A Review of Graphical, Hybrid and Multifactor Authentication Systems

Hassan Umar Suru[1*], Abubakar Atiku Muslim[2], Salihu Umar Suru[3], Hussaini Umar Suru[4]

[1, 2, 3] Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Kebbi State, Nigeria

[4] Department of Industrial Safety and Environmental Technology, Petroleum Training Institute, Effurun, Delta State Nigeria

suruhassan@yahoo.com*, alatiku@gmail.com, surusalihu@yahoo.com, hsuru2000@yahoo.com

Keywords: Authentication systems, graphical authentication systems, hybrid authentication, multifactor authentication, security, usability

Abstract

Since the advent of computing systems, users have stored volumes of information on computers and computing devices and have relied on passwords for the protection of these devices and valuable information. Considerable research has thus been carried out in the field of user authentication to ascertain the best way to protect devices and data as well as the most promising options in the design of user passwords. Graphical passwords have been proposed as alternatives to text based or alphanumeric passwords that have remained the most dominant authentication methods in spite of their weaknesses. Many researchers have complemented the development of graphical systems through the merging of graphical and alphanumeric systems, while others have proposed the use of several media to collectively support single user authentication schemes. These have together brought to light newer and more sophisticated hybrid and multifactor authentication models. This paper explores the developmental trends in the evolution of graphical passwords as well as in the design and implementation of several hybrid and multifactor authentication models. The paper also discusses the main security challenges for graphical password schemes.

2.1 Introduction

Human Computer Interaction (HCI) is a multidisciplinary area in computer science that deals with the interaction between humans (users) and computers. Usable security is the branch of computer science that merges human computer interaction and computer system security. According to Patrick et al [1], the importance of human computer interaction is realized in three main areas.

These are: (1) authentication, (2) security operations, and (3) the development of secure systems. Authentication is the process of ensuring that legitimate system users are granted access to computers and computing resources and ensuring that the same is denied to illegitimate users.

Over the years, many authentication systems have developed. The oldest and most widely used of these systems are the text based or alphanumeric systems. Due to numerous problems associated with the development and use of alphanumeric systems, graphical authentication systems or graphical passwords were developed as an alternative to text based systems. These problems include the fact that text based passwords could be written down and hence get stolen by illegitimate users. They could also be intentionally or mistakenly communicated directly or across various media to illegitimate users. An important flaw in alphanumeric systems is the fact that users tend to choose passwords they could easily remember, but that could also be easily guessed. These include the use of the names of relatives or pets as passwords, as well as the use of addresses, phone numbers and birthdays in PIN based systems. In view of these issues, graphical authentication systems were proposed as alternatives to text based systems.

Various types of graphical authentication systems have been proposed, developed and investigated. Some of these systems have even been commercialized. In spite of their growing acceptance, graphical authentication systems also inherit some of the weaknesses attributed to text and PIN based systems such as guessability and observability. It has, however, been observed that the tendency to make authentication systems more secure has rendered them less usable, while that to make them more usable has rendered them less secure. Bridging the gap between usability and security in the design and development of these systems has remained elusive. Hence researchers and developers alike have suggested various ways through which graphical authentication systems could be improved. These have brought about the proliferation of hybrid and multifactor systems that have either combined graphical with other authentication factors such as text or used various media to combine several authentication factors in one authentication scheme.

This paper explores the design and development of various graphical authentication models, discusses the security and usability issues faced by each of the models and how these issues are being mitigated. An important step in this direction is the development of hybrid and multifactor authentication systems which have also been discussed in the paper.

2.2 Existing Authentication Methods

Authentication systems are classified on the basis of what is needed by the authentication protocol to be able to distinguish a legitimate from an illegitimate computer user. There are basically three methods for user authentication. These include: (a) Something a user possesses (also known as token/card based authentication), (b) Something a user knows (also known as knowledge based authentication), and (c) Something a user is (also known as biometric authentication).

Token based systems are those in which a user is provided an additional device such as a bank card, key fob or hardware token in order to authenticate. Token based system are mostly used alongside knowledge based components to complement each other and to provide additional levels of security. These systems have been greatly adopted and utilised in the past decade especially by a growing number of financial institutions.

In biometric systems, a human characteristic or trait is used in the authentication process. Many biometric authentication systems have been proposed and developed. Systems that have used human fingerprints, facial recognition, iris scan, palm scan and DNA have become ubiquitous. Behaviour based systems such as gait and gaze based systems have also been developed and studied. Although biometrics are seen to provide better security than token based and knowledge based systems, they are unreliable as 1at a stage they are likely to reject legitimate users as human physiology is like to change the biometrics due to either old age or ill health. These systems may also sometimes be slow and cumbersome. The main security issues associated with biometric systems today include ‘spoof attacks’ [2] and ‘template database leakage’ [3]. These problems involve the learning of human biometrics, especially behavioural biometrics, in order to trick computing systems into granting system access illegitimate system users as well as the tendency to steal and alter biometric data templates from computing systems in order to gain system access. Biometric systems also mostly require the attachment of additional components to traditional computing systems and handheld devices, which may often be very expensive.

Knowledge based systems are the most widely used systems today and they involve a shared secret between the system and the system user. Most knowledge based systems use alphanumeric passwords and PINs [4, 5, 6]. Quite significant research interest has been geared towards the design and development of knowledge based systems especially in relation to their strengths and weaknesses in terms of security and usability as well as acceptability among system users. Scholars have investigated the attitudes of users towards passwords selection, strength and memorability of single and multiple user passwords, and the use of passwords among large corporations [7].

Graphical passwords are a type knowledge based systems that authenticate system users through the use of images in place of the text used in alphanumeric systems and have been introduced as an alternative to text based systems in order to mitigate the numerous security and usability challenges faced by alphanumeric passwords that have remained the most dominant. There are different kinds of graphical passwords. They are classified into recognition based, recall based and cued recall based systems [8, 9].

2.3 Recognition Based Systems

Recognition based graphical authentication systems are graphical password systems that depend on the user's ability to recognise images he had seen and chosen earlier as his password from a large collection of images. Each authentication system has a registration phase in which a user is expected to register unto the system. In this phase, the user selects his chosen password images from a large collection of images. He then needs to identify and select the earlier chosen passwords in each round of authentication. In the authentication phase, the user is presented with many images including his pre-selected images from which he is expected to recognise and correctly select the images that represent his chosen password.

Many recognition based schemes have been developed and evaluated. The déjà vu scheme developed by Dhamija and Perrig [10] is a recognition based graphical authentication scheme that uses the Harsh Visualisation Technique [11] to generate abstract images using a computer algorithm (fig. 1). Although the images in the déjà vu scheme are abstract, hence they have no definite form, each image is unique, and the system stores the seed for each of the images generated so as to generate the image accurately in the future. Designers of the déjà vu scheme believe that it provided better memorability than text based passwords, its only problem being the idea that the system has to store the seeds for all images to ensure their generation in the future. An improvement to the déjà vu scheme was done in [12]. The new system used the SHA-1 harsh function. It was believed to be more secure and use less memory than the earlier version. Although in spite of its use of abstract images, the déjà vu scheme was believed to have good security as well as good usability, researchers believe that systems using images to which distinctive meanings could be attached to them will have better memorability [13]. Researchers have also compared the usability of the passfaces scheme, the déjà vu scheme and the VIP scheme with alphanumeric PINs and passwords. The researchers discovered that although déjà vu compared better to the alphanumeric PINs and passwords in terms of memorability, the efficiency of déjà vu was lower as it was slower to authenticate using the déjà vu scheme as compared to the others. Weinshall and

Kirkpatrick proposed a number of graphical schemes in [14]. Their proposed schemes used picture, object and pseudo word or language recognition with a considerably large number of images. The systems had good memorability as users could recognise their chosen images even after several weeks. The picture based implementation, however, proved to be more usable than all the others. No security experiments were performed with these systems.

