Review of Graphical Authentication Models and User Studies

Hassan Umar Suru*, Abubakar Atiku Muslim, Salihu Umar Suru, Hussaini Umar Suru

Abstract— Authentication is the process of ensuring that access to computing systems and resources is granted only to legitimate system users. Many authentication systems have been proposed and tested. The most common authentication involve the use of alphanumeric text. Alphanumeric systems, however, have many weaknesses that systems make them insecure as a means of user authentication. Users tend to select passwords they can easily remember, but that can also be easily guessed. Hence researchers proposed the use of graphical passwords as alternatives to text based systems. Graphical passwords are authentication systems that employ the use of images in place of alphanumeric text. This paper explores and compares various graphical authentication system approaches that have been proposed and implemented based on user studies. The paper also looks at the various usability and security studies conducted for these methods as well as the various security threats and vulnerability issues for these approaches.

Index Terms— Graphical Authentication, Cued Recall, Recall Based, Recognition Based, Security, Usability.

1 INTRODUCTION

AUTHENTICATION systems are developed and classified according to the authentication factor, that is, the method by which a user authenticates onto the system. According to [1,2], these methods include:

Something you have (Token based authentication)

Something you are (Biometric authentication)

Something you know (Knowledge based authentication)

Token based authentication systems use devices such as bank cards, key fobs, and hardware tokens given to systems users for the purpose of authentication. Token based systems such as banking platforms and ATM machines are, however, mostly complemented with a knowledge based component.

Biometric authentication systems utilise human traits and characteristics for user authentication. Such systems use human face recognition systems, fingerprint recognition, palm scan, iris scan, and DNA sequencing and other genetic and trait based characteristics for the control of computing system and resource access control. Gait and gaze based biometric authentication systems have also been developed. Among all authentication systems, biometric systems provide the highest level of security, they however, mostly have usability issues such as being slow and sometimes unreliable, as human characteristics and physiology may change with time due to old age, ill health or injury. Security issues related to biometric authentication systems include 'spoof attacks' [3], which are attacks in which the attacker masquerades himself as a legitimate user by stealing a user's biometric traits and 'template database leakage' [4], where the database template containing users' biometric identities is stolen. These systems also mostly require the attachment of external components to computing systems such as scanners and small handheld devices, which are often very expensive.

Knowledge based systems are the most widely used systems today. These systems make use of information only known to the user as a means of user authentication. Text based systems that use alphanumeric text and PINs as means of user authentication are the most common of these approaches [5,6,7]. Immense research and considerable body of knowledge has been built around the usage and performance of knowledge based systems including that on people's attitudes towards the selection of passwords, the strength and memorability of user chosen passwords, the number of passwords possessed by users, and the use and vulnerability of passwords in corporations [8]. Graphical passwords were developed as alternatives to text based passwords and are

- *Hassan Umar Suru, Abubakar Atiku Muslim and Salihu Umar Suru are all lecturers in the Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Kebbi State, Nigeria*
  E-mails: suruhassan@yahoo.com, alatiku@gmail.com, surusalihu@yahoo.com
- *Hussaini Umar Suru is a lecturer in the Department of Industrial Safety and Environmental Technology, Petroleum Training Institute, Effurun, Warri, Delta State, Nigeria.*
  E-mail: hsuru2000@yahoo.com
  ** Corresponding Author*

subdivided into recognition based, recall based and cued recall based systems [9,10].

2 Overview of Recognition Based Systems and Methods

Recognition based graphical authentication systems are those graphical systems that depend on a user's ability to recognise images he had selected earlier from a large collection of images to authenticate on a computing system. In each round of authentication, the user is expected to remember and select his chosen images when presented with many images from an image pool which contains both the chosen password images (portfolio) and other images (decoy).

A number of recognition based systems have been proposed and developed. The déjà vu scheme was developed by Dhamija and Perrig [11] and used Harsh Visualisation Technique [12] to generate abstract images by using a computer algorithm (fig. 1). Déjà vu is one of several examples of grid based type of recognition based graphical password systems. In order to effectively study the déjà vu scheme its proponents developed and analysed a number of system prototypes for interviews and web-based user studies. Two user studies were conducted for the déjà vu scheme designed to use photographs and random art images. Twenty research participants were used (11 males and 9 females) to compare the déjà vu scheme to traditional text based systems (passwords and PINs). A within user study was used and each user was made to test each of the four system prototypes presented in the experiment, two for the déjà vu scheme and two for each of the textual and PIN based passwords. Two experimental sessions were used to conduct the tests, one week apart. The results show that although being relatively slower in password creation and login time, memorability of the déjà vu scheme was better than in text based passwords ad PINs. No login failure was recorded for the déjà vu schemes during the first session, unlike the text and PIN based passwords that recorded 1 failure (5%) each. After a week, the login failure had increased to 7 (35%) for PIN and 6 (30%) for text passwords while the déjà vu systems recorded 2 (10%) and 1 (5%) for the random art and photo based schemes. In spite of the improved memorability, a usability issue with the déjà vu system is that the seeds of each of the algorithms had to be stored separately to ensure that the exact image could be reproduced in the future. A flaw of this experiment was the very low participant population size. An improved version of the déjà vu scheme was developed in [13]. Their Image Based Registration and Authentication System (IBRAS) used a function called a SHA-1 harsh function. The system is believed to be more secure and used less memory than the earlier version. Although similar in their storage of initial seeds, the main difference between the implementation of the IBRAS and the déjà vu schemes is that in the IBRAS, a user chooses and uses a single graphical authentication image. Although the déjà vu scheme performed well with its use of abstract images, researchers believe it is easier to remember images that have some meaning attached to them [14].

