Chapter 2

Related Work

Graphical passwords can be categorized into three methods recognition based, recall based and cued recall based on the cognitive load on the user in retrieving the passwords from the memory [40,50,64]. In this chapter, we present the previous work done in these three categories and we discuss the limitations of these techniques. We also present existing shoulder surfing resistant authentication techniques.

Many researchers worked on authentication systems and designed various graphical password techniques to enhance the usability and security. No author has measured all the metrics of usability and security, only some of the aspects are highlighted by each author. For some proposed techniques, no user study was done. There is no standard defined for measuring these metrics and each author followed his own method to evaluate memorability, usability and security. So it is not possible to compare the results of various methods and make conclusions. We discuss the method followed by the author and the results reported by him as part of evaluation.

The metrics considered for memorability and usability are recall success rate, password registration (creation) time, login time and the errors made by the users while entering the password. The security is verified by the resistance against password guessing and the password capturing attacks. Brute force, dictionary and (personalized) guessing attacks are password guessing attacks. Shoulder surfing, social Engineering and malware attacks are password capturing attacks.
2.1 Recognition based techniques

In recognition based systems, users generally select a set of images during password registration and he has to recognize these images during login time. The studies of cognitive scientists say that humans have unlimited memory for pictures and they can remember and recall pictures easily than text [9,43,55]. Hence, the precise recall of textual passwords is replaced by recognizing images to reduce the cognitive load on the user.

2.1.1 Deja Vu

Dhamija and Perrig [15] designed a graphical system known as Deja Vu using recognition based authentication. In this technique, from a set of sample images, user selects a fixed number of images to form an image portfolio. During login time, a challenge set with number of images will be displayed on the user’s system. The challenge set contains a few images from the user’s portfolio and the rest of the images from the remaining image samples which are called as decoy images. For authentication user must recognize the images from his portfolio which are part of the challenge set. The images are random art images generated using an initial seed and the server maintains 10000 seeds of random art images for selection of images by the user to form his portfolio.

They conducted user study with 20 participants for PIN, password, photographs and random art images. In a challenge set, 25 random art images are displayed and among the challenge set 5 images are from user’s portfolio. The total password space is $25^5$. 
The recall test was conducted after one week of password creation. They reported 90% success rate using random art images, 95% using photographs and 65-70% using PINs and passwords. The average login time was recorded and given in table 2.1. For shoulder surfing, to capture all images in the user’s portfolio, multiple logins were required because for each login apportion of the portfolio is displayed. They claimed that the technique is resistant to dictionary, social engineering and guessing attacks because of system generated images and each image description was different for different users. Guessing attacks is easy using photographs than random art images.

<table>
<thead>
<tr>
<th>Create</th>
<th>PIN</th>
<th>Password</th>
<th>Art</th>
<th>Photo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login (immediately)</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>60</td>
</tr>
<tr>
<td>Login (after one week)</td>
<td>27</td>
<td>24</td>
<td>36</td>
<td>31</td>
</tr>
</tbody>
</table>

Fig 2.1: Average create / login time in seconds for Deja Vu
2.1.2 Passfaces

Real User Corporation developed the technique Passfaces [49,45]. Many researchers worked on finding the effect of pictures than text on human brain. They reported that humans are good in recognizing pictures or images than text. In this technique, user selects a set of human faces during password creation. During login, a panel of human faces will be displayed in a grid in multiple rounds and the user must recognize the face that belongs to his portfolio in each round. The face should be correctly recognized in all rounds for authentication. For testing 3x3 grid is used with five rounds. The official website reported the password creation time as 3 to 5 minutes for a panel of 9 faces in 5 rounds. The password complexity is $9^5$.

Valentine [72] conducted a user study with 77 participants for Passfaces. They reported the range of the login success rate for Passfaces as 72% to 100%. The success rate was calculated considering three attempts for every login at different recall intervals up to 5 months.

Brostoff and Sasse [7] conducted user study in the field with 34 participants for textual passwords and for Passfaces in a period of 3 months. They reported the failure rate for passwords as 15.1% and for Passfaces as 4.9% which was one third rate of textual passwords. It was observed that, due to more login time for Passfaces, people
logged in to the system less often using passfaces than textual passwords which reflects the usability problem.