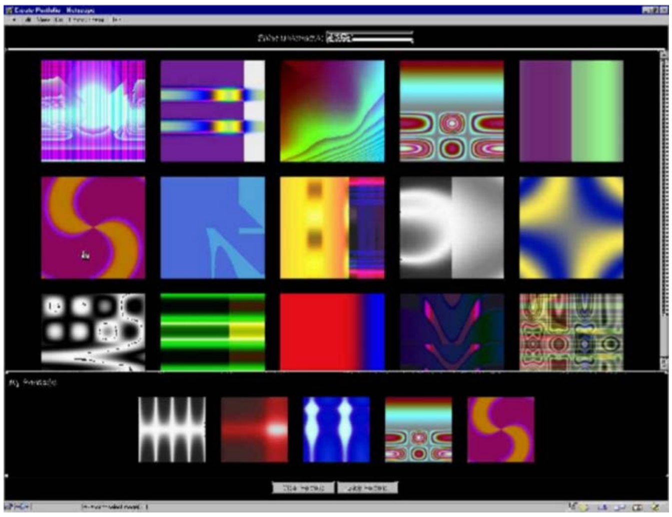


Fig. 1: Abstract images (Deja vu)

The convex hull schème was proposed by Sobrado and Birget [15] in order to counter the shoulder surfing attack. Shoulder surfing is the ability of someone to observe a user's password entry by simply looking over their shoulders [16]. In this scheme, in each authentication, a user is presented with many icons on a computer screen. He is then expected to locate his password images among many decoy images. There were three implementations of the convex hull scheme. In the first implementation, a user had to locate any three of his chosen password images and click inside the convex hull (triangle) formed by those images (fig. 2) in order to authenticate. In the second approach, the user needed to position one of his chosen images in a movable frame, and then move the frame to align with any other two of his chosen images to authenticate. In the third approach, the user had to locate any four of his chosen images and then click on the point of intersection of the invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. To decrease guessability, the researchers suggested the use of thousands of images, which in turn made the screen highly compacted thereby creating usability issues. Although the system may have good security, especially as it mitigates the problem of shoulder surfing, authentication in this system may be considerably slow due to the time it may take in locating the images, lowering the efficiency and in turn the usability of the system.

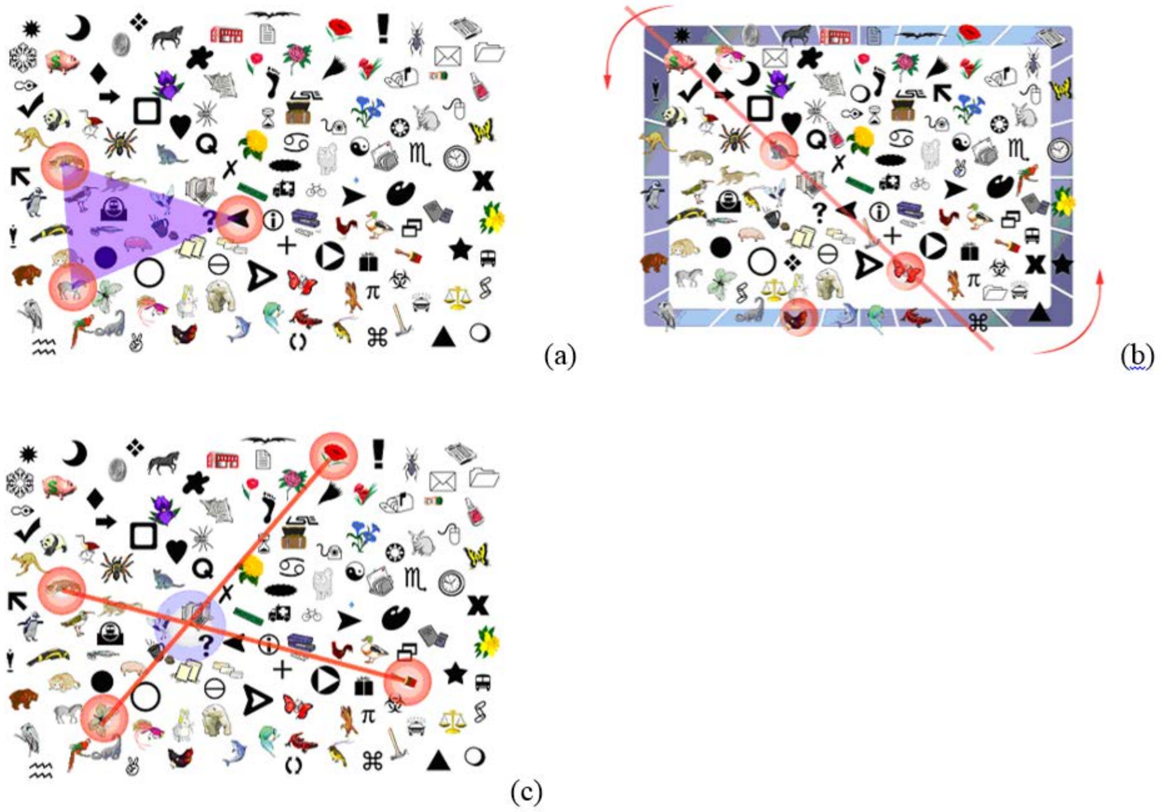


Fig. 2: Sobrado and Birget schemes [15]: a – Convex hull, b – Movable frame, c – Intersection.

An algorithm for filtering distractor (doodle) images was suggested in [17]. The algorithm was used to filter out images due to their similarities based on the number of black and white regions as well as the number of joints possessed by each image. The aim of the algorithm was to identify similarities in distractor images to be presented as decoy images in the course of authentication. The assurance that simple doodle distractor images do not possess obvious similarities with the users pass images improves usability by reducing user input errors.

In [18], Man et al. proposed a system that used image variance to counter shoulder surfing. In this system, every image had several variants and each variant was associated with a unique code. Users are presented with several scenes during each authentication round, each scene contains the user’s pass object variants randomly selected and presented among many decoy images. To authenticate, the user simply types the code associated with his pass image variant and the relative position of his pass image among decoy images as presented on a computer screen. The security advantage of the system was that it proved resistant to shoulder surfing. However, the system suffered on the usability side as users had to both recognise their images and memorise the codes for the various image variants. The idea of memorizing many things at the same time may seriously affect the memorability and overall usability of the system. An improvement to this system was, however, proposed by Hong et al [19] in which the user assigns his own codes to each of his preselected pass images (fig. 3). The need to memorise the code, although assigned by the user himself, however, meant that it suffered the same fundamental usability flaws as the system it sought to improve upon.

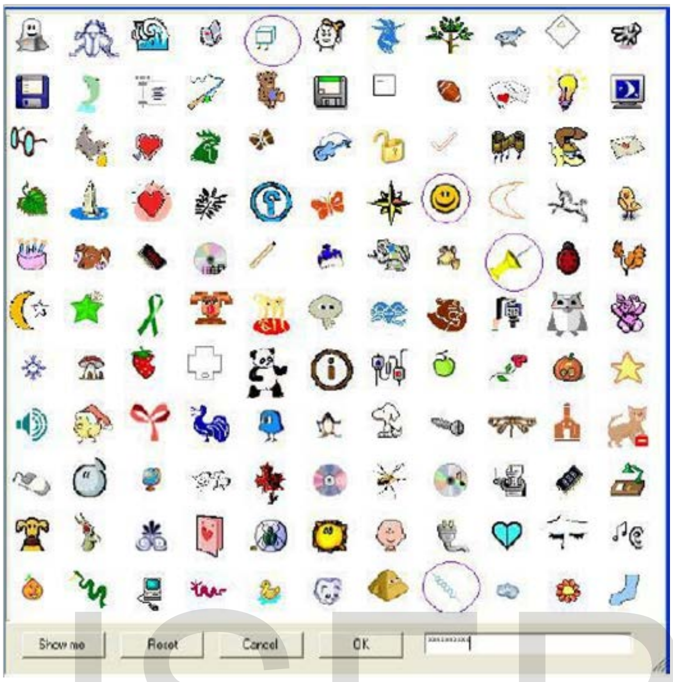


Fig. 3: Shoulder surfing resistant scheme by Hong et al. [40]

Real User Corporation [20] developed and commercialized the *passfaces* technique which used human faces as a means for user authentication. The idea came from the belief that humans find it easy to remember the faces of others even after prolonged periods of time. In the implementation of this scheme, a user is presented with a number of grids containing human faces from which he is expected to select any four faces. During each authentication round and for each authentication step the user is presented with four successive grids, each grid containing nine human faces, among these faces is one of his preselected face images and eight decoy (non-pass) images. The user is expected to recognise and select his chosen faces, one face from each grid of nine faces (fig. 4). A lot of research effort has been geared towards understanding the usability and security issues of the passfaces scheme.

