A Survey on Recall-Based Graphical User Authentications Algorithms

D.Aarthi[1], Dr.K.Elangovan[2]

[1] School of Computer Science and Engineering, Bharathidasan University, Trichy, India

[2] School of Computer Science and Engineering, Bharathidasan University, Trichy, India

[1] aarthiviji89@gmail.com

[2] murthy.elango@gmail.com

Abstract- A password is a secret word or combination of alphabets used for user authentication to establish self identity. This password should be kept secret from those not allowed to access. Now-a-days data security is the most describing problem. Token based authentication like Smart card, Biometric based authentication like iris, fingerprint, facial, Knowledge based authentication like text based and Image based password. Graphical user authentication (GUA) has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. In recent years, many networks, computer systems and Internet-based environments try used GUA technique for their user's authentication. All of GUA algorithms have two different aspects which are usability and security. Unfortunately, none of graphical algorithms were being able to cover both of these aspects at the same time. In this paper we will study survey of different types of Recall-based graphical user authentication algorithm based on usability attributes and attack pattern those we found and also different factors affecting to it.

Key words: *Graphical Password, User authentication, pure recall-based algorithm, cued recall-based algorithm, Attack Pattern.*

I. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. Humans have used three methods for authentication. These methods are:

Something you know (the password)

Something you have (credit card, university ID card)

Something you are (face, voice, signature, fingerprints, DNA, iris)

Today, these methods are called the three factors of authentication. They are

Token based authentication (smart cards, credit cards)

Biometric based authentication (fingerprints, iris scan, or facial recognition)

Knowledge based authentication (text based, graphical based)

The use of passwords goes back to ancient times when soldiers guarding a location by exchange a password and then only allow a person who knew the password. In modern times, passwords are used to control access to protect computer operating systems, mobile phones, auto teller machine (ATM) machines, and others.

A typical computer user may require passwords for many purposes such log in to computer accounts, retrieving e-mail from servers, accessing to files, databases, networks, web sites, and even reading the morning newspaper online. In graphical password, the problem arises because passwords are expected to have two fundamentals requirements:
i. Password should be easy to remember.
ii. Password should be secured.

In a graphical password system, a user needs to choose memorable image. The process of choosing memorable images depends on the nature of the process of image and the specific sequence of click locations. In order to support memorize ability, images should have meaningful content because meaning for arbitrary things is poor. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques .Now we discuss about Recall-based technique.

II. RECALL-BASED ALGORITHMS

A user is asked to reproduce something that he or she created or selected earlier during the registration stage .Recall-based password authentication are categorize in
two parts :
i) Pure Recall Based Technique
ii) Cued Recall Based Technique

Pure Recall Based:
In this procedure, a user generate his password without giving any clue or reminder. It follows many algorithms, which include:

1. Passdoodle (Pure recall)
Passdoodle 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 crack due to a theoretically much larger number of possible doodle passwords than text passwords.

Figure 1: An Example of a Passdoodle

2. Draw A Secret (DAS) (Pure recall)
In 1999, this method present by allowing the user to drawing a simple picture on a 2D grid as in Figure. The interface is consisting of a rectangular grid of size G * G. Each cell in this grid is denoted by discrete rectangular coordinates (x,y). As 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).

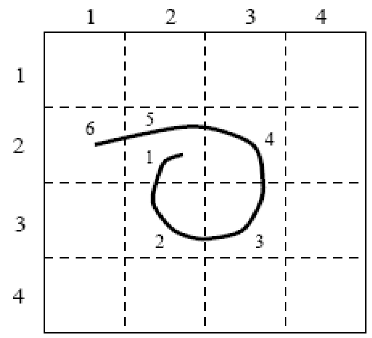


Figure 2: Draw a Secret (DAS) method on a 4*4 Grid

3. Grid Selection (Pure recall)

In 2004, Thorpe and van Oorschot further studied the impact of password length and stroke-count as a complexity property of the DAS scheme. Their study 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 as strong as the stroke-count. To improve 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 selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password. This would significantly increase the DAS password space .

