# AUTHENTICATION USING TEXT AND GRAPHICAL PASSWORD

Abhilash M Joshi, Balachandra Muniyal
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal
abhilashjoshi1234@gmail.com, bala.chandra@manipal.edu

***Abstract*—Graphical password tends to be very promising and trending alternative technique to traditional methods like simple text password and alphanumeric passwords. It is the ease of use which attracts people. Traditional simple text passwords were too simple to guard the information and alphanumeric passwords possessed one huge disadvantage i.e., users ability to remember these passwords. Overcoming these problems of old techniques, graphical password came to life since it was a fact that people or users will remember the pictures better than the text or alphanumeric passwords. In this paper, a graphical password is developed which is in a form of a 3x3 matrix. Images in this matrix will be shuffled within, to avoid eavesdropping and shoulder surfing. The shuffle feature of this graphical password will stand against various attacks.**

***Index Terms*—Authentication, Graphical Password.**

## I. Introduction

Authentication is the most fundamental concept of security. Authentication portrays a very significant role when it comes to protection of data. It is defined as a function where in, user needs to provide a proof of his authorization, set of credentials which in turn should be exactly similar to the existing information stored in the system, then the user will be authorized or otherwise. Access control and accountability of users are the prime features of the authentication. [1]

Authentication is the only way to confirm ones identity and credentials to state whether the person is authorized to access the resources and information. This identity of a person can be anything including the digital certificate to that website.

There are three types of authentication based on the type of identity, they are as follows:

- *Approval of identity provided by the convincing person*: First-hand of the personality is certified. When verification may be obliged about craftsmanship or physical objects, this proof might be a friend or team members to accomplish a verification on the origin of the item, maybe by spotting or detecting the product in makers possession.
- *Comparing the attributes of the object*: This type is based on comparing the attributes of the object to the pre-existing knowledge of that object. For example, person expert in examining art will always look for the similarities in the paintings style and signatures form. Archaeologist, on the hand probably uses the carbon dating for verification of the artifacts age. Attribute comparison is also very delicate in the cases of forgery.
- *Depends on other external affirmations*: Criminal court is the best example, where evidence frequently needs the confirmations from the external sources. This can be done by using a evidence log or more like a testimony from the police, forensics department that took the case. The records which come from the external sources are already vulnerable to forgery.

Computer science has a different way to provide access to the user on the basis of his/her credentials. Administrator of the network may provide user a password or a key or any other device to allow access to the system.

Authentication serves following purposes:

- *Confidentiality*: Only authorized sender and the recipient should be allowed to see the contents.
- *Integrity*: Contents of the message or the data should not be compromised until it reaches the designated recipient.
- *Access Control*: Access Control specifies and controls which user can access what resources.

Authentication is mainly categorized into three different types: [2]

- *Token Based Authentication* is determined on the basis of what do you own or what is in your possession. For example, college id of a student, license to drive can act as an identity of the user. Demands user to submit his/her user name or id with the corresponding password, which in turn gives a token to access the system resources. Examples like ATM cards with PIN numbers. To make this method more stronger, it is used alongside knowledge based authentication which is discussed below.
- *Knowledge based techniques* is put widely in use. Comprising of both the levels i.e text and picture based. Picture based level is further divided into two categories, *recall based*: is users ability to recall and reproduce something which was already done while in registration; *recognition based*: user will tend to recognize the same images which he/she selected in the registration phase.
- *Biometrics Based Authentication* extends to the knowledge of identifying the users on the basis of their behavioural pattern. This method works on the foundation of what you are. Facial identity, eye scanner, voice recognition, fingerprints too are the examples of biometric authentication. Biometric scanning devices take the data from facial patterns, finger prints and transfers it to the system, which in turn validate it by converting it into

978-1-5386-5314-2/18/$31.00 ©2018 IEEE

the digital information. Only disadvantage is it is very expensive.

Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. Authentication based on text-based passwords has major drawbacks. Text passwords are subjected to phishing attacks and dictionary attacks. Text passwords can also be stolen by using a malicious software (e.g. key loggers) when being entered from keyboards. Therefore, text based password authentication is no more secure enough to authenticate users into the system.

