AUTHENTICATION SYSTEM – OVERVIEW OF GRAPHICAL PASSWORDS

Ms.DHIVIYAA.S[1], Ms.RAKSHITHA.K.R[2], Ms.VIJAYABHARATHI.R[3]

[1]Assistant Professor, Department of Computer Applications and Master of Software Systems, Sri Krishna Arts and Science College, Coimbatore, India
[2,3] Student, Department of Computer Applications and Master of Software Systems, Sri Krishna Arts and Science College, Coimbatore, India

---***---

Abstract - *Nowadays, user authentication is one of the significant topics in information security. Text-based strong password schemes could provide with a certain stage of security. However, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even deliver them in a computer file. Graphical authentication was proposed as an alternative to text passwords as it is easy to remember and provides better security. Nowadays graphical techniques are used for authentication by many networks, computer systems, and Internet-based environments. This paper presents a review of the recognition based and recall based authentication algorithms and finally describing the proposed systems called cued click points and persuasive click points for better security using graphical passwords.*

***Key Words*:** **Token, Biometric, Textual passwords, Graphical passwords, Recall based algorithms, Recognition based algorithms**

1. INTRODUCTION

In recent years, computer and network security have been developed as a technical problem. A central area in security research is the authentication which is the determination of whether a user should be allowed access to a given system or resource. In this respect, the password is a common and widely authentication method still practiced up to now. A password is a form of secret authentication information that is used to control access to a resource. It is kept confidential from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. In modern times, passwords are used to moderate access to protect computer operating systems, mobile phones, auto teller machine (ATM) machines, and others. Passwords may also be required by users for many purposes such as logs into computer accounts, recovering email from servers, accessing of files, databases, networks, and websites. Some drawbacks of normal password appear like stolen the password, forgetting the password, and a weak password. Thus, a big necessity to have a strong authentication method is needed to secure all our applications as possible. Today, another method such as graphical authentication is one of the potential alternative solutions. Psychological studies have demonstrated that people can remember pictures better than text passwords hence graphical passwords are believed to be a good alternative for text passwords. Images are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures.

2. AUTHENTICATION TECHNIQUES

The process of identifying a person by username and password is called as authentication. Authentication methods can be divided into three types such as token-based, biometric-based and knowledge-based.

2.1. TOKEN-BASED AUTHENTICATION

In this technique cards like smart cards, ATM cards, credit cards, etc., are mostly used for authentication purpose

2.2. BIOMETRIC BASED AUTHENTICATION

In biometric authentication technique for security purpose fingerprints, iris, and facial expressions are used as words. Sometimes the voice is likewise used for security purpose. This furnishes a strong security system, but it requires highly expensive devices.

2.3. KNOWLEDGE BASED AUTHENTICATION

In this knowledge-based authentication, text-based password and graphical passwords are utilized.

- **TEXT PASSWORDS**

The commonly used authentication technique is text password. In this, the sequence of characters is applied as the password. The text password is very easy to get around. Thus in order to make a strong character password symbols, numbers, and other special characters should be added. Length of character is also a keen concern.

- **GRAPHICAL PASSWORDS**

In graphical password system user have to select from images in a particular order that is presented in the graphical user interface. Graphical passwords were originally described by Blonder. In his description, an image may appear on the screen and the user would click on the image if right places are clicked then the user will be authenticated. In a graphical password system, a user should choose a memorable picture. The procedure of choosing memorable images depends on the nature of the process of image and the specific sequence of click locations. In ordination to support memorize ability; images should have meaningful content because the meaning of arbitrary things is poor. The graphics authentication techniques can be parted into two categories of graphical techniques:

- Recognition based
- Recall based

3. RECOGNITION-BASED TECHNIQUES

3.1. PASS FACE SCHEME

In 2000, this method developed which used faces as an object for a password. During the registration process, the user's select whether their Pass face consists of a male or female picture. And so they choose four faces from the database as their future password. On the next step, a trial version is started for the user in order to determine the real login process. During the visitation, the others took twice through the Pass face login procedure with their Pass face which is shown to them. The registration will be completed by correctly identifying their four Pass faces twice in a row with no prompting, entering an enrollment password.

