An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns

Navnath D. Kale, Megha M. Nalgirkar

***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 password are more secure than the text password because they are easy to remember and hard to crack. 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. We will also implement multi-line grid algorithm.**

***Index Terms*— Graphical Password, Attack Pattern, User authentication, pure recall-based algorithm, cued recall-based algorithm, multi-line grid algorithm.**

I. INTRODUCTION

In recent years, Network security is the most describing problem. Information stored in the database are much more precious for the user. To remember the password:

1) Should be easy to remember
2) Should be quickly and easily executable
3) Should be changeable

User may forget the password if it is too long and complicated. The text based password can be stolen by any powerful software. Phishing is another serious threat to text based password. Phishing is the action of getting secured information such as username, password and other further details by masquerading. Graphical password may be solution to the text based password vulnerabilities. One of the most constrain reasons for exploring the use of a graphical password scheme that humans ability for recalling pictures, whether they are line drawings or real objects. [1]

The most widely explore paradigm for the graphical password by recognizing the images that comprise it from among many more images. This image can be of any person, nature, flower or any blur image. In this procedure, a user is asked for her user name and password i.e. graphical password. Within a fraction of second user is presented with an image portfolio. The user must correctly select, photograph presented for the account verification. If the hacker responds to the wrong image the access to the particular account is denied, and site can give all time wrong image to the hacker and hacker think he is cracking the account. Using the text password one can hack very easily.

Manuscript received on April, 2013.

Prof. Navnath D. Kale, Department of Computer Engineering, University of Pune, Pune, India.
Ms. Megha M. Nalgirkar, Department of Computer Engineering, University of Pune, Pune, India.

In the survey 83% people are in the favor to use image as a password to protect their account [1]. It is always proved that human brain is better in recognition and recalling by graphical password. Graphical password should not write down or stored in plain text. According to psychological research human brain is very good recognizing the image. Graphical password was first described by blonder. Different type of image based password is described as below:

II. LITERATURE REVIEW

As we know graphical images are more easily recalled then text. In this selection so graphical password system based on recognition and recall based are discussed.

1) Recognition- Based Technique: In this type of technique, users will select pictures, logos or any symbols from prestored image. For authentication process user need to recognize the image, which he choose as a password.

2) Recall-Based Technique:

Again recall-based password authentication are categorize in two parts [2] :

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:

a) ***Passdoodle:***

Which introduced in 1999 technique, is a graphical password authentication which is hand drawn design and other cannot perfectly redraw doodle as the original one. It means that anyone can give a hard signature as a password and the attacker might be not redraw the same. As shown in the fig. 1 we used a sample signature as a passdoodle.

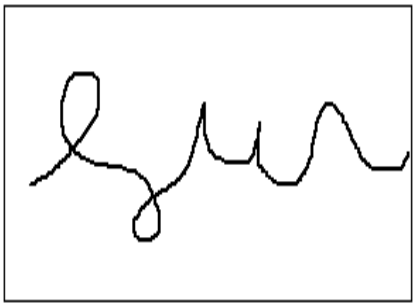

Figure 1: A Passdoodle Example

b) ***Draw-A-Secret (DAS):***

In this technique user can draw a simple image or picture on grid , of size say N*N. Each cell is denoted by two dimensional coordinate (x,y), € [1,N]*[1,N] [1] [2] .

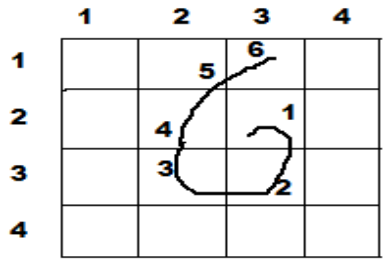

Figure 2: Draw-A-Secret method on 4*4 grid

As shown in the fig. 2 the coordinate sequence generated by design is:

(2,3), (3,3), (3,2), (2,2), (1,2), (1,3).

c) ***Qualitative DAS:***

It is an enhancement of DAS method created by making code of each stroke. We draw a raw coding which only consist of starting cell, where the direction is change when a pen cross the previous cell boundary [1] [2] .