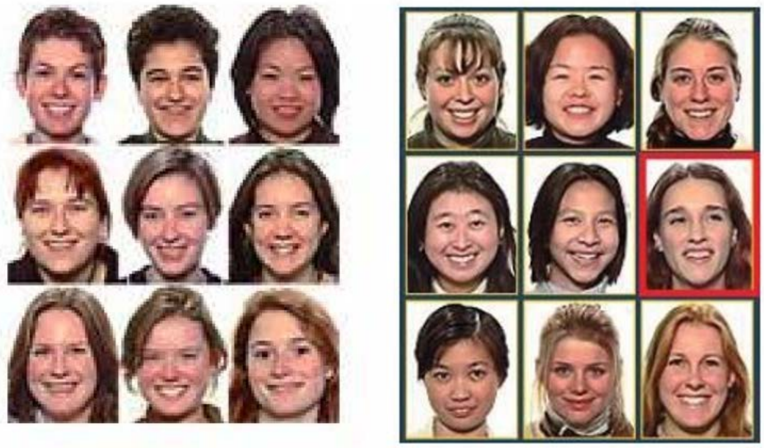


Fig. 4: The Passfaces Scheme

Memorability studies conducted on the passfaces scheme in [21, 22] have indicated that password created with the passfaces scheme could easily be remembered even after a prolonged periods of time. Studies in [23] revealed that the login failure rate of the passfaces scheme was by far less than that of text based passwords, but the login time was longer. Davis et al. [24], however, discovered predictable patterns in the passfaces scheme as users were attracted to beautiful faces, faces of members of the opposite sex as well as members of their own races. This trend in password selection creates serious predictability problems which is a serious drawback for security. System assigned passwords is suggested as a possible solution to the predictability problem. This, however, may render the system less memorable, hence negatively affecting its usability. Researchers in [25] analysed the vulnerability of the passfaces scheme to descriptions. The study was aimed towards understanding the possibility of verbal descriptions on the passfaces scheme and how such vulnerabilities could be reduced. The study discovered that passfaces could effectively be described and suggested the presentation of similar faces in a grid as an effective way of reducing facial disparity, and in turn the possibility of password description. Keyboard entry was suggested in [16] as a better alternative in the implementation of the passfaces scheme in a study that compared the security of keyboard based versus mouse based data entry in the passfaces scheme. Keyboard entry is believed to provide better security than mouse based password entry.

Jansen et al. in [26-28] proposed the theme based set of graphical passwords for mobile devices. In this schemes, a user selects images which represent various themes. These themes comprise of pictures (such as those of the sea, the forest, an animal, etc.). Each theme comprises many thumbnails of a picture which when put together will form the needed image. A user selects a number of thumbnails in a sequence within this theme (picture) as his password (fig. 5). During authentication, the user needs to select his thumbnails within the theme (image) in a definite order. The main limitation of this method was the fixed size of the mobile screen, which limited the number of thumbnails that could be used, which was a great hindrance to the efficiency and usability of the system.

Takada and Koike [29] proposed a novel graphical password scheme which used personal images. The scheme allowed a user to submit his favourite images to the server as his password. In each round of authentication, the user only needs to recognise the images he had submitted among other decoy images. Several image grids are presented to the user in each user login and the user is expected to locate and select one of his chosen images in each grid. If none of the user's images is presented on the screen, the user selects nothing. Submitting one's own images greatly improves memorability, which improves the usability of the system, but also makes it easier for an intruder who knows the user to easily guess the password [24, 30], a setback for security.

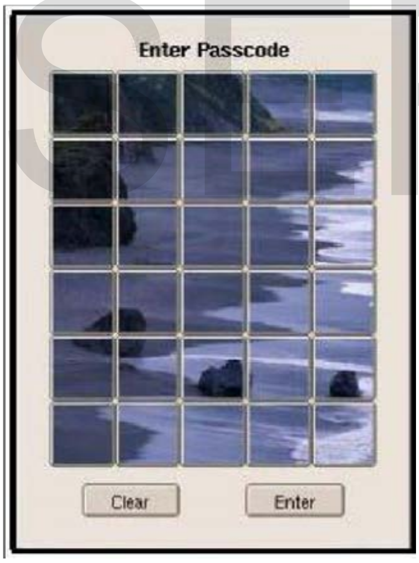


Fig. 5: Theme based graphical technique (Jansen et al.)

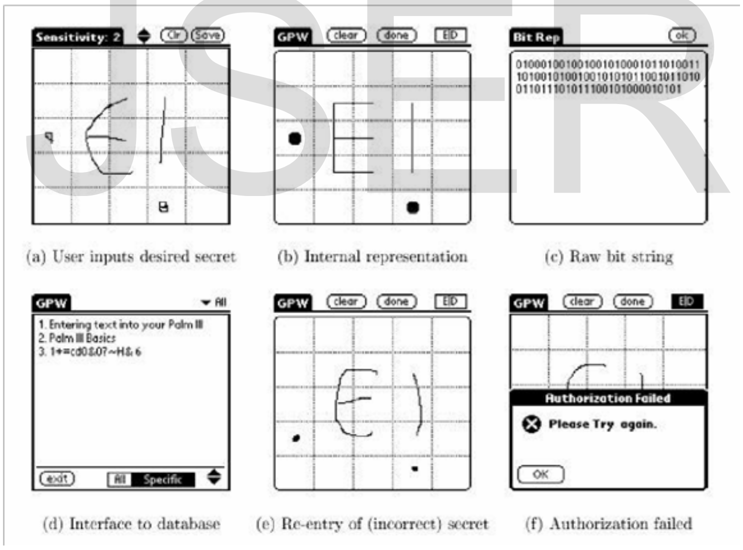
2.4 Recall Based Systems

A recall based authentication system is an authentication system in which a user performs a series of actions during the password creation stage and is expected to repeat the same actions, in the same order, during each authentication round. Recall based systems are mainly divided into two groups: (1) Pure recall based systems (2) Cued recall based systems.

2.4.1 Pure Recall Based Systems

Pure recall based systems are systems in which a user is expected to fully recall a piece of action from past memory without any aid in order to authenticate. Most of these systems present the user with a blank touch sensitive screen upon which a user is expected to reproduce an image he had drawn earlier in the password creation stage.

