# Security Enhancement of Recall based Graphical Authentication System by using Biometric Features

Mohd. Aqil Khan
Ph.D Scholor
Venkteshwara University

Y.D.S. Arya
Director
IIET, Bareilly

Gaurav Agarwal
Assistant Professor (CS)
Invertis University

## ABSTRACT

Studies have showed significant convenience in remembering pictorial representation of passwords over the textual passwords. The motivation behind exploring a graphical password scheme is based on the remarkable ability of humans to recall pictures easily. In this paper we are presenting the novel approaches for security of pure recall based techniques with the help of biometric authentication i.e. stroke analysis and mouse movement.

## Keywords

Graphical passwords, Recall based graphical passwords, Authentication, DAS, and Biometric Security

## 1. INTRODUCTION

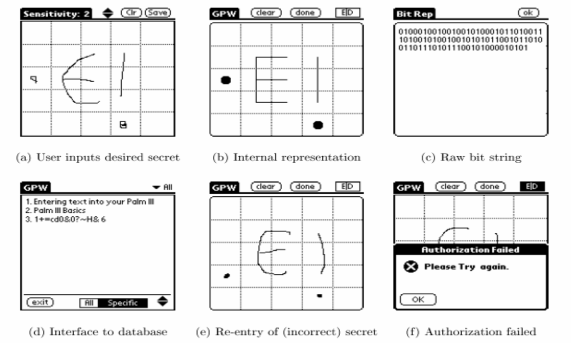
Notation of graphical passwords was first introduced by Blonder [4]. He presented two classes of graphical password schemes that were, recall–based graphical passwords and recognition-based graphical passwords [12]. Jerman et al.[5] proposed a recall-based graphical password scheme. In this paper, we will focus on recall-based techniques. We summarize both these techniques and then discuss the proposed system to make these techniques more secure with the help of biometric authentication.

## 1.1. Introduction to pure recall based authentication

In pure recall-based graphical password scheme, the user is asked to reproduce some drawings on grid that she had created/selected earlier during the registration phase. In this group, user needs to reproduce the passwords without any help or reminder by the system. Draw- A-Secret technique [8], grid selection [5],and pass doodle [7] are some examples of pure recall based techniques.

### *1.1.1. DAS( Draw-A-Secret)*

Jermyn et al. [5] and Sobardo L. and Birget J. [10] presented a recall based scheme named DAS (Draw-A-Secret). This scheme is based on a two dimensional grid. Users have to draw some graphics or drawing to represent their passwords. Each of the grid's coordinates from the drawn graphics is stored in the order of the drawing. For authentication, user needs to redraw the picture again. If the drawing lines match the grid's coordinates with the registration phase in the right sequence, then the user is authenticated.



```
0100010010010010100010110100111
1010010100100101010110010110 10
01101110101110010100001010 1
```

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Authorization Failed
Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

**Fig.1 (Draw- A-Secret)**

### *1.1.2. Pass Doodle*

Pass Doodle, is a graphical password technique of hand written drawing or text, which is sketched over a touch screen as shown in figure 2.Goldberg et al.[6] have shown that users were able to recognize a complete doodle password as accurately as text-based passwords. Unfortunately, the Pass Doodle scheme has many drawbacks; users were fascinated with other user's drawn doodles, and usually entered other user's password merely two a different doodles from their own. It was found that the Pass Doodle scheme is vulnerable to several attacks such as guessing, spyware, key logger, and shoulder surfing.

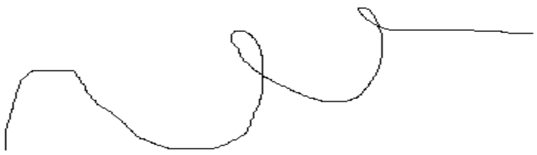


**Fig 2 (Pass doodle Technique)**

### *1.1.3. Grid Selection*

In 2004, the grid selection technique was initially proposed by Thorpe an Van Oorschot[7] to enhance the password space of DAS. To improve the DAS security level, they suggested a new approach named "Grid Selection" technique, where the selection grid is large at the beginning, but users had to select another drawing, rectangular area to zoom in on, in which they could enter their passwords as shown in figure 3. This technique was intended to increase the password space of DAS, which also improves the security of the system

