Journal of Physical Science and Innovation Volume 6, No. 2, 2014
ISSN: 2277-0119

# GRAPHICAL PASSWORD AUTHENTICATION METHODS IN INFORMATION SECURITY

**Obasan Adebola, Patrick Owohunwa, and Abdulazeez Sikiru**

*Kaduna Polytechnic, Department of Mathematics, Statistics & Computer Science, College of Science & Technology, Kaduna State, Nigeria.*

*E-mail: aolukay@yahoo.com, owohunwapatrick@yahoo.com,*

## ABSTRACT

Password authentication is a basic form of information security for computers and communication systems where passwords recalled from human memory are used to validate users before allowing them access to their different secure resources like personal computers, e-mail, individual bank accounts, social networks to mention a few. Therefore, today users have many passwords and find it difficult to create them according to the established password security guidelines. Instead, most users write down their passwords, and use one password for multiple accounts while others settle for simple, short, personal names of family members, dates, dictionary words, and unsecure passwords due to human memory limitation. Recall-based graphical password schemes are one of many proposed mechanisms for user authentication based on the premise that human memory is better at remembering images than textual information. Most of these schemes have worked on the usability and security enhancement. The present study is mainly focused on the security analysis of the existing graphical authentication methods with discussions on different aspects of password security. The paper starts by categorizing the existing graphical schemes into three major types according to memory tasks: recall, cue recall and recognition tasks of human memory.  A total of seven schemes are chosen from each of the three categories and each of the schemes was extensively discussed. We review a number of criterions for measuring efficiency of authentication systems and examined different conventional password attack methods. Password space and password entropy formulae and calculations related to the schemes are also presented in this paper. A comprehensive analysis of each authentication method highlighting their password entropy and vulnerability to different password attacks was presented. In conclusion, some suggestions are given for future work.

**Keywords:** **Graphical authentication; Password Space; Password Entropy; Security Attacks**

## INTRODUCTION

Graphical Passwords are one of the several proposed alternatives to traditional user authentication method based on alphanumetic username and passwords. User authentication is part of security requirements which is often used to secure internet communications and ensure the most needed protection of both the user and service provider. However, most text-based passwords are prone to a number of memorability and security challenges. Most of these problems are caused by weak user authentication passwords which arose from weak choice of keyboard-based passwords intentionally made by the user to enhance his or her memorability because users generally find it difficult or impossible to remember high-quality passwords that would guarantee security. In attempt to 'enjoy unethical' convenience to aid memorability, where users do not follow all the rules required of them for forming strong and secure passwords. These rules include; passwords must not relate to personal information like name, birthday, even words found in a simply dictionary, password must have at least eight alphanumeric characters which should be combination of upper and lower case letters with at least one digit[1] or passwords could be strings of characters chosen from printable ASCII codes[2]. Mostly, the users enjoy easy passwords to achieve cheap memorability or some convenience at the expense of general security of the system. This violation of password rules in terms of user behavior is responsible for passwords' predictability and ultimately make them easy to guess. Therefore, user authentication system should be designed to provide two important features memorability and security simultaneously. But in reality, one of these features is achieved while the other is ignored even though both are important and necessary. This problem is peculiar to text-based authentication systems because of human memory requirement for its implementation. As a result of these inadequacies in text passwords, alternative technologies such as public key cryptography , security token, biometric[3,4], cognitive passwords and even hybrid of these authentication factors are gaining much attention to overcome problems in the text-based password authentication[2]. However, the problem with these systems is that most of them are designed by the service providers to be cost effective, scalable and secure, without minding the inconvenience and poor usability from the users' viewpoint. Thereby making such authentication mechanisms not to achieve their envisioned objectives in terms of security because the average users may not want to sacrifice convenience to pay for security and even when users try balance between security and convenience, the forgetting nature of human memory manifests to undermine memorability. Furthermore, it is worthwhile to say that these alternative authentication mechanisms do not provide solution to authentication problems without taking another cost just simply because none of them is perfect in terms of convenience and security strengths.

Illustratively, token could improve the level of security and protection but the simplest vulnerability is should it lose authentication could be more difficult if not totally impossible. Similarly, biometric technology has both his good and bad sides. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods, however, the database for storing of biometric identifiers is problematic when is compromised[5].

Therefore, in an attempt to improve the memorability limitation of passwords, another form of knowledge-based authentication called usable authentication which uses graphical password schemes was brought to lime light in 1999[6]. They are potentially more memorable and secure than conventional text-based passwords because of the fact that human users have the ability to recognize images better than words[5]. The main focus of this study is to review a good number of graphical password methods and analyse their security strenghts in terms of password space and entropy. Discussions will also be focused on them to analyse their sesceptitability and resistance to to conventional passwords attacks to provide diverse views aimed at simplifying the understanding of the existing graphical schemes and ease the creation/ development of efficient schemes that offer improved memorability and security simulteneously. It could also influence the identification of some underlying design strategies to inform the design of other image-based authentication schemes based of existing security features. A number of work had been done , which resulted into the existence and implementations of some graphical schemes with varying degrees of security limitations[7,8].

## EXISTING GRAPHICAL PASSWORD SCHEMES

Today, there are a number of graphical password schemes available in literature and they are grouped into different classifications based on three important factors. Firstly, based on the cognitive activities which is the memory tasks of the user to recall the password [6,9-12]. Secondly , based on the image/grid background of the schemes[12,13] and thirdly, based on the users' action with input device like mouse during both registration and authentication stages [6,14]. By considering the memory tasks of the users to memorize and recall their passwords, the current study classifies the existing graphical password schemes into three main categories; namely pure recall-based, cued recall-based, and recognition-based. Seven (7) examples are given as illustration for each of the three categories as presented in Figure 1.