2.1.3 Faces / Story

Davis et al [13] proposed two authentication systems - Faces(based on Passfaces) and Story(based on order of images). In faces scheme, during password creation, user selects a set of faces, each face from a different class of faces. There were 12 classes of faces like typical Asian male and female, typical black male and female etc. In Story system, during password creation, user selects a sequence of images and makes a story with the images to remember the sequence. The images for Story are taken from different types of images like animals, children, sports, male and female models which are used in a day to day life. During login, user has to identify the images in the same sequence.

Fig 2.3: Sample panel for Story

They conducted user study of these two techniques and found that story passwords were difficult than Face passwords. Nearly half of the participants didn’t form a story, they just selected four interesting pictures and tried to remember the sequence of selection. But recalling the images in sequence is a difficult job unless the selected images are linked by some concept.
In case of Faces, the passwords were predictable due to the selection of good looking images by the users. They reported that some mechanism is required to reduce the effect of attraction and race in Passfaces/Faces system. The success rate for Faces varied from 90% to 98% and for Story varied from 74% to 92% approximately at different intervals of time, Story is more vulnerable to shoulder surfing than other recognition based techniques because all user’s portfolio images are displayed in a single login. No time requirements were specified.

Dumphy et al [17] tested the Passfaces authentication system against social engineering attack. They found that the success of the attack can be reduced by choosing decoy images carefully. Tari et al [67] investigated for shoulder surfing attack on Passfaces. They showed that usage of mouse was more vulnerable than using keyboard. In case of usage of keyboard, the intruder has to use key loggers and screen scrapers to capture the passwords.

2.1.4 For mobile devices

Jansen et al [27] designed a system for mobile devices such as PDAs. In this graphical authentication system, themes (like cat, sea etc.) are used where each theme contains 30 thumb nail photos. During registration, user selects a theme and then selects a sequence of thumbnail photos on the theme. For authentication, during login time, user recognizes and touches the thumb nail photos selected by him in the same sequence using stylus. A number is assigned to each thumbnail photo and the sequence of thumbnail photos form a number password. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small.
2.2 Recall based techniques

The (pure) recall based passwords are same as traditional passwords as they require the user to remember and recall the passwords during login time. In recall based systems, users draw their password either on a blank canvas or on a grid. There are no cues to help the user to recall the passwords. The cognitive load on the user is more and it is harder than all other techniques [12].

2.2.1 DAS (Draw-A-Secret)

Jermyn et al [28] proposed a graphical password technique which is more secure than textual passwords. In this technique, user draws a secret (picture) on a grid using stylus during password registration. The password is an ordered sequence of coordinate pairs of grid cells touched during the password drawing by the user. The drawing may contain one or more pen strokes separated by pen up events. For authentication, during login time, user has to draw the picture touching the grid cells in the same sequence. Considering the size of memorable graphical passwords with the size of the dictionary of usual textual passwords, DAS was claimed as more secure than traditional system.
The complexity of passwords in DAS depend on the size of the grid, length of the password and number of strokes in the password. For a 5x5 grid, the theoretical password space for password of length less than or equal to 12 is 58 bits. This technique is vulnerable to shoulder surfing. The intruder can capture the password in a single observation. It is vulnerable to malware and phishing attacks and other forms of social engineering were not possible unless the user draws the secret on a paper. For each cell, in the neighbour set, diagonal elements were not considered in drawing a picture. During drawing, if the user draws a stroke too close to a grid-line then wrong sequence may be considered as password entered by the user.

Nali and Thorpe [41] conducted a user study on paper. Users were requested to draw the passwords on a paper to measure the predictable features in passwords selected by the users. They reported some symmetries and no predictions about start and end points of strokes. They showed that 45% of the passwords were symmetric, 80% of the passwords contain 1-3 strokes and 86% were centred or approximately centred within the grid. According to their report, 29% of the passwords drawn were invalid because users draw the strokes too close to a grid line.

Thorpe and Van Oorschot [69] introduced the concept of graphical dictionary and analyzed the memorable password space of graphical passwords using DAS. Using
graphical dictionaries, they tested the possibility of exhaustive search and showed that lengthy passwords of length greater than or equal to 8 on a 5x5 grid may be less vulnerable than traditional passwords.

Attneave [3] and French [19] reported that people recall symmetric images better than asymmetric images. Van Oorschot and Thorpe [73] showed that the space of mirror symmetric graphical passwords is significantly smaller than the full DAS password space and reported that efficient graphical dictionaries make the intruder’s job easy.