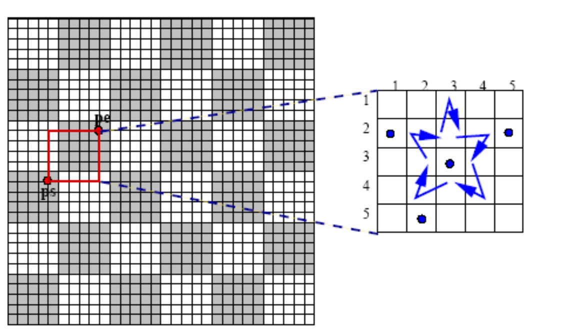


**Fig 3 (Grid Selection Technique)**

## 2. RELATED WORK

As Suo et al.[12] pointed out that graphical passwords authentication methods are the most widely used techniques for secure applications over the textual passwords. Under the graphical passwords authentication there are two divisions (1) Recognition-based –authentication, here user must recognize and identify images already chosen during a password registration stage; and (2) Recall-based authentication, where user must recreate something that was developed during the password registration stage. Blonder [4], proposed a recall based technique, in which, a user is requested to select a reason from a predefined image to generate password, for authentication, user is required to select same reason which was selected in registration process. Wiedenbeck et al. [11] introduced another technique named the Pass Point scheme as recall based graphical passwords, in this, using user chosen images, a user can select arbitrary regions of the images to generate the password. The user must reselect the same regions in the correct order for authentication. Syukri et al. [1] proposed a recall based password scheme based on reproducing the signature of the user on the screen using a mouse. After the user first brows his/her signature for initial password generation, the user is again authenticated by redrawing the signature same as in registration phase. The initial password is normalized for scale and rotation. To add to the security and ease-of-use of graphical passwords, Jermyn et al. [5] proposed the DAS scheme. Thorpe et al. [8, 7] provided an analysis of the password space of the DAS scheme [5]. Thorpe et al. studied the impact of mirror symmetry and stroke-count on the size of the DAS password space. To improve the security, they proposed a grid selection technique where the user selects a sub-grid from a large fine grained grid, on which the user enters the password. Nail [3] conducted further security analysis of the DAS scheme [5] for predictable character sticks in the graphical passwords chosen by users.

Rest of this paper, consists of the security question for the recall based techniques and its solutions. It is influenced by biometric authentication, for example, the key pressed by the user for drawing the picture and the time taken from one click to another. For the mouse movement, there is also some work done as the term mouse dynamics. Mouse dynamics includes mouse movement, drag and drop, point and click etc. These actions can be used to generate a unique profile for user authentication purpose [9] as each and every human being is having different characteristics towards the mouse dynamics. Pusara et al.[9] classified mouse movement event into two groups, mouse wheel movements and clicks. Click data is further divided into single and double click data. Weiss et al.[2] concentrated on button press and mouse drag data for a fixed pattern to gather features, and to create feature vector. In their work, they proposed a scheme in which all the data related to movement was collected. They designed some features like size of mouse curve, mouse speed, mouse click etc. In this paper, we have taken the total time and mouse click feature of mouse movement to secure the recall base graphical password scheme.

## 3. RESEARCH QUESTION

Now, we have discussed about the pure recall based techniques for authentication, but the question arrives how secure they are? It has been shown that the graphical passwords are more secure than the textual passwords but they are not attack free. First we will study various attacks and then we will propose solution for these attacks.

### 3.1 Possible Attacks on Graphical Password Techniques

Very less study has been done by researchers for the security of graphical password. Most of the researchers have shown that the graphical passwords are more secure than the textual passwords. But there are some loopholes or attacks which can crack the graphical passwords. These are discussed next.

### *3.1.1 Brute Force Attack*

Brute force attack is based on the password size. This is normally more common in text based passwords than the graphical based passwords. In text based password scheme, the password space is 94 N, where N is the length of the password and 94 is the number of printable characters. While in graphical based techniques, the password space is less than text base passwords. But there are some exceptions in recognition based techniques, those are not up to the mark so brute force attack is easily possible on graphical password schemes.

### *3.1.2 Guessing*

There is a serious problem with text based passwords as well as with the graphical passwords, which is, guessing attack. Study shows that people using passwords usually choose weak and easily predictable passwords for their convenience, which results attacks on passwords by guessing.

### *3.1.3 Spyware Attack*

It is quite difficult to crack graphical passwords by using key logging and key listening. Also, if an attacker detects the mouse motion of the user, that will not be enough to break graphical passwords. There must be some information such as position and size of grid used. Also there should be some information available about the time taken by authorized user for mouse movement.

### *3.1.4 Shoulder surfing*

Most of the graphical passwords are vulnerable to shoulder surfing like text based passwords. A few recognition-based techniques are designed to resist shoulder surfing. Not any of the recall based techniques are resistant to shoulder surfing attack.