Text passwords remain ubiquitous, despite endless criticism. Text passwords were made for the users to consider the usability factor. Almost all the websites or the web applications on the internet use text-based password method. Users and developers are also aware that having only text based password technique is not secure enough anymore for many different reasons. The text passwords when developed were more like a plain text which would consist either of sequences of alphabets which started in 1961 by MIT. These plain text passwords were made in order for users convenience. Later, as the research went on, the vulnerability of these clear plain text was discovered and hence the numbers were also combined in the password field to make it more strong which is now called alphanumeric passwords. This scheme was in the use for a while, but later even this got exhausted and special characters like @ were also included in the password field. Later on as the development in security section went on, passwords were constrained according to the criteria like at least one capital letter, at least one small letter, at least one numeric value and any special characters. Todays trend combines all this schemes along with the length constraint of the passwords. Alphanumeric stood against many attacks, but somehow even this hybrid of password authentication came to an end. Looking at the traditional, modified authentication methods getting exhausted, graphical passwords came into an evolution.

Use of pictures password came into existence when it was concluded that humans are more skilled in remembering the images, pictures as compared to the string of characters [3]. Greg Blender in 1996, defined the idea of the graphical password and later, based on this idea, many graphical password authentication schemes were made. Blonder, came up with one such idea of graphical password where, user has to choose few regions of the images and then have to select the same regions while logging in, then the user will be authenticated. Graphical password can be divided into two parts:

- *Recall-based techniques* also known as the draw metric system. user has to reproduce something(like image or signatures) which he/she has already done during the registration. Recall based method is bit tedious as user can't accurately recall exactly as it is.
- *Recognition-based techniques* compared to the above recall method recognition based method is slightly easier. User has to just recognize their password images. As, the name says, recognition is way better than recalling. Only task user has to do is to identify the same images which he chose as his password during the registration phase.

## II. Literature survey

The author Syukri et.al., [4] invented a technique where authorization is done with the signature of the user, signed with the use of the mouse as shown in Fig 1. This technique is carried out in two different steps registration and verification. While in the registration stage it is mandatory for the user to draw the signature with the help of the mouse, later which the system records it. In the verification part the signature is fed as an input to the system, normalization is done and the parameters are extracted. Disadvantage of this is duplicates of the signature can be made. This is because of the fact that drawing a signature with the help of the mouse is usually a difficult task and cannot be the same as that the time of redrawing it for verification.


Fig. 1: Signature technique by Syukri[4].

The author Wiedenbeck et.al., [5] put forward a technique where a user selects a triangle measuring a defined part of the picture password space as shown in Fig 2 which makes it difficult to guess. Advantages of this are that a password surface is very crowded which makes it harder to be identified. Disadvantages are that the convex surface assigning process takes longer time.

Fig. 2: Interface design for password login[5].

Grinal Tuscano et.al., [6] came up with an idea of two step graphical password authentication system which is based on pass faces. They developed a system which can be user friendly as well as secure; by combining images along with the texts. The original pictures selected by the users can be subjected to guessing attacks. The attacker even though doesnt have background knowledge about the user can still obtain the images by guessing. The Distortion Technique as shown

in the Fig 3 can comparatively reduce the risk of collective educated guess attacks based on the Biases in users choices of authentication images.

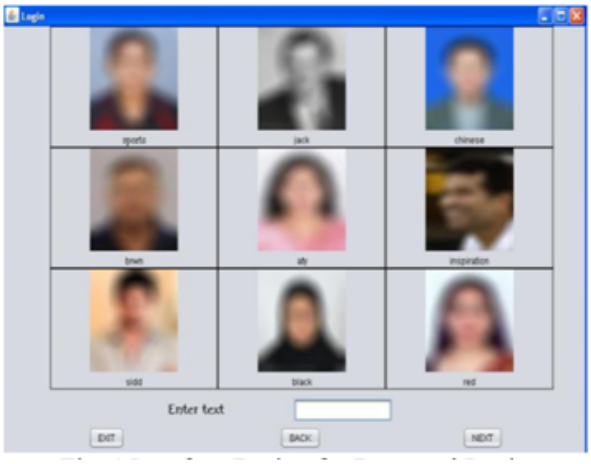


Fig. 3: Triangle Based Scheme[6].