Researchers in [15] developed and evaluated the Convex Hull Click (CHC) scheme. In this scheme, a user selects a number of icons from a large set of icons during the registration stage. In each authentication round, the user is expected to identify his pass-icons in every challenge set. An authentication round consists of several challenge sets. A challenge set is a set of images presented in an image grid containing some of the user's pass-icons and many decoy icons. A participant is expected to click inside any triangle (convex hull) formed by any three of his pass-icons. Using software prototypes, the researchers conducted a usability studies in two experimental sessions, one week apart. The study was a between user study with 15 participants (6 males and 9 females), mean age 37 (StdDev = 13.6). The first session took about 15 minutes to collect data on the number of correct and incorrect logins, the number of correct and incorrect challenges, and the total time for each correct and incorrect login and challenge. Each participant was asked to authenticate himself on the system until he/she is able to get up to ten successful logins. Experimental results indicated that the mean correctness of entries was 90.35%, the mean correctness of the challenge sets was 97.95%, while the mean time for correct password input was 71.66 seconds. Statistical evaluation of the results show a statistically significant smooth reduction in authentication times between the ten correct logins collected from participants. The results also indicated that participants whose challenge sets comprised of 5 pass-icons were faster in login times than those with 3 and 4 pass-icons in their challenge sets. No statistically significant correlation was identified between the login times of those with 3 and 4 pass-icons in their challenge sets. In the follow up session that took place a week later, the participants were shown a list of 112 icons and told to identify the 5 pass-icons they had used in the previous experiment. Only 1 of the participants was unable to identify all the 5 pass-icons, the participant was only able to identify 4 of his pass -icons.

In order to compare with other recognition based systems, the researchers detailed a number of experiments to compare the usability of the passfaces, déjà vu and the VIP schemes with alphanumeric PINs and passwords. The VIP scheme is a graphical PIN authentication system that is designed for use with both a PIN and a bank card. 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 due to the longer times it took to authenticate. Weinshall and Kirkpatrick proposed a number of graphical schemes in [16]. Their methods used picture, object and pseudo word recognition schemes with a considerably large number of images. With the aid of prototypes, they ran user trials that lasted for three months. The researchers realized that for the picture based model, three aspects of their procedure made the largest influence on the accuracy and retention. These were: choosing picture groups with a clear theme but individual distinctions, the number of training sessions, and the frequency of testing. Overall, 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 effective than the others. While the pseudo-word model had a 70% success rate at the end of the three months period, the picture based model recorded about 90%.

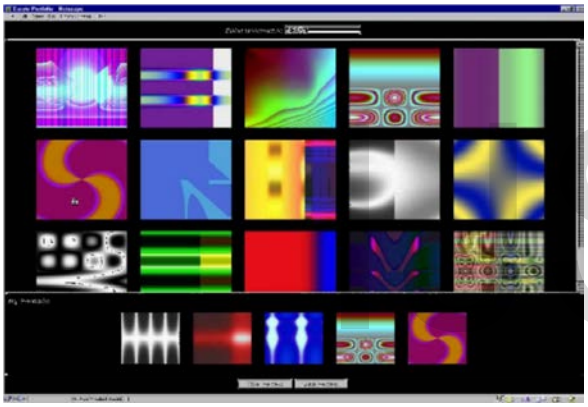

Fig. 1. Abstract images (Déjà vu)

Sobrado and Birget [17] proposed a number of shoulder surfing resistant schemes. Shoulder surfing is the ability to observe a user's password by simply looking over their shoulders [18]. Their models were an extension of the Convex Hull Scheme (CHC) proposed by Wiedenbeck et al. [15]. In their first approach a user had to locate any three of his chosen password images and click inside the convex hull formed by those images (fig. 2). In the second approach, the user needed to position one of his chosen images in a movable frame, and then move the frame such that the image aligns with any other two of his chosen images to authenticate. The researchers also introduced a third scheme in which a user had to locate any four of his chosen images and then click on the point of intersection of invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. No details of experimentation with these schemes has been reported in the literature. To decrease guessability, the researchers suggested the use of thousands of images. According to the researchers, the number of possible passwords is a "Binomial Coefficient" $\binom{N}{K}$ (choose any K objects among N). Hence when N = 100 and K = 10, the number of possible passwords becomes $\binom{1000}{10} \approx 2.6 * 10^{23}$, which is slightly more than the number of alphanumeric passwords of length 15. However, a large number of images on a small computer screen makes the screen highly compacted thereby creating usability issues. In fact researchers in [20] discussed two significant drawbacks of this scheme. The first was a technical drawback in which the researchers developed a system prototype using 1000 icons as suggested in [17]. However due to the size of a standard computer screen, it became impossible to distinguish one icon from the other. The second drawback was a "theoretical complication". Let K denote the number of user chosen pass-images, N the total number of images displayed on the screen and h the number of authentication screens for an authentication round. They argued that 10 pass icons (K) were suggested in [17] and that from a theoretical assumption: *"There is a constant c > 1, which depends only on the size of the screen used such that the probability of the center of the screen being in the convex hull of the K randomly placed pass-objects is greater than* $1 - \frac{1}{c^{k-1}}$ *"*. This means that if K objects are randomly placed on computer screen, an attacker can play a wait-and-hunt. For each challenge set (screen), the attacker may just click in the center of the screen and the probability of a successful login is $q = (1 - \frac{1}{c^{k-1}})^h$. For a standard sized screen, c ≈ 1.5, and thus, q ≈ 0.77 when K = 10 and h = 10, and q ≈ 0.45 when K = 10 and h = 30. Therefore, the K pass icons will have to be moved as a group all over a screen. This complicates analysis of the scheme as a mouse click always gives an attacker some hint. Another drawback is that authentication in this systems may be considerably slow due to the time it may take in locating the images, lowering the efficiency of the system.

