rate was determined and the result from the experiment revealed that the RGAS adaptation rate was better than that of AFDGPS and HGPBS algorithms. It was also noted that the participant's weekly performance was directly proportional to the percentage number of adaptation rate for RGAS, AFDGPS and HGPBS algorithm. That is, as the number of week increased, the percentage number of participants' adaptation rate also increased.

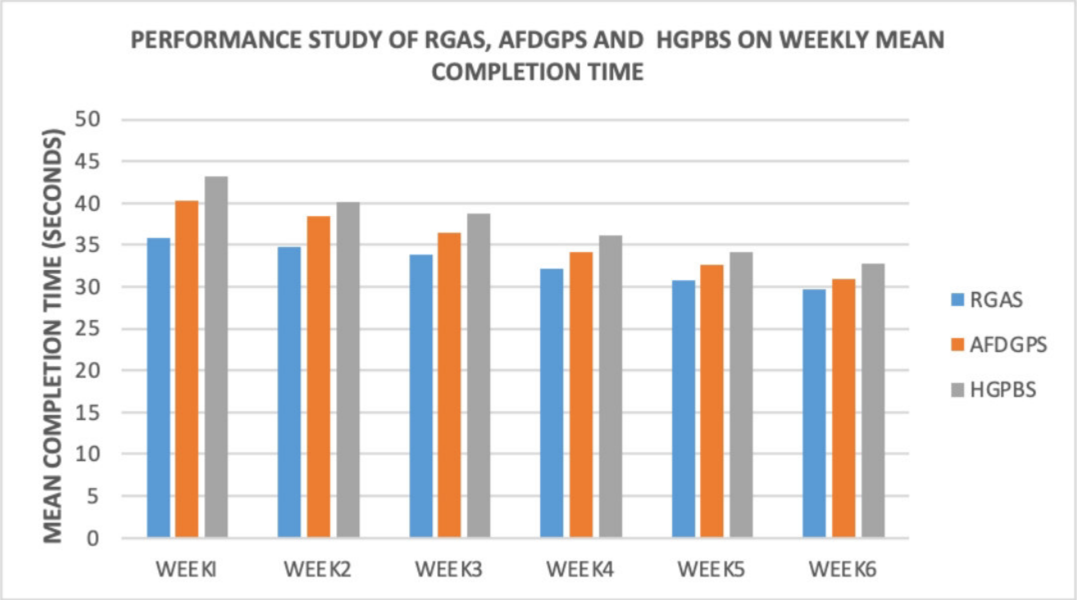

Figure 9: Participants' Weekly Performance of RGAS, AFDGPS and HGPBS on Mean Completion Time

The result of the third experiment conducted on the FCES datasets which comprised of varied mean completion time (second) between 0 and 40 based on the participants' weekly performance.

In Figure 9, the participants' weekly performance based on their mean completion time were also generated and the result from the experiment highlighted that the RGAS participants' mean completion time was better compared with that of AFDGPS and GHPBS algorithms. It was also clear that, despite the differences in completion time, the participants' weekly performance was inversely proportional to its equivalent mean completion time. That is, as the number of weekly sessions increased, the mean completion time decreased.