Man, et.al., [7] proposed an algorithm which can resist the attack of shoulder surfing. This algorithm give user a flexibility to choose a significant number of images as pass-objects. Objects have many variants in it. Each variant is given a code which is unique. At the time of authentication the user faces many objective with plenty of scenes as shown in the Fig 4. Each and every scene consists of a large number of pass-objects (each in the form of a randomly chosen variant) and many other decoy-objects. The user has to mention the unique code which gives back the variants of the pass objects embedded in the scene as well as a code corresponding to the relative location of the pass objects reference to a pair of eyes. It becomes difficult for the attacker to crack a password even if attacker film the whole login process.

Fig. 4: Shoulder Surfing resisting attack[7].

Martin, et.al., [8] came up with an idea of the image pass system in which a 4x4 grid of images is presented to the user, which contains user's desired image and the other decoys. User have to login by clicking the images with a strict sequence. This technique is mainly divided into two stages; enrolment stage where user have to register by selecting the username, if username is available then moving further to graphical password selection , where a 6x5 grid of images will be given to the user with some useful functional buttons as shown in Fig 5. User have to select minimum four images to create a password and also remember the sequence in order to login. In case of forget password scenario, user has to contact the administrator for a key which will allow user to change the password.

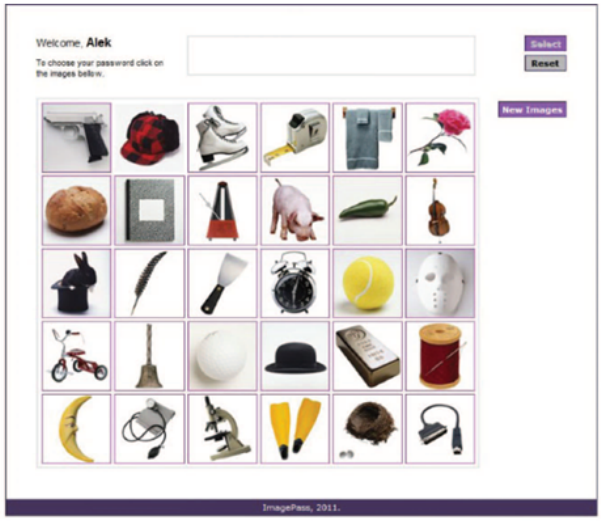


Fig. 5: 6*5 matrix presented to user to make their own password[8].

Yuxin Meng et.al.,[9] coined the method of CD-GPS (Click-Draw Based Graphical Password Scheme), user will select some n images from the image pool. Images will be no different than the general or everyday topics. User should remember the order of images as a story which can be literally convenient for the users. Further more, user have to select another set of k images from the above selected n images as shown in the Fig 6. These k images are used for the further step i.e., draw a secret. For example , out of 10 N images in the image pool, 4 n images are selected and 1 k image is chosen for draw a secret. After selection of images, user will now have to draw a secret on N*N grid. This secret can be anything like number or alphabet. User will choose suitable size of grid to remember the co-ordinates of their secret image as shown in Fig 7. This completes the actual registration of the use to the system. During the login, user has to select the images in the same order and then draw this secret image to login.

Andrea et.al., [10] proposed a graphical password authentication system which is known as PassByop (bring your own picture as graphical password). This technique involves many gadgets like a plastic box of a certain dimension with a Logitech camera facing upwards with display features of 30 frames per second and resolution of 640x480 pixels. Camera connected to a PC which runs this PassByop, its interface is shown on ipad. Resolution of video taken is 450x600 pixels on ipad. Now, user can make the password by selecting the portions of the image on. User can select only four regions of image. This data is given as password of the user to the

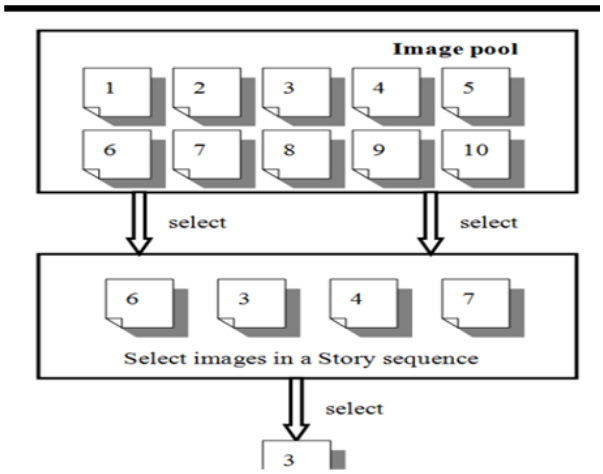


Fig. 6: Showing the selection of images from an image pool[9].