Dumphy and Yan [18] introduced BDAS in which a background image is drawn on a blank canvas of the grid. They conducted user study and reported that BDAS helps the user in selecting strong passwords and also reduces the problems of symmetry and centering within the drawing grid.

2.2.2 Passdoodle

Passdoodle allows users to create hand written drawings as passwords with a stylus on a touch screen without a visible grid. Goldberg et al [20] conducted user study on a paper using Passdoodle and found that users were able to remember their passwords but failed in recalling the order or direction of the pen strokes. For password registration, the technique requires training to recognize the password. The success depends on the user’s ability to recall and reproduce their doodles. This technique is vulnerable to shoulder surfing, one login may be sufficient to observe the password. No further study was done on this technique.

Syukri et al [65] proposed a technique for authentication in which user draws a signature using mouse at the time of registration. The system extracts the signature area. During verification, the system takes user’s signature, normalizes it and the
extracts the parameters of the signature for comparison. Drawing the signature with a mouse is a difficult task.

2.2.3 Pass-Go

Tao and Adams [66] designed a new scheme Pass-go based on Chinese board game Go. User draws password on the grid using intersections of the grid cells. For each intersection, sensitive areas are defined and touching any point inside a sensitive area is equal to touching the intersecting point. The grid of size \((G+1)\times(G+1)\) in DAS is equal to \(G\times G\) grid in Pass-go. An ordered sequence of intersecting points with pen up events forms the password. Colors can be used to create strong passwords. They conducted user study and reported that Pass-go keeps most of the advantages of DAS scheme and offers more security and better usability.

![Login screen for Pass-Go](image)

**Fig 2.6:** Login screen for Pass-Go

In Pass-go, dot and line indicators are used to display the password. By using an encoding scheme, the password can be inputted using keyboard. They conducted user study with 158 participants over a period of three months. They reported the success rate as 78% and the weekly success rate varied from 68% to 95%. Pass-go has more
password space than DAS. For a password of length n, for pass-go-9 the password space is 77 bits.

The technique is vulnerable to shoulder surfing. Two solutions were suggested for shoulder surfing problem. First solution is not to show the indicators. By observing the mouse pointer, it is difficult for the user to create passwords. Second solution is to use disguising indicators. For every input by the user, one or more disguising indicators may be displayed at random points. But, it confuses the user. Sensitive areas around intersection points play an important role in usability. If the sensitive area is too small, it is difficult for the user to select or touch it. If it is too large, there may be overlapping of sensitive areas which may lead to wrong point selection.

Drawing the password in Pass-go is difficult than DAS, and remembering the sequence of dots or lines is also a difficult job. It may not be convenient to draw some shapes using only intersecting points or lines. Por et al [47] added background images to Pass-Go to support the user in remembering the password. This technique is more vulnerable to shoulder surfing.

2.2.4 PassShapes

De Luca et al [2] evaluated different authentication techniques for ATM usage and found that many users depend on the shapes in order to remember the PIN. In an online survey, 86 members participated and 40% of them expressed that they use geometric shapes to remember the password. A shape password may contain many shapes like square followed by rectangle. Instead of remembering the PIN, they remember the shape on the key pad and enter the digits in the shape as password.
Weiss and De Luca proposed PassShapes [78] for authentication. Users select simple geometric shapes for authentication. A PassShape may contain several strokes. PassShapes can be represented by a string for internal representation. During registration, he selects a shape and for authentication he has to produce the same shape using touch pad or touch screen. In this technique, shape is important and size and location are not considered, only the order of the strokes is considered. PassShapes are drawn by hand which helps the user to remember the shapes. They conducted user study with 52 participants to evaluate memorability of PassShapes.

They divided the participants into three groups- five digit PINs, seven stroke Passshapes with no strategy and PassShapes with repeated drawing. PINs and passshapes were created using random generators. The third group participants (PassShapes with repeated drawing) were requested to repeat their passshape 24 times. Three tests were conducted for memorability evaluation. First test was taken immediately after the learning phase and the other two tests were conducted after 5 days and after 10 days. The results were given in table 2.2. It was found that the performance of PassShapes with repeated drawing is better than the other two techniques and performance of PIN was better than PassShapes with no strategy.
From the results, it was clear that PassShapes with repeated drawing was more memorable than the other two schemes.