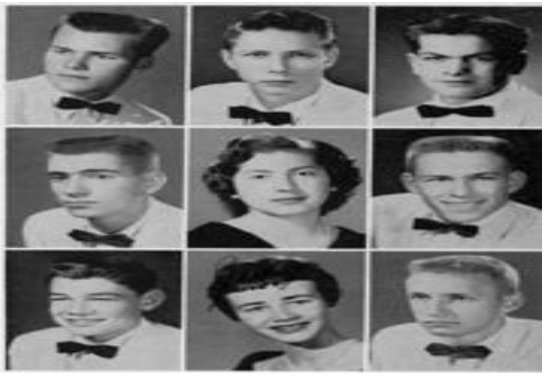


Fig1. Pass face Scheme, 1999

3.2. DÉJÀ VU SCHEME

This model proposed in 2000, by letting users select a specific number of pictures among large images portfolio. As the designer wanted to cut down the chance for description attack, the pictures create according to random art. Firstly, one initial seed (a binary string) is given, and then one random mathematical formula generates which defines the color value for each pixel in the icon. The turnout will be according to one random abstract image. Because the image depends only on the initial seed, it is not necessary to store the picture pixel by pixel so only the seeds need to be stored on the trust server. During the authentication stage, the user should think a challenging set which his portfolio mixes with some decoy images. If the user can name his entire portfolio successfully, he will be authenticated.

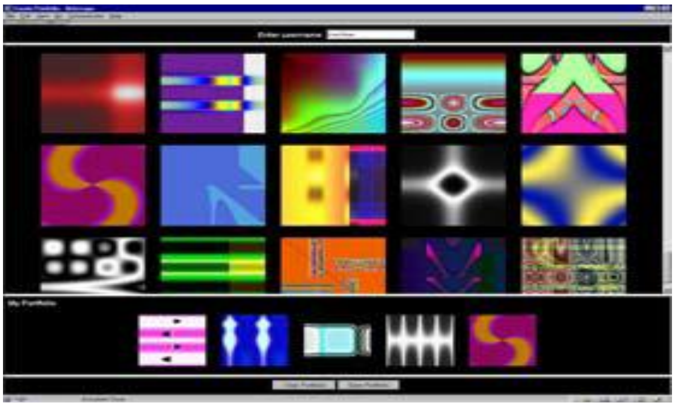


Fig2. Déjà vu Scheme, 2000

3.3. TRIANGLE SCHEME

In 2002, Triangle algorithm was suggested. This system randomly assigns a set of N objects which could be a hundred or a thousand on the screen addition, there is a subset of K objects previously selected and memorized by the user.er. In other languages, these K objects are the user password during login the system will randomly select a placement of the N objects, then the user must get three of his passwords objects and click inside the invisible triangle created by those three objects or click inside the convex hull of the pass objects that are displayed.

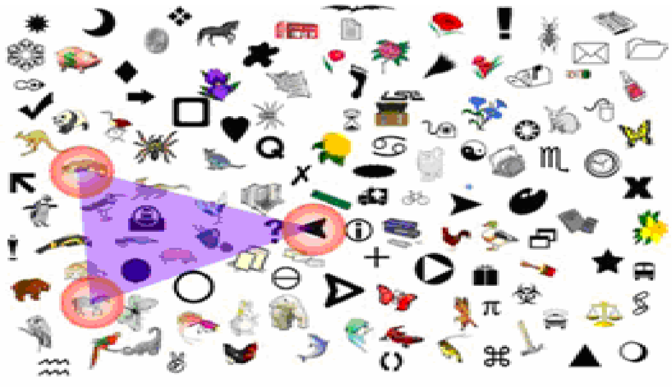


Fig3. Triangle Scheme, 2002

3.4. MOVABLE FRAME SCHEME

In 2002, this model produced using the same ideas and presumptions as a Triangle scheme with the same designers. In this method, the user must place three out of K objects which these three are user passwords. Only three pass objects are displayed at any fed time and only one of them is placed in a movable frame. During the login phase, the user has to displace the frame and the objects within it by dragging the mouse around the frame until the password object placed on the frame lines up with the other two pass objects. To downplay the likelihood of randomly moving the frame, the procedure is repeated a few times.