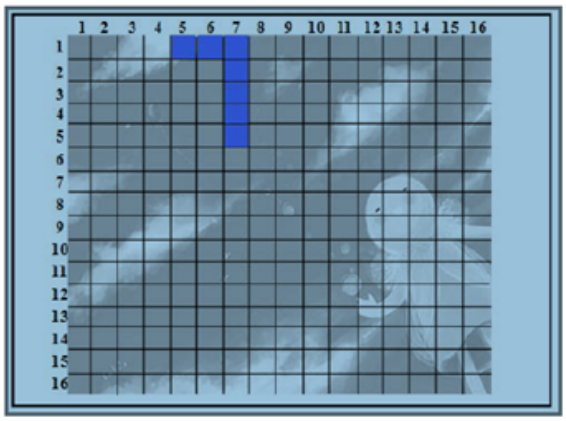


Fig. 7: Grid display shows the draw a secret formation by user[9].

pc through i-pad. The regions of the image once selected is shown to the user as a feed back and is stored internally for every login verification. User can choose to either reset it or just keep it as a password as shown in Fig 8.

Anmol et.al., [11] works on the basis of the CCP (Cued Click Points). Since, Passpoints have a huge disadvantage of making a password by selecting the different regions on the same image, which can be vulnerable to the guessing attack. Hence, the main problem was the HOTSPOT, is the area where user clicks. So, the proposed system, in this paper was use of CCP as shown in Fig 9. CCP technique is of making a password by clicking the different points of different images as their password. Users registration process is divided into two parts , first is simple email verification, second phase is making of CCP and again confirming the CCP as their password. This CCP password is stored in the server for the further validation. During the login time, user has to first put the text password, then reproduce the CCP password to login. Any failure, user

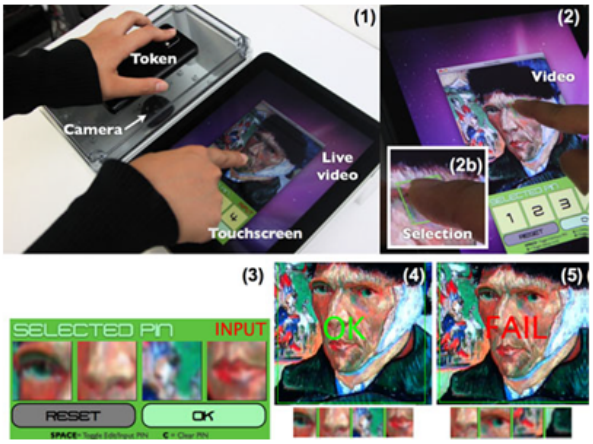


Fig. 8: (1) Overview of the PassBYOP system. (2) Input selection and closeup(2b). (3) Input selections that make up a password. (4) Successful authentication and (5) denied authentication[10].

will be sent an alert through email.

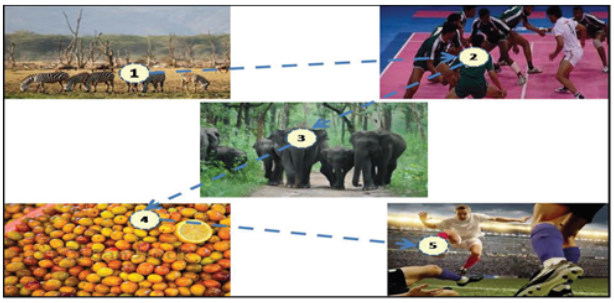


Fig. 9: Application of CCP[11].

Abutalha Danish et.al., [12] made an graphical password authentication scheme in which user have to align the graphical images to each other. Since, every authentication is divided into the two phases, registration and login. In this training phase, user have to select any number of images from a set of image pool as their password. later the graphical password appears to be in the form of the rings with a submit button in the middle. If user selects three images, then three rings formation can be seen, these rings of images are nothing but the concentric circles. These circles will contain valid , selected images along with the other decoys. In order for the login session, user have to align the valid images to each others as shown in Fig 10 below. If the alignment is executed properly then, user is authenticated.