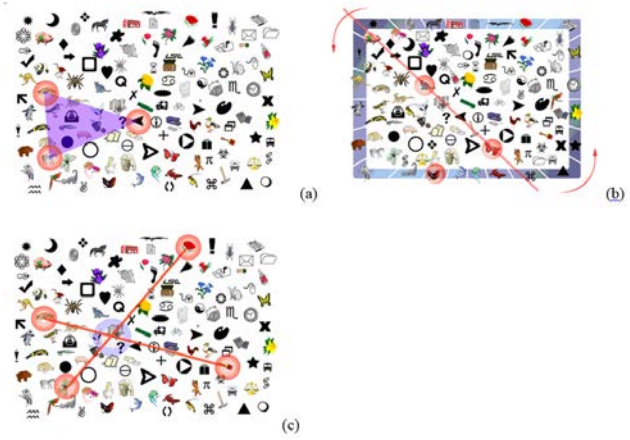

Fig. 2. Sobrado and Birget schemes [17]: a – Convex hull, b – Movable frame, c – Intersection.

An algorithm for filtering distractor (doodle) images was proposed in [19]. 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 user 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.

Man, et al. proposed a system [20] called WIW (where is Waldo?) which borrows its name from a popular puzzle game. In this scheme, the graphical interface is made up of several login images (each called a scene). Each scene is made up of several objects from which a user selects his pass-objects and a set of perturbations. Each authentication round is performed such that a user is presented with several scenes depending on his exact selection. Each scene represents a challenge set in which a user is presented with his pass-objects and many decoy or non-pass-objects and is expected to identify and select his pass objects from a mixture of pass and non-pass-objects contained in the scene. The perturbations are a number of variants developed for both the pass and non-pass objects such that during authentication the user can select any of the various perturbations (or variants) of his chosen images. A monitor's screen can be viewed as a rectangle with width a, and height b. Each scene is displayed on such a screen. For each scene, WIW renders two small icons of eye shape at $(\frac{a}{3}, \frac{b}{2})$ and $(\frac{2a}{3}, \frac{b}{2})$, respectively. These icons are designated as the left and the right eye. In the process of authentication, as the pass and non-pass objects are shuffled across each scene, the user has to relate the position of each of the designated eyes to the various positions of his pass objects within the scene. Although a prototype of the system was developed and experimentation was performed using a number of research participants, the methodology adopted for the experiment as well as the details of its results were not provided in the paper.

The system in [20] was improved upon by Hong et al. [21] in which every image had several variants and each variant was associated with a unique code. System users are presented with a scene during authentication, the scene contains pass object variants randomly selected and presented among many decoy images. To authenticate, a user types the code associated with his pass image variants and the relative position of his pass image among decoy images as observed on the computer screen. According to the researchers, the system proved resistant to shoulder surfing, although users had to both recognise their images as well as memorise the codes for the various image variants which may seriously affect the memorability and overall usability of the system. Although an experiment was reported to have been conducted by the researchers, the details of the experiment as well as its results were not reported. An improvement to this system was also proposed in which a system user assigns his own codes to his preselected images (fig. 3). The need to memorise such code, however, meant that it suffered the same fundamental usability flaws as the previous scheme.

Fig. 3. Shoulder surfing resistant scheme by Hong et al. [21]

The *passfaces* scheme was developed and commercialized by the Real User Corporation [22]. The idea came from the belief that humans find it extremely easy to remember the faces of other people even after prolonged periods of time. In the implementation of this scheme, a user is presented with a large database of human faces from which he is expected to select any four random faces. During authentication, the user is presented with four successive grids, and is expected to recognise and select one of his chosen faces among eight distractor face images (fig. 4) in each grid. The passfaces scheme has been studied rigorously.

Fig. 4. The Passfaces Scheme [22]

Studies into the effectiveness of the passfaces scheme conducted by [23, 24] indicated that passfaces could easily be remembered even after a prolonged period of time. One of these studies involved a within user experiment conducted by T. Valentine [23] with 77 staff and students of Goldsmith's College to test the memorability of the passfaces scheme. All participants used the passfaces scheme to test 3 conditions. For the first condition, 29 participants were asked to login on the system every working day for a period of 2 weeks. The participants remembered their passwords in 99.98% of logins. The second condition used 29 participants to login after about 7 days of initial enrolment. Most (83%) of the participants were able to login on their first attempt. Every participant was, however, able to login on the third attempt. For the third condition, 19 participants were asked to login once after about 30 days of initial enrolment. In this condition too, 84% of participants were able to login on their first attempt, while all others were able to login by their third attempts. The passfaces scheme is also believed to withstand long term recall as the study participants were asked to login to the systems after more than five months of their last use [24]. While 56 participants participated in the follow up trial, 72% were able to login on their first attempt and 84% by the third attempt. It was also reported that the participants that used the everyday login condition could remember their passwords the best, with 87% remembering the passwords in the first attempt and 100% remembering them in their third attempt.

