Image Based User Choice and Design of Graphical Password Authentication

Selvakani.M#1, R. Sankar#2

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
selvakani267@gmail.com
[2]*Asst Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
sankar@saec.ac.in

Abstract— The general computer substantiation system is to use alphanumerical usernames and passwords. This appraoches has momentous drawbacks. It is hard to guess and hard to remember alphanumerical passwords. To address this problem developed authentication methods are using pictures as passwords. Recognition-based and recall based approaches draw-a-secret passwords are used by grid to draw the password.

The user choices to obtain any doodle or logo password using 6*6 grid. Graphical password is much more secure than textual passwords. Using image of faces can randomly selected as password to secure the passwords from the attacker. Graphical input devices enable the user to decouple the position of inputs from the sequential order in which those inputs occur, and we show that decoupling can be used to generate password schemes with substantially larger password spaces.

Keywords—Authentication; Rotational DAS Password; Personal Identification Pattern; Grid Selection.

1. Introduction

The users using a alphanumerical passwords which is hard to remember but easily guessed by the hacker. So we are moving to graphical passwords. Draw-a-secret (DAS) form of graphical was proposed by Jermyn et al. in 1999. DAS is purely graphical password selection and input scheme.

The scheme modifies in part password strings, with a picture drawn on a two-dimension, i.e. (5x5) grid using a stylus or mouse. Instead of typing a password, DAS authentication method allows users just to reproduce the drawing process to login.

The system that relies on recall based, and recognition based techniques for authentication. Draw-a-secret with the sequence of coordinate pairs with “pen-up” event such as (2,2), (3,2), (3,3), (2,3),(5,5) in a 5x5 grid.

The size of the DAS password space is reduced from 58 to 48 bits. Random selecting faces from the grid 3x3 of three-dimensional used as a password with more secure. Graphical password schemes also emerged and it is suitable for provide access to systems that are not keyboard-based as a means of data input.

2. A graphical password scheme

A password is a confirmation method by the user to select from images, in a unique order, presented in graphical user interface (GUI). We are presenting proposed scheme as graphical password authentication based on Color Image Gallery which is very useful for some computer related application such as web authentication, desktop and laptop logins, critical servers.

2.1 Textual Password with Graphical Assistance

This approach is alphabet independent, thus making it equally accessible for speakers of any language. Variations on inputting password (e.g. tomato is a password). Step 0 is an initial row of blanks, and steps 1-6 indicate temporal order in which the user fills in the blank spaces [1].

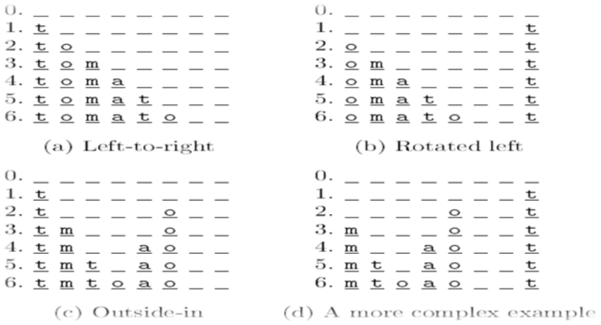

(a) Left-to-right
(b) Rotated left
(c) Outside-in
(d) A more complex example

Fig. 1: Textual based graphical password:
The coordinate sequence generated by drawing the pairs:
(2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5)

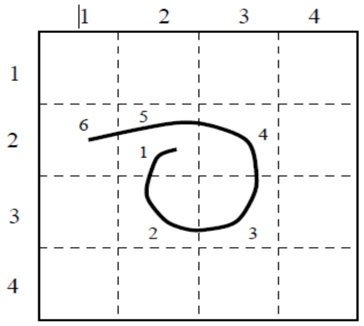


Fig.2: Drawing with Coordinate pair of password

A password is then defined to be a sequence of caresses sectioned by "pen up" proceedings, anywhere (5,5) is the distinguished pen up indicator. The length of a stroke is the number of coordinate pair contain the total length of passwords is the length of its component strokes. We partition the liberty of promising picturing into, two drawings being equivalent if they have the same encrypting, or if they annoyed the identical progression of network cells, with the breaks between strokes occurring in the same places. Input of a graphical password on a 4x4 grid. The drawing is mapped to a sequence of co- ordinate pairs by recording the cells in the sort which the stylus exceeds through them, with a distinguished co-ordinate pair inserted in the progression at whatever time the stylus is raised from the picturing surface.

2.2 *Background DAS Password*

BDAS scheme is exactly the same as DAS except that image background was superimposed over the blank canvas DAS grid to help users remember where they began the drawing that is being used as a password. DAS scheme with a background image enhances memory of the more complex and secure passwords.