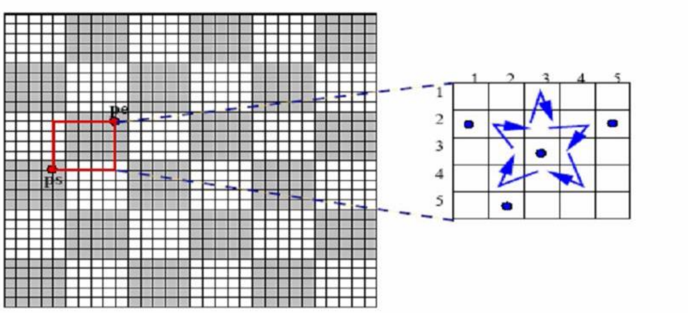


Figure 3: A sample of Grid Selection method

4. Qualitative DAS (QDAS) (Pure recall)

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

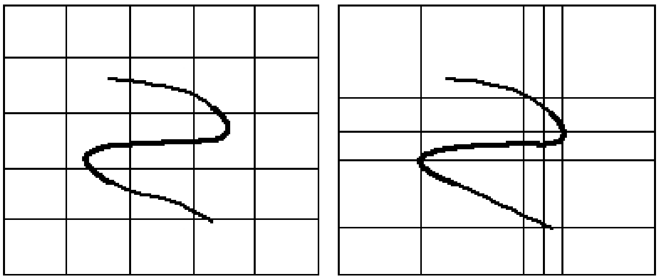


Figure 4: A sample of Qualitative DAS Algorithm

5. Syukri Algorithm (Pure recall)

Syukri algorithm proposes a system where authentication is conducted by having user drawing their signature using mouse. This technique includes two stages, namely, registration and verification. During the registration stage, user will first be asked to draw their signature with mouse, and then the system will extract the signature area and either enlarges or scale-down signatures, rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. The system conducts verification using geometric average means and a dynamic update of database. According to the study, the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake.

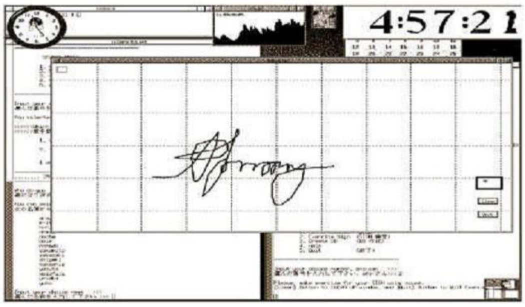


Figure 5: A sample of Syukri algorithm

Cued-Recall Based:

In the cued recall based technique, the image cues the user. For example to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords. It follows many algorithms, which include:

1. Blonder (cued recall)

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

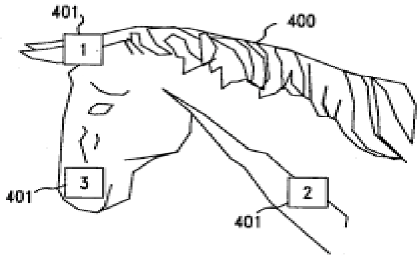


Figure 6: A sample of Blonder method

2. PassPoint (cued recall)

Passpoint was designed in order to cover the limitation of Blonder algorithm. The picture could be any natural picture or painting but at the same time should be rich enough in order to have many possible click points. In this technique image is not secret and has no option to user to remember the click point by passing to next click. Another source of flexibility is that there is no need for artificial predefined click regions with well-marked boundaries like blonder algorithm. The user is choosing several points on picture in a particular order.

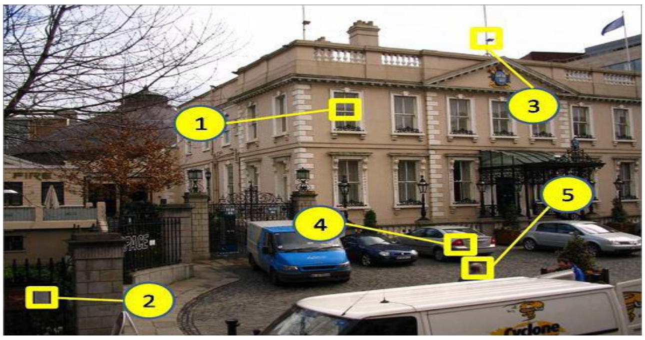


Figure 7: A sample of Passpoint method

3. Background DAS (BDAS) (cued recall)

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

i. The user have secret in mind to begin, and then draw using the point from a background image.
ii. The user's choice of secret is affected by various characteristic of the image.
iii. A mix of two above methods.