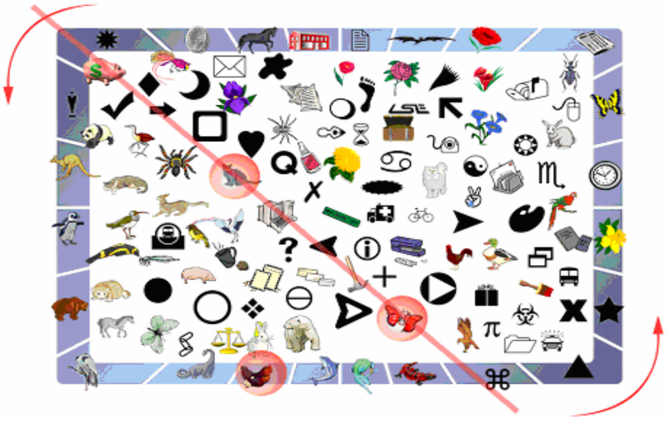


Fig4. Moveable Frame Scheme, 2002

3.5. PICTURE PASSWORD SCHEME

In 2003, this algorithm designed especially for a handheld device like a Personal Digital Assistant (PDA). During enrollment, a user selects a theme, placing the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used as a future password. When the PDA is turned on, the user must insert the currently enrolled image sequence for verification to gain access to the device. After a successful authentication, the user may change the password and select a new sequence or composition. As the numbers of thumbnail photos are limited only to 30, the size of the password space is considered low. To match the password space of alphanumeric password, the designer added another method of selecting thumbnail element.

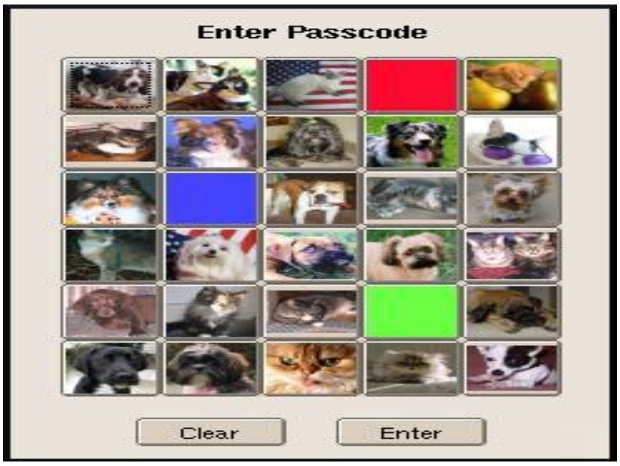


Fig5. Picture Password Scheme, 2003

3.6. MAN ET AL. SCHEME

In 2003, this algorithm proposed a novel method for graphical password shoulder-surfing resistant. In this algorithm, all the pictures have been allotted a unique code. A screen appears which consists of several password objects and many decoys one during the time of authentication to the user. Equally, there is a unique code for each password object; the user will enter the string of code for his password. It is really hard for shoulder surfers to crack this kind of password even if the whole authentication process is recorded. Nevertheless, this method still requires users to memorize the code for each password object variant. For instance, if there are 4 pictures each with 4 variants, then each user has to memorize 16 codes which are a drawback.