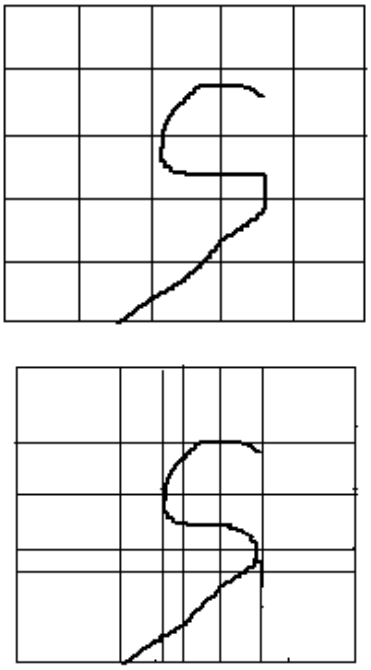

Figure 3: A Sample QDAS Image of original image

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:

a) Blonder:

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 [2] .

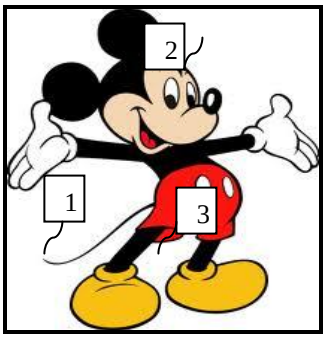

Figure 4: A Sample of Blonder method

b) Passpoint:

Passpoint was designed in order to cover the limitation of Blonder algorithm. In this technique image is not secret and has no option to user to remember the click point by passing to next click [3].

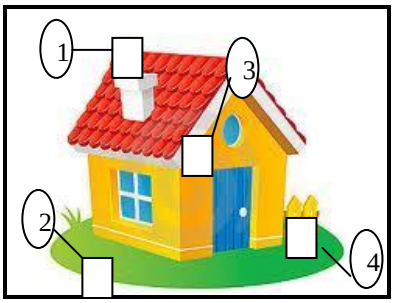

Figure 5: A Sample of Passpoint method

c) PASSMAP:

These password are good are hard to remember and those are easy to remember are hard to secure. In the PASSMAP technique one can use a password as landmark on a well known journey. This is very common technique to use image based password to secure the personal site and protect the database.

It is very common technique to give password to remember. PASSMAP is used previously and now-a-days also [2] .

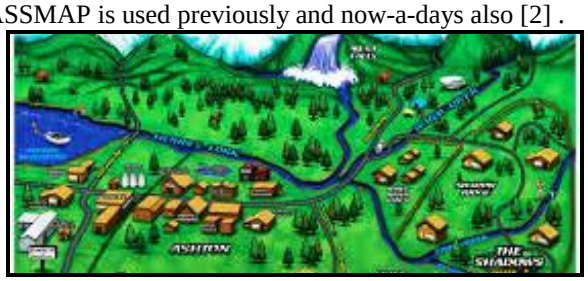

Figure 6: A Sample of PASSMAP method

Common Attacks Pattern on Graphical Passwords:

1) **Brute Force Attack:** In this type of attack an attacker attempts all possible combination of hacking the valuable password. If our password is more complicated it is more secure against this attack. One important thing come to notice that this attack is more difficult to carry out in image base password than text based password. This attack is resource expensive.

2) **Dictionary Attack:** It is a type of attack in which the intruder trying to determine the password by searching a large no of possibilities. It is different from Brute Force Attack in which all possibilities are searched.

There is a convective pressure on user so this attack is mainly successful. It is very much more complex for text based password.

3) **Guessing:** If a person using a text based password, which is very much common, so to remember this they use as a password their name, their family member name, date of birth. This is very easy to guess for the attacker. Many user use "password" word as a password. This type of attack is known as guessing attack.

4) **Spyware:** It is one kind of software which is installed in the computer without knowledge if user. It stores all the information about the user. And give it to outsider source. In the case of graphical password authentication attacker try to gain sensitive information about the user select the prestored images from database and hack the personal account.

5) **Shoulder Surfing:** In this case an observation is very much important for the hacker. The attacker pay full attention towards the shoulder to know the password while the user enter the password. It is very common and ancient technique [1] [5] .

