Hybrid Graphical User Authentication by Mesh of Matrix

Salim Istyaq#1, Mohammad Sarosh Umar\*2

*#Computer Engineering, EES*

*University Polytechnic, Faculty of Engineering & Technology, AMU, Aligarh, U.P., India*

*\*Department of Computer Engineering, Faculty of Engineering & Technology, AMU, Aligarh, U.P., India*

1saleemishtiyak@gmail.com

2saroshumar@zhcet.ac.in

*Abstract*— Most of the companies, people etc. use text based password. The reason is that it is easy to handle from previous time, but the user doesn’t know the disadvantage of using these loose passwords. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and short comings. Validating the identity shall establish a trust relationship for further interactions. Authentication even enables the accountability by making it possible to integrate both access and actions to specific identities. If the user is not very intelligently constructed the password with extra security measures, it is very easy to hack for an expert hacker. On the contrary, if a password is hard to guess, then it is often hard to remember. A person has to memorize as many passwords as many different websites he/she is accessing. So he/she gets confused and/or forgets the correct user id/password combinations. We should have an alternative system to overcome these problems. In this paper, a comprehensive study of the existing graphical password schemes and shoulder surfing problem is performed. The best way is to convert the passkey in any format to authenticate the user.

Keywords— Matrix authentication; encoded format; shoulder surfing; passkey; graphical authentication.

# Introduction

Textual password is the most common password used for authentication. The disadvantages of these methods are the system is prone to dictionary attack, shoulder surfing, social engineering etc. The concept of using long password is also good but there are many problems i.e. these are not easy to remember due to their complexity. Study shows that the user tends to choose their password which is short and friendly to remember [1]. So we move on to the new concepts i.e. graphical passwords and biometrics. But these techniques are also have their own barriers, e.g. in biometric like iris scan, retina scan, finger print etc. The cost of establishment is too much high compare to the others security modules and authentication process is too much slow. Huge numbers of techniques are coming day by day. From last decade most of those were suffered from vulnerabilities like shoulder surfing .There are graphical passwords scheme that have been proposed which are resistant to shoulder surfing. But have own disadvantages like usability issue or taking more time for login or having tolerance level. In this paper, we introduced a system which has very rare chance of all the cracking possibilities. We provided very deep complexity to our system for unknown user and only the legal user knows the combination of lines and sequence of their selection.

# RELATED WORK

1. Dhamija and Perrig [1] proposed a graphical authentication system based on the hash visualization technique. In this authentication system the user has to select the images from the set of random images. To authenticate in the system, he or she asked to select the preselected image as selected earlier in the registration phase. The weakness of the system is that the server needs to store the seeds of the selected image of each and every user in the simple or plain text.

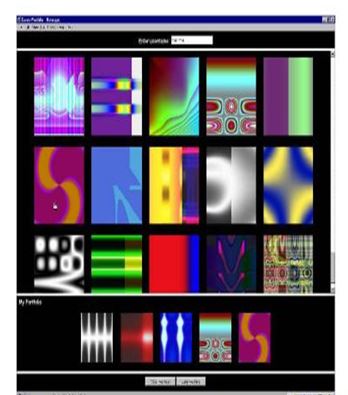
****

Fig. 1 Random images used by Dhamija and Perrig

2. Passface [2] is supported by the fact that the human brain can quickly recognize the face. It is a technique in which a user has to select the faces from the grid. The user is asked to select the images for given period of time.



Fig. 2 Passfaces

3. Jermyn et al.,[3] proposed a new technique on which user has to draw a secret i.e. DAS on a given 2D grid. If the drawing matches on the same grid in same sequence then the user is authenticated on the basis of their selection.

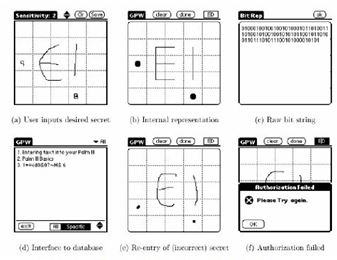


Fig. 3 DAS technique by Jermyn

4. Syukri[4] proposed a system in which the user has to draw the signature using the mouse. It includes registration and verification phases. At the time of registration, the user draws a signature on an area through which it has to be saved on the database and at the time of verification this signature is extracted from the database.