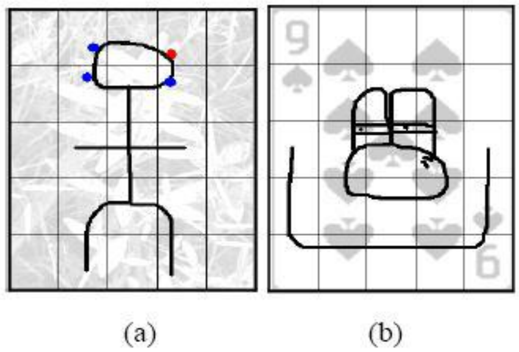


Fig. 3: BDAS Graphical scheme

2.3 *Grid Selection*

- Input a password can be a challenge if a user has problem in identifying the correct grid cell used.
- It so predictable that most of users will still choose symmetric passwords when using this method [2].

2.4 *Pass Doodle Algorithm*

Pass doodle is another scheme similar to DAS except that it does not require use of visible grid. The scheme was based on the idea of hand written designs or words, drawn with a pen onto a sensitive touchable screen without any visible grid. Doodle-based graphical passwords have been developed as an alternative to traditional passwords in touch screen-enabled devices. Within biometrics, name proof is the mainly comparable peculiarity with respect to doodles [4].

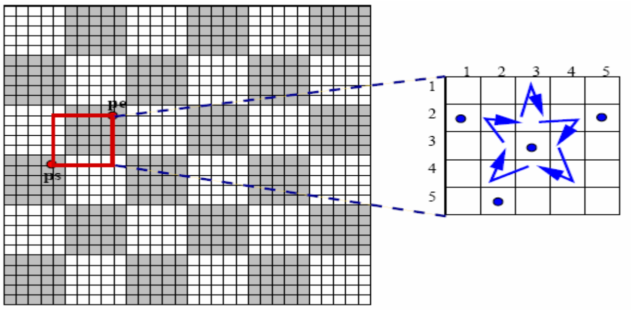


Fig. 4: Grid Selection: Where User Selects A Drawing Grid For The Password

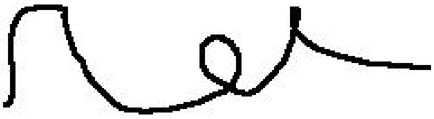


Fig.5: An Example of a Pass doodle

2.5 *Pass-Go*

For user to enter password in this scheme, he selects intersections instead of cells on a grid. By this difference of usage, the algorithm is referred to as a matrix of intersections, which is different from cell as in the case of DAS's scheme. The use of intersections as against cells allows the user to use password from greater password space. The size of the grid in Pass-Go can be 9*9 [5].

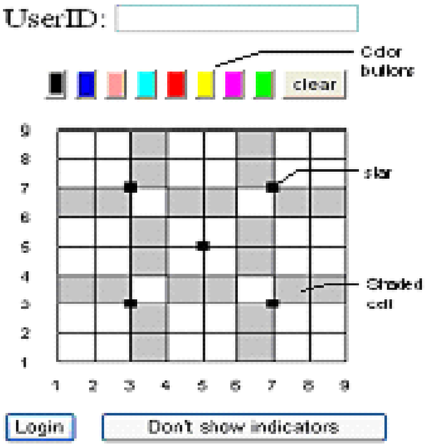


Fig.6: Pass-go

2.6 *The Grid sure Graphical Scheme*

Grid sure is a commercial graphical scheme that uses 5X5 grid for accepting pattern during registration and displaying digits during authentication. Registration grid displays bland cells of which four are used to register personal Identification pattern (PIP). During registration, users select and memorize a pattern over any four ordered cells in the grid of 25cells. During the authentication stage, digits are randomly displayed on the grid then user enters only four digits appearing on the chosen pattern in the specific order with the help of keyboard without touching the grid. For the subsequent logins, users enter the new sequence of digits corresponding to the cells of their memorized pattern from randomly displayed digits over the grid cells. The digits in the grid change randomly for every authentication because the system relies on One-Time Password or PIN (OTP) concept for its operation [3].