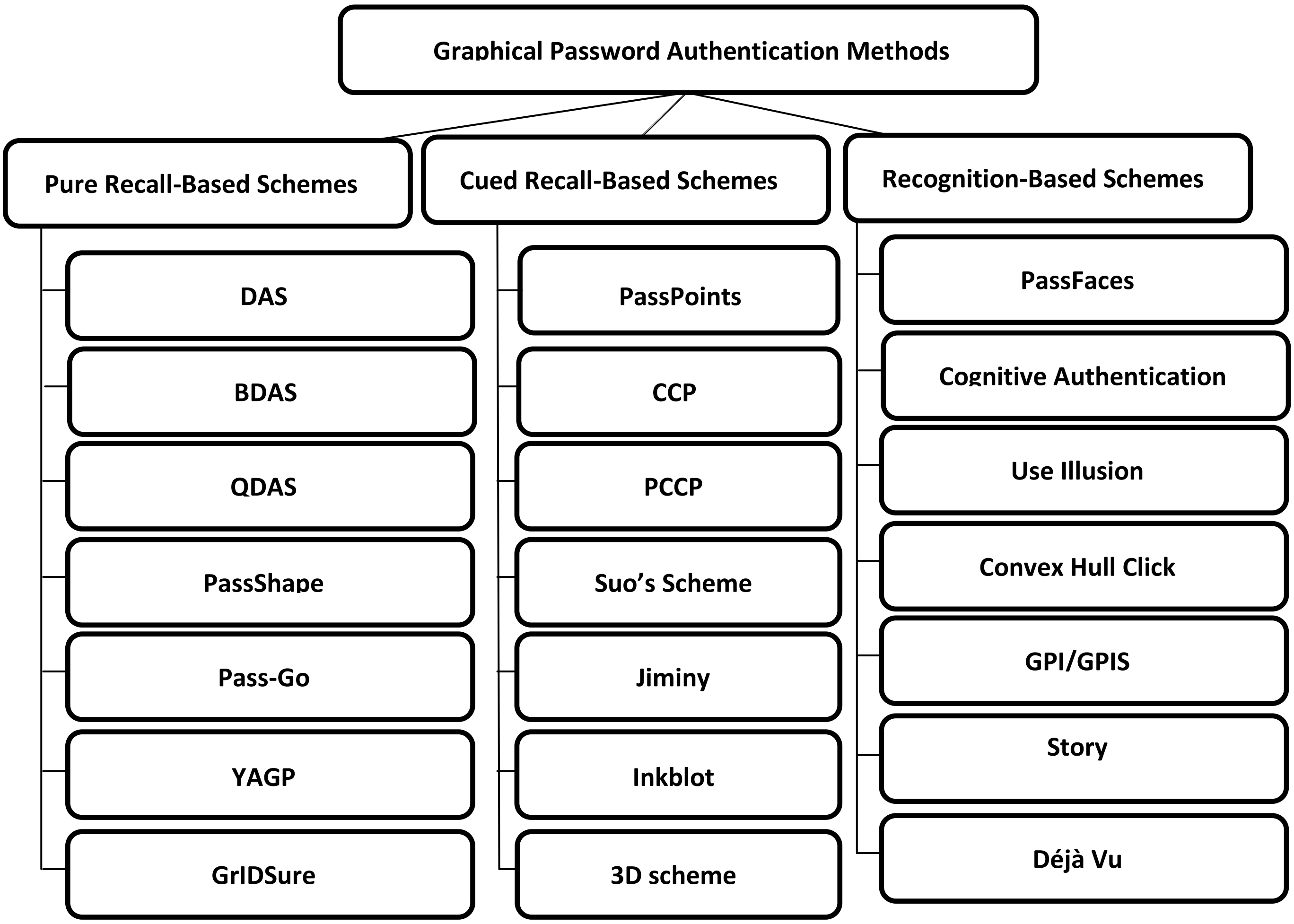

Figure 1: Classification of the existing Graphical Passwords

## PURE RECALL-BASED GRAPHICAL PASSWORDS

The pure recall-based systems also called drawmetric systems require users to memorize and reproduce their secret drawings which were drawn or selected earlier on a blank canvas or on a grid during the registration process[6]. In pure-recall systems, passwords are usually generated and recalled without memory cue. There are a number of graphical password algorithms which are designed by using pure recall-based methods. Pure recall-based schemes are many in literature today and vast majority of these schemes were presented as improvements of Draw-A-Secret (DAS) which is the first of its kinds [1]. In DAS, password is a free-form drawing produced on a 5x5 grid and the same secret drawing is recalled and reproduced during authentication to gain access to secure resource. Since both registration and authentication processes simply depend on drawings, DAS system is said to be alphabet independent and as such the scheme is accessible to users of any language for applications[2]. DAS scheme has some limitations which have negative effects on its security. To enhance the security of original DAS scheme, BDAS scheme was introduced simply by adding background images to the original DAS scheme to encourage users to draw more complicated passwords and ultimately gain better security[3].Two comparative user studies conducted by Dunphy and Yan confirmed that introduction of background images to the original DAS scheme was an effective and marvelous enhancement because the users were truly aided to draw memorable and secure passwords on the grid. By the result of their experiments, predictable characteristics problem was reduced. Another form of recall-based scheme includes Qualitative Draw-A-Secret (QDAS) designed. In QDAS, each stroke is encoded according to the starting cell and the sequence of direction changes relative to the grid. QDAS scheme is a method was design to prevent against shoulder-surfing attacks with the help of dynamic grid transformations but the mechanism achieved better security at the expense of memorability[1]. Studies were intensified with introduction of Pass-Go, and Yet another Graphical Password scheme (YAGP) was introduced by Gao and his other colleagues. The scheme was another alternative improvement for DAS and was able to provide trend-sensitive judgment mechanism an enhancement with the help of soft matching which eased the password drawings to the users because with the mechanism the exact stroke positions are no longer necessary to ensure successful registration and authentication[5]. An enhanced version of YAGP with the adoption of a triple-register process was also designed by Liu, Gao and their other colleagues to implement the strengths of DAS while the rigid restrictions and memorability problems were relaxed according to the experiments carried out by them[6]. However, the improvement is not substantial enough to justify the cost of a triple-register process adopted in YAGP scheme.