III. MULTI-LINE GRID ALGORITHM FOR GUA

To overcome from all these attacks to make our information more secure this paper propose a new algorithm. This proposed algorithm focus on the size of grids in the log in phase by ensuring that they are user choice . For example suppose we register images on the grid as 3*3 of grid than for increasing security we can convert password from 4*4, 5*5, 6*6 grid. During the registration phase we can save size of grid in the system so that image can find randomly and different grid for different user. The registration phase of user on 3*3 grid is shown in fig 7.

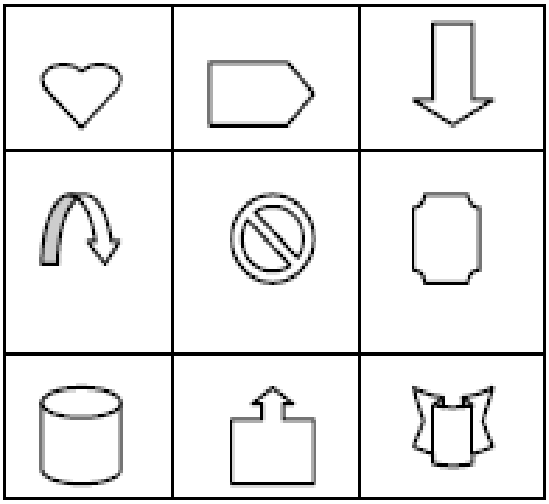

Figure 7: The registration phase 3*3 grid

When a user wants to login in the system will always used to prefer saved grid size during registration phase. After that user can choose a random image among the available grid like 4*4, 5*5, and 6*6. The system will store different sizes of the grid used during the registration phase to allow the user to find the different grid during the login phase. And also create using the user's password and some fake images. When user wishes to login the system will refer to the saved grid sizes used during the registration phase. A use it to choose random no. from the available grids for example: 4*4, 5*5, 6*6 as shown in figures 8, 9, 10 [1].

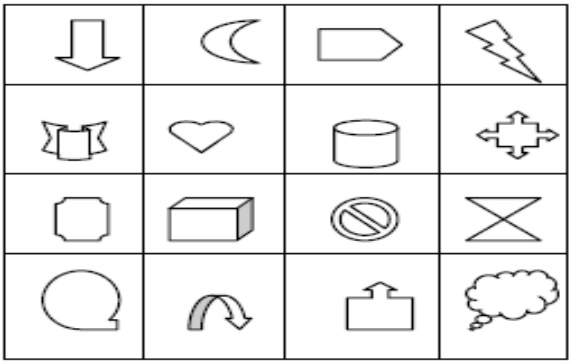

Figure 8: The registration phase 4*4 grid

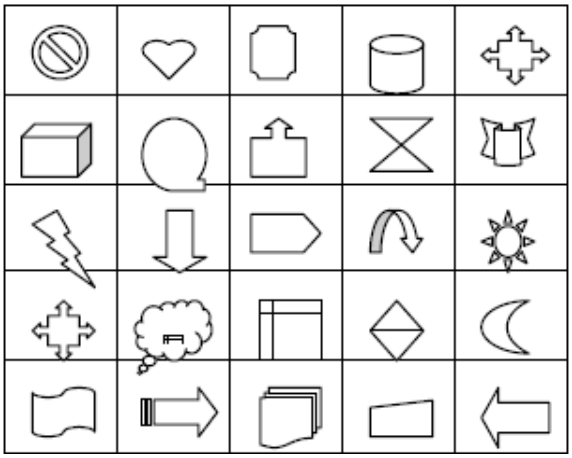

Figure 9: The registration phase 5*5 grid]