Other studies in [25] revealed that the login failure rate of passfaces was less than that of text based passwords, but login time was longer. Davis et al. [26], however, discovered predictable patterns in the passfaces scheme as users were attracted to beautiful faces, faces of the opposite sex and members of their own race. In this study, the researchers analyzed observations collected during a roughly four month semester period of two universities in which two graphical password systems were used by 154 research participants. One of the schemes was a face based password systems modelled after the passfaces scheme [22], while the other was a story scheme developed by the researchers. Each participant was randomly assigned one of the two graphical schemes. Each of the students used his graphical password to access published content that included his or her grades, class assignments, assignment solutions and reading materials through the use of Java enabled browsers. In total, 174 passwords were created during the semester, indicating that a number of students changed their passwords at least once during the study. A total of 2648 login attempts were recorded, out of which 2271 (85.76%) were successful logins. At the end of the semester, an exit questionnaire was used to both capture the demographics of the participants as well as the reasons why they each selected their faces (for the face scheme) or their chosen stories (for the story scheme). The results of the experiment revealed that in the face scheme, both males and females chose the faces of females significantly more often than the faces of males. In fact, over 68% for females and over 75% for males selected female faces. It was also observed that when males chose the faces of females, they almost always chose the faces of models. This accounted for roughly about 80% of male selection of female faces. This fact was also supported by participants' remarks in the research questionnaire. The researchers also recorded a significant correlation among members of the same race. Asian and Caucasian females selected faces of people from within their own race about 50% of the time, Caucasian males chose the faces of Caucasians over 60% of the time, while black males chose the faces of blacks about 90% of the time. With these results, the researchers refuted the argument that user-chosen graphical passwords of the face and story schemes are likely to offer additional security over text passwords without users being trained to select better passwords. System assigned passwords was suggested as possible solution to the predictability problem. This, however, may render the system less memorable, hence negatively affecting its usability. Vulnerability of the passfaces scheme to descriptions was analysed in [27]. The study was aimed at understanding the possibility of verbal descriptions on passfaces and how such vulnerabilities could be reduced. The study was conducted using images from the passfaces online demo using 45 face images (18 males and 27 females). The experiment evaluated three test conditions: random groups (the base condition) in which decoy face images for a target face image were selected randomly, visual groups in which decoy images for a target face image were selected based on visual similarities with a target face image and verbal groups in which decoy face images were selected based on verbal similarities with a target face image. The researchers recruited 56 participants (31 male and 25 female) with an average age of 22 Standard dev. = 7 that conducted lab based trials during a computer science practical sessions. Five face grids were provided for each test condition out of which each participant was expected to identify a target face among decoy images assembled based on the criteria for the test condition in a within users study. A group of 18 contributors (9 males and 9 females) were recruited for the decoy image selection process. The results indicated that of all the 158 login attempts collectively made in the entirety of the experiment, only 13 (8%) were successful. That is, only 8% identified all five target face images in the five face grids of any particular test condition. The random groups had the highest login success rate and the verbal groups had the lowest. The average login success (out of 5) for the random groups was 3.57 (standard deviation = 0.91), for the visual groups was 2.87 (standard deviation = 1.07). The mean variation was statistically significant ($t=3.63$ $p< 0.0$). The average login

success rate for the verbal group condition was 2.81 (standard deviation = 1.14). The mean variation between the verbal and he random conditions was also statistically significant ($t=3.64$ $p < 0.01$). The study concluded 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 hence description. It is observed in [16] that keyboard entry was 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.

A theme based set of graphical passwords [28-30] were proposed by Jansen et al. for mobile devices. In this systems, a user selects images which represent themes (such as the sea, the forest, group of animals, etc.). Some themes comprise thumbnails of pictures which when put together will form a particular image, others comprise a set of similar images. A user selects a number of images in a sequence within this theme as his password (fig. 5). During authentication, the user needs to select his images within the theme in a definite order. The system also allowed users to submit and use their own set of images [29]. A method called "salting" was proposed to increase the security of the system against observational and specialized dictionary attacks. Salting is the process whereby the clear text value of an image password is prepended with a random numerical value *R* called a salt. Through salting, the search space of an attacker is increased by a factor $2^{|R|}$ if the attacker does not know the salt. Although details of the system implementation were provided in [30], the researchers did not publish any details of any experiments or experimental results. The main limitation of this system was the fixed size of the mobile screen, which limited the number of thumbnails used, a great hindrance to the efficiency and usability of the system.

Another graphical scheme was proposed by Takada and Koike [31] which 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. If none of the user's images are presented on the screen, the user selects nothing. The idea of an online registration for every image submitted by the user as well as the use of image notifications as provided by the system greatly improve security. No experimental or design details were, however, reported for the system. Submitting one's own images greatly improves memorability, but also makes it easier for an intruder who knows the user to easily guess the password [25,32], a great setback on security.

Fig. 5. Theme based graphical technique

3 Overview Pure Recall Based Systems and Methods

Pure recall based systems are systems in which a user is expected to fully recall a piece of action from past memory to authenticate. Majority of these systems present a blank touch sensitive screen during each authentication round upon which a user is expected to reproduce an image he had drawn earlier during registration.