<table>
<thead>
<tr>
<th></th>
<th>Test1 (%)</th>
<th>Test2 (%)</th>
<th>Test3 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>100</td>
<td>93.75</td>
<td>81.25</td>
</tr>
<tr>
<td>PassShapes</td>
<td>78.94</td>
<td>68.42</td>
<td>63.15</td>
</tr>
<tr>
<td>PassShapes with repeated drawing</td>
<td>100</td>
<td>76.47</td>
<td>94.11</td>
</tr>
</tbody>
</table>

Table 2.2: Success rate for PassShapes

Another user study was conducted with 12 participants for usability. It was reported that the average login time for five digit PIN was 4.2 seconds and for passShapes it was 6.5 seconds. The results showed that entering PIN is faster than all schemes but, PassShapes is within an acceptable range when compared to PINs. The passShapes without repeated drawing is less memorable than PINs.

The password should be drawn using touch pad or touch screen and all systems may not be having these devices. The security analysis was not done for this technique. This technique is vulnerable to shoulder surfing, phishing and malware attacks. No grid is required to draw a password. The password space depends on the number of strokes. As each point contains eight possible strokes, for a password of length n, the complexity is $8^n$.

### 2.3 Cued-recall techniques

Cued-recall is an easier task than pure recall because cues help the users to recall the password [70,77]. In cued-recall systems, generally users select specific locations on a single image. Instead of remembering the entire image, user has to remember few locations on the image.
2.3.1 PassPoints

G.E. Blonder [5] designed the first graphical authentication technique. In this technique, user selects certain locations on an image as password. During login time, user has to reselect the same locations in the same order for authentication. No user study was done for this. Users can not click on the background in password selection as it was simple.

Weidenbeck et al [79,80] designed Passpoints extending Blonder’s design by increasing clickable areas. In this technique, user can click anywhere on the image to create a password. User clicks on a set of points on the image using a mouse. The sequence of points clicked during registration forms the password. During login, user has to click on the same points of the image in the same order within a specified tolerance. They conducted user study in the lab and reported password registration time as 64 seconds on average and training time as 171 seconds. Login success rate was reported as 55% to 90% at different login periods. The tolerance area should be at least 14x14 pixels for acceptable usability. The PassPoints technique is vulnerable to hotspots and simple geometric patterns within images [74].

Figure 2.8: Blonder’s image
Viskey [53] is the commercial product of Passpoints designed for mobile devices for screen unlocking. User taps locations on the image using a stylus or finger. The major problem is input tolerance. It is tough to tap exact locations on the image during login, the tolerance areas should be properly defined.

2.3.2 Cued click points

Chiasson et al [10] proposed cued click points and persuasive cued click points. In Cued click points, user clicks on one point on an image to go to next round. Another image will be displayed in that round and the user has to click a point in that image. This process will be repeated five times making a password of five click points for five images. During login user has to click the same points in the same sequence. If the user clicks a wrong point, an unknown image will be displayed which gives an implicit feedback to the user. Then, the user restarts the process. Implicit feedback is not useful in the case of intruder because he knows nothing about images.

They conducted user study and reported password registration time as 25 seconds, login time as 7 seconds and login success rate as 96%. They analyzed the user choice in click points and found that passwords are predictable because most of the click
points fall within known hotspots. Chiasson et al [11] proposed persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. Persuasive technology motivates and influence people to behave in a desired manner.

![Cued click points](image)

Fig.2.10: Cued click points

### 2.3.3 Inkblot authentication

Stubblefield and Simon [63] proposed Inkblot authentication. During password registration, user watches an inkblot, assumes a word that describes the inkblot and enters first and last letters of word as part of the password. This will be repeated for number of inkblots to generate a long password. During login, the inkblots will be displayed in the same order and the user has to enter first or last character of the words assumed for those inkblots. They conducted user study in the lab with 25 users using 10 inkblots and reported 80% login success rate after one day and 72% success rate after one week. They showed that the passwords formed by Inkblot authentication are relatively strong as they have no meaning. The inkblots should be selected in such a way that the intruder should not guess the word, otherwise passwords are predictable.
2.3.4 Passlogix V-GO

V-GO [46] is the authentication technique designed by Passlogix Company. In this technique, the user clicks/drags number of background objects for password creation. The sequence of activities like preparing a meal by choosing required items and cooking is a password. The password creation depends on the environment selected for password. During login, user has to repeat the same process. This is fun to use but the passwords are predictable because of the limited objects in the environments.
2.4 Shoulder surfing resistant techniques

Graphical passwords are more vulnerable to shoulder surfing attacks than conventional textual passwords. The intruder captures the password either by direct observation or by using hidden cameras. Many shoulder surfing resistant techniques have been proposed and each technique has its own way in providing security against shoulder surfing attack.