The *Draw a Secret* (or DAS) scheme was a technique proposed by Jermyn et al [31] which allowed users to draw their own pass images on a 2D grid using a touch sensitive screen. The coordinates of the drawn image on the grid are stored on the system in the order in which the drawing occurred. The user is expected to repeat the drawing in exactly the same order as it was drawn each time he wants to authenticate. The password space for the DAS system is larger than the text or alphanumeric password space.



```
0100010010010010100010110100011
101001010010010101011001011010
0110111010111001010000010101
```

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

Authorization Failed

Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 6: The "Draw-a-Secret" (DAS) system by Jermyn, et al. [32]

The DAS password scheme (fig. 6) is one of the researched authentication systems. Many researchers have investigated the usability and security of the DAS password scheme. One of these works was presented in [32]. In analyzing the memorable password space of DAS scheme, the researchers developed the concept of graphical dictionaries. This method was used to study the susceptibility of the DAS scheme to brute force attacks. Researchers also compared the performances of mirror symmetric and asymmetric images in the creation of DAS passwords, which led to the researchers concluding that symmetric images were more preferred and hence more used by system users, but were also less secure. Since the very idea of the tendency for symmetry user drawn images makes the passwords more predictable. The impact of stroke count on DAS password strength was studied in [33]. The researchers observed that the higher the stroke count the stronger the password. To further strengthen the DAS password, they proposed the grid selection technique (fig. 7) in which a user selects a small rectangular section of the grid as his drawing grid, which is then zoomed into before the password is created [32]. The grid selection technique significantly increased the password strength of the DAS password system. Background images were introduced to the DAS password system to improve its usability by Dunphy et al [34] in a method they called Background DAS (or BDAS). In the BDAS method, a user first had to select an image, and while the chosen image appears at the background of the DAS grid, the user draws his password image on the grid as is done in a normal DAS password (fig. 8). The researchers concluded that in spite of the apparent increased complexity, the BDAS greatly improved the memorability of the DAS password system.

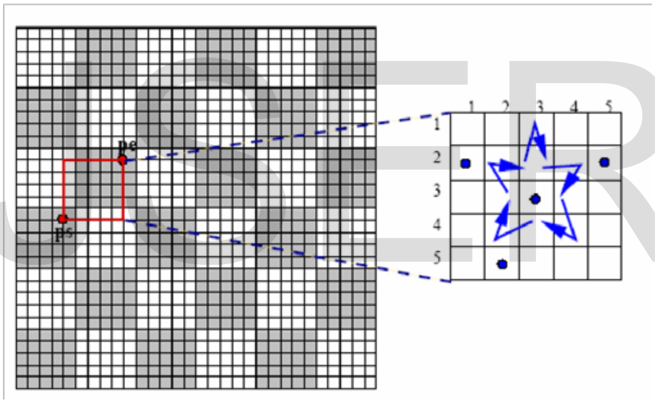


Fig. 7: Grid selection technique [33]

The *passdoodle* technique (fig. 9) was proposed by Goldberg et al [35] is similar to the DAS technique. In the passdoodle scheme, a user produces a small design or text on a touch screen which does not have a grid. The researchers observed that users could accurately remember how they drew complete graphical images, although they mostly forget the order in which the various components of the image were drawn in the registration phase.

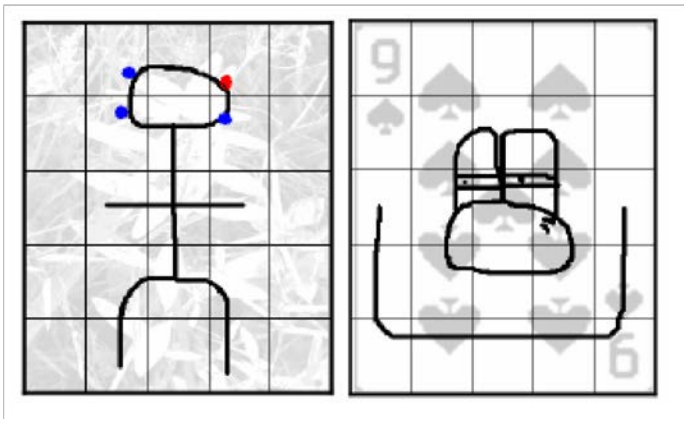
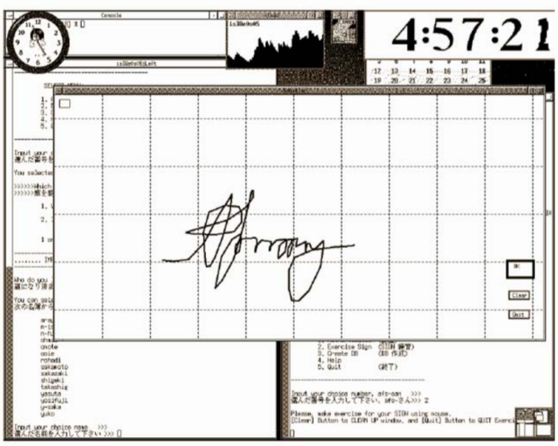


Fig. 8: The Background DAS (BDAS) scheme [34]

Fig. 9: An image in the passdoodle scheme [35]

A study was conducted in [36] to determine the predictability of the DAS password scheme. In spite of the fact that the DAS was seen to lack predictable patterns, it was observed that it was possible to compromise DAS passwords since both the beginning and end points of the password strokes contained characteristics such as rectangles, letters, numbers and that users generally preferred passwords that could be easily guessed in favour of memorability.



```
onote
ooie
rohadi
sakamoto
sakazaki
shigeki
takashig
yasuta
yosifuji
y-saka
yuko
Input your choice name.  >>>
選んだ名前を入力して下さい >>> 
```

```
2. Exercise Sign  (SIGN 練習)
3. Create DB      (DB 作成)
4. Help
5. Quit           (終了)

Input your choice number, afs-san  >>>
選んだ番号を入力して下さい, afs-さん>>> 2

Please, make exercise for your SIGN using mouse.
[Clear] Button to CLEAN UP window, and [Quit] Button to QUIT Exerci
```

Fig. 10: The signature scheme

Researchers in [37] proposed the signature scheme. The signature scheme is similar to the DAS scheme except that the user's signature is drawn in the grid (fig. 10) in place of hand drawn images used in the DAS scheme. The coordinates of the user's signature are stored on the system and confirmed by a further verification stage before any rounds of authentication. The signature scheme is believed to be both usable and secure. The success of the scheme is brought about by the fact that users did not have to memorize their signatures. Users could also replicate their signatures with almost exact precision. The signature scheme, however, needed proficiency with the stylus as well as the need for additional devices. Moreover, some tolerance threshold needed to be set as the password is captured. When the tolerance threshold is large, it improves upon the usability of the system while its security is compromised, and when the tolerance threshold is small, it improves upon the security of the systems while the system's usability is compromised.

Pass-Go is a graphical authentication system (fig. 11) developed in [38] in which a user connects the points of intersections of grid lines as his password. Pass-Go is believed to be similar to the DAS password scheme in terms of protection against shoulder-surfing, phishing and social engineering.

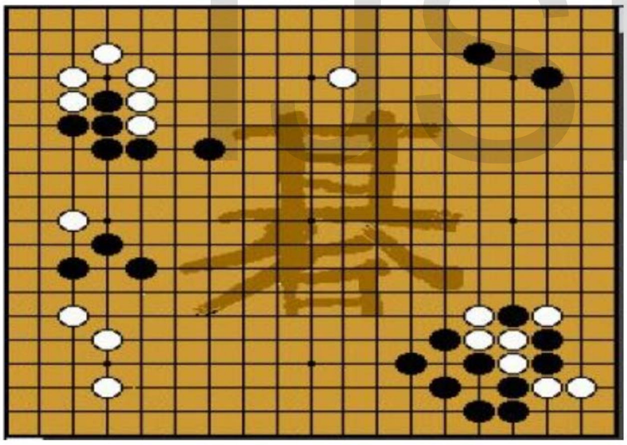


Fig. 11: The Pass-Go system

2.4.2 Cued Recall Based Systems

In cued recall based authentication systems, an image is normally presented unto which a user is expected to 'mark' or designate certain locations of the image (normally click points) as his password during each authentication round. The image itself serves a *cue* and assists a user in recollecting the exact points selected by the user as his password. In pure recall based schemes, such as the signature and the DAS schemes, activities are done on an empty grid. The idea of click points was first proposed by Blonder [39]. In his design (fig. 12), an image was displayed on a computer screen which had predefined click points. The user had to click on these points in a definite order to register and continue to click on these exact points in the same order as in the registration phase each time he authenticates. As in the pure recall based systems, some tolerance threshold is, however, provided for each click point.