A technique called *Draw a Secret* (or DAS) was proposed by Jermyn et al [33] which allowed users to draw their own pass images on a 2D grid using a touch sensitive screen (fig. 6). The coordinates of the drawn image on the grid are stored on the system in the order in which the drawing occurred. The user has to repeat the drawing in exactly the same order each time he wants to authenticate. The password space for the DAS system is larger than the text password space. Another advantage of the DAS scheme is that since it is independent of any alphanumeric strings, it can well be used by speakers of any language.

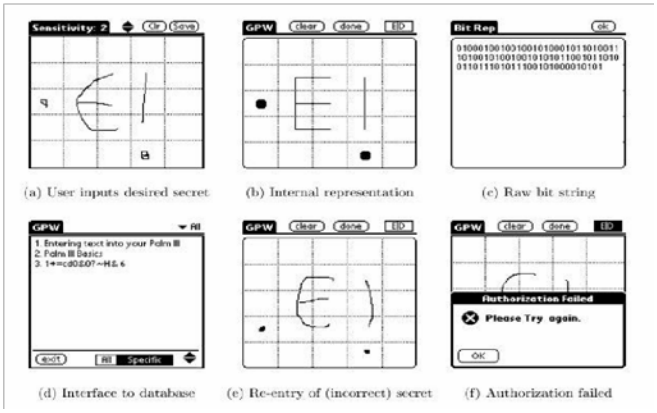

Fig. 6. The "Draw-a-Secret" (DAS) system by Jermyn, et al. [33]

A number of researchers have investigated the usability and security of the DAS password scheme. One of such was presented in [34]. In an analysis of the memorable password space of DAS, the researchers developed the concept of graphical dictionaries which was used to study the susceptibility of the DAS scheme to brute force attacks. They postulated that since mirror symmetry had a significant position in human cognitive memory, it was possible to develop an attack dictionary based on symmetric patterns. A performance comparison of mirror symmetric and asymmetric images was also performed, which led to the conclusion that symmetric images were more preferred by system users, but were also less secure. Another study [35] investigated the impact of stroke count on DAS password strength and observed that the higher the stroke count the stronger the password. The study was aimed at investigating the relationship between the number of composite strokes, the dimensions of the grid and the length of the DAS password in the DAS password space. In doing this, the researchers introduced DAS password complexity properties based on pattern complexity factors which included password length, number of composite strokes (or the stroke count), symmetry, or the number of turns in each stroke. The study was to understand if any of these factors could have an effect of the DAS password space such that it was possible to perform a brute force attack on a DAS password using a graphical dictionary. The study proved that when users choose with less than 5 strokes with a password of length less than 13 on a 5 × 5 grid, instead of the maximum of 12 strokes, the password space of the DAS password is reduced from 58 bits to 40 bits. To further strengthen the DAS password, the researchers 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. This method significantly increased the password strength of the DAS system with an increase of up to 16 more bits. The researchers, however, did not report any user study. Dunphy et al. [36] also tried to improve the security of the DAS password through the introduction of background images in a method called Background DAS (or BDAS). In this method, a user first had to select a background image, and while the chosen image appears faintly at the background of his DAS grid, the user draws an image on the grid as is done in a normal DAS password (fig. 8). In two laboratory studies with paper based prototypes, the researchers investigated the effects of background images on the memorability of the DAS password as well as the effects of background image choice on user performance in the BDAS password scheme. A total of 21 subjects were recruited for the first experiment, 15 male and 6 female aged between 18 and 50+ that cut across technical and non-technical disciplines. Participants were split into two groups, the control group that used a prototype representing the original DAS system and the BDAS group that used BDAS prototype. Five (5) picture images were used for the background and participants were allowed to use images of their choice. The results of the first study (the pilot study) revealed that 90% of the DAS group employed global symmetry as opposed to 50% in the BDAS group. Also, 90% of the passwords used in the DAS scheme used were centred within the grid as opposed 70% in the BDAS scheme. The lengths of the passwords created by the BDAS user was significantly greater than that created by the DAS users. The t-test results showed $t=2.377$, $p < .0$. These results imply that the users of the DAS scheme employed centralization and symmetry as means to aid recall and that the BDAS users created longer passwords. In the second study, 46 participants were recruited, 32 male and 14 female with most participants between the ages of 18 and 25. While 20 participants had technical backgrounds, 26 were from non-technical disciplines. Participants were equally split into two groups as in the first stud. The results from this study indicated that 43% of the BDAS group exhibited global symmetry as compared to 57% for the DAS group. In terms of image centering, 43% of the BDAS passwords exhibited image centering as against 87% for the DAS group. While the recall rate was better for the DAS password after the first five minutes (96% and 100%), the recall rates were same at the end of the first week (95% for both). The study also indicated that the complexity of the passwords selected by the BDAS users was significantly higher than that for the DAS users with t-test indicating $t=2.78$ $p < 0.01$. In spite of the increased complexity and length of the BDAS passwords over the DAS passwords, user performances in both systems were similar. Hence the researchers concluded that in spite of its apparent increased complexity, the implementation of BDAS helped improve the memorability of DAS passwords.