2.4.1 S3PAS

Zhao and Li [82] proposed a shoulder surfing resistant authentication system S3PAS. During registration user selects a password and the characters in the password are known as original pass characters. The login image of S3PAS consists of randomly scattered 94 printable characters. For authentication, user has to find the positions of original pass characters and assumes invisible triangles known as pass triangles for every three pass characters in sequence. The user has to click inside the pass triangle following some rules. The clicks in sequence generate a session password.

The login image will be changed every time and in turn the session password changes. The changing login image makes S3PAS immune to the brute-force search towards the session passwords. The system might be broken once by chance with a small probability using brute-force attacks towards session password like any password system, but it is hard to get actual original password to login every time.
2.4.2 Convex Hull click

Sobrado and birget [56] developed shoulder surfing resistant graphical authentication technique. During registration, user selects pass objects from a set of objects. The login involves several rounds. For authentication, user recognizes pass objects and clicks within the convex hull of 3 pass objects. It is impossible to clearly identify pass objects on the login interface if 1000 objects are used as specified by the authors. The login time with 5 challenge was 72 seconds. The time required to rearrange the icons between the challenges was 17 seconds and total login time was 89 seconds.
2.4.3 Fake Pointer

Takada [68] designed an authentication system which is resistant to shoulder surfing and hidden cameras. User has to register two things a PIN and answer indicator which contains different shapes. The user interface of the fake pointer contains two layers the first layer contains digits and second layer contains shapes. The digits on the first layer can be rotated using key operations. Each digit of the pin should come on top of the corresponding answer indicator by key operations. The intruder may not understand the PIN even after capturing both PIN entered and login interface number of times. The major problem of this technique is user has to remember the PIN as well as answer indicator which is a difficult task.

Fig 2.15: Two layers of Fake pointer

2.4.4 CDAS (Come from DAS and Story)

Haichang et al [22] designed a shoulder surfing resistant graphical password scheme for PDAs based on the concept of DAS drawing and sequence retrieval in Story. In this technique, user selects number of images known as pass images in sequence during registration. During login, degraded images are randomly placed on the screen. The user has to draw a curve across their pass images in the same sequence without lifting the stylus from the drawing surface including the pass images and the decoy images. The user can make a story connecting the pass images to remember the
sequence. The randomly placed degraded images on the interface makes the technique strong against shoulder surfing. They conducted user study for CDAS and Story techniques in the lab with 20 students and five images as pass images. A recall test was conducted one week after the initial session. They reported the average password creation time as 49.5 seconds for CDS and 42.9 seconds for story scheme and average login time as 19.8 seconds for CDS and 23.1 seconds for story after one week.

Fig 2.16: A drawing of CDAS

2.4.5 GrIDsure

GrIDsure [21] is a pattern based authentication. Humans remember patterns much better than PINs, and this helps to create session PINs using dynamic grid. They enter PIN based on the pattern selected by him during registration. During login, a grid is displayed with randomly placed digits. User follows his pattern and enters the digits in pattern as PIN. For the pattern in the fig 2.17, the PIN is 7834. This technique is strong against shoulder surfing when the intruder captures password only. If the intruder captures both login grid and the password, it is easy to get the password.
Brostoff et al [8] evaluated usability and security of the graphical system GrIDsure scheme with 83 participants and the recall tests were conducted at different intervals. The recall success rate was 91% after 3 to 4 days and 97% after 9 to 10 days. A recall test was conducted after two years and out of 25 members participated, 27% members passed the recall test. Weber [76] analyzed and reported that grIDsure passwords are much more secure than traditional PINs against shoulder surfing attacks. Bond[6] analyzed GrIDsure and reported weaknesses of the technique.