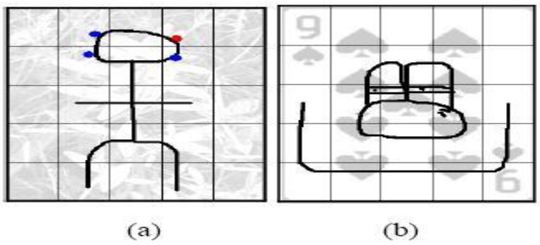


Figure 8: A sample of BDAS algorithm

4. PASSMAP (cued recall)

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

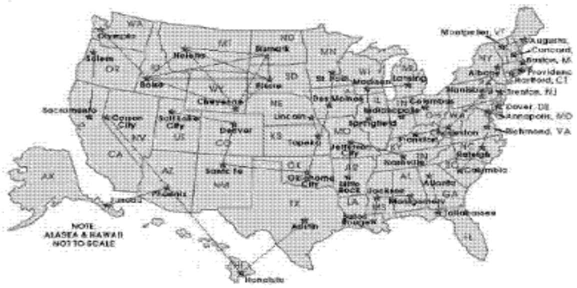


Figure 9: A sample of PASSMAP method

5. Passlogix v-Go (cued recall)

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 means creating a password by a chronological situation. In this scheme, user can select their background images based on the environment, for example in the kitchen, bathroom, bedroom or others. To enter a password, user can click and/or drag on a series of items within that image.

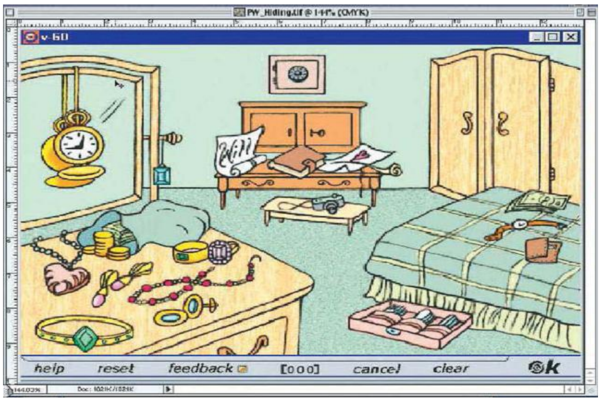
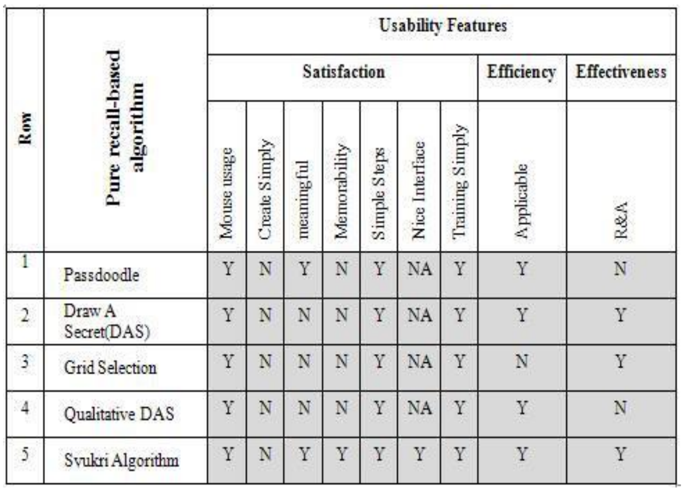


Figure 10: A sample of PASSMAP method

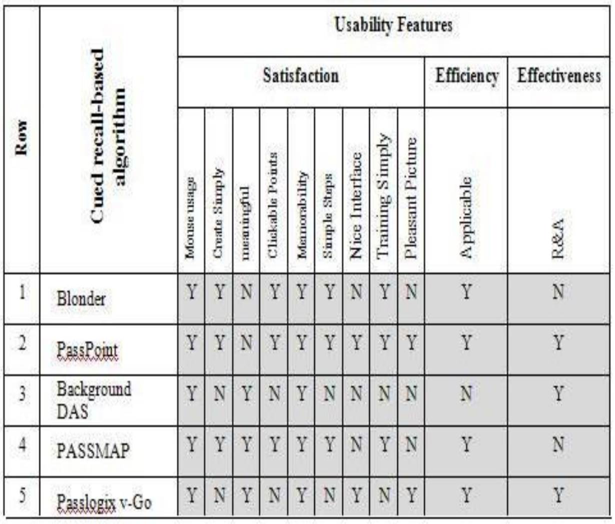
III. USABILITY IN RECALL-BASED TECHNIQUES

We can make a comparison table among all recall-based algorithms in two categories as pure and cued recall-based algorithm that you can find in tables below



Row	Pure recall-based algorithm	Usability Features								
		Satisfaction							Efficiency	Effectiveness
		Mouse usage	Create Simply	meaningful	Memorability	Simple Steps	Nice Interface	Training Simply	Applicable	R&A
1	Passdoodle	Y	N	Y	N	Y	NA	Y	Y	N
2	Draw A Secret(DAS)	Y	N	N	N	Y	NA	Y	Y	Y
3	Grid Selection	Y	N	N	N	Y	NA	Y	N	Y
4	Qualitative DAS	Y	N	N	N	Y	NA	Y	Y	N
5	Syukri Algorithm	Y	N	Y	Y	Y	Y	Y	Y	Y