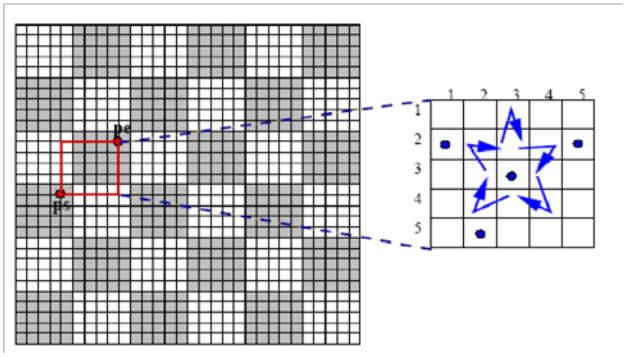

Fig. 7. Grid based techniques developed by Thorpe and Van Oorschot [32]

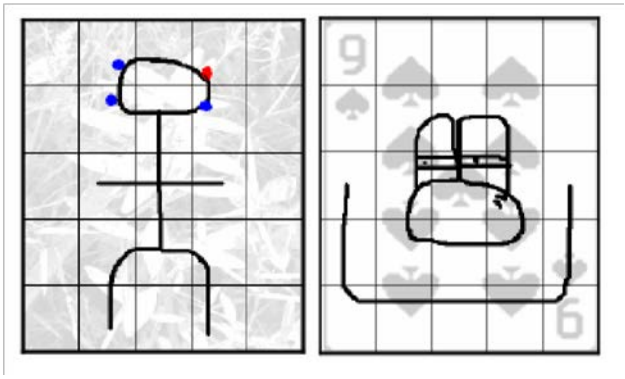

Fig. 8. The Background DAS (BDAS) scheme [36]

Goldberg et al [37] proposed the *passdoodle* technique in which the user produces a small design or text on a touch screen. The researchers used a between-user design with 13 participants using paper prototypes to investigate the viability of the passdoodle scheme in user authentication through an understanding of the memorability and user preferences in comparing the passdoodle scheme to alphanumeric passwords. The study was divided into two login sessions one week apart to create and recall a username and one alphanumeric and one doodle password. Their studies observed that users could accurately remember how they drew complete graphical images, yet mostly forget the sequence in which the various components of the image were initially produced. Hence the researchers observed that if the restriction of ordered login is removed for subsequent implementations of the passdoodle scheme, it will greatly enhance the usability and memorability of the system.

A further study to analyse the predictability of the DAS password was conducted in [38]. In spite of lacking any predictable patterns, it was discovered that at both the beginning and the end points of the password strokes, some characteristics such as rectangles, letters, numbers and crosses were common and that users generally preferred passwords that were predictable, hence insecure, in favour of memorability. In a paper based study with 16 participants, 10 male and 6 female, aimed at understanding if predictable patterns will appear in the implementation of the DAS password scheme, the researchers discovered that approximately 45% of the users chose symmetric passwords, 2/3 of which were mirror symmetric (reflective). Approximately 80% of users chose passwords composed of 1-3 strokes, 10% chose passwords composed of 4-6 strokes, and 10% of the users chose 6 or more strokes. With regards to the centering of passwords within grids, 56% of the passwords were centered, an additional 30% more were approximately centered, that is, centered on a set of cells adjacent to the central grid lines.

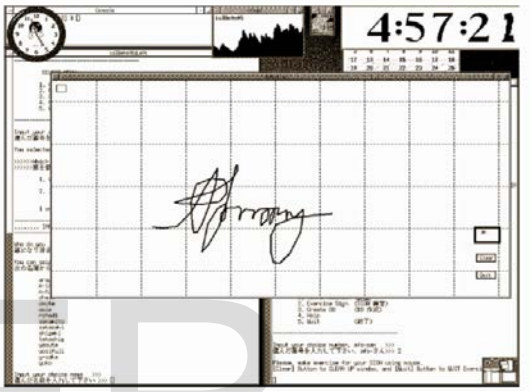

Fig. 9. The signature scheme

The signature scheme was proposed in [39]. The scheme is presented in figure 9. In this scheme, a user is asked to draw his signature on a grid during the registration stage. The coordinates of this signature are immediately stored on the system and confirmed by a further verification stage before any round of authentication. The success of the scheme was satisfactory as the users did not have to memorize their signatures. Users could also replicate their signatures with almost exact precision. To understand the distinguishing factors between user and imposter signatures, the researchers developed a set of signature writing parameters such as number of signature points, coordinates of points, signature writing time, velocity and acceleration and used these parameters against user and imposter signatures. The greatest variation was observed in the use of the acceleration parameter. This was then used in the experiments to differentiate user and imposter signatures. The researchers evaluated the system using two experiments; one with a static signature database in which signature data is registered into the system and kept in the system's database during the registration phase. The data is kept and used for user authentication until a new copy of the signature data is again registered onto the system and used to replace previous data.

It was however discovered by the researchers that users become more efficient in the use of the scheme as the number of authentication cycles increased. The signatures became more accurate and took less time to write. Hence, in the second experiment, the researchers used a dynamic database in which the signature data in the system's database was changed occasionally and automatically by new signatures written by the users. In the static DB experiment, the successful verification rate was 91%, while the successful rejection rate was 92%, while in the dynamic DB experiment, the successful verification rate was 93% and the successful rejection rate was 96%. The signature scheme, however, needed proficiency with the stylus as well as the need for additional devices. Moreover, some tolerance threshold had to be set as the password is captured. This allows for better usability, while compromising security.