2.4.6 Hybrid password authentication scheme

zheng et al [83] proposed a hybrid password authentication scheme for resisting shoulder surfing attack. The technique uses shapes and strokes as password and text as input. Initially, user selects a shape as password. During login, an interface grid is displayed with randomly placed bits on the grid. User maps the shape of the password to the text on the grid and enters the password. The grid contains randomly placed bits, for every login grid changes and the password changes. So, the technique generates session passwords. the authors suggested to select a number or alphabet or geometric or random shapes. They claimed that the technique is resistant against shoulder surfing, hidden cameras. No user study was done for this technique. We adopted this technique and extended it for native language character passwords for shoulder surfing resistance.
2.4.7 Shoulder surfing defence

Zakaria et al [84] proposed shoulder surfing defence for recall based graphical passwords. They proposed three techniques for protecting DAS systems from shoulder surfing – decoy strokes, disappearing strokes and line snaking. Decoy strokes draw additional strokes in addition to the strokes drawn by user while drawing the secret. Disappearing stroke defence scheme removes the stroke from the screen after it was drawn by the user. Line snaking scheme disappears the stroke drawn by the user, but it leaves some portion of it on the screen for some time. They evaluated the security and usability of the techniques and reported that 63% of the passwords were stolen in DAS and 57% passwords stolen using decoy strokes. Disappearing strokes scheme and line snaking capture 20% of the passwords. These schemes are vulnerable to hidden cameras and malware attacks.

2.4.8 Other techniques

Lin et al [35] proposed QDAS (Qualitative Draw-A-Secret) which is a variation of the DAS technique. Qualitative mapping between user strokes and the password is used to make the technique shoulder surfing resistant. The use of qualitative spatial relations relaxes the tight constraints on the reconstruction of a secret; allowing a range of deviations from the original.

Man et al [38] proposed a technique which is resistant to shoulder surfing. During registration user selects number of pass objects. Each pass object has several variants and each variant is assigned a unique code. During login time, the login interface contains number of pass objects along with decoy objects. User recognizes the pass objects and enters the code assigned to them and the relative location of the pass...
objects with respect to a pair of eyes. User has to face several such interfaces for authentication.

Hong et al [24] extended the technique proposed by man et al. It permits to assign codes to the pass objects variants by the users. When the codes are assigned by users, they are able to remember the codes better than the codes assigned by the system. User has to remember many codes for these two techniques.

Malek et al [37] proposed a haptic based authentication technique. In this technique haptic device is used to measure the pen pressure applied by the user while drawing the secret which is not visible to the intruder. The user study conducted to evaluate the usability reported that users apply very little pen pressure and hardly lifted the pen while drawing.

Sreelatha et al [60] proposed image based authentication techniques for PDAs. Pair based image authentication technique uses recognition based approach in which user has to recognize his pairs. Text based image authentication uses both recognition and recall based approaches where user has to recognize his images and recall the characters assigned to them.

Sreelatha et al [57] proposed two techniques for generating session passwords for PDAs with text and color and the techniques are resistant to shoulder surfing. Sreelatha et al [59] proposed two authentication schemes - color and image signature scheme and coded color authentication scheme. These techniques generate session passwords and are resistant to shoulder surfing attack and hidden cameras.

Sreelatha and Shashi [58] proposed a technique to provide confidentiality to the data being transmitted. They used shape based technique to send data from a sender to
receiver. In a 5x5 grid, the data to be transmitted is placed in the cells that form the shape of the character and remaining part is filled with random data by the sender and the grid data is transmitted to the receiver. The receiver follows the same process and extracts the actual data transmitted. Sreelatha et al [61] proposed color coding instead of bits to increase the amount of data being transmitted. Mahansaria et al [16] designed SS7.0. During registration, user selects a password. The login interface contains a matrix with randomly placed alphabets, digits and special characters. User refers the matrix and enters the row number and column number of each character in the password for generating a session password. For every login, interface changes and thus the session password changes. Though user study was not done, login takes more time to find rows and columns of each character.

The three types of techniques - recognition based, recall based and cued recall were studied and drawbacks of those techniques were given.