Shivani et al [13] proposed an authentication which is a combination of the graphical password as well as one time session key. During the registration phase, user will give a name and the password to enter into the system. User then have to select any four images of his choices , user should remember the sequence of the image selection. This completes the whole registration process. During the login, user will be given two grids, one is pictorial grid and other is alphanumeric grid. In the pictorial grid, user will be shown his valid images as well


Fig. 10: Alignment of the images in this graphical password[12].

as other system selected random images. On selecting his valid images in a strict sequence, two digit number will be attached to every image as shown in Fig 11. First digit shows the row , second digit shows the column in the alphanumeric grid. User should now refer that alphanumeric grid to see the value of the cell of that row and column as shown in Figure 12. These values from every image's numeric string is combined which will make a key for the session. Once, the key is developed, user has to input it to the system and system will give access to the user.

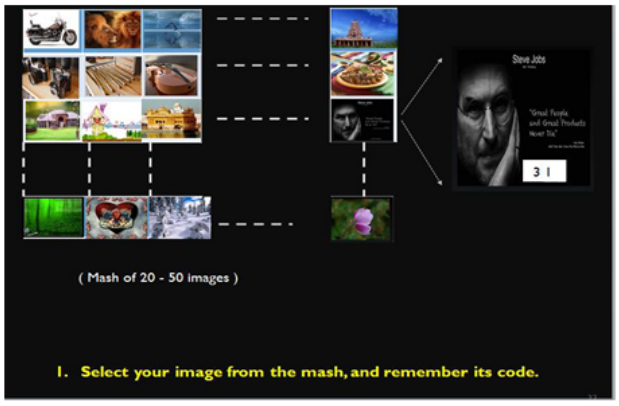


Fig. 11: On selection of strict sequence of the image, a two digit number is shown[13].

## III. Methodology

Proposed method of authentication is used mainly in web. The welcome page of the authentication system will be displayed as the user will just open the application. This welcome page of the system gives the user two options login and sign-up in order to browse him through the contents of the web

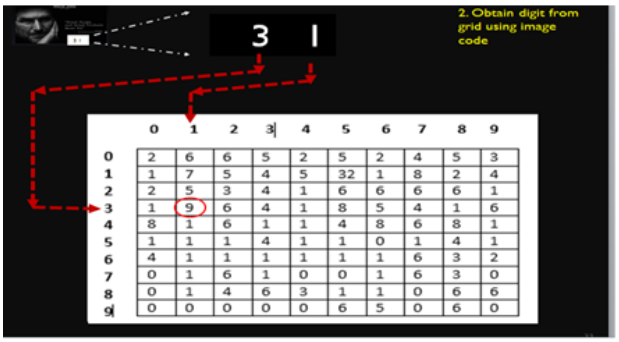


Fig. 12: Referring alphanumeric table for obtaining the key on every selected image[13].

app. Further section will discuss about how the user will be logged in and signed up.

When the user is new to the application, he/she must or should always sign up in order to register successfully and to browse through the contents of the web app. As soon user selects the sign up option , personal details of the user is asked like first name, last name, email-id, which should be valid and in use. In this page, user will be allowed to select a user name which can be anything even the alphanumeric. If user name is taken already, then user have to fill in with some different name.

Provided, if all the details of user is valid, then the user will receive one alphanumeric password which will be sent to their mail-id by using one administrator email. As the users are registered successfully, all the details are stored in the back end handled or managed by the phpmyadmin. User can use this password for the first time or numerous times to log into the system. User can also change the password when he or she wishes to. Once, the user is done with the text password registration, a matrix of 3x3 size containing images is prompted to select for their registration as shown below in Fig 13. User can only select three images as a constraint. Once, this part of level in sign-up is done, user is successful in registration.

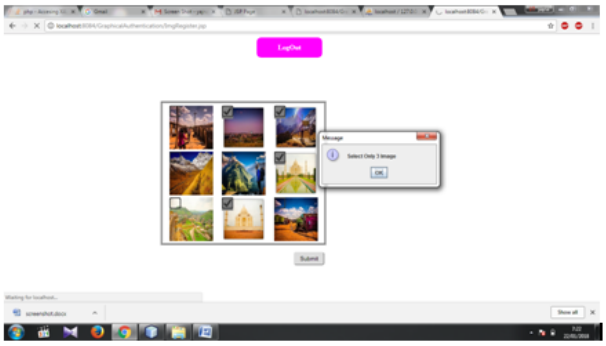

Fig. 13: User selecting their graphical password.