4 Overview of Cued Recall Based Systems and Methods

In cued recall based systems, a user is required to locate and click on a number of click points chosen earlier on an image. The image itself serves a *cue* and assists a user to recollect the series of actions carried out, since these actions were all carried out on the image. In pure recall based schemes activities are done on an empty grid. The idea of click points was first proposed by Blonder [40]. In his design, an image was displayed on the screen which had predefined click points. The user had to click on these points to register and do so in the same order anytime he intends to authenticate (fig. 10). Some tolerance threshold is, however, provided for each click point. No experimental prototype of Blonder's scheme was every developed. Hence, no user studies have ever been conducted.

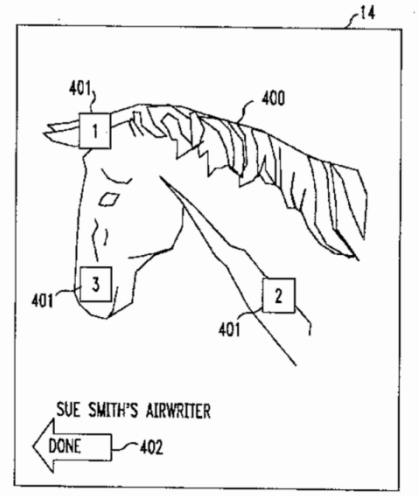

Fig. 10. Blonder's scheme

Passlogix [41] developed a scheme based on repetitive actions (fig. 11) which a user had to choose such as preparing a meal or picking of cards as his password. Researchers have also proposed the variation of grid sizes [42] for grid based systems during each authentication round. Through a web based prototype, the researchers reported that the system was 92% resistant to shoulder surfing attacks. No details of experimentation and or analysis were, however, reported. It was also reported in [43] that Microsoft proposed a graphical scheme in which users click on predefined areas on an image to register and authenticate. The details of the system was not, however, published.

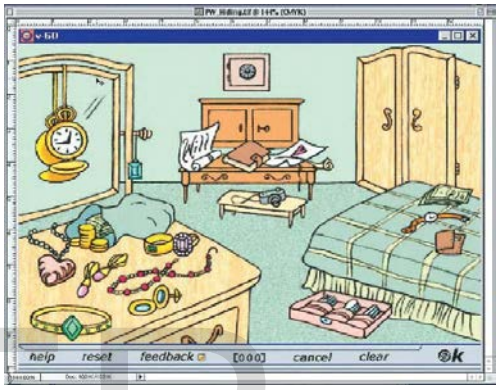

Fig. 11. The Passlogix scheme

The ideas of Blonder were further improved through the elimination of fixed boundaries and use of different images by Weidenbeck et al [44-46]. In their models, a user was allowed to click on any part of an image in any order to form his password (fig. 12) with some tolerance allowed for each click point. The system adopted the quantization method proposed in [47] and with hundreds of click points to click from, it is believed to possess a large password space. The researchers reported an empirical study comparing the use of the PassPoints scheme to alphanumeric passwords. The participants were split into two groups that created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over a period of 6 weeks. The results showed that the graphical password users created valid passwords with fewer difficulties than the alphanumeric users. However, the graphical password users also took longer and made more invalid password inputs than the alphanumeric password users during the practice sessions. In the longitudinal trials, the two groups performed similarly in the memorability of their passwords, but the graphical group took more time to input their passwords. The researchers also observed that an increase in the size of the image increased the

number of available click points within the image thereby increasing both the security and usability of the image. The system of cued click points was also developed and studied in [48] as an optimized version of the click based password scheme. In this system, multiple click-based images are used with one click point per image. The next image is based on the previous click point. The system was tested with 24 participants in a lab study which revealed that the system had considerable promise in both usability and security. From the results, the performance was very good in terms of speed, accuracy, and the error rate. Participants also preferred CCP to PassPoints [46], claiming that selecting and remembering only one point per image was easier, and that seeing each of the images triggered their memory of where the corresponding click point was located. The researchers believed that CCP will provide greater security than PassPoints because the number of images involved increases the workload for attackers. The study, however, suggested further investigation into the memorability (usability) of this systems and the problem of hotspots (security) through more elaborate and longitudinal trials. The effect of tolerance and image choice was studied in [45]. The tolerance study was conducted with 32 participants (undergraduate students), 22 males and 10 females. The mean age was 22.7 (SD = 1.33). The participants were divided into two groups with varying tolerance regions (error margins) of 10x10 pixels (.26cm^2) and 14x14 pixels (.37cm^2). The results showed that accurate memory of the password was greatly reduced when the tolerance was reduced from 14x14 to 10x10. It was observed that small tolerances can greatly increase the space of possible passwords and therefore make the passwords more secure. The nature of the images used in the system may also have a large effect on people's ability to remember their click points. It was observed that allowing users to choose their own images may lead to high memorability for the user, but may also result in images with poor security characteristics such few click points or high guessability. The study revealed that countless images could be used in the implementation of the passpoints scheme. Further studies conducted in [46] showed that click-based graphical passwords had better security than text passwords, although user training may also take longer. The problem of hotspots in picture based passwords was studied in [49]. The aim of the study was to explore popular points (hotspots) in click based passwords and examine the strategies to predict and exploit them in guessing attacks. The researchers reported both short-term and long-term studies. The first was lab controlled test 43 participants and 17 diverse images and the second was a field trial involving 223 user accounts. The research discovered that hotspots existed in varying degrees from one image to another. The researchers explored the use of 'human computation' to predict hotspots from images and to generate two 'human seeded' attacks. The first was based on a first-order Markov model while the second was based on an independent probability model. Within 100 guesses, the first-order Markov model based attack reveals 4% of passwords in one image's data set and 10% of passwords in a second image's data set. The independent model based attack reveals 20% of passwords within 233 guesses in one image's data set and 36% passwords within 231 guesses in a second image's data set. The researchers also evaluated the first-order Markov model based attack with cross-validation of the field study data, which revealed an average of 7-10% of user passwords within 3 guesses. The research concluded that all click based graphical passwords were predictable and hence vulnerable to online and offline attacks.