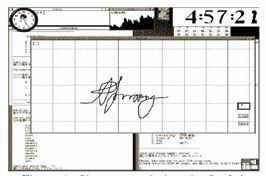


Fig. 4 Signature technique by Syukri

Further, normalization takes place with the input signature of the user, in order to match. This technique also has disadvantage i.e. the user is not friendly with signature done by mouse and forgery may also take place.

5. Blonde [5] proposed a system in which the user must check the approximate area of predefined location. Passlogix [6] encoded this scheme by giving permission to users to check as many objects to prove their authentication.

6. Haichang et el., [7] proposed a new shoulder surfing resistant scheme as shown in Fig. 5, where the user is required to draw a curve. This graphical scheme is the combination of DAS and story scheme that provide the user great authenticity.



Fig. 5 Haichang’s shoulder-surfing technique

7. Wiedenback et al.,[8] proposed a system which is resistant to shoulder surfing on some extent. In this method, the user has to click the convex hull formed among the different objects in the search of passwords. The password length depends on area of solution; it acts as indistinguishable or hard to guess if the area of picture is more.

****

Fig. 6 Example of a convex hull

8. Jansen[9], [10] proposed a graphical password scheme for mobile devices [17]. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the numbers of images are limited to 30, the password space of this scheme is not large.

9. Weinshall and Kirkpatrick [11] proposed several authentication schemes such as picture recognition object recognition pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes.

10. Goldberg [12] designed a technique known as “passdoodle”. This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen.

To overcome the shoulder surfing problem, many techniques are proposed.

1. Zhao and Li [13] proposed a shoulder surfing resistant scheme “S3PAS”. The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security.
2. Man, et al., [14] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants.
3. More graphical password schemes have been summarized in a recent survey paper [15]. Zheng et al., [16] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.

# PROPOSED work

There are three stages in authentication system:

1. *Registration Phase*

User enters his username and password in phase first and mesh of matrix is displayed in which the user has to choose the sequence by clicking on the matrix (row, column) i.e. in order to get registration index.

1. *Login Phase*

During login phase, the user has to enter the password based on the interface and after the authentication of username and password a blank matrix is displayed in which user has to click the particular block of (row, column) same as in registration phase in order to get the login index displayed on the screen.

1. *Verification Phase*

The system verifies the entered data with the data at registering time i.e. the system verifies the login index to the register index from the database.

.

# Hybrid Authentication Scheme

In our proposed system, we approach a new method of authentication technique which is composed of both textual and graphical password [18]. Each phase in our system is described below in details:

1. *Registration Phase*

In registration phase, the user first enters his username, the system checks whether the username exists or not in system. If it exists then the user has to choose another, if it does not then the user go further forward to choose their textual password. After choosing the textual password, the user has to click on some block of matrix on a blank matrix. When the user clicks on the matrix, the sequence of their selection is traced and saved to database as user presses the button to save as shown in Fig. 7. First user selects the username like (saleem) and password (1234), and then the user selects some block on a matrix. He selects the block (a1 b3), (a3 b4), (a5 b5), (a4 b3), (a5 b1). These selections are saved on the database after registration is successfully done. These act as a registration index.

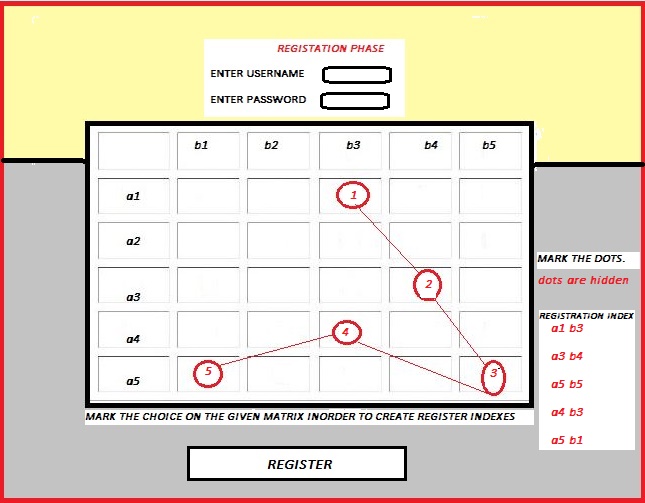


Fig. 7 Registration Phase

1. *Login Phase*

In login phase, the user enters his username and password. The system checks the username and password is matching correctly with the username and password in the database or not. If the given user id is correct then the user have a blank matrix in which he/she has to click on the block sequentially as he/she has done in registration phase. In Fig. 8, the user has to click the blocks as he/she selected in login phase i.e. (a1 b3), (a3 b4), (a5 b5), (a4 b3), (a5 b1), this will act as a login index.