PassShapes graphical authentication mechanism is a draw-based scheme proposed by Weiss et al. The scheme consists of 8 strokes directions and two neighboring strokes are set at $45^0$ intervals to each other and form $360^0$ which is a complete circle altogether as presented in Figure 2.16. The 8 strokes are all labeled with character representation to indicate different stroke directions. Like “U” denotes “Upper”, “D” denotes “Down” and “L” and “R” denote “Left” and” Right” respectively. While the 4 numbers stand for directions corresponding to the position of the number on a standard pad. Like “9” stands for “Upper Right” and “3” represents “Down Right”. Each of the alphanumeric characters denotes a pen-down operation while any different character like “X” can be used to represent pen-up which is a character for separating two stroke sequences. In this system, users are authenticated by drawing simple geometric shapes constructed from an arbitrary combination of eight different strokes (Weiss & De Luca, 2008). That is, passwords are encoded from the alphanumeric characters with respect to 8 strokes directions and reproduced in the same order for authentication. The passwords are then represented in alphanumeric strings for both storage and retrieval. The passwords are not affected by size because the system does not require grid cells and they are processed based on the strokes directions and order of drawing only. Studies reveal that Pass Shapes scheme provides better memorability but relatively small password space in terms of security because of the limited stroke directions requirement in the system. GrID sure is system which displays random digits in a $5^x5$ grid. To register, users are required to select a memorable pattern of 4-cell password on the grid. User is expected to memorize and recall the same password to be authenticated[15].

| Password Schemes | Authentication method | Remarks |
|---|---|---|
| DAS[16] | Users are required to draw simple images as their secrets on 5x5 grid cells. To login, they reproduce their secret images on the same 5x5 grid cells. | DAS is the first recall-based system proposed where the password is composed of the coordinates of the grid cells that the drawing covers. |
| BDAS[7] | BDAS an extension of DAS scheme and it works exactly the like DAS. | Background image is added to DAS scheme to serve as memory cue and to improve security of the scheme |
| QDAS[17] | In QDAS system, the password consists of stroke from the starting cell and the sequence of direction changes relative to the grid cells. To authenticate, the user recreates every cell-crossing in the correct order. The scheme helps the user to deviate from the literal spatial definition of the secret unlike DAS. | The involves use of dynamic grid transformations to mask the password creation process and provide protection against shoulder surfing e.g. stroke 5,"down","right",and "up" instead of using grid cells coordinates directly. |
| PassShape[18,19] | User draws a simple picture as his or her password by using one or more arrows from among 8 strokes directions (or arrows) instead of grid cells. These 8 directions are set at intervals $45^0$ around a circle labeled as:1,3,7,9,U,D,L and R. | Password is encoded using alphanumeric characters corresponding to: 1,3,7,9,U,D,L and R representing 8 strokes directions used in the system. |

| | | |
|---|---|---|
| Pass-Go[13] | User draws his or her password on a grid through the intersections instead of grid cells. | Pass-Go implements a discretization method that uses grid intersections for user's password. |
| YAGP[20] | YAGP system is an extension of DAS by using the idea of approximately correct drawings | Approximation algorithm is used for comparing secret drawings |
| GrIDsure[15] | GrIDsure is system which displays random digits in a $5^x5$ grid. To register, users are required to select a memorable pattern of 4-cell password on the grid. User is expected to memorize and recall the same password to be authenticated [15]. | For every authentication, the login panel digit is randomized. Users are expected to select the digits in the correct order. |

**Table 1: Comparison of Recall-based graphical passwords**

## CUED RECALL-BASED GRAPHICAL PASSWORDS

The cued recall-based systems also called iconmetric or locimetric systems are systems that require users to memorize and recall their passwords within a system that provides image as memory cue with the purpose of influencing user's memory on his or her chosen passwords (Robert Biddle *et al.*, 2012; Ray, 2012). The first person who pioneered and presented the initial idea of graphical passwords was Greg Blonder in1996. In this scheme, the user clicks with a mouse or other device like stylus on a few chosen regions in a single image-based background that appears on the screen (Blonder, 1996). A password is a number of clicks on these locations in a particular order. Table 2 presents 7 typical cued recall-based graphical password schemes. Different studies revealed that most of the schemes in this category are susceptible different attacks illustrated in Table 3.

**Table 2: Comparison of Typical Cued Recall-Based Graphical Password Methods**

| **Password Schemes** | **Authentication method** | **Remarks** |
|---|---|---|
| PassPoints [21] | Users are required to select a password of five (5) points on a system assigned image. To login, | Robust discretization, centered discretization, or optimal discretization can be done to |

| | | |
|---|---|---|
| | the users click the 5 registered points in the correct order. | enhance the efficiency of the scheme |
| Cued Click-Points (CCP)[22] | Users are required to select 5-point password on 5 different system assigned images presented in a given sequence. To login, the users re-enter the 5 points in the correct order. | The authentication system suggests the use of at least 1200 images at each round, making $1200^5$ images available to users. |
| Persuasive Cued Click-Points (PCCP)[23] | PCCP is an alternative implementation to CCP. It works exactly like CCP except that user are persuaded to select random points by dimming function at the registration stage. (i.e to create a password, users choose each point from a randomly positioned viewport) | The dimming function is used for security reason. It darkens most of the image except a small rectangle to force users to a new location for password creation. |
| Suo's Scheme [24] | It's an alternative implementation of PassPoints. To authenticate, the user either types Y for "yes" if the selected point is located within the focus area or N if it does not for at least 10 rounds until 5 points are identified for authentication process. | During the login process, the entire image is blurred except a small focus area to prevent from being seen. |
| Jiminy[25] | In Jiminy system, a grid of alphanumeric characters are displayed over an image and the users places a set of templates over the grid. The selected password consists of the characters being seen through the template. | The prototype implementation of the schemeinvolves both image and a grid of alphanumeric characters. |
| Inkblot Authentication[26]. | In inkblot authentication system, a number of inkblots are displayed and users are asked to | The first and last letters of the word are typed in 5 rounds and the password is created with the 5 |

| | | |
|---|---|---|
| | type the first and last letter of the word that best describes the inkblot in five rounds. The 5 pairs of 2 letters used for the selected password. | pairs of letters |
| 3D scheme[27] | 3D scheme user travels through a virtual 3D world and perform actions which is later evaluated and converted to a password | The memory cue implemented in this scheme is the virtual world and it influences user's memory. |

## RECOGNITION-BASED GRAPHICAL PASSWORDS

Recognition-based systems also called cognometric or searchmertic systems require the users to memorize a portfolio of images at the password creation time and must be able recognize them (their previously seen images) from among decoys to be authenticated [6]. Table 3presents 7 typical recognition-based graphical password schemes which include Passfaces, Cognitive Authentication, Use Your Illusion, Convex Hull Click scheme, and Graphical Password with Icons (GPI)/Graphical Password with Icons suggested by the System(GPIS) [28-32] and others.