Table 1: The Usability features in Pure Recall-Based Techniques



Row	Cued recall-based algorithm	Usability Features										
		Satisfaction									Efficiency	Effectiveness
		Mouse usage	Create Simply	meaningful	Clickable Points	Memorability	Simple Steps	Nice Interface	Training Simply	Pleasant Picture	Applicable	R&A
1	Blonder	Y	Y	N	Y	Y	Y	N	Y	N	Y	N
2	PassPoint	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
3	Background DAS	Y	N	Y	N	Y	N	N	N	N	N	Y
4	PASSMAP	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N
5	Passlogix v-Go	Y	N	Y	N	Y	N	Y	N	Y	Y	Y

Table 2: The Usability features in Cued Recall-Based Techniques

IV. ATTACKS ON RECALL-BASED ALGORITHMS

In reference to the Common Attack Pattern Enumeration and Classification (CAPEC) Standard Abstraction Attack Pattern List and other resources of attacks, finally we found six attacks method that is efficient in graphical user authentication (GUA) algorithms. Now, explain these attacks methods and then tries to make a comparison table among all recall-based algorithms

BRUTE FORCE

The main defence against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords . Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

DICTIONARY ATTACKS

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

GUESSING

Password guessing attacks can be broadly categorised into online password guessing attacks and offline dictionary attacks. In an online password guessing attack, an attacker tries a guessed password by manipulating the inputs of one or more oracles. In an offline dictionary attack, an attacker exhaustively searches for the password by manipulating the inputs of one or more oracles. As many users try to select their password based on their personal information like the name of their pets, passport number, family name and so on, the attacker try to guess. More research efforts are needed to understand the nature of graphical passwords created by real world users.

SPYWARE

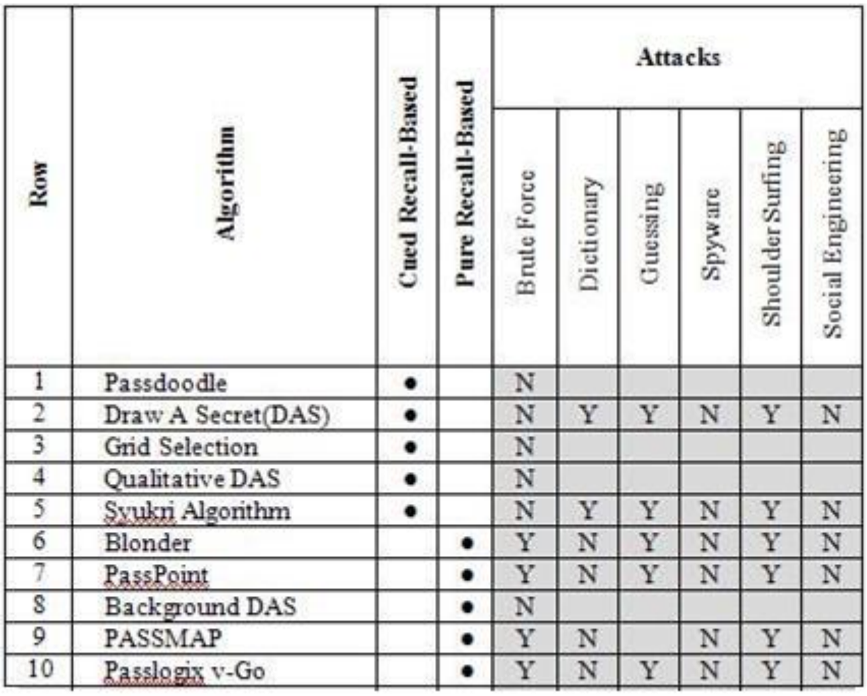
Spyware is a type of malware which installed on computers with the aim of collecting sensitive information of users, using a key logger or key listener. This information gathered without user's knowledge and report back to an outside source. During graphical password authentication the attacker attempt to gain sensitive information like user names or selected passwords images by intercepting information exchanged. Such information has to be correlated with application information, such as window position and size, as well as timing information.

SHOULDER SURFING

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is effective in crowded places because it's really easy to stand near someone and watch them entering a PIN number at an ATM machine. This attack is also possible at a distance using vision-enhancing devices like miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.

SOCIAL ENGINEERING (DESCRIPTION)

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming. Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.