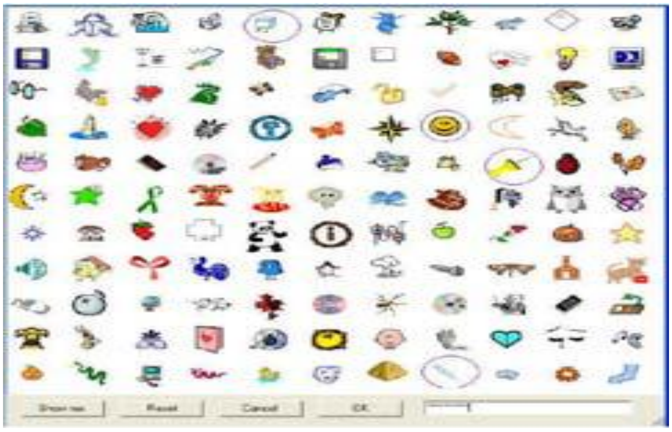


Fig6. Man et al Scheme, 2004

3.7. STORY SCHEME

In 2004, the story scheme proposed by categorizing the available picture into nine classes which are animals, cars, women, food, children, men, objects, nature, and sport. The users have to select their passwords from the mixed pictures of nine classes in order to make a story easy to remember. In that location were some users who used this method without defining a story for themselves. This research indicated that the story scheme was harder to remember in comparing to Pass face authentication.

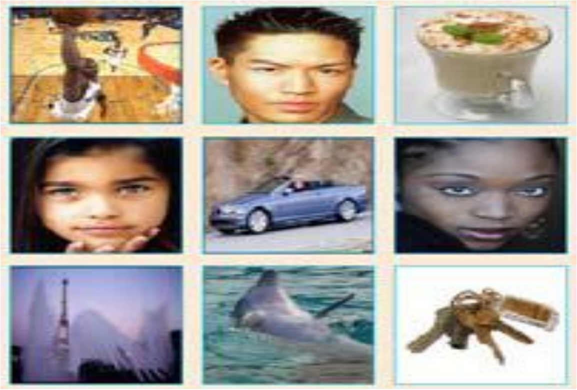
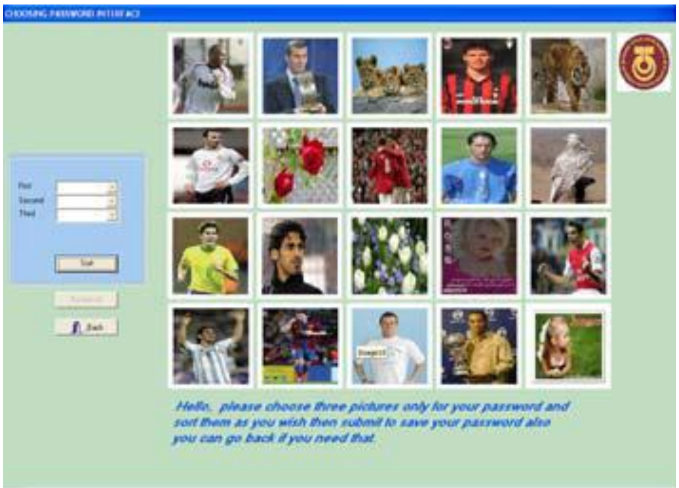


Fig7. Story Scheme, 2004

3.8. JETAFIDA SCHEME

In 2008, this model is offered based on trying to gather all the usability features, like the ease of use, easy to create, easy to memorize, easy to learn and acceptable design and layout in one algorithm. During registration, the user will choose three pictures as a password and then sort them according to the way he wanted to see them in login phase.



Hello, please choose three pictures only for your password and sort them as you wish then submit to save your password also you can go back if you need that

Fig8. Jetafida Scheme, 2008

4. RECALL BASED TECHNIQUE:

A user should reproduce something that the user had produced before during registration stage. Recall-based, password authentication is categorized into two sections:

- Pure Recall Based Technique
- Cued Recall Based Technique

A. PURE RECALL BASED:

In this procedure, a user generates his password, without yielding any clue or reminder. It follows many algorithms, which include:

4.1. PASS DOODLE

Pass doodle is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch-sensitive screen. In their 1999 paper, Jermyn et al. prove that doodles are harder to break due to a theoretically much larger number of possible doodle passwords than text passwords.