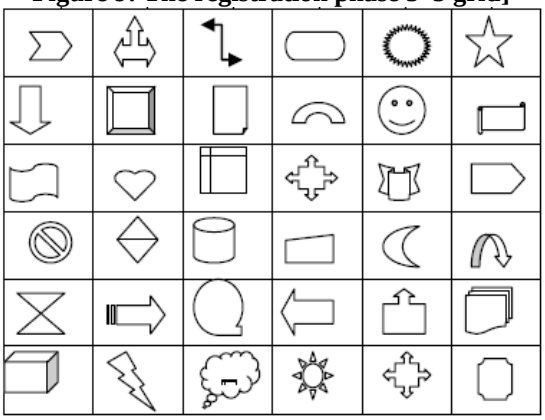

Figure 10: The registration phase 6*6 grid

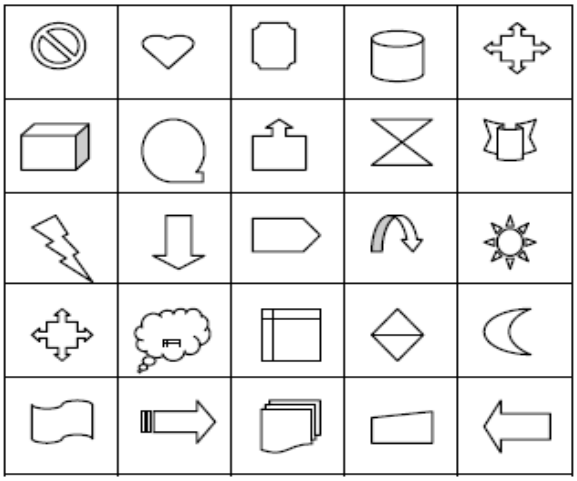

Figure11: The registration phase 5*5 grid

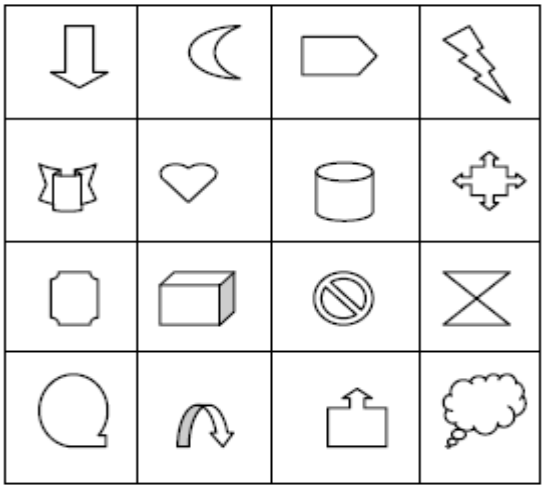

Figure12: The registration phase 4*4 grid

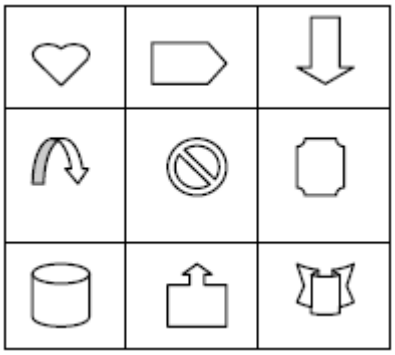

Figure 13: The registration phase 3*3 grid

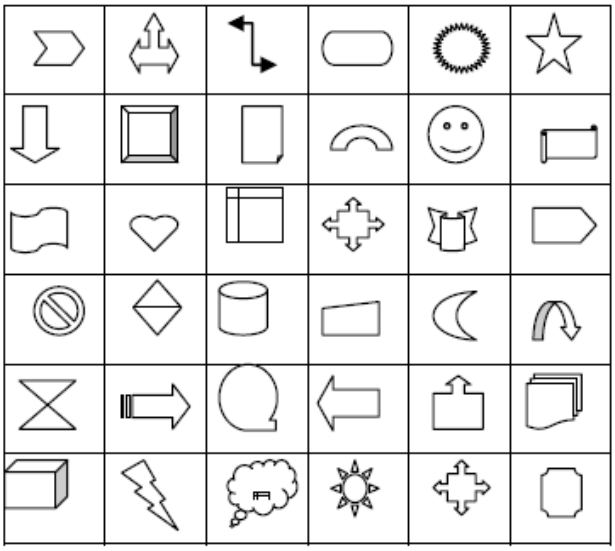

Figure 14: The registration phase 6*6 grid

Creation of password: Image based passwords are created during registration process. This process must follow the policy. A graphical password policy which must be generated by the site operator. This policy defined, the user select pictures as a password for verification these images can be come to screen randomly from prestored database. Our password may be eavesdrop by attacker which make intercept in communication between client and user. Furthermore for the verification of the password length of password is considered for text based password length may be of I character so, i.log2c, where c is constant , bit characters make entropy for choose alphabet but in image based password the size of image portfolio is checked [7] .