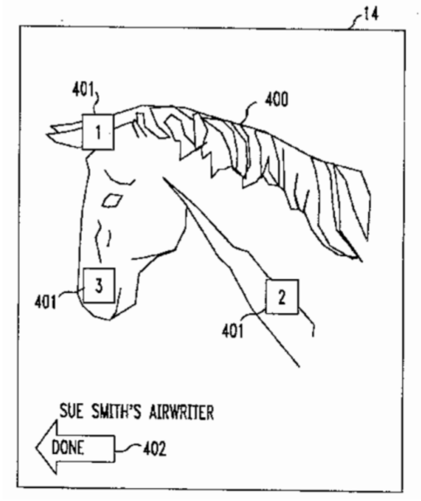


Fig. 12: Blonder's scheme

A scheme based on repeating a series of actions (fig. 13) was developed by Passlogix [40]. In the Passlogix V-Go, a user had to choose a number of activities that are linked such as preparing a meal or picking of cards as his password. The variation of grid sizes for grid based systems during each authentication round was suggested by researchers in [41] as a counter measure against the shoulder surfing attack. This has not, however, been found to have any significant effect on the vulnerability of these systems to observational attacks. Microsoft in [42] was also reported to have proposed a graphical scheme in which users click on predefined areas on an image to register and authenticate. No details of this system were, however, made public.

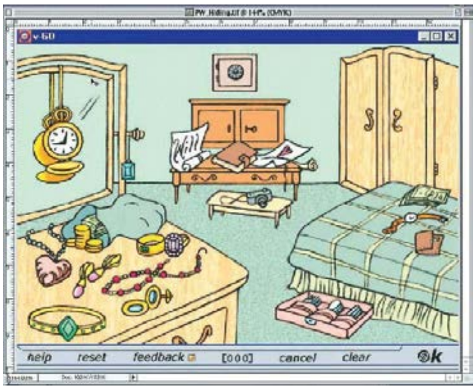


Fig. 13: The Passlogix scheme

Weidenbeck *et al* [42-44] improved upon Blonder's method through the elimination of fixed boundaries and the use of different images. In their models (fig. 14), a user was allowed to click on any part of an image in any order to form his password. Like in the other cued recall based methods, some tolerance allowed for each click point. The system adopted the quantization method proposed in [45] and with hundreds of click points to click from, the system possesses a very large password space. Researcher in [46] developed a system called *cued click points* (fig. 15) in which several click-based images were used with one click point per image. A lab based test with 24 participants revealed that the system was good both on the sides of usability and security. The study, however, suggested further investigation into the memorability of this systems and the problem of hotspots through more elaborate and longitudinal trials. The effects of tolerance and image choice were studied in [43] and while it was observed that tolerance could be used to improve user success rates, image choice was seen to make very small difference. The study also revealed that countless images could be used in the implementation of the passpoints scheme. Further studies conducted in [44] showed that graphical passwords were stronger than text passwords, although user training involved in the use of graphical passwords may also take longer. The problem of hotspots in picture based passwords was studied in [47]. The study proved that all click based password were predictable and hence vulnerable.

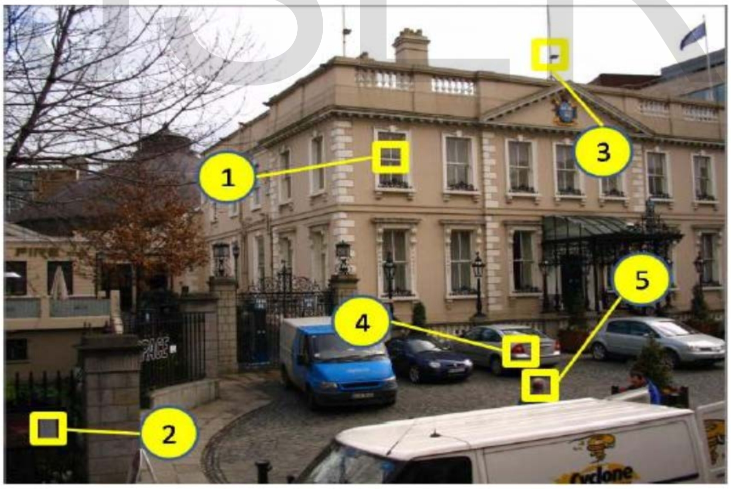


Fig. 14: The Passpoints scheme by Weidenbeck et al.

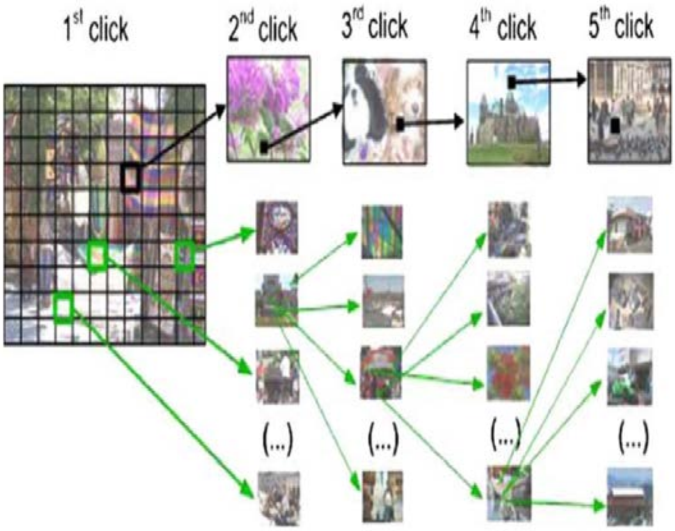


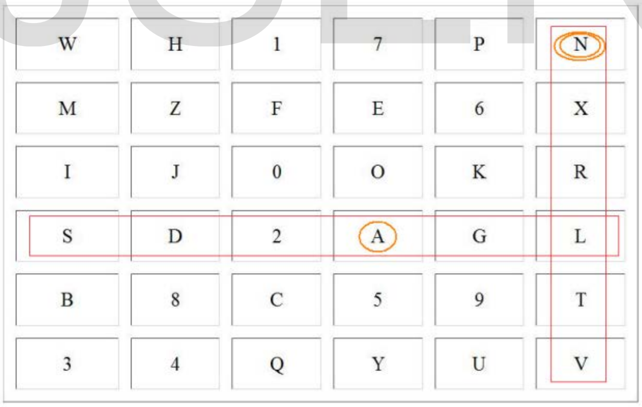
Fig. 15: Cued Click Points Scheme

According to [42], a system of navigation through a virtual world for authentication was proposed by a man named Adrian Perrig. In this system, users could randomly create virtual environments and be authenticated by navigating through the virtual spaces. Although researchers believe it may have the potentials of creating strong passwords, there is no documentation detailing the design and development of this system. The use of mnemonics to aid recall have also been studied in [48], where the use of mnemonics was incorporated into a number of graphical systems. Their study proved that mnemonics could aid even the recall of multiple graphical passwords. The use of mnemonics and degraded images in a recognition based system was also studied in [49, 48]. This scheme, which borrowed its ideas from the story scheme, used a trace line across both the user's pass-images and the distractor images, to safeguard against the shoulder-surfing problem. In the story scheme, a user is presented with many images from which to select his pass-images. In doing this, however, he creates a story that links the images and assist in the memorability of the user passwords. In each authentication round, the user uses the story earlier created to remember his chosen images and to authenticate.

In several studies, the combination of several graphical passwords has been explored. In [50], the researchers deployed the use of a recognition based system in the first stage and a recall based system in the second stage. A set of questions (three, specifically) were associated with the recall based phase. The questions help the user in identifying his click points as the click sequence is randomized in each authentication round.