Row	Algorithm	Cued Recall-Based	Pure Recall-Based	Attacks					
				Brute Force	Dictionary	Guessing	Spyware	Shoulder Surfing	Social Engineering
1	Passdoodle	●		N					
2	Draw A Secret(DAS)	●		N	Y	Y	N	Y	N
3	Grid Selection	●		N					
4	Qualitative DAS	●		N					
5	Syukri Algorithm	●		N	Y	Y	N	Y	N
6	Blonder		●	Y	N	Y	N	Y	N
7	PassPoint		●	Y	N	Y	N	Y	N
8	Background DAS		●	N					
9	PASSMAP		●	Y	N		N	Y	N
10	Passlogix v-Go		●	Y	N	Y	N	Y	N

Table 3: The attacks peruse in Recall-Based algorithms

V.STRENGTH AND WEAKNESS OF RECALL-BASED ALGORITHMS

We can make a table for explaining the strength and weakness among all recall-based algorithms in two categories as pure and cued recall-based algorithm.

Algorithms	Pure Recall based Algorithm	Cued Recall based Algorithm	Strength	Weakness
Passdoodle	•		Harder to crack due to a theoretically much larger number of possible doodle passwords than text passwords	People were less likely to recall the order in which they drew a doodle than the resulting image.
Draw A Secret	•		User can draw a simple image or picture on grid , of size say N*N. when compare to passdoodle is more than harder to crack	The users tend to choose frail graphical passwords that are vulnerable to the graphical dictionary attack
Grid Selection	•		It significantly increase the DAS password space	The lacks of DAS doesn’t solve yet
Qualitative DAS	•		The image which has more area of interest (Hot Spot) could be more useful as a background image	This model have more entropy than previous DAS but it has less memorable than the original one

Syukri Algorithm	•		user drawing their signature using mouse and there is no need to memorize one's signature and signatures are hard to fake	Not everybody is familiar with using mouse as a writing device
Blonder		•	Blonder which a pre-determined image and predeterermined click points. the method is secure according to a millions of different regions	This scheme was that the number of predefined click regions was relatively small so the password had to be quite long to be secure.
PassPoint		•	The user is choosing several points on picture in a particular order	The login time, in this method is longer than alphanumeric method
Background DAS (BDAS)		•	Both background image and the drawing grid can be used	Memory decaying over a week is one of the major problems
PASSMAP		•	Users are relatively easy to remember landmarks on a well-known journey	It is respect to Brute Force Attacks
Passlogix v-Go		•	User can select their background images based on the environment, for example in the kitchen, bathroom, bedroom or others	The passwords to be somewhat guessable or Predictable

Table 4: The strength and weakness of Recall-Based Techniques

VI. CONCLUSIONS

In this study, ten algorithms from Recall-Based explained in two Pure and Cued categories. Then, tables 1 and table 2 showed the comparison among all pure and cued recall-based algorithms on our usability founded attributes and sub attributes. In the second part, we found the effective attack patterns on graphical user authentication (GUA) and explained them and then we made a comparison table among impressibility of all recall-based algorithms based on standard attack patterns. Finally, in the last part we made a strength and weakness of all Recall based algorithms.

References

[1] Xiaoyuan Suo, Ying Zhu and G. Scott. Owen, "Graphical Passwords: A Survey", Proceedings of the 21st Annual Computer Security Applications. IEEE. 463-472; 2005.

[2] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin,"The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.

[3] Julie Thorpe, P.C. van Oorschot,"Towards Secure Design Choices for Implementing Graphical Passwords", Proceedings of the 20th Annual Computer Security Applications Conference. Ottawa, Ont., Canada, IEEE. 50 – 60; Dec 2004.

[4] Ali Mohamed Eljetlawi, "Study and Develop a New Graphical Password System", University Technology Malaysia, Master Dissertation, 2008.

[5] A..H. Lashkari, Samneh Farmand: A wide survey on Recall-Based Graphical User Authentication algorithm based on ISO and attack Patterns , *IJCSIS Vol. 6, no. 3, 2009.*

[6] Sonkar S.K., Paikrao R.L., Awadesh Kumar," Graphical Password Authentication Scheme Based On Color Image Gallery", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012.

[7] Navnath D. Kale, Megha M. Nalgirkar," An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns", International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013.

[8] Swetha Sathish , Asha B Joshi , Ganeshayya I Shidaganti," User Authentication Methods and Techniques by Graphical Password", International Journal of Computer Applications & Information Technology Vol. 2, Issue III Apr-May 2013.