### *3.1.5 Social Engineering*

It is quite difficult to describe a graphical password by the social engineering as compared to text based passwords. For example, it is difficult to describe graphical password on phone. But an attacker can set graphical password on phishing website through it will be very time consuming process.

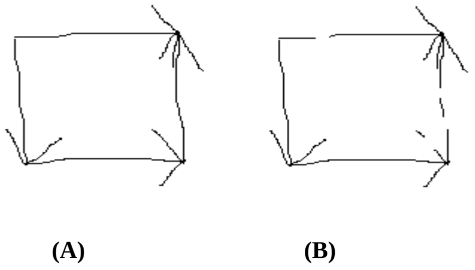
## 4. PROPOSED SOLUTION

In the proposed solution, A system has designed with biometric security. Here, the system will record the average strokes used by the user at the time of registration and login.

Also, considered the time taken by mouse for registration and login time. Proposed system will allow only those users who will take same amount of time and save number of strokes as at the time of registration.

## 4.1 Stroke analysis

Stroke is known as the attribute of the user as the distance covered by the user from one click to another click. For a legitimate user the stroke count will be less as user will know where the mouse button should be released but for the attacker it will be difficult to maintain the stroke count as attacker will be more conscious about the rejection. Figure 4 shows the stroke count for legitimate user and the attacker.



**(A) For Authorized Users**
**(B) For Unauthorized Users**

figure 4 shows two different stroke graph for authorized and unauthorized user. As we can see that in figure A there is secret drawn by authorized user which will take 12 strokes (4 for line drawing and 8 for arrow) and for unauthorized used it may take more than 12 strokes because of over consciousness. The experimental results will be shown next.

## 4.2 Time taken in mouse movement

Next biometric property we have considered is the time taken by the mouse from one click to another click. Authenticated user will take less time to move mouse from one point to another while an unauthorized user will take more time to prove authenticity. This feature is directly concerned with human behavior.System will calculate the number of strokes and the time taken for the mouse movement with the recall based graphical authentication for each user. The work is carried out using Mat Lab tool.

## 5. EXPERIMENTAL RESULTS

For describing the above two features five authorized users have been taken, who know their passwords and five unauthorized users who tend to make the same secret as drawn by authenticated users. The experimental results are as given below.

## 5.1 Stroke Count

For stroke count we have taken the different shapes, signatures and grids for different users.

**Table 1 Stroke Count**

| S.No. | Shape for participant | Stroke count for authorized user | Stroke count for unauthorized user |
|---|---|---|---|
| 1 | Simple Rectangle (with arrow on edge) | 12 | 15 |
| 2 | Triangle with arrow on edge | 9 | 13 |
| 3 | Circle (with an arrow) | 3 | 5 |
| 4 | Grid (edge 4) | 4 | 6 |
| 5 | Signature named "John" with cursive writing | 8 | 15 |

As we can see in Table 1, the unauthorized user is having more strokes to represent the same shapes. So, by using the graphical passwords over the textual passwords, one can deny an unauthorized user access.

## 5.2 Time taken in mouse movement

For the time taken in movement of mouse same participants took part for the same shapes. Table 2 shows the difference in time for authorized and unauthorized users.

**Table 2 Time Taken in mouse movement**

| Shapes | Average Distance (Pixels) | Mouse Speed (pixels/milli second) (Authorized users) | Mouse Speed (pixels/milli second) (Unauthorized users) |
|---|---|---|---|
| Simple Rectangle (with arrow on edge) | 712.871 | 1.4387 | 1.9830 |
| Triangle with arrow on edge | 502.485 | 1.0472 | 2.0142 |
| Circle (with an arrow) | 227.458 | 1.0267 | 1.7902 |
| Grid (edge 4) | 1481.287 | 2.4787 | 3.1039 |
| Signature named "John" with cursive writing | 1263.452 | 3.5735 | 5.6309 |

As shown in table 2 , for the same shapes authorized user is taking much less time than unauthorized user. So, the proposed system will deny registering unauthorized access user due to excess time taken. The graphical representation of above analysis is shown in figure 5.