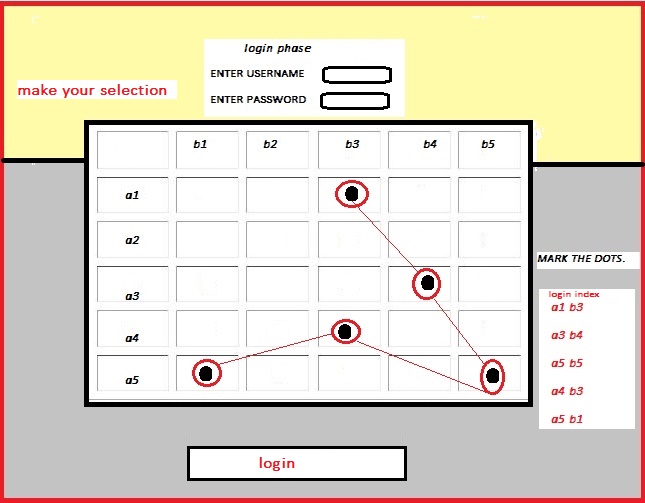


Fig. 8 Login Phase

1. *Verification Phase*

In this phase, the system fetches the database first in order to match the login index with the registration index as shown in Fig. 9. If all the details are matched successfully then the user becomes able to login the system. The flowchart of proposed system is show in Fig. 10.