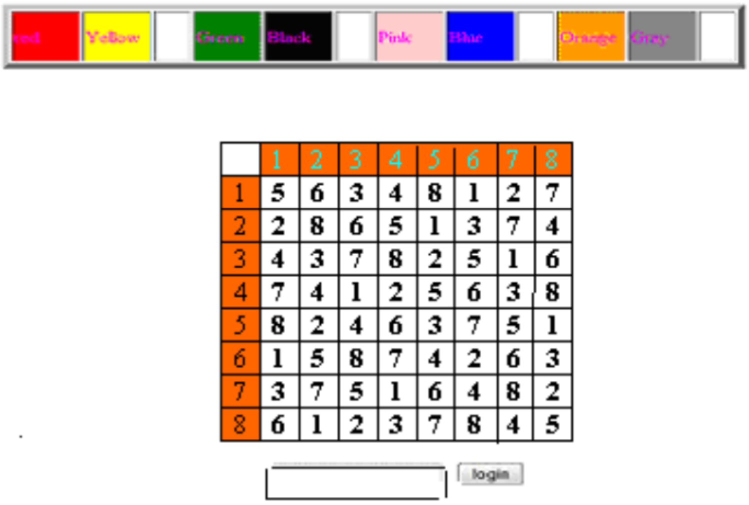
2.5 Hybrid Authentication Schemes

A number of hybrid authentication systems have been developed. These are systems that combine the elements of recall and recognition based authentication systems or text and graphical authentication systems in order to benefit from the usability and security advantages of both systems [51, 52]. A hybrid system for the generation of session based passwords was presented in [51] and [53], and extended in [54]. The system combines graphical and text based authentication schemes, and during registration, a user needs to select both a graphical and a text based password. To authenticate, the user has to correctly enter both the graphical and text based passwords. Two implementations of the system were proposed. In the first implementation, the user is presented with a text grid (fig. 16) from which the user choses his password from an intersection of the various rows and columns of the grid which represent his password, while the second implementation suggested the ranking of colours, both of which the user has to remember accurately. The mixing of upper and lower case letter and augmentation with special characters was suggested for the text-based password. The registration phase for this model is presented in figure 17. Although the system is believed to be resistant to most common password security attacks, there is high likelihood that the system will suffer from usability issues. A usability evaluation has, however, not been conducted.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 16: Intersection letter for the passwords pair ‘AN’.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig. 17: Authentication grid and associated colour pairs [51]

Another hybrid graphical scheme is presented in [52] which incorporates a recognition based scheme with dynamic graphics. In this scheme, during the registration process, a user is presented with a 4x4 grid of images from which he selects his chosen password images. Below each image, however, is a random three digit number, and at the bottom of the image grid is a text box. On selecting an image, the user needs to enter the three digit code for his chosen image in the text box. At the end of the selection of all password images, the textbox contains a string of digits which represent the user's password that is saved by the system. The user thus has to remember the exact order in which the password images were chosen.

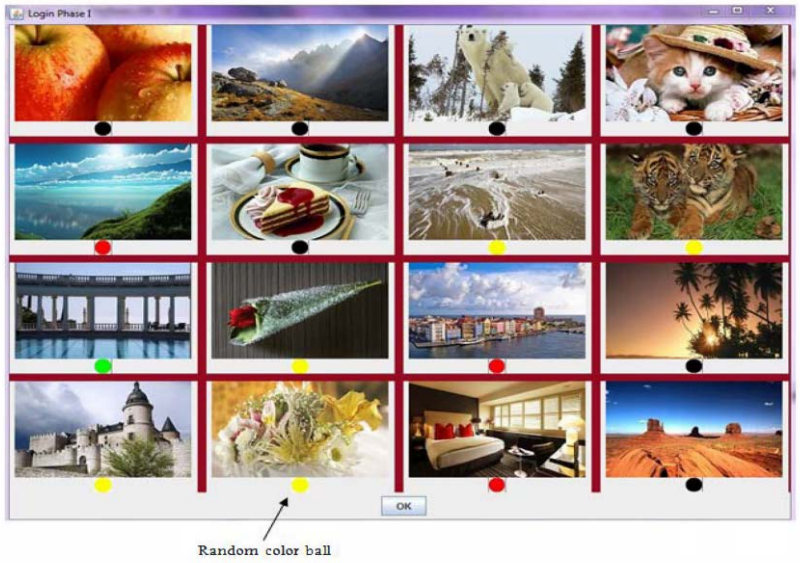


Fig. 18: The first authentication phase, 4x4 grid and associated colour balls

The authentication phase for this system is divided into two phases for each of the chosen password images. In the first phase, the user is presented with a 4x4 grid (fig. 18) to select his password images. Associated with each of the images and below each image is, however, a colour ball. The user has to both recognise each of his chosen images in the grid as well as remember their associated colour balls. The colour balls associated with each image are randomly assigned per session. In the second authentication phase (fig. 19), the user is presented with a 16x1 grid also with a colour ball associated with each of the images. The colour ball associated with each image in the grid is, however, randomly reassigned according to a specific timeframe. The user has to recognise his first selected image and its associated colour ball in phase one and click on this image in phase two only at the time when the colour ball bears the same colour as that associated with it in phase one. The user then repeats phase two for all of his remaining images.

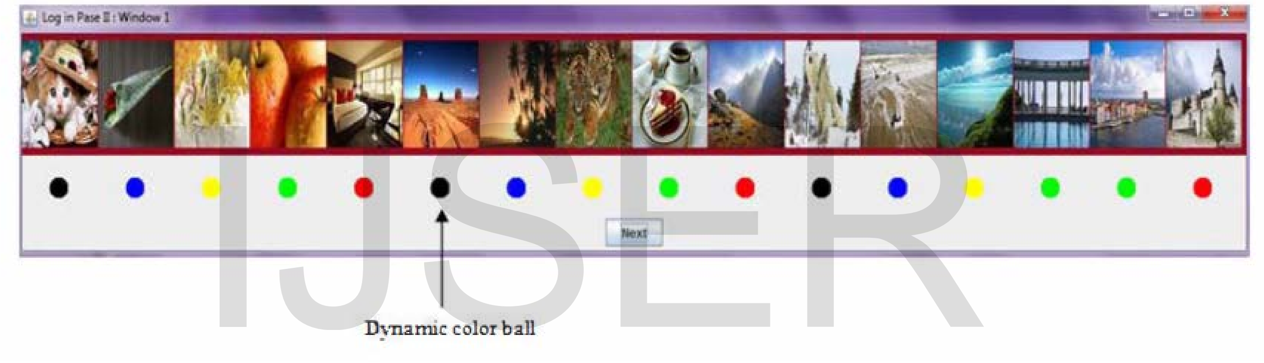


Fig. 19: The second authentication phase, 16x1 grid and associated colour balls

In this scheme, when images are presented in the grid for authentication in the first phase, a user is not expected to select any image, but to only observe the colour of the ball below the images. The actual image selection is done in the second phase. This provides extra security to the system as an onlooker may not even understand that the first phase is actually a part of the authentication process. According to the researchers, the system has a large password space, high entropy and is resistant to most common password intruder attacks. Another parameter that enhances the security of this system is the time window within which a user has to select the image in the second phase when the coloured ball for the image seen in the first phase appears.

According to the researchers the system had both good usability as well as good security as it was both easy to use and to remember as well as being resistant common security attacks. One would expect, however, that the need to memorize a set of images selected by the user in the registration phase as well as the colour balls allocated to them in the first authentication phase as well as the need to interact with two separate grids in the system's authentication phase creates additional concerns on the usability of the system.