**Table 3: Comparison of Typical Recognition-Based Graphical Password Methods**

| Password Schemes | Authentication method | Remarks |
|---|---|---|
| Passfaces[28] | To login, users are required to recognize and click 1 of the 4 pre-registered human faces from among decoys in 4 rounds of 9 images being displayed in a panel. | System generated faces are used in commercial version of Passfaces to avoid predictable passwords because users tend to choose faces from their own their race or attractive faces. |
| Cognitive Authentication[30] | Authentication process requires users to calculate a path through a panel of images based on whether particular images belong to Passimagesor not. | The login process is slow. |
| Use Your Illusion[31] | Uses selected images that are visibly distorted by non-photorealistic algorithms. The login process asks | The scheme is based on the assumption that users can still recognize their photos |

| | | |
|---|---|---|
| | users to recognize their distorted photos from among 27 photos. | even after applying distortions. |
| Convex Hull Click scheme[29] | Its uses icons instead of images. The login process requires users to click inside a visualized convex geometrical shape made by the icons in 5 different rounds. | users never have to click directly on their password images. |
| Graphical Password with Icons (GPI)/Graphical Password with Icons suggested by the System(GPIS)[32] | User click6pre-registered order dependent icons out of 150 to login. GPI allows users to select their own passwords while GPIS assigns the passwords to the users. | The 150 icons are grouped into 15 categories to ease the login process. Each category has 10 icons making it 15x10 grids. |
| Story[28] | Users select a sequence of 4 images for their portfolio and login by identifying one image from among decoysin 4sequential rounds. | Story scheme authentication process has a sequence of 4 rounds of 9 images per challenge panel. |
| Déjà Vu[33] | The scheme generates images from mathematical formulae with the help of a seed which serves as user specific data. To authenticate successfully, user has to recognize 5 images out of a total of 25 randomly generated images in any order. | The seeds are stored in the server in clear text to facilitate image generation process. |

## CRITERIONS FOR MEASURING GP SCHEMES

The efficiency and effectiveness of graphical password algorithms could be measured using the following criterions [34]:

- **Security**: Passwords provide security mechanism for authentication and protection of services against unwanted access to resources. User authentication is the first stage of computer and communication systems. It is a security process of determining whether someone or something is, in fact, who or what it is declared to be. The degree of authentication security is measured in terms of password length, password space, password entropy, and resistance of the graphical password schemes to a number of attacks.

- **Usability:** This is a measure of users' convenience of a given graphical password scheme in terms learnability, satisfaction memorability, and interface. Learnability criterion includes easy to learn, ease of use, ease of reset of forgettable secret, and the quality of guidance the system can offer. While the memorability criterion includes two main characteristics which are retrieval – is it easy to recall the secret during login and the second one is memorizing- is it easy to memorize the secret after a long period of time. Satisfaction is the overall users' opinion on the level of ease of use, and the appropriateness of login time. A graphical password system is satisfactory when no frustration was experienced when using the scheme. While the interface criterion covers characteristics like use of image, screen size, the use of texts and fonts, the type of error messages used in the scheme and any guidance offered by the scheme before and after authentication [12, 35]. A major usability problem among graphical password users is that password creation and authentication processes take too much more time than text-based passwords. The reason is because more activities are involved during registration and registration stages: a user has to pick images from the database especially in recognition-based scheme, and that same user has to scan through a number of images to recognize his or her Passimages in one or more authentication rounds during authentication stage. For example, in Passface, an authenticating user has to scan through 100 faces and must recognize four (4) faces correctly from among distractors[28]. This is a process which many users consider more time consuming and tedious than text-based password scheme.
- **Reliability:** This is a measure of accuracy of graphical password schemes in terms of reliable use of graphical input devices for drawing, selecting or clicking while creating or authenticating passwords graphically. The design of graphical password schemes should be good enough in a way that users can draw their secrets as fast, accurate as possible during the registration and authentication stages without encountering any usability problem.
- **Availability:** The storage space required for implementing graphical passwords is much more than alphanumeric username password system. The simple reason for this difference is the number of pictures or images that are needed to be maintained in a centralized database for recognition-based graphical password schemes implementation. Recognition-based graphical password algorithms are characterized by network transfer delay in a situation where series of pictures may need to be displayed for a number of verification rounds and it is imperative to solve the availability problems and ensure that the images are available at all times for the scheme to be functional.

## SECURITY ANALYSIS OF GP SCHEMES

An effective and efficient authentication system must provide satisfactory security services for its intended environment, otherwise it fails to meet its primary goal. Research on security of the graphical password schemes was pioneered and extensively analyzed by Jermyn, Mayer *et al.* primarily to compute the size of the password space of DAS scheme [36]. The knowledge of size of password space could directly help to obtain password entropy.

## SIZE OF PASSWORD SPACE GP SCHEMES

Password Space is a very important factor regarding to a password algorithm in terms of security. Password Space is usually calculated from the password length which is a fundamental parameter and its value affects password strength against attack like brute force in telecommunication and other areas in computing. To ensure good management of passwords, users choose their passwords with the help of some guidelines which provide information on the character sets allowed for the creation of the passwords. Such rules help users generate secure passwords if strictly followed. The more character sets a password consists of, the harder it will be to guess for attackers. Different character sets include lowercase letters, uppercase letters, numbers, punctuation marks, or other symbols. This measure of password strength is based on the principle that longer length will allow users to have more alternatives and use of long passwords with respects dictionary attacks. This will be outlined below. The collection of secure passwords which are generated without circumventing the guidelines constitutes the password space. The majority of users fail to follow the rules therefore reducing password space. The larger the password spaces the better secure the system. Large password space and long passwords are means to secure systems.

The password space of length $L$ may be defined simply by the following permutation Equation 1. Permutations are used instead of combinations when order of $L$ is important [37]:

$$S_L = \sum_{L=1}^{n} N^L \tag{1}$$

$$S_L = \sum_{L=1}^{d} \left(\left\{\frac{N}{N_O}\right\}\right)^L \tag{2}$$

Applicable when an image can be chosen repeatedly. That means one can choose an image more than once in L to form a password and the order is important.