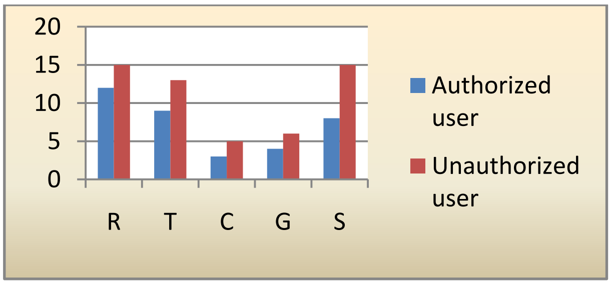


**Figure: 5 Graphical Representation of stroke count**

In figure describes that the stroke count for authorized user for different shapes is less than the unauthorized user. The terms in horizontal axis R, T, C, G, and S represent the shape rectangle, triangle, circle, grid, signature respectively and the vertical axis of figure shows the number of count for each user.Now, for the mouse speed and time for movement of mouse figure 6 shows the time in millisecond per pixel.

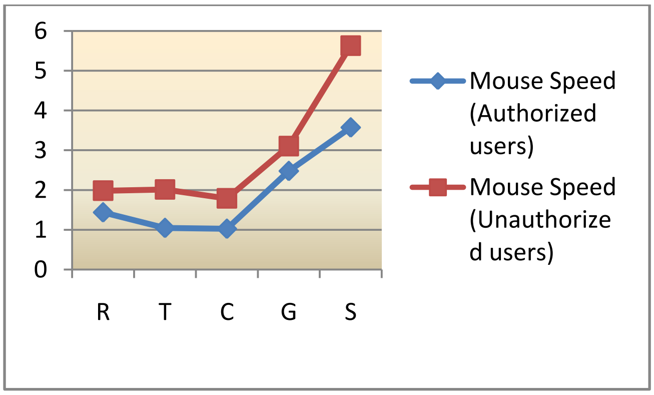


**Figure: 6 Graphical Representation of time taken for mouse movement**

This figure shows the difference between the time for mouse movement for authorized and unauthorized users. The horizontal axis of graph represents the shape used for authentication and the vertical axis represents the mouse speed in pixels/milliseconds.

## 6 CONCLUSION.

From the above experimentation we can conclude that the pure recall based authentication system are more secure than textual passwords but there may be possibility of some attacks. For preventing these attacks we can introduce some biometric features in our system. In the proposed system we have introduced two features that are stroke analysis and mouse movement. As discussed earlier, the stroke count and time taken by mouse for unauthorized user is more than authorized user so attacker will be denied system access.

## 7 FUTURE WORK

We have introduced two features of biometrics in the graphical system. There may be few more physical biometric features, for example the typing speed of human, pressure on mouse on each click etc. more work can be done in this area if any attacker practices to break the authentication procedure.

## 8 REFERENCES

[1] A.F. Syukri, E. Okamoto, and M. Mambo. A user identification system using signature written with mouse. *In proceedings of ACISP* pages403-414. Springer-Verlang1998.

[2] A.Weiss, A. Rarnapanicker, P.Shah, S.nobble, and L.Immohr. Mouse movements'biometric identification: A feasibility Study. In Proc. Student/faculty Research Day,CSIS.Pace University,pages1-8, May 2007.

[3] D.Nali and J.Thorpe. Analyzing user choice in graphical passwords, technical report, may 2004.

[4] G. Blonder. Graphical Passwords. 1996 United States Patent 5559961.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th *USENIX Security Symposium*, 1999.

[6] J. Goldberg, J. Hagman and V.Sazuwal, " Doodling our way to better authentication;" presented at proceedings of Human Factors in Computing System (CHI), Minneapolis.minnesota, USA,2002.

[7] J.Thorpe and P.C. van Oorschot Graphical dictionaries and the memorable space of graphical passwords. *In proceedings of the 13th USENIX security Symposium,* pages 135-150, 2004.

[8] J.Thorpe and P.C. van Oorschot towards secure design choices for implementing graphical passwords. In *proceedings of ACSAC*, pages 50-60. IEEE Computer Society, 2004

[9] M.Pusara and C.F. Brodley, User reauthentication via mouse movements VizSEC/DMSEC '04 : Proceedings of the 2004 ACM workshop on Visualization and data mining for computer society, ACM Press, Washington DC, USA, 2004, pp. 1-8.

[10] Sobardo L. and Birget J. (2007). http://rurgersscholar.rurers.edu/volume04/sobrbirg/sobrbirg.htm.

[11] S.Wiedenbeck, J.Waters, J. C. Birget, A. Brodskiy and N. Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *Int. J. Hum. Comput. Stud*, 63 (1-2): 102-127, 2005.

[12] X. Sou, Y. Zhu, and G.S. Owen. Graphical passwords: A survey in *Proceedings of ACSAC,* pages 463-472 IEEE Computer Society, 2005.