Many other hybrid graphical authentication systems have also been proposed. In [55], a system that uses shape and text is proposed. The system combines a traditional text based password with a shape drawn on a grid as in the DAS scheme. Although the system is believed to be strong against shoulder surfing and brute force attacks, the researchers themselves agree that the system suffers from several usability flaws. Another hybrid model is presented in [56] which combines a traditional password based authentication system with a recognition based graphical authentication system. The registration phase for the text and graphical passwords are done normally. A user enters his text based password which consists of alphanumeric and special characters and then selects a number of images from an image grid. In the authentication phase, the user enters his alphanumeric password and then selects his chosen images from an image grid provided for the selection of the images. The image grid is, however, slightly different from the traditional image grid in which a user needs to click on his password images to select them. In the image grid for this system, below each image is assigned a unique number (fig. 20). This number is randomly assigned and changes in each authentication round. A selection panel is provided at the bottom of the image grid in which the numbers are arranged in ascending order from the smallest to the largest. A user selects an image by clicking on its corresponding digit in the selection panel. Hence a user does not need to click directly on an image to select it, but to click on the digit that represents it in the selection panel. This is a strong mechanism against shoulder surfing attacks. The selection panel also helps a user keep track of the various pass images he has already selected as the selected digits in the selection panel remain highlighted till the end of the authentication process. Although the system is believed to be strong against common password security threats, actual user studies to verify and analyse its security and usability potentials had not been conducted.

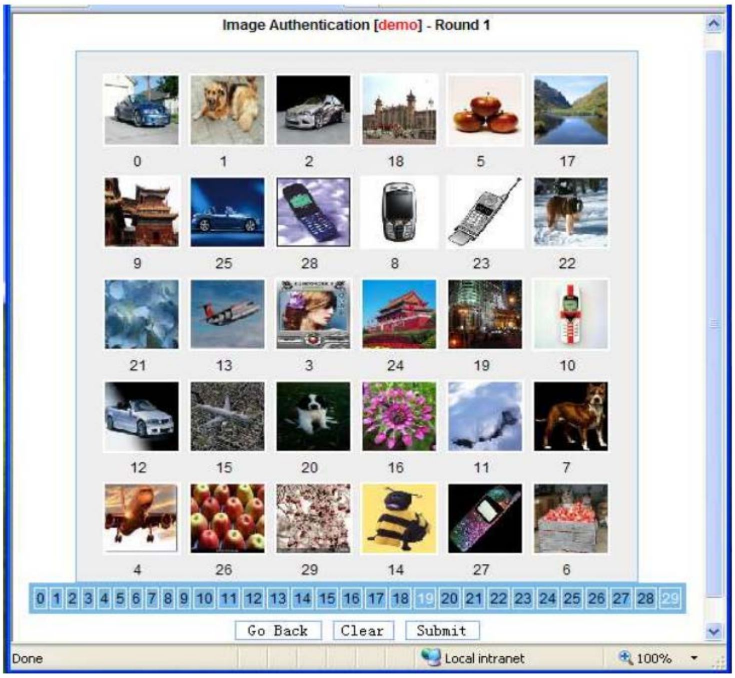


Fig. 20: Selection panel for graphical authentication

2.6 Multifactor Authentication Schemes

Section 2.2 discussed the various authentication methods through which a legitimate user can authenticate unto a computing device. These include; token based authentication, biometric authentication and knowledge based authentication. Two factor authentication involves the use of any two of these methods in a single authentication system. A typical example is in the use of the bank ATM machine. The ATM smart card serves to provide the user ID and helps the machine understand which account(s) are being accessed. The user then enters his PIN (Personal Identification Number) to show that he/she is the legitimate owner of the designated account. Several authentication systems have been developed that adopt the two factor paradigm for user authentication. The most common of these systems include the use of smart cards [57] for physical access mechanisms, hardware tokens and OTP (One Time Password) for mobile and online applications. The most common security problem with smart-card based systems is the *offline guessing attack* [57]. The greatest usability problem associated with multifactor authentication systems is the need to carry additional device. Systems that combine biometric authentication such as fingerprint recognition with tokenised devices have also been proposed [58]. In [59], however, a gait based two factor system for mobile devices was proposed. Other researchers have proposed the use of three factor [60] and four factor [61] authentication systems as a means of improving upon the security of two factor authentication techniques. This increased complexity may, however, add increased constraints on the usability of the systems.

2.6 Main Security Challenges for Password Systems

A number of threats have significantly affected the use of text-based passwords. The exact extent of the effects of these threats on graphical passwords is not fully understood as the deployment of graphical passwords in real user environments is still undergoing research and is in its infancy. The threats include the following:

Brute Force Attack: Brute force attack is the use of the brute force search algorithm to try all possible combinations of user passwords to gain access to a user's account. Since passwords are a combination of letters, numbers and special symbols, brute force attacks take a considerably long period of time. Hence, having a considerably large password space is a good defense strategy against brute force attacks. Graphical passwords are believed to be more difficult to compromise than text based techniques as they are believed to possess a similar or sometimes even larger [34, 37, 45, 62] password spaces. Recall based techniques normally have larger password spaces than both the text and recognition based techniques. The dependency on mouse movements makes graphical passwords more resilient to brute force attacks than text based methods.

Dictionary Attack: A dictionary attack is a password security threat in which the attacker repetitively tries a list of words, called a dictionary to gain access to a computing system. Unlike a brute force attack that uses all possible combinations, a dictionary attacked uses a list of weak passwords that are insecurely used as passwords by system users. Although it is believed that dictionary attacks could be used against some recall based graphical passwords [37], it is definitely more complex to execute especially as they mostly involve the use of the mouse and not the keyboard.

Guessing Attacks: The ability to guess a user’s password is common in text passwords and is further simplified by having some information about the user. Forming passwords with the names of family members or pets and known places or dates is therefore highly discouraged. Guessing is also possible in user defined passwords and password systems with predictable patterns such as the passfaces scheme [20] in which users select beautiful faces, faces of the opposite sex and of members of their own race. The DAS system [31] also showed predictability especially in symmetric and non-symmetric images, according to [36].

Spyware Attack: Spyware are mischievous programs or devices intended to "spy" or gather sensitive information from any system to which they are attached. They are normally used to spy on persons or organisations and may retransmit the information gathered to a third party. Keyloggers are hardware and software designed to keep track of and automatically log user keystrokes onto external media, while mouse trackers are software and hardware designed to capture and store mouse or cursor movement on the screen. Although, it is believed that keyloggers cannot be used against graphical passwords [18, 19], mouse trackers are seen as a potential risk.

Shoulder Surfing Attack: Shoulder surfing is the ability of an intruder to obtain useful password information by simply observing the user's actions from across the user's shoulder. Shoulder surfing is a potential risk in most graphical schemes [18, 19].

Smudge Attack: Most android phones and other mobile devices today use a form of authentication called a pattern lock [63] in which a user tracks a set of dots on the screen. The use of this system may sometimes lead to the pattern becoming traceable due the formation oily deposits on the face of the phone over time. This pattern ‘smudge’ can be used by attackers as investigated by [64].

Social Engineering Attack: Social engineering is the ability to fraudulently obtain useful information from a person through pretext. Social engineers exploit human attributes of love, fear, respect, trust and pity to deceive system users into divulging sensitive information which they later use to gain access into applications or devices. Phishing is the ability to impersonate an entity such as a bank to obtain personal security details from users. For password systems, however, social engineering is effective only if a user password could be described.

Vulnerability to Description: Vulnerability to description is the ability to clearly describe, verbally or in writing, the characteristic features of a user password. Text based passwords can mostly be effectively described, and it is a main concern that many graphical passwords can also be described. Vulnerability to verbal and written descriptions of various image types used as authenticators was studied in [25, 65].

2.6 Conclusion and Future Work

Graphical authentication systems have been introduced as an alternative to text based systems that have been the most dominant authentication system for both data and device protection. This need has been greatly driven by the insecurity of text based passwords, especially due to their vulnerability to observational attacks. In spite of the growing acceptance, however, graphical systems have inherited some of the vulnerabilities associated with text based passwords. In the last few decades, considerable research effort has been geared towards the design and development of more robust and more secure graphical authentication systems.

This paper has examined the trend in the gradual growth and proliferation of graphical authentication systems and the efforts being made to improve upon their usability and security. It has, however, been difficult to efficiently combine or to improve upon both the security and usability of these systems. Hence researchers have sought the combination of authentication models or authentication factors in order to bridge the security/usability bottleneck, hence the development of hybrid and multifactor system.