Where $N$ stands for the number of characters where passwords are being chosen from or number of available regions in image-based scheme, $L$ represents the password length which is the number of regions selected from $N$ to form a password, and $S$ still represents the password space of length $L$. Equation 2 is applicable to cued recall-based graphical algorithm like PassPoints, where system requires the users to select dots as passwords on a given image. Since users simply click on a pixel which is set at the center by the system, and select a certain threshold value of $N_o$ as the password region in a given order. Clearly, N represents the image size while $N_o$ represents tolerance. It is also important to note that password space calculations of recognition-based graphical schemes often involve combinations since it involves random selection of images for choosing graphical passwords [37]. Given a set of size $N$ images, the number a ways of choosing $L$ passimage is called combinations when the order of selection of $L$ images out of total images of $N$ unimportant and the Equation 3 as follows:

$$S_L = \binom{N}{L} = \frac{N!}{L!(N-L)!} \tag{3}$$

The Equation 3 shows that the possible number of passwords is the "binomial coefficient" (choose any $L$ object from among $N$). Applicable when an image can be chosen repeatedly. That means that the overall password space of a graphical password schemes where users choose an image more than once in $L$ to form a password and order is unimportant [38] can be calculated by Equation 3.

$$S_L = \binom{N+L-1}{L} = \frac{(N+L-1)!}{L!(N-1)!} \tag{4}$$

Equation 4 is applicable when an image cannot be chosen repeatedly. That means, one cannot choose an image more than once in $L$ to form a password and order is unimportant. In draw-based schemes, the passwords are drawn during the registration stage and the users are expected to reproduce the outline to be authenticated. There are two types of draw-based schemes, namely: the grid-based and gridless-based. For the draw-based schemes in grid environment like DAS and BDAS, a password are strokes on a grid which are divided into cells and its security is largely influenced by the number of strokes and the grid cells consisting each stroke of the passwords . While the draw-based schemes in non-grid environment like PassShapes, every password stroke is the sequence of qualitative direction changes. Since every draw-based scheme is characterized by strokes, cells or direction changes, the theoretical password space $T$ with $i$ number of strokes denoted by $S_i$

may be defined as follows in terms of the overall or total number of strokes which is denoted by $Z_{Ovarall}$ in the system.

$$S_i = \sum_{i=1}^{Lmax} (Z_{Ovarall})^i \qquad (5)$$

Assume $S_i$ = password with $i$ strokes, and 1<= $i$<= $Lmax$ for every password. Since stroke sequences are used for making passwords, it implies that theoretical password space,$T$ is equal to $S_i$ as illustrated in Equation 6.

$$T = S_i = \sum_{i=1}^{Lmax} (Z_{Overall})^i \qquad (6)$$

This implies that the total number of passwords (the theoretical space) on the system, given the maximum length $Lmax$ is computed as the number of passwords of each length $i$ from 1 to $Lmax$.

Similarly, $Z_{Overall} = \sum_{k=1}^{L} (Z_k)$ (7)

Where $1 <= k <= L$ for number of grid cells in every stroke)

$Z_{Overall}$= The overall total number of strokes in any given system.

By substituting Equation 7 in Equation 6, Equation 8 was obtained as follows:

$$T = \sum_{i=1}^{Lmax} (\sum_{k=1}^{L} (Z_k))^i \qquad (8)$$

$Z_k$ attributes depend on the system , whether it is grid-based or otherwise. $Z_k$may be defined by the Equation 9 in terms of pen-up, pen-down, neighboring grid cells because they are the basic components of a password stroke:

$$Z_k = \sum_{(x,y)\varepsilon[1..G\,]*[1..G]} n(x, y, i, G) \qquad (9)$$

The $n(x, y, i, G)$in Equation 9 represents the number of strokes of length $i$ (e.i. $i$ number of co-ordinate pairs in the strokes) and end at $(x, y)$ cell on a grid $G * G$ dimension may also be defined in terms of 4 neighboring cells where either $x$ or $y$ of cell $(x, y)$ increases or decreases by 1 at a time as illustrated below in Equation 10:

$$n(x, y, i, G) = n(x - 1, y, i - 1, G) + n(x, y - 1, i - 1, G) + n(x + 1, y, i - 1, G) + n(x, y + 1, i - 1, G) \qquad (10)$$

Given that: $n(x, y, 1, G) = 1$

While the $Z_k$for gridless draw-based schemes like PassShapes may be computed from the number of qualitative direction changes. In PassShapes scheme, there are 8 different possible directions and the 8 directions are set at $45^0$ intervals to one other as illustrated in Figure 3.

Therefore, going by Equation 9 illustrations, $Z_k$ for PassShapes system could be as follow:

$$Z_k = 8 * Z_{k-1}\,, and\ Z_1 = 8$$

**Examples:**

To illustrate password space of text-based password system, consider the set of all possible 8-character alphanumeric passwords. Including symbols, there are 95 keyboard characters to choose from, giving a theoretical password space of $P^r$=$95^8$ ≈ 6.6 × $10^{15}$ possible permutations. Let's consider another example; a cued recall-based graphical password has 450x330 picture size with a square size of 20x20. The user is expected to choose 5 to 10 points as a password.  To calculate the theoretical password space, Equation 2 is applied as follows:

$$S_L = \sum_{L=1}^{d} \left(\left\{\frac{N}{N_O}\right\}\right)^L$$

Where N= 450x330 and $N_o$ = 20x20, by substitution we obtain the following:

$$S_L = \sum_{L=5}^{10} \left(\left\{\frac{450\times330}{20\times20}\right\}\right)^L = 4.97\text{x}10^{25}$$

## SIZE OF PASSWORD ENTROPY GP SCHEMES

Secure Passwords are generally made up of jumble of lowercase letters, upper case letters, numbers, and special symbols of specific length. The longer the password, the harder it will be to guess by the attackers. Password entropy determines the degree of uncertainty of a password. This means that the number of possible combinations of characters required to write out the possible characters in the password. In other words, it measures the numbers of possible guesses. This measure can also determine the strength of a password and is calculated by computing the information entropy of the random process that produced it. The entropy equation of every symbol in the password consisting number, letters or special characters can be produced independently by using the Equation 11 as follows according to Shannon's work [39]. It is a conventional estimator that measures the amount of information in X.

$$H(X) = -\sum_{x \in X} \mathrm{pi} \log p\mathrm{i} \quad (11)$$

In a simpler and different approach, Hlywa and his colleagues calculated entropy by using the following formula [40,41] :

$\mathrm{H} = \mathrm{L} * \log_2 N(12)$

Where H represents the password entropy which measures the number of binary digits (0 and 1) has passwords when the password space is converted to base 2 number. L is the length of the password while N denotes the character size (number) of images per screen or the possible symbols from where passwords are being formed. Also, in the formula is the base-2 logarithm, meaning that password entropy is usually measured in bits. An illustrative example of a single digit password has 10 possible combinations, and 10 written in binary notation has four binary digits ("1010"). Therefore, a single digit password has 4 bits of uncertainty. More examples are illustrated in Table 4. It is a useful measure for comparing the relative resistance of different passwords to dictionary attack.