User with their account credential can sign in whenever they want to. With appropriate credentials, any user can log into the system. The first phase which user has to undergo is text password authentication which is nothing but the usual user-id and the alphanumeric password. There are five attempts given

to the user for text password authentication, if given chances are exhausted then, forgot password option will appear and user have to type in their email id and then can change their password.

The user is done with the first level; there is one more level of security he has to go through i.e. graphical password authentication. This graphical password developed is in the form of the matrix of 3x3 size with nine cells and all filled with the valid and decoy images. When the user comes across this graphical password, they have to select the same images which they have selected in the registration phase regardless of any sequence. Once, the user is done with the valid selection, he or she can successfully login to the system as shown in the Fig 14.

Fig. 14: Shows a scenario of successful login.

This authentication also comes to track the lifetime of the user on the internet. This can be seen and managed only by the administrator himself. The lifetime of the user on the internet is shown in the form session start and session stop column of the table. The administrator will be the master of this tool completely. The password for accessing the user details will be only with admin.

## IV. Conclusion

Text passwords were exhausted while protecting the information and resources. Alphanumeric passwords was a hybrid method, stood against all the various attacks for a while but also got subjected to it's many disadvantages. Authentication technique developed in this paper, uses both text and graphical password. User gets the first password through his mail id which is alphanumeric in nature and user is given liberty to change the password any time he/she wants. Alphanumeric passwords may stand against guessing attacks for a while(if attacked).Adding graphical password to the authentication gives on more security level. Graphical password is in form of a matrix 3x3, with shuffle feature. Images selected by user in the registration phase will be still shuffled at every login, which gives attacker no advantage on eaves dropping. Developed method provides double security check for the user to login. Hence,this authentication is more secure.

## References


[1] A. Almulhem, "A graphical password authentication system," in *Internet Security (WorldCIS), 2011 World Congress on*, pp. 223–225, IEEE, 2011.

[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Computer security applications conference, 21st annual*, pp. 10–pp, IEEE, 2005.

[3] O. Ayannuga Olanrewaju and F. Olusegun, "Graphic-text authentication of a window-based application," *International Journal of Computer Applications*, vol. 21, no. 6, pp. 36–42, 2011.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Australasian Conference on Information Security and Privacy*, pp. 403–414, Springer, 1998.

[5] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*, pp. 177–184, ACM, 2006.

[6] M. G. Tuscano and A. Tulasyan, "Graphical password authentication using pass faces," *International Journal of Engineering Research and Applications*, vol. 5, no. 3, pp. 60–64, 2015.

[7] S. Man, D. Hong, and M. M. Matthews, "A shoulder-surfing resistant graphical password scheme-wiw.," in *Security and Management*, pp. 105–111, Citeseer, 2003.

[8] M. Mihajlov, B. Jerman-Blazic, and M. Ilievski, "Recognition-based graphical authentication with single-object images," in *Developments in E-systems Engineering (DeSE), 2011*, pp. 203–208, IEEE, 2011.

[9] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on*, pp. 39–48, IEEE, 2012.

[10] A. Bianchi, I. Oakley, and H. Kim, "Passbyop: bring your own picture for securing graphical passwords," *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 3, pp. 380–389, 2016.

[11] A. Bhand, V. Desale, S. Shirke, and S. P. Shirke, "Enhancement of password authentication system using graphical images," in *Information Processing (ICIP), 2015 International Conference on*, pp. 217–219, IEEE, 2015.

[12] A. Danish, L. Sharma, H. Varshney, and A. M. Khan, "Alignment based graphical password authentication system," in *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 2950–2954, IEEE, 2016.

[13] S. Agrawal, A. Z. Ansari, and M. S. Umar, "Multimedia graphical grid based text password authentication: For advanced users," in *Wireless and Optical Communications Networks (WOCN), 2016 Thirteenth International Conference on*, pp. 1–5, IEEE, 2016.