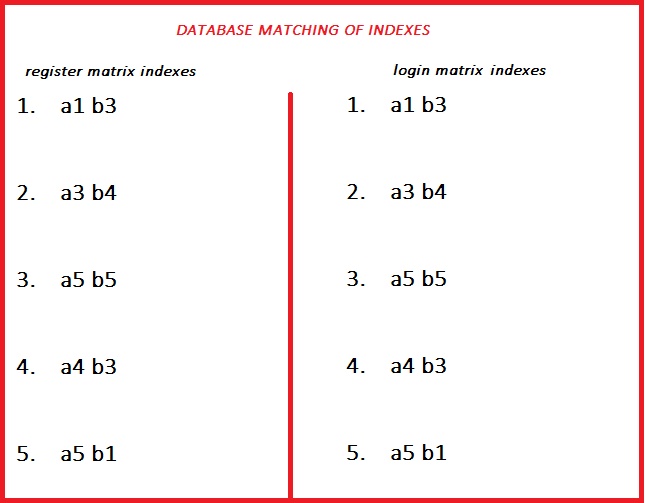


Fig. 9 Database matching of indexes

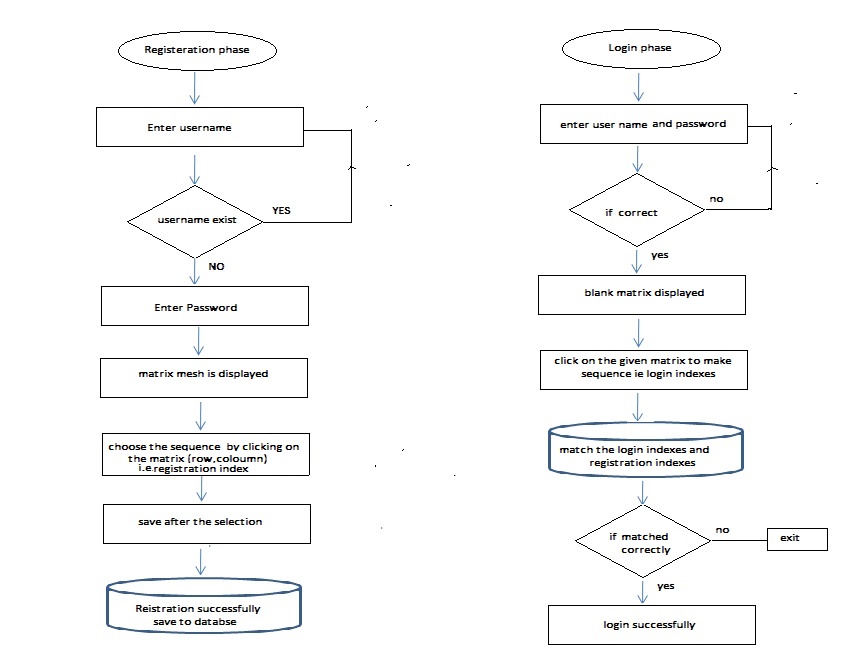
**

Fig. 10 Flowchart

# SECURITY AND USABILITY

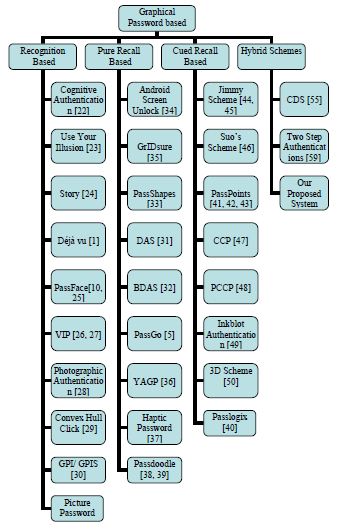


Fig. 11 Different types of system

The proposed system is hybrid and too much secure as you compare with the other authentication techniques, here it is too complex to the faulty user in order to pass through the different phases of system i.e. click on the correct grid and placed in a sequential manner to access OTP.

Our proposed system is too much secure as compared with others as shown in Fig. 12.

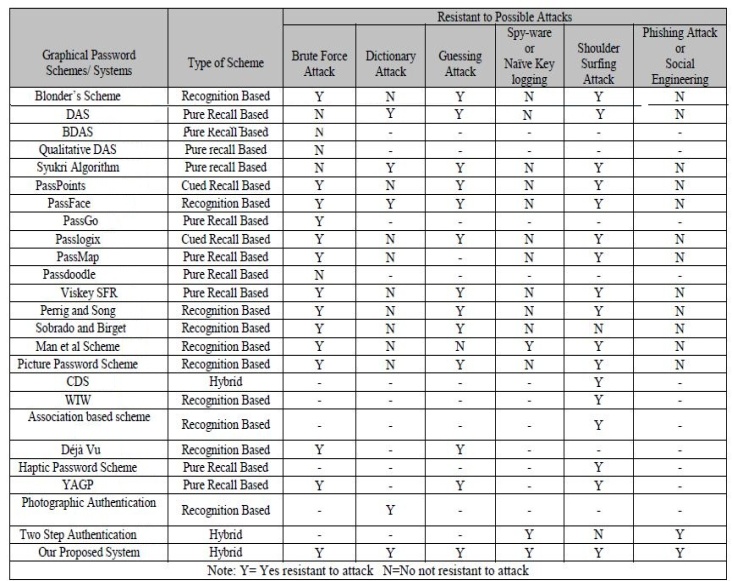


Fig. 12 Compare of our system

The possibilities of passwords generate in this system is very complex and depend on the indexes (positioning) and correct option of the matrix and finally a onetime password is to be send on the users phone.

# CONCLUSION

In this paper we proposed a new way of authentication which is composed of both textual and graphical authentication schemes. The user one by one follows the schemes as he further able to login the system. The combination of this hybrid scheme will further provide a great protection from threatening attacks like shoulder surfing, brute force attack, dictionary attack etc. This concept of choosing the block in sequential manner from the mesh of matrix will create huge impact in authentication scheme in present and future. Through the medium of this paper, we now approach new way of authentication in coming future.

# REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: “A User Study Using Images for Authentication” in 9th USENIX Security Symposium, 2000.

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent,Ed. United States, 1996.

[6] Passlogix, site http://www.passlogix.com.

[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu and Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing”.

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”, International Journal of Human-Computer Studies 63 (2005) 102-127.

[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.

[10] W. Jansen, "Authenticating Users on Handheld Devices” in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[11] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[12] J. Goldberg, J. Hagman and V. Sazawal, "Doodling Our Way to Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[13] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*, Las Vegas, NV, 2003.

[15] X. Suo, Y. Zhu and G. Owen, “Graphical Passwords: A Survey” in Proc. ACSAC'05.

[16] Z. Zheng, X. Liu, L. Yin, and Z. Liu “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5 May 2010.

[17] Mohammad Sarosh Umar and Mohammad Qasim Rafiq, *A Novel Graphical Interface for User Authentication on Mobile Phones and Handheld Devices*, International Journal On Advances in Intelligent Systems, volume 4, numbers 3 and 4, pp 380 to 387, 2011 (IARIA Journals) Publication Date April 30, 2012.

[18] Salim Istyaq, “A New approach of Graphical Password with Integration of Audio Signature Combination of Recall and recognition” i*n International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 6, Issue 4, Aug 2016, 45-50.*