Recognition based techniques are good in memorability, users are able to remember and recognize the passwords successfully. The server has to maintain large number of images or faces and for every round of authentication, server has to prepare the challenge set for every user. Due to the limited number of images in the challenge set and few rounds used for authentication, the password space is less in recognition based techniques and in turn these are vulnerable to password guessing attacks. The Password capturing attacks require multiple logins to get the complete portfolio of the user. The password creation time and login times are more compared to recall based techniques.
Recall based techniques have large password space and are secure against password guessing attacks. There is no need to maintain large number of images or faces by the server and no requirement of forming the challenge set. The Password creation and login times are less than the other two techniques. The recall based techniques are vulnerable to password capturing attacks because in a single session or by single observation the intruder may get the password. The password complexity depends on the number and the length of the strokes in password. But it is difficult to remember the order of the multiple strokes in random shape passwords. Drawing a password with mouse is inconvenient.

Cued recall systems are good in memorability. Cues help the users to retrieve the passwords from memory without writing anywhere. The security of passwords in cued recall system depends on the image selected for authentication. Generally, images will be having limited number of clickable points for password selection which reduces the password space and in turn, passwords are vulnerable to password guessing attacks. These are vulnerable to password capturing attacks because entire password or user’s portfolio will be displayed for every login which can be observed by the intruders. Password creation and login times are more compared to recall systems.

The details collected for various graphical authentication techniques from different sources (approximate values) were given in table 2.3. Each technique has its own way for evaluation of usability and security. The details about shoulder surfing systems were given in table 2.4.
Table 2.3: Details of Graphical authentication systems

<table>
<thead>
<tr>
<th>Name</th>
<th>type</th>
<th>Registration time(seconds)</th>
<th>Login time (seconds)</th>
<th>Recall success rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deja Vu</td>
<td>Recognition</td>
<td>45</td>
<td>32-36</td>
<td>90-100 %</td>
</tr>
<tr>
<td>Passfaces</td>
<td>Recognition</td>
<td>180-300</td>
<td>14 - 88</td>
<td>72 – 100%</td>
</tr>
<tr>
<td>Faces</td>
<td>Recognition</td>
<td></td>
<td></td>
<td>90 – 98%</td>
</tr>
<tr>
<td>Story</td>
<td>Recognition</td>
<td>42.9</td>
<td>23.1</td>
<td>85%</td>
</tr>
<tr>
<td>DAS</td>
<td>Recall</td>
<td></td>
<td></td>
<td>57 – 80%</td>
</tr>
<tr>
<td>PASS-GO</td>
<td>Recall</td>
<td></td>
<td></td>
<td>78%</td>
</tr>
<tr>
<td>PassShapes</td>
<td>Recall</td>
<td></td>
<td></td>
<td>63-100%</td>
</tr>
<tr>
<td>Pass doodle</td>
<td>Recall</td>
<td></td>
<td></td>
<td>38 – 46%</td>
</tr>
<tr>
<td>PassPoint</td>
<td>Cued</td>
<td>64 + 171</td>
<td>9 – 25</td>
<td>55 – 90 %</td>
</tr>
<tr>
<td>Cuedclickpoints</td>
<td>Cued</td>
<td>&lt;=30</td>
<td>&lt; 10</td>
<td>96%</td>
</tr>
<tr>
<td>PCCP</td>
<td>Cued</td>
<td></td>
<td>11 – 89</td>
<td>83 – 94 %</td>
</tr>
<tr>
<td>Inkblot</td>
<td>Cued</td>
<td></td>
<td></td>
<td>68 – 80%</td>
</tr>
</tbody>
</table>

Table 2.4: Details of shoulder surfing resistant systems

<table>
<thead>
<tr>
<th>Name</th>
<th>Registration time</th>
<th>Login time</th>
<th>Recall success rate</th>
<th>Shoulder surfing capture rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDS</td>
<td>49.5</td>
<td>19.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHC</td>
<td>89 (72+17)</td>
<td></td>
<td>90 %</td>
<td></td>
</tr>
<tr>
<td>GrIDsure</td>
<td></td>
<td></td>
<td>87 %</td>
<td></td>
</tr>
<tr>
<td>SS7.0</td>
<td>20 – 90</td>
<td></td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td>DAS (zakaria)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAS with decoy strokes</td>
<td></td>
<td></td>
<td>57 %</td>
<td></td>
</tr>
<tr>
<td>DAS with defence</td>
<td></td>
<td></td>
<td>20 %</td>
<td></td>
</tr>
</tbody>
</table>