Fig. 12. The Passpoints scheme by Weidenbeck et al.

According to [43], a system of navigation through a virtual world for authentication was proposed by a man named Adrian Perrig by which users could randomly create virtual environments and be authenticated by navigating through these virtual spaces. Although it is believed to have the potentials of creating strong passwords, there is, however, no documentation for this system. The use of mnemonics to aid recall has also been studied in [50, 51], where the use of mnemonics was incorporated into a number of graphical systems. In [51], a between-users retention test was conducted for multiple passwords for a control group (Group 0) using PIN based password entry, a graphical password group (Group 1), a group with graphical passwords with signature color background for graphical images to augment memorability (Group 2), a group with graphical passwords with mnemonic strategy to augment memorability (Group 3) and a groups with graphical passwords with mnemonic strategy and colour background to augment memorability (Group 4) where each participant was randomly allocated one of the groups. The study was conducted over a period of four weeks and each participant was allocated 5 passwords. A total of 172 participants participated in the user study. Due to the high dropout rate, however, only 61 participants completed the study. The dropout rate was highest in group 0 in which

some participants thought it was impossible to retain multiple PIN based passwords over a relatively long period of time. Their study results proved the superiority of retention of multiple graphical passwords over multiple PINs and 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 [52]. 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 a between-user study with 20 participants (10 males and 10 females) with an age range of 20 to 30 years, the researchers compared the new scheme called CDS (meaning "Come from DAS and Story" scheme), with the story scheme in two login sessions, an initial session and a follow up session one week later. The mean password creation time was 42.9 seconds for the story scheme and 49.5 seconds for the CDS scheme. The mean login time was 9.2 seconds for the story scheme in the first session and 23.1 seconds in the second session, while it was 13.7 seconds for the CDS scheme in the first session and 19.8 seconds in the second session. The success rate for the CDS was 80% as compared to 60% for the story scheme. A comparison of the new scheme with the story scheme in terms of observational attacks, was, however, not conducted in the research.

In several studies, the combination of several graphical passwords has been explored. In [53], the researchers deployed the use of a recognition based system in the first stage and a recall based system in the second stage of user authentication. A set of questions (three, specifically) were associated with the recall based phase. The questions help the user in knowing his click points as the click sequence is randomized in each authentication round. No user study was reported for this scheme.

5 Conclusion and Future Work

The field of graphical authentication systems has been a vibrant and rapidly evolving research area. Many authentication systems have been developed and evaluated while new ones are being proposed. In this paper, the researchers have tried to provide a comprehensive review of the existing methods of graphical authentication approaches as well as the user studies carried out to evaluate these systems.

The variation in the design of graphical authentication systems as well as the variation in methodologies adopted in user studies and data analysis tools as well as the size of study populations has, however, made an accurate comparison of the different models of graphical authentication exceptionally difficult. It is therefore necessary for researchers in this area to provide standard tools and methods for the development and evaluation of authentication systems.

In the future, the researchers hope to look further into the development and evaluation of newer and more robust authentication systems as well as in hybrid and multifactor systems. It will also be interesting to study other areas of user authentication as highlighted in the paper. These include biometric and token based authentication models that have received the attention of researchers in recent years. Many of the developed systems have also been commercialized and are thus being employed in access control many organisations.

REFERENCES

[1]. B. Coskun and C. Herley "Can "Something You Know" Be Saved?" In *ISC* (Vol. 8, pp. 421-440). September, 2008.

[2]. A. De Luca, M. Denzel and H. Hussmann "Look into my eyes!: Can you guess my password?." In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 7). ACM. July, 2009.

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

[4]. 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

[5]. 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.

[6]. 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.

[7]. 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.

[8]. S. Chiasson "Usable authentication and click-based graphical passwords." PhD Thesis, School of Computer Science, Carleton University, 2008.

[9]. 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.

[10]. 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.

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

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

[14]. 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

[15]. S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget "Design and evaluation of a shoulder-surfing resistant graphical password scheme." In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184). ACM, May 2006.

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

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

[18]. 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.

[19]. 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

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

[21]. 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.

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

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

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

[25]. 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.

[26]. 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.

[27]. 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.

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

[29]. 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.

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

[31]. 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.

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

[33]. 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.

[34]. J. 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.

[35]. 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.

[36]. P. Dunphy, 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.

[37]. 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.

[38]. 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.

[39]. 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

[40]. G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 16.

[41]. M. R. Albayati and A. H. Lashkari. "A New Graphical Password Based on Decoy Image Portions (GP-DIP). In *International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2014* (pp. 295-298). IEEE. September, 2014.

[42]. 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.

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

[44]. 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.

[45]. 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.

[46]. 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 .

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

[48]. 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.

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

[50]. 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.

[51]. 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.

[52]. H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", *International Conference on Cyberworlds*. 2010, IEEE: Singapore pp. 194 – 199, 2010.

[53]. 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