More examples, to obtain the password entropies of the last 2 examples, we obtained the following:

i.) $\mathrm{H} = \log_2(6.6\mathrm{x}\ 10^{15})$= 53 Bits

ii.) $\mathrm{H} = \log_2(4.97\mathrm{x}\ 10^{25})$= 85 Bits

Table 4 presents the analysis of the selected graphical password schemes and compares their password space, password entropy. Here "-" denotes "Not available"

**Table 3.4: Comparison of Typical Graphical Password Entropy**

| Password Schemes | Password Space | Password Entropy |
|---|---|---|
| DAS, BDAS, and QDAS [17] | $2.88 \times 10^{17}$ | 58 |
| PassShape[18] | $2.10 \times 10^{6}$ | 21 |
| Pass-Go[13] | $1.51 \times 10^{23}$ | 77 |
| YAGP[20] | $2.04 \times 10^{90}$ | 300 |
| GrIDsure | $2.62 \times 10^{5}$ | 18 |
| PassPoints, CCP, and Persuasive Cued Click-Points (PCCP)[23] | $8.8 \times 10^{12}$ | 43 |
| Suo's Scheme [24] | $8.8 \times 10^{12}$ | 43 |
| Jiminy | $5.12 \times 10^{2}$ | 9 |

| | | |
|---|---|---|
| Inkblot | $1.98 \times 10^{28}$ | 94 |
| 3D Scheme | $-$ | $-$ |
| Déjà vu | $6.56 \times 10^4$ | 16 |
| Passfaces<br>[28] | $P^r = 9^4 = 6.6 \times 10^3$ | 13 |
| Story | $4.10 \times 10^3$ | 12 |
| Cognitive Authentication[30] | $9.4 \times 10^{21}$It can be reduced to 10Bits by side-channel attacks. | 10/73 |
| Use Your Illusion[31] | $\frac{27^3}{3!} = 3.28 \times 10^3$ | 11 |
| Convex Hull Click scheme[29] | .<br>$P^r = 83^5 = 4.29 \times 10^9$ | 32 |
| Graphical Password with Icons (GPI)/Graphical Password with Icons suggested by the System(GPIS)[32] | .<br>$P^r = 150^6 = 8.8 \times 10^{12}$ | 43 |

## SECURITY FACTORS GP SCHEMES

Authentication schemes security can also be measured by showing the scheme's resistance to a number of attacks. It is widely believed that it is more difficult to break graphical passwords than text-based passwords by using the traditional attacks. Table 3.5 summarizes the security of graphical passwords schemes selected and analyzed for this study. "-""Y" and " N" are used in Table 5 to denote "NOT AVALIABLE", "YES" the scheme is resistant to that form of attack and "NO" the scheme is not resistant to that form of attack respectively. While "N/A" means "NOT APPLICABLE". In this section, discussions will be focused on these attacks as follows:

a.) **Dictionary attack**: In this attack a list of likely passwords is compiled based on knowledge or assumptions of typical user behavior. Entries in the dictionary can be further prioritized to test passwords with higher probability of success first (if these probabilities can somehow be calculated or predicted), increasing chances of quickly finding a match. Dictionary attacks can lead to efficient password guessing because users are likely to select from a relatively small and predictable password space. It is possible to use a dictionary attack for some recall-based graphical passwords but with use of mouse it could be impracticable to carry out dictionary attacks against recognition-based graphical passwords.

b.) **Brute force search or exhaustive attacks:** It is executed in a similar manner to dictionary attacks, except that every possible password permutation is generated and used to attack the real passwords. In a more sophisticated attack, these permutations may also be prioritized in order of decreasing probability of being selected by users, if such probabilities are somehow predictable. Like dictionary attacks, exhaustive attacks can be launched either online or offline. The advantage to this type of attack is that with enough time and computing power, a match will be found (unless an online attack is detected and stopped before the list is exhausted), but with large password spaces it may not be feasible to search the entire space. Therefore, the main defense against this attack is to have a sufficiently large password space. It is more difficult to lunch a brute force attack against graphical passwords than conventional text-based passwords.

c.) **Guessing:** Just like in text-based passwords, users often choose predictable and weak graphical passwords in order to ease recollection of them. Studies on recognition and recall-based which are Passfaces and DAS authentication algorithms respectively and they both revealed that people often choose weak and predictable graphical passwords [16,42]. The results of their studies simply showed that Passfaces and DAS passwords can be guessed.

d.) **Spyware attack:** This is a form of malicious software (or malware) that is usually installed on the victims' personal computers without their knowledge for the purpose of making unlawful collection of information on the victims. The spyware suitable for attacking graphical passwords include keystroke-loggers, mouse-loggers and screen-scrapers. Trojan horse is another example of spyware. The graphical input devices like mouse used in graphical authentication mechanisms make graphical passwords less susceptible to spyware attack than text-based passwords. It is difficult to imitate the mouse motion. Therefore, graphical passwords can better resist the spyware attack.

e.) **Shoulder surfing:** This a situation where malicious user observes records one or more logins and derive enough information necessary to successfully login at later time without the knowledge of the correct owner of the password. In graphical passwords, a user draws or identifies images being displayed in the screen; as he or she does that any other person within the close vicinity observe the images as well. This is due to design problem in some schemes which make them to reveals the password details partially or completely in every login. Such observer can login successfully when sufficient login information has been captured. A few recognition-based schemes are not vulnerable to shoulder surfing. Recall-based graphical password authentication methods do not have resistance to shoulder surfing attacks[11,43].

f.) **Social engineering**: This a process by which weak password users are freely tricked into releasing confidential information such as usernames and passwords for the purpose of committing fraud or compromising seemingly secure system. When the control of computers has been given away to hackers or other attackers through social engineering attack, they have the full rights like the real owners to "break" into the systems without using any electronic or algorithmic hacking mechanisms[44]. It is ridiculous and less convenient to release graphical passwords to unauthorized users or third party compared to text-based passwords. It is very convenient to give away text-based password over the phone via SMS or voice calls and even email message but to obtain such information on graphical passwords through these means could be difficult, time consuming, or even almost impracticable. The common and typical examples of social engineering include Tricking, Phishing and Pharming. Tricking is a crafty method of sharing confidential information like usernames, and passwords with attackers who appear as friends. While phishing is a dangerous scam by which confidential information on victim's password and valuable information is acquired by an attacker via e-mail spoofing or instant messaging. Pharming is social engineering attack where the attackers use sophisticated technology to acquire confidential information such as valuable security details of the victims with the intention of redirecting a website's traffic to another bogus site. Both phishing and pharming methods are not applicable when none of authentication data is required from the server.

g.) **Replay Attack**: It is a situation where an attacker can capture the password credentials and reuse them to gain unauthorized access to 'secure' resources

Table 5 presents the analysis of some selected graphical password schemes susceptibility to possible attack methods.