Fig9. A sample of a Pass doodle algorithm

4.2. DRAW A SECRET (DAS)

In 1999, this method present by letting the user draw a simple picture on a 2D grid as in the Figure. The interface consists of a rectangular grid of size G * G. Each cell in this grid is denoted by discrete rectangular coordinates (x, y). Equally, it can be seen in the figure, the coordinate sequence generated by drawing is: (2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5, 5).▯

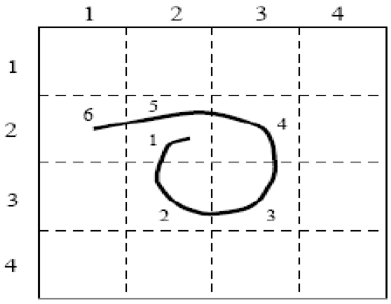


Fig10. Draw a Secret (DAS) method on a 4*4 Grid

4.3. GRID SELECTION

In 2004, Thorpe and van Oorschot further studied the impact of word length and stroke-count as a complexity property of the DAS scheme. Their work showed that stroke-count has the largest impact on the DAS password space -- The size of DAS password space decreases significantly with fewer strokes for a fixed password length. The length of a DAS password also has a significant impact, but the impact is not equally strong as the stroke-count. To better the security, Thorpe and van Oorschot proposed a "Grid Selection" technique. The selection grid is an initially large, fine-grained grid from which the user takes a drawing grid, a rectangular region to zoom in on, in which they may enter their password and thus DAS password space is increased.

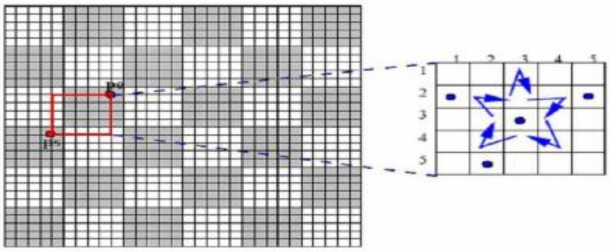


Fig11. A sample of Grid Selection method

4.4. QUALITATIVE DAS (QDAS)

It is an enhancement of DAS method created by establishing a code of each stroke. The raw encoding consists of its starting cell and the succession of qualitative direction change in the stroke relative to the grid. We depict a raw coding, which only consists of starting cell, where the direction is changing when a pen across the previous cell boundary.

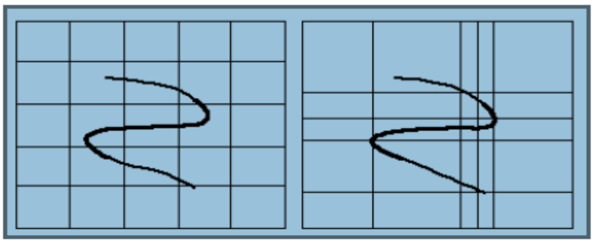


Fig12. A sample of Qualitative DAS algorithm

4.5. SYUKRI ALGORITHM

Syukri algorithm proposes a system where certification is conducted by having user drawing their signature using the mouse. This technique includes two stages, namely, registration and check. The users are asked to draw their signature with the mouse during registration stage and the signature area will be then extracted from the system which may be either enlarged or rotated if needed. The information will subsequently be saved in the database. The verification stage first takes the user input, and makes out the normalization again, and then extracts the parameters of the signature. The system conducts verification using geometric average means and a dynamic update of the database. According to the subject area, the rate of successful verification was satisfying. The greatest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake.

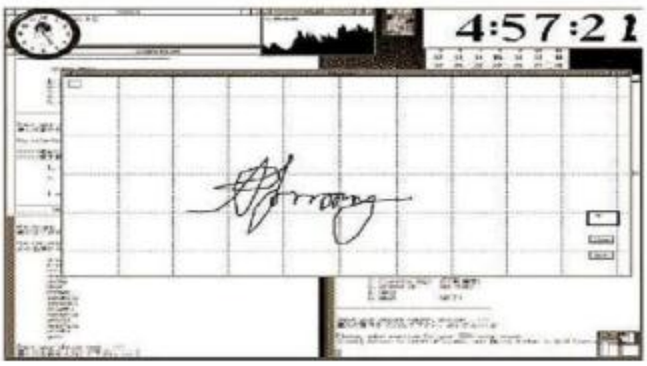


Fig13. A sample of Syukri algorithm

B. CUED-RECALL BASED:

In the cued recall based technique, the images are cued for the user from which the user has to click set of points and also hints will be provided which will help the user to reproduce it again during login phase. It follows many algorithms, which include:

4.6. BLONDER

This method was originated by Greg. E. Blonder, in which there are restored images in the database of account to use on visual presentation and user supposed Tap region by pointing location in the image. According to Blonder, this is a more dependable method. The drawback of this scheme was clicking region was very small and may be crackable. Blonder is the first technique used by the user as a graphical password. Because of its limitation, Blonder technique is further stretched as a Draw-A-Secret.

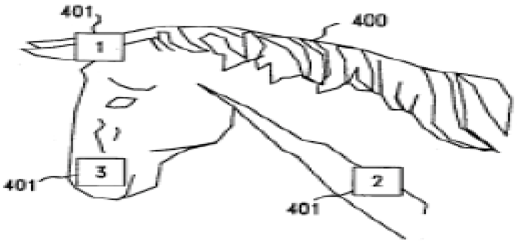


Fig14. A sample of Blonder algorithm

4.7. PASS POINT

Pass point uses natural pictures or even paintings which should be rich enough to have many click points. This system was proposed to wrap the limitations of Blonder algorithm. In this technique, the image is not secret and has no option for the user to remember the click point by fading to the next click. Some other source of flexibility is that there is no need for artificial predefined click regions with well-marked boundaries like the blonder algorithm. The user chooses several points on the picture in a particular society.

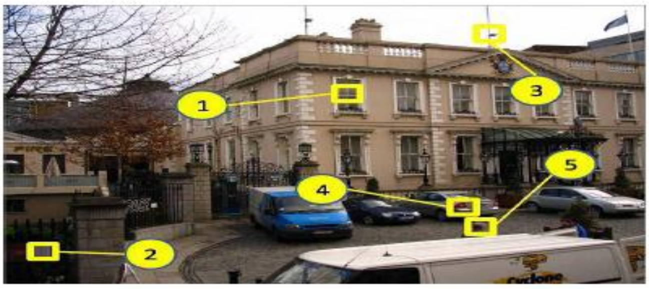


Fig15. A sample of Pass point algorithm

4.8. BACKGROUND DAS (BDAS)

In 2007, this method proposed by adding a background picture to the original DAS for improvement, so that both background image and the drawing grid can be used to provide cued recall. The user begins by using three different ways:

i. The user holds a secret in mind to begin, and then draw using the point from a background image.

ii. The user's choice of a secret is affected by the various parts of the image.

iii. A mix of two above methods.

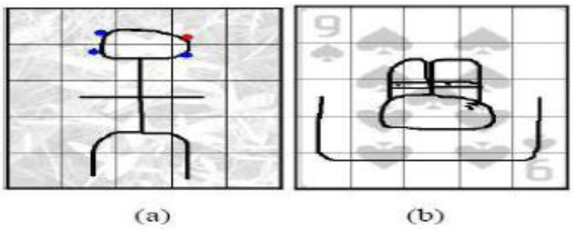


Fig16. A sample of BDAS algorithm

4.9. PASS MAP

One of the primary problems with passwords is that very good passwords are hard to remember and the one which is easy to remember is too short of simple to be secured. From the subjects of human memory, we know that it is relatively easy to remember landmarks on a well-known journey.

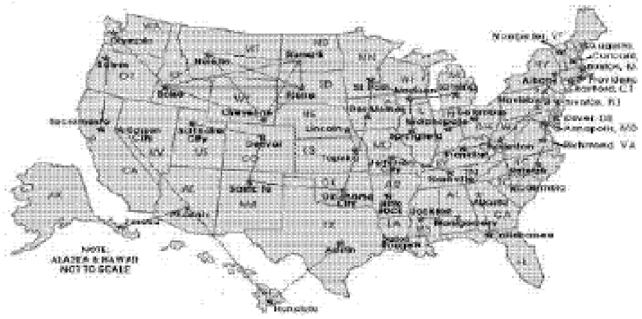


Fig17. A sample of PASS MAP algorithm

4.10. PASSLOGIX V-GO

Passlogix Inc. is a commercial security company located in New York City USA. Their scheme called Passlogix v-Go uses a technique known as "Repeating a sequence of actions" which entails creating a password by a chronological situation. In this system, the user can select their background images based on the environment, for instance, in the kitchen, bathroom, bedroom or others. To enter a password, the user can flick and/or drag on a series of items within that image.