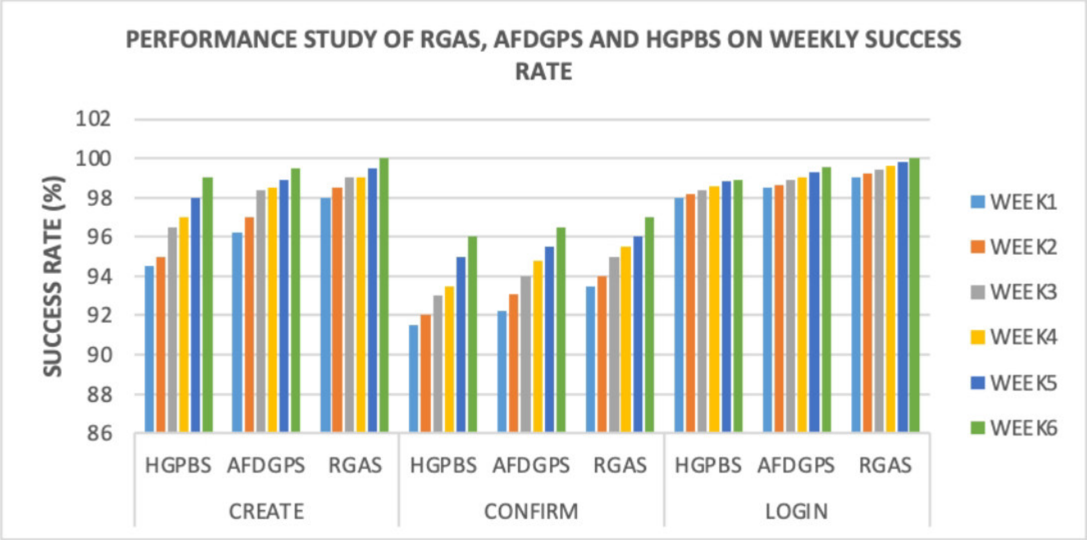

Figure 10: Weekly Success Rate of RGAS, AFDGPS and HGPBS on Password for Create, Confirm and Login phase

The result of the fourth experiment conducted on FCES datasets varied between 10% and 100% based on the successful trials in password creation, confirmation and login phases for RGAS, AFDGPS and GHPBS algorithms.

In Figure 10, the effect of weekly participants' success rate of RGAS, AFDGPS and HGPBS schemes on password for create, confirm and login phases were carried out. The result obtained showed that the RGAS weekly successful rate was better than that of AFDGPS and HGPBS algorithms during password creation, Confirmation and Loging-in phases. It was also clearly revealed that, the participants' weekly performance was directly proportion to their success rate. That is, as the number of weekly activities increased, so the participants' success rate increased.

References

[1] Alice, J.L. and Fuhua (frank), C. 2009. A free Drawing Graphical password Scheme.Computer- Aided Design and Applications 6(4): 553-561.

[2]Anjum, J. S., Chaitali, C. P., Vijary, S. J., and Sindhu, M. R. (2015). *User Authentication Using Graphical System.* Progress In Science and Engineering Research Journal. PISER 17, vol. 3, ISSN 2347-6680 (E), PP. 056-061.

[3]Ayannuga O.O (2012). Usable Knowledge-based Authentication System: A thesis Submitted to the Department of Computer Science, Federal University of Agriculture, Abeokuta.

[4]Birget, J.C., Hong, D., and Memon, N. (2003). *"Robust discretization, with an applicaion to graphical passwords, "* Cryptology ePrint archive.

[5]Blonder, G. E. (1996). *"Graphical passwords,"* in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States.

[6]Carrillo-Torres, D.; Pérez-Díaz, J.A.; Cantoral-Ceballos, J.A.; Vargas-Rosales, C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. Appl. Sci. 2023, 13, 1374. [CrossRef]

[7]Chiasson, S., Forget, A., Biddle, R., and Van Oorschot, P.C. (2009) *"User Interface Design Affects Security:* Patternsin Click-Based Graphical Passwords," Int"l J. Information Security, vol. 8, no. 6, pp. 387- 398.

[8]Chiasson, S., van Oorschot, P.C., and Biddle, R. (2009). *"Graphical Password Authentication Using Cued Click Points,"* School of Computer Science, Carleton University, Ottawa, Canada.

[9]Coventry L., Cranor, L. and Garfinkel, S. 2005. Usable biometries in Security and Usability:Designing Secure Systems that People can use. O'Reilly Media pp175-197.

[10]Davis, D., Monrose, F. and Reiter, M. K. (2004). *"On user choice in graphical password schemes,"* in Proceedings of the 13th USENIX Security Symposium. San Diego, CA.

[11]Dhamija, R., and Perrig, A. (2000) "Deja Vu: *"A User Study Using Images for Authentication, "* in Proceedings of 9th USENIX Security Symposium, 2000.

[12]Di, L., Paul, D., Patrick, O., and Yan, J. (2007). *Graphical Passwords and Qualitative Spatial Relations*, Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania. ACM, 161-162; July.

[13]Dunphy, P., and Yan, J. (2007). *"Do Background Images Improve "Draw a Secret" Graphical Passwords?"*; CCS'07, Alexandria, Virginia, USA.