.

**Table5: Comparison of Typical Graphical Passwords with Possible Attacks**

| Password Schemes | Dictionary Attack | Replay Attack | Shoulder Surfing | Tricking | Spyware | Phishing/ Pharming |
|---|---|---|---|---|---|---|
| DAS, BDAS [7] | N | N | N | N | N | N/A |
| QDAS[17] | Y | N | Y | N | N | N/A |
| PassShapes[18] | N | N | N | N | N | N/A |
| Pass-Go[13] | N | N | N | N | N | N/A |
| YAGP[20] | N | N | N | Y | N | N/A |
| GrIDSure | N | N | N | N | Y | N/A |
| PassPoints, CCP, and | N | N | N | Y | Y | Y |
| Persuasive Cued | N | N | N | Y | Y | Y |

| | | | | | | |
|---|---|---|---|---|---|---|
| Click-Points (PCCP)[23] | Y | N | N | Y | Y | Y |
| Suo's Scheme [24] | Y | Y | Y | Y | Y | Y |
| Jiminy | Y | N | N | Y | N | Y |
| Inkblot | Y | N | N | Y | N | N |
| 3D Scheme | - | - | - | - | - | - |
| Déjà vu | Y | N | Y | Y | N | Y |
| Passfaces [28] | N | N | N | Y | N | Y |
| Story | Y | N | N | Y | N | Y |
| Cognitive Authentication[30] | Y | Y | N | Y | Y | Y |
| Use Your Illusion [31] | Y | N | Y | Y | N | Y |
| Convex Hull Click scheme[29] | Y | Y | Y | Y | Y | Y |
| Graphical Password with Icons (GPI)/Graphical Password with Icons suggested by the System(GPIS)[32] | Y | N | N | Y | N | Y |

## CONCLUSION AND RECOMMENDATION

Password mechanisms are the mostly used methods for identifying users in computer and communication systems. Based on the widely known claims that human memory has remarkable capability to remember graphics and images much easier than random texts, many graphical password schemes have since been proposed as alternatives to text-based password authentication schemes that use images instead of texts. By considering three memory tasks of the users to memorize and recall their passwords, the current study classifies graphical Password schemes into three main categories; namely pure recall-based, cued recall-based, and recognition-based. In this paper, discussions were focused on the existing graphical passwords under this categorization with the view of analyzing their security strengths in terms of password entropy and resistance to conventional passwords attacks. From the comparative analysis of the password entropy of schemes, the average was computed and the results showed that pure recall-based schemes had 85 bits, followed by cued recalled-based schemes which had 46 bits while recognition-based scheme had the least average of 29 bits. This clearly shows that pure recall-based schemes would have better resistance to password space based attacks like the brute force attacks and dictionary attacks than the remaining schemes. Unfortunately, QDAS is the only pure recall-based scheme that is not vulnerable to dictionary attacks while the remaining schemes are vulnerable. Dictionary attacks suppose not be a serious issue against graphical passwords because of the large password space advantage and significant amounts of processing time required to recognize millions of byte of graphical information compared to textual information. The password scheme designers should do more in this regard to take of these two main advantages to ensure the improved and better security for graphical authentication mechanisms. Among the remaining traditional attack methods, the comparative analysis shows that shoulder surfing problem constitutes major draw back to almost all the graphical password systems. Sixteen (16) out of 21 schemes are highly vulnerable to shoulder surfing, especially the pure recall-based and cued recall-based schemes. With this weakness, it means that graphical passwords could never be securely used in environments where the view of the screen is not exclusive to the password owner at the login time. Despite the claims that graphical passwords are less susceptible to password attacks like guessing, brute force search than the text-based schemes, many of existing schemes are not working up to expectation. Another important issue of password authentication is human factor. Users generally circumvent security guidelines to achieve memorability, designers must ensure that graphical password schemes are professionally made to counteract this human affinity and achieve the equitable security and memorability characteristics. Since graphical schemes are expected to lessen the burden of human memory with the help of graphics and images, authentication scheme designers should consider graphics and images that relate to day to day life events of the users to ease memorability problem and encourage users to create secure passwords. To achieve this, designers should implement the following memory and security concepts in the design of graphical password schemes:

- Self-generation effects by making users to generate images and passwords
- Self-referencing effects by making the user to select passwords related to self
- Ageing effects of memory by making available the right images to the right age
- Breaking graphical passwords into pieces of chunks
- Memory retrieval: Remember and Know processes
- Associative-strength theory, and encoding specificity
- Suitable and reasonable password space increase
- Disguise the login process as a defense against shoulder surfing problem
- Enforce basic security control

The findings of the review show that more efforts should be intensified to achieve equitable security and memorability. It is worthwhile to notice that the outcome of this paper could be used in the research community to determine what should be done to further realize the full potentials of graphical password authentication mechanisms in computer and commutation system security.

## REFERENCES

1. Jakobsson, M. and M. Dhiman, *The Benefits of Understanding Passwords*, in *Mobile Authentication*. 2013, Springer. p. 5-24.

2. English, R., *Modelling the Security of Recognition-Based Graphical Password Schemes*. 2012, University of Glasgow.

3. Gilhooly, K., *Biometrics: Getting Back to Business*. Computerworld, May, 2005. **9**.

4. Maltoni, D., *et al.*, *Handbook of Fingerprint Recognition*. 2009: springer.

5. Suo, X., Y. Zhu, and G.S. Owen. *Graphical Passwords: A survey*. in *Computer Security Applications Conference, 21st Annual*. 2005. IEEE.

6. Biddle, R., S. Chiasson, and P.C. Van Oorschot, *Graphical Passwords: Learning from the First Twelve Years*. ACM Computing Surveys (CSUR), 2012. **44**(4): p. 19.

7. Dunphy, P. and J. Yan. *Do Background Images Improve Draw a Secret Graphical Passwords?* in *Proceedings of the 14th ACM Conference on Computer and Communications Security*. 2007. ACM.