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y

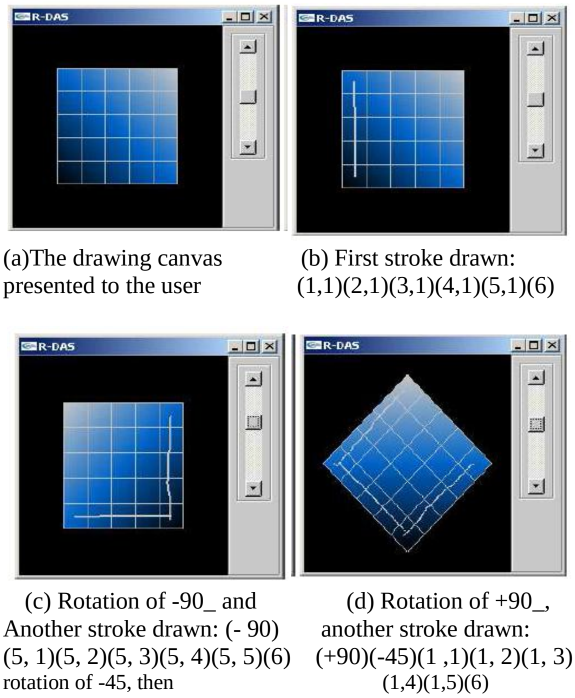
A) Registration Stage for Drawing User’s Choice Pattern.

3	7	0	2	9
0	1	9	6	0
4	3	8	1	2
6	1	9	7	1
5	4	8	4	9
Enter Code:	*	*	*	*

B) Authentication Stage for Displaying Selecting Digits Corresponding To the Chosen Pattern via the Keyboard

Fig.7: One time password

2.7 *Rotational DAS Password*

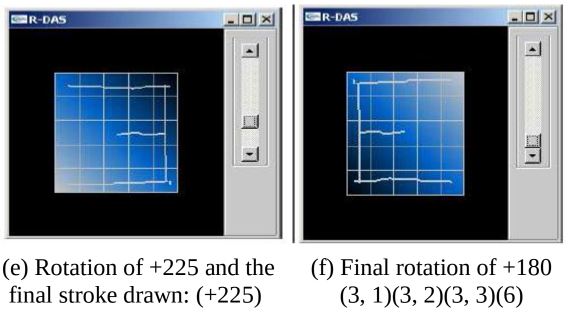


(a)The drawing canvas presented to the user

(b) First stroke drawn: (1,1)(2,1)(3,1)(4,1)(5,1)(6)

(c) Rotation of -90_ and Another stroke drawn: (- 90) (5, 1)(5, 2)(5, 3)(5, 4)(5, 5)(6) rotation of -45, then

(d) Rotation of +90_, another stroke drawn: (+90)(-45)(1 ,1)(1, 2)(1, 3) (1,4)(1,5)(6)



(e) Rotation of +225 and the final stroke drawn: (+225)

(f) Final rotation of +180 (3, 1)(3, 2)(3, 3)(6)

Fig.8: Rotational DAS password

3. Conclusion

Graphical passwords are primarily made to address the usability and security limitations of text-based passwords which include memorable passwords that are vulnerable to attack while the random and long passwords are secure and not memorable. Draw based graphical passwords was started with DAS that is able to provide passwords clearly stronger than alphanumeric passwords but not extensively difficult to remember. Other modifications of DAS are surveyed in this study where in the course of study it was discovered that modified DASs are designed to solve DAS limitations in terms possible attacks against the DAS, centering effect and other usability challenges. In this paper we have encouraged that considerable attention should be given to the choice of background image for schemes that require it to achieve better memory.

4. Future work

For random passwords to be useful, users employ coping practices which are not in agreement with laid down rules of password security. It will be worth to search this claim in the design of graphical passwords by taking one image from each group for memory test.

References

[1] Monrose. F and M.K. Reiter, “Graphical Passwords Security and Usability”, ACSAC ’10 In Proceeding of Conferenceon the 26th Annual Computer security applications, Vol .1, 2005, pp.79-88.

[2] Obasan Adebola o, “Memorability Features of Draw Based Graphical Passwords”, University Technology Malaysia, Faculty of computing, 81310 UTM, Skudai Jorhor-Bahnu, Malaysia, 2010, pp.49

[3] Varenhorst, C., Pass doodles, “A lightweight authentication method”, Research Science Institute, 2004, pp.78-86.

[4] George V. Landon Novothea, Inc. “Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom”, 117 Chestnut Ridge Drive Lexington, KY 40511 USA, 2007, pp.831

[5] P.Rajeswari, “Providing Security using Touch Screen Pattern”, Special Issue of Engineering and Scientific Inter.l Journal, Technical Seminar & Report Writing – MCA-SAEC, May 2015, PP.65-68.

[6] Millee Panigrahi, Rina Mahakud, Minu Samantaray and Sushil Kumar Mohapatra, “Comparative analysis of different Edge detection techniques for biomedical images using MATLAB”, Engineering and Scientific International Journal, Vol.1, No.1, Dec. 2014, PP.23-28.