[14]Dunphy, P. and Yan, J. (2008). *Do background images improve "Draw a Secret" graphical passwords?* In 14th ACM Conference on Computer and Communications Security (CCS), October. Experimental Psychology: Human Learning and Memory, 2(5):523–528.

[15]Elugbadebo, O.J, Sodiya, A.S, and Folorunso, O. 2016. An Efficient and Secured Graphical Authentication System. 2nd International conference on nintelligent Computing and Emerging Technology (ICET) 2: pp195-203.

[16]Goldberg, J., Hagman, J., and Sazawal, V. (2002). *"Doodling Our Way to Better Authentication,"* presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA.

[17]Iranna, A. M., and Pankaja, P. (2013) " Graphical Password Authentication Using Persuasive Cued Click Points," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, July 2013.

[18]Jain, A., Hong, L. and Pankanti, S. 2000. Biometric identification. Communication of the ACM 43(2): 91–98.

[19]Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D (1999). *"The Design and Analysis of Graphical Passwords,"* in Proceedings of the 8th USENIX Security Symposium, 1999.

[20]Jonathan, W. S. (2015). The Impact of Image Synonyms in Graphical-Based Authentication System: A thesis submitted to the Graduate school of Computer and Information Science, College of Engineering and Computing, Nova Southeastern University.

[21]John, M. S., Parvathi, V. S., Sekhar, M.R., and Babu, P. R., (2010). "Enhancing security of passpoints system using variable tolerance" International Journal of Advanced Networking and Applications Vol. 1 (4), pp. 270 – 274.

[22]Kamlesh, B., Ashish, D., Bhakti, S., prashnnnaki, G., and Akash, W. (2013). Id Wisdow through click based graphical password Authentication international Journal of computing and Engineering (IJSCE). ISSN. 2231-2307, Vol 3, January 2003.

[23]Lapin, K.; Šiurkus, M. Balancing Usability and Security of Graphical Passwords. In Proceeding of the 9th Machine Intelligence and Digital Interaction Conference, Warsaw, Poland, 9–10 December 2021; pp. 153–160.

[24]Passlogix, "www.passlogix.com," last accessed in June, 2005.

[25]Paulson, L. D. (2002). *"Taking a Graphical Approach to the Password,"* Computer, vol. 35, pp. 19.

[26]Ray, P. P. (2012) "Ray's scheme: Graphical password based hybrid authentication system for smart hand held device," Journal of Information Engineering and Application, vol. 2, no. 2, (2012).

[27]Sabrado, L., and Birget, J. C. (2002) *"Graphical passwords"*, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol 4.

[28]Sasse, M., Brostoff, S. and Weirich, D. 2001. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal 19(3): 122–131.

[29]SFR, "www.viskey.com/tech.html," last accessed in June, 2005.

[30]Sharna, S.A.; Ali, S.A. Image Based Password Authentication System. arXiv 2022, arXiv:2205.12352. [CrossRef].

[31]Suchita Sawla, Z. K., Fulkar, A., and Solanki, S. "Graphical password authentication system in an implicit manner," International Journal of Cryptography and Security, vol. 2, no. 2249-7019, pp. 27-29, 2012.

[32]Suo X., Zhu Y. and Owen G. (2005). *Graphical passwords: A survey*. In Annual Computer Security Applications Conference (ACSAC), December 2005.

[33]Towhidi, F., Masrom, M., and Manaf, A. A. "An enhancement on Passface graphical password authentication," Journal of Basic and Applied Scientific Research, vol. 2, no. 2, 2013.

[34]Wazir, Z. K., Yang, X., Mohammed, Y. A., and Quratulain, A. (20110). ICA3PP 2011 Workshops, Part II, LNCS 7017, pp. 153-164.

[35]Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., and Memon, N. (2005). *"Authentication using graphical passwords: Basic results,"* in Human-Computer Interaction International (HCII 2005). Las Vegas, NV.

[36]Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., and Memon, N. (2005). *"Authentication using graphical passwords: Effects of tolerance and image choice,"* in Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh.

[37]Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., and Memon, N. (2005). "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human Computer Studies, to appear.

[38]Ziran, Z., Xiyu, L., Lizi, Y. and Zhaocheng, L., (2010). "A Hybrid Password Authentication scheme Based on Shape and Text", Journal of Computer: DOI 104304/jep vol. 5(5), pp. 765- 772.