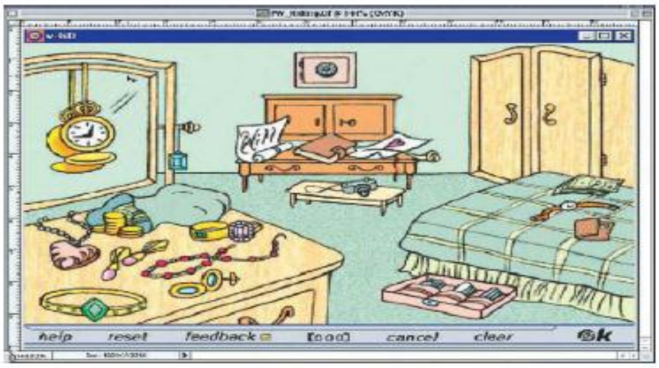


Fig18. A sample of PASS MAP algorithm

4.11. CUED CLICK POINTS

By selecting all click point on single image introduces hotspot creation. In CCP user have to select different five images instead of selecting, click a point on the same picture, the next image will be displayed. In the CCP address of adjacent images is stored in previous click point. If click point is wrong, then the wrong image will be exhibited. Users have to select a sequence of click point on correct images.

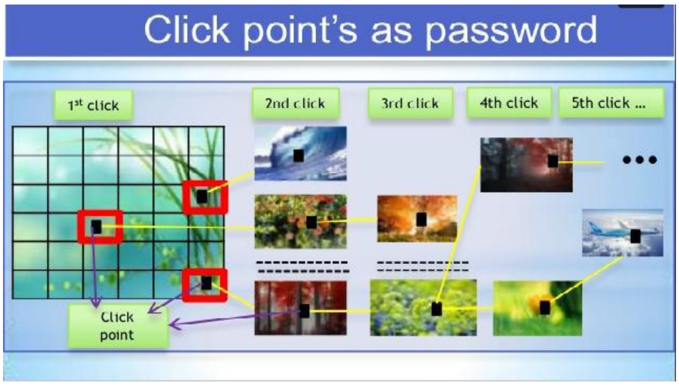

Click point's as password

Fig19. A sample of CCP

4.12. PERSUASIVE CUED CLICK POINTS

Persuasive Cued click point technique was proposed by Fogg, in which the user will select the image that automatically selects the block named viewport. The viewport can be gone anywhere on an image by shuffle button will be displayed.

Fig20. A sample of PCCP

5. CONCLUSION

In time to come, it has a great scope. It can be used everywhere instead of a text-based password. We can increase the surety of this system by increasing the number of levels used, the number of tolerance squares used. Currently, there are many authentication systems, but they have their own advantages and disadvantages. Text password can be hacked easily with various methods whereas biometric authentication can cause more cost. This system is more dependable and cheap than old methodologies. This system allows more reliable and easily recognizable system to the users.

REFERENCES

[1] M.Swathi, M.V.Jagannatha Reddy, ”Authentication Using Persuasive Cued Click-Points”, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 7, July – 2013, ISSN: 2278-0181.

[2] Farnaz Towhidi, Maslin Masrom, “A Survey on Recognition - Based Graphical User Authentication Algorithms”, International Journal of Computer Science and Information Security (IJCSIS), Vol.6, No. 2, 2009, ISSN 1947-5500.

[3] Maslin Masrom, Farnaz Towhidi, Arash Habibi Lashkari, “Pure and Cued Recall-Based Graphical User Authentication” Research Gate Conference paper DOI: 10.1109/ICAICT.2009.5372534