8. Chiang, H.-Y. and S. Chiasson. *Improving user Authentication on Mobile Devices: A Touchscreen Graphical Password*. in *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*. 2013. ACM.

9. Ray, P.P., *Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices*. *Journal of Information Engineering and Applications*, 2012. **2**(2): p. 1-11.

10. Chiasson, S., *et al*. *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords*. in *Proceedings of the 16th ACM Conference on Computer and Communications Security*. 2009. ACM.

11. Zakaria, N.H., *et al. Shoulder Surfing Defence for Recall-Based Graphical Passwords.* in *Proceedings of the Seventh Symposium on Usable Privacy and Security.* 2011. ACM.

12. Zangooei, T., M. Mansoori, and I. Welch. *A Hybrid Recognition and Recall Based Approach in Graphical Passwords.* in *Proceedings of the 24th Australian Computer-Human Interaction Conference.* 2012. ACM.

13. Tao, H. and C. Adams, *Pass-Go: A Proposal to Improve the Usability of Graphical Passwords.* IJ Network Security, 2008. **7**(2): p. 273-292.

14. Jali, M.Z., *A Study of Graphical Alternatives for User Authentication.* 2011.

15. Dimitropoulos, L.K., *GrIDsure: Effects of Background Images on Pattern Choice, Usability and Memorability.*

16. Jermyn, I., *et al. The Design and Analysis of Graphical Passwords.* in *Proceedings of the 8th USENIX Security Symposium.* 1999. Washington DC.

17. Lin, D., *et al. Graphical Passwords & Qualitative Spatial Relations.* in *Proceedings of the 3rd Symposium on Usable Privacy and Security.* 2007. ACM.

18. De Luca, A., R. Weiss, and H. Hussmann. *PassShape: Stroke Based Shape Passwords.* in *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User interfaces.* 2007. ACM.

19. Weiss, R. and A. De Luca. *PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability.* in *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges.* 2008. ACM.

20. Gao, H., *et al. Yagp: Yet Another Graphical Password Strategy.* in *Computer Security Applications Conference, 2008. ACSAC 2008. Annual.* 2008. IEEE.

21. Wiedenbeck, S., *et al., PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. International Journal of Human-Computer Studies,* 2005. **63**(1): p. 102-127.

22. Chiasson, S., P.C. van Oorschot, and R. Biddle, *Graphical Password Authentication using Cued Click Points,* in *Computer Security–ESORICS 2007.* 2007, Springer. p. 359-374.

23. Chiasson, S., *et al., Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism.* Dependable and Secure Computing, IEEE Transactions on, 2012. **9**(2): p. 222-235.

24. Suo, X., *A Design and Analysis of Graphical Password.* 2006.

25. Renaud, K. and E. Smith. *Jiminy: Helping Users to Remember their Passwords.* in *Annual Conference of the South African Institute of Computer Scientists and Information Technologists. SAICSIT.* 2001.

26. Stubblefield, A. and D. Simon, *Inkblot Authentication.* Microsoft Research, 2004.

27. Alsulaiman, F.A. and A.E. Saddik. *A Novel 3D Graphical Password Schema.* in *Virtual Environments, Human-Computer Interfaces and Measurement Systems, Proceedings of 2006 IEEE International Conference on.* 2006. IEEE.

28. Davis, D., F. Monrose, and M.K. Reiter. *On User Choice in Graphical Password Schemes.* in *USENIX Security Symposium.* 2004.

29. Wiedenbeck, S., *et al. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme.* in *Proceedings of the Working Conference on Advanced Visual Interfaces.* 2006. ACM.

30. Weinshall, D. *Cognitive Authentication Schemes Safe Against Spyware.* in *Security and Privacy, 2006 IEEE Symposium on.* 2006. IEEE.

31. Hayashi, E., *et al. Use your Illusion: Secure Authentication Usable Anywhere.* in *Proceedings of the 4th Symposium on Usable Privacy and Security.* 2008. ACM.

32. Bicakci, K., *et al. Towards Usable Solutions to Graphical Password Hotspot Problem.* in *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International.* 2009. IEEE.

33. Dhamija, R. and A. Perrig. *Deja Vu-A User Study: Using Images for Authentication.* in *USENIX Security Symposium.* 2000.

34. Hu, W., X. Wu, and G. Wei. *The Security Analysis of Graphical Passwords.* in *Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on.* 2010. IEEE.

35. Eljetlawi, A.M. *Graphical Password: Existing Recognition Base Graphical Password Usability.* in *Networked Computing (INC), 2010 6th International Conference on.* 2010. IEEE.

36. Jermyn, I., *et al. The Design and Analysis of Graphical Passwords.* in *Usenix Security.* 1999.

37. van Oorschot, P.C. and T. Wan, *TwoStep: An Authentication Method Combining Text and Graphical Passwords*, in *E-Technologies: Innovation in an Open World.* 2009, Springer. p. 233-239.

38. Meng, Y. *Designing Click-Draw Based Graphical Password Scheme for Better Authentication.* in *Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on.* 2012. IEEE.

39. Shannon, C.E., *A Mathematical Theory of Communication.* ACM SIGMOBILE Mobile Computing and Communications Review, 2001. **5**(1): p. 3-55.

40. Hlywa, M., R. Biddle, and A.S. Patrick. *Facing the Facts about Image Type in Recognition-Based Graphical Passwords.* in *Proceedings of the 27th Annual Computer Security Applications Conference.* 2011. ACM.

41. Kim, H. and J.H. Huh, *PIN Selection Policies: Are They Really Effective?* Computers & Security, 2012. **31**(4): p. 484-496.

42. Nali, D. and J. Thorpe, *Analyzing user Choice in Graphical Passwords.* School of Computer Science, Carleton University, Tech. Rep. TR-04-01, 2004.

43. Khan, W.Z., *et al.*, *A Hybrid Graphical Password Based System*, in *Algorithms and Architectures for Parallel Processing.* 2011, Springer. p. 153-164.

44. Gao, H., *et al.*, *A Survey on the Use of Graphical Passwords in Security. Journal of software*, 2013. **8**(7): p. 1678-1698.

**Reference** to this paper should be made as follows: Obasan Adebola, Patrick Owohunwa, and Abdulazeez Sikiru (2014), Graphical Password Authentication Methods in Information Security. *J. of Physical Science and Innovation,* Vol. 6, No. 2, Pp. 1-20.