Considerable work is still needed to effectively compare the designs and performances of various authentication systems, as new systems are continuously developed. This is in part due to the fact that the various system designs vary. The evaluation of these systems and the tools that are used for these evaluations as well as the result data analysis have also varied. It will be interesting to discover new ways, methods and standards though which these systems can be effectively evaluated.

References

[1]. S. Patrick, A. C. Long and S. Flinn "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[2]. Gafurov D., Snekkenes E. and Bours P. “Spoof attacks on gait authentication system”. IEEE Transactions on Information Forensics and Security, 2(3), Special Issue on Human Detection and Recognition. 2007

[3]. M. Babaeizadeh, M. Bakhtiari and A. M. Mohammed “Authentication Methods in Cloud Computing: A Survey” Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015

[4]. E. Hayashi and J. I. Hong, “A Diary Study of Password Usage in Daily Life,” In *Proceedings of the 29th Annual Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada, May 2011.

[5]. M. D. H Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, “Towards identifying usability and security features of graphical password in knowledge based authentication

technique". In *Modeling & Simulation,. AICMS 08. Second Asia International Conference on* (pp. 396-403). IEEE, May 2008.

[6]. G. Devansh "A new approach of authentication in graphical systems using ASCII submission of values."*Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017.

[7]. H. Zhao and X. Li "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme." In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on* (Vol. 2, pp. 467-472). IEEE, May 2007.

[8]. S. Saeed and M. S. Umar. "A hybrid graphical user authentication scheme." In *Communication, Control and Intelligent Systems (CCIS)*, (pp. 411-415). IEEE. November, 2015.

[9]. P. Dunphy, A. P Heiner, and N Asokan. "A closer look at recognition based graphical passwords on mobile devices". In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 3). ACM, July, 2010.

[10]. R. Dhamija and A Perrig "Déjà Vu-A User Study: Using Images for Authentication" In *USENIX Security Symposium* vol. 9, August, 2000.

[11]. A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.

[12]. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," In *Proceedings of Midwest Instruction and Computing Symposium*, 2004.

[13]. S. Chowdhury and R. Poet "Comparing the usability of doodle and Mikon images to be used as authenticators in graphical authentication systems". In *Proceeding of Conference on User science and Engineering, pp. 54-58, 2011*

[14]. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, pp. 1399-1402., 2004

[15]. L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[16]. F. Tari, A. Ozok and S. H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords". In *Proceedings of the second symposium on Usable privacy and security* (pp. 56-66). ACM. July, 2006.

[17]. R. Poet and K. Renaud. “A Mechanism for Filtering Distractors for Graphical Passwords”. In 13th Conference of the International Graphonomics Society Melbourne, Australia, volume 11, pg 14, 2007

[18]. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[19]. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2004.

[20]. Passfaces: Two factor authentication for the enterprise". [Available online] at www.realuser.com, (Accessed July 2015)

[21]. T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London, 1998.

[22]. T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London, 1999.

[23]. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in *People and Computers XIV - Usability or Else: Proceedings of HCI*. Sunderland, UK: Springer-Verlag, 2000.

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

[25]. P. Dunphy, J. Nicholson, and P. Olivier. "Securing passfaces for description." In *Proceedings of the 4th symposium on Usable privacy and security*, pp. 24-35. ACM, 2008.

[26]. W. Jansen, "Authenticating Mobile Device Users through Image Selection," in *Data Security*, 2004.

[27]. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[28]. W. A. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[29]. T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images," In *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[30]. X. Suo, Y. Zhu and G. S. Owen Graphical passwords: A survey. In *21st annual Computer security applications conference* (pp. 10-pp). IEEE, 2005.

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

[32]. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," In *Proceedings of the 13th USENIX Security Symposium*. San Deigo, USA: USENIX, 2004.

[33]. J. Thorpe and P. C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *20th Annual Computer Security Applications Conference (ACSAC)*. Tucson, USA. IEEE, 2004.

[34]. P. Dunphy, Paul, and J. Yan. "Do background images improve Draw a Secret graphical passwords?" In *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 36-47. ACM, 2007.

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

[36]. D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada, May 2004.

[37]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," In *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer- Verlag Lecture Notes in Computer Science (1438), pp. 403441, 1998

[38]. T. Hai. “Pass-Go, a new graphical password scheme.” PhD Thesis, University of Ottawa (Canada), 2006.

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

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

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

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

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

[44]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system, "*International Journal of Human Computer Studies 63*(1), 102-127, 2005 .

[45]. J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," *Cryptology ePrint archive*, 2003.

[46]. S Chiasson, van P. C. Oorschot, and R. Biddle. "Graphical password authentication using cued click points". In *Computer Security–ESORICS 2007* (pp. 359-374). Springer Berlin Heidelberg, 2007.

[47]. P. C. van Oorschot and J. Thorpe. "Exploiting predictability in click-based graphical passwords". *Journal of Computer Security:* 19(4):669–702, 2011.

[48]. W. Moncur, and G. Leplâtre. "Pictures at the ATM: exploring the usability of multiple graphical passwords". In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 887-894). ACM. April, 2007.

[49]. S. Chowdhury, R. Poet and L. Mackenzie. "A study of mnemonic image passwords." In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*, pp. 207-214. IEEE, 2014.

[50]. A. Haque and B. Imam “A New Graphical Password: Combination of Recall and Recognition Based Approach” International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 8, No:2, 2014

[51]. M. Sreelatha, M. Shashi, M. Anirudh, et al. “Authentication schemes for session passwords using color and images.” In *International Journal of Network Security & Its Applications, 3*(3), 111-119. 2011.

[52]. S. Saeed and M. S. Umar “A hybrid graphical user authentication scheme”. In *Communication, Control and Intelligent Systems (CCIS),* (pp. 411-415). IEEE, November 2015.

[53]. N. P. Sachin, D. V. Panjabi “An Overview: Passwords using Text, Color and Images Techniques Discussion, Implementation and Comparison”. In *International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Computer Technology* NCETCT, 2014.

[54]. M. S. Tidke, M. N. Khan and M. S. Balpande “Password Authentication Using Text and Colors.” *Computer Engneering, Rtm Nagpur University, Miet Bhandara*. 2015.

[55]. Z. Zheng, X. Liu, L. Yin and Z. Liu “A Hybrid Password Authentication Scheme Based on Shape and Text”. *JCP*, *5*(5), 765-772. 2010

[56]. P. C. Van Oorschot, and T. Wan “TwoStep: An Authentication Method Combining Text and Graphical Passwords”. *MCETECH*, 233-239. 2009.

[57]. G. Yang, D. S.Wong, H. Wang, and X. Deng (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160-1172

[58]. A. T. B. Jin, D. N. C. Ling and A. Goh, “Biohashing: two factor authentication featuring fingerprint data and tokenised random number.” *Pattern recognition*, *37*(11), 2245-2255., 2004.

[59]. T. Hoang and D. Choi “Secure and privacy enhanced gait authentication on smart phone.” *The Scientific orld Journal*, 2014.

[60]. S. Abu-Nimeh, “Three-Factor Authentication.” In *Encyclopedia of Cryptography and Security* (pp. 1287-1288)., Springer, US. 2011.

[61]. J. Brainard, A. Juels, R. L Rivest, et al. “Fourth-factor authentication: somebody you know”. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 168-178). ACM. October, 2006.

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

[63]. W. C. Summers and E. Bosworth. "Password policy: the good, the bad, and the ugly." In *Proceedings of the winter international symposium on Information and communication technologies*, pp. 1-6. Trinity College Dublin, 2004.

[64]. E. von Zezschwitz, A. Koslow, A. De Luca and H. Hussmann. "Making graphic-based authentication secure against smudge attacks". In *Proceedings of the International Conference on Intelligent User Interfaces 277–286.*, 2013.

[65]. S. Chowdhury, R. Poet, and L. Mackenzie "Exploring the Guessability of Image Passwords Using Verbal Descriptions". In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 768-775). IEEE, July 2013.