IV. FACTORS AFFECTING AND USABILITY

When we registered the password in the login page, we have to gone through many of the stages which are part of graphical password. These factors are as follows, which we studies one by one:

1) User:

In Graphical password user is one of the main factors which perform important role. User should be intelligent and clever. Any time of login he/she should be alert at the time of entering the password.

Table 1: Diff. Attack Pattern Regarding Recall-Based Password

Sr no	Algorithm	Cued Recall based	Pure Recall based	Brute force	Dictionary	Guessing	Shoulder	spyware
1	Passdoodle		√	N				
2	DAS		√	N	Y	Y	Y	N
3	QDAS		√	N				
4	Blonder	√		Y	N	Y	Y	N
5	Passpoint	√		Y	N	Y	Y	N
6	PASSMAP	√		Y	N		Y	N

2) Task:

Each user should give time to complete the session to enter the correct password. If the password is correct then we assume that the task is completed successfully and vice versa. It is the task done by the hacker than with first click on image can understand and send the wrong images to entertain the hacker.

3) *Data Collection*:

Data collection must be twisty. It should not give any clue to outsider. A qualitative and quantitative data should be covered during the registration. Beside the collection of coordinates we should collect and fix the points.

4) Accuracy:

The entire User should be accurate while choosing their password. To find out the accuracy we can analyze by correct click method. It the entered password is accurate to the prestored password than its accuracy is 100%.

5) Perception and Opinion:

The entire user must be sure with their password. Many users have perception and opinion while using this password.

6) Times for Password Entry:

There is one problem regarding entering image based password. Many users think while watching the image, where to click? There should be Stime limit to enter the appropriate password. If the user enter password in given time then it is acceptable, if not then they must give answer for another image after 30 sec.

7) Success Rate:

The success rate should be calculated from the correct attempt of user. These may be combination of success rate of conforming and success rate of login.

From prestored image in the database suppose we stored 20 images out of that user must enter the 7 successful image. For every login phase success rate must be calculated and stored in separate table.

These are the factors which give a simulation result to make strong password. We can also use colored password to make more combination and permutation for hacker colors. We can give colors as basic colors (Red, Green, and Yellow) or can give combination of these colors.

V. CONCLUSION AND FUTURE WORK

In this paper, we have studied in brief 6 attacks of recall based algorithm. Three from pure recall-based algorithm and three from cued recall-based algorithm. In the next part we have studied different attack patterns regarding the recall based algorithm. In last section of this paper we studied graphical password authentication using multi-line grid during login phase which can be changed from 3*3 to 4*4, 5*5, 6*6 to increase the probability of finding their passwords.

In future we will try to implement this multi line grid algorithm on the real time based system and will graduate the performance for this algorithm. We will also implement this in mobile with android operating system.

ACKNOWLEDGMENT

We feel great pleasure in submitting this paper . We would like to express our sincere gratitude towards our family for always being there when we needed them the most. With all respect and gratitude, I would like to thank all the people who have helped me directly or indirectly.

REFERENCES

1. A.H. Lashkari, Abdullah Gani: A new algorithm on graphical user authentication based on multi-line grids. *A full length research paper. 18 Dec 2010.*
2. 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*.
3. Ahmet ED, Nasir M, Jean-Camille B (2007). Modeling user choice in the passpoints graphical password scheme, Symposium on usable privacy and security. Pittsburgh, Pennsylvania, USA. ACM,, 20-28; July.
4. Di Lin, Paul Dunphy, Patrick Olivier and Jeff Yan, "Graphical Passwords & Qualitative Spatial Relations", Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania. ACM. 161-162 ; July 2007.
5. S. Chiasson. *Usable Authentication and Click-Based Graphical Passwords*. PhD thesis, Carleton University, Ottawa,
6. Greg E. Blonder , Graphical Password U.S. Patent No. 5559961, 1996.
7. Di L, Paul D, Patrick O, Jeff Y (2007). Graphical Passwords and Qualitative Spatial Relations, Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania. ACM, 161-162; July.