Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hybrid Graphical Password System with Recovery of Passwords using Text and Sound Signature

Manoj Bhole, Prof. Pravin Shrinath
Department of Computer Engineering, MPSTME
NMIMS University, Mumbai, Maharashtra, India

Abstract—Graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have described our new hybrid graphical password based system, which is a combination of recognition and recall based techniques and also provides the password recovery facility. In recognition method, user will have to register password by selecting sequence of images and selecting particular region of each image by click points and then assigning textual characters to each image and then sound signature is assigned by recording voice to each click point. Textual characters and Sound signature here in this case is used for recovery of password, textual characters used for recovery of image sequence and sound signature is used for recovery of click points assigned for each image. In spite of slower registration and login process, this hybrid scheme offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. Thus, this scheme is suitable for high level security system such like personal lockers, bank lockers etc. which are not accessed for daily purpose.

Keywords— Hybrid graphical password, Recognition method, Click based method, Textual characters, Sound signature, Recovery of passwords.

I. INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumerical password [1]. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches. The graphical user authentication system requires a user to select a memorable image. Such a selection of memorable images would depend on the nature of the image itself and the specific sequence of click locations. Images with meaningful content will support the user's memorability

A. Background of Alphanumeric passwords:

Textual passwords are the traditional scheme of authentication in which user chooses the password using characters, numbers, symbols or combination of all. It is easy to use the traditional scheme. But textual passwords are vulnerable to different of the attacks. The easy the password it is easy to guess by the imposter where difficult passwords are difficult to remember sometimes.

II. GRAPHICAL PASSWORDS AND RELATED WORK

Graphical passwords refer to using pictures as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should be more resistant to brute-force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques [1]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Pass-faces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces. An early recall-based graphical password approach was introduced by Greg Blonder in 1996. In this approach, a user create a password by clicking on several locations on an image. During authentication, the user must click on those locations. Pass-Points builds on Blonders idea, and overcomes some of the limitations of his scheme.

A. Classification of Graphical Passwords

Graphical based passwords schemes can be broadly classified into four main categories [4]:

- Recognition Based
- Pure Recall Based
- Cued Recall Based
- Hybrid Schemes

Following figure shows the classification of graphical based passwords:

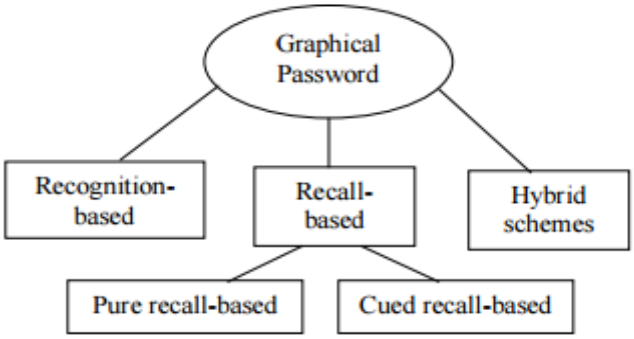

Fig 1.Classification of graphical based passwords [4].

*1) Recognition Based:*Recognition based Systems which are also known as Cognometric Systems or Searchmetric Systems. Recognition based [3] techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. For Eg: Pass faces, Picture passwords. Table I shows some of the algorithms which were created based on this technique.

Table I RECOGNITION BASED TECHNIQUES ORDERED BY DATE

Algorithm	Proposed Date	Created By
Passface	2000	SachaBrostoff , M. Angela Sasse
Déjà vu	2000	RachnaDhamija,AdrianPerrig
Triangle	2002	Leonardo Sobrado ,J-CanilleBirget
Movable Frame	2002	Leonardo Sobrado ,J-CanilleBirget
Picture Password	2003	Wayne Jansen, et al.
WIW	2003	Shushuang Man, et al.
Story	2004	Darren Davies, et al.

Jensen et al. [9] proposed a graphical password scheme based on Picture password[5]. Throughout the password creation, the user has to select and register a sequence of the selected thumbnail photo to form a password (Fig. 2). The user needs to recognize and identify the previously seen photos and click it in the correct sequence order to be authenticated.

Fig 2. Picture Password [5]

Based on the assumption that human can recall human faces easier than other pictures, Real User Corporation [10] has developed their own commercial product named Pass-faces[2],[5]. In pass-face scheme user have to select the human face from the grid of nine faces (Fig .3). This step is continuously repeated until all the four faces are identified.

Fig 3. Pass-face scheme

2) Cued-Recall Based: Cued Recall based systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password to reproduce their passwords or make a reproduction that would be much more accurate. For eg. Blonder scheme, Cued click point CCP). Table II shows some of the algorithms which were created based on this technique.

Table II CUED RECALL BASED TECHNIQUES ORDERED BY DATE

Algorithm	**Proposed Date**	**Created By**
Blonder	1996	Greg E. Blonder
Passlogix v-Go	2002	Passlogic Inc. Co.
VisKey SFR	2003	SFR Company
PassPoint	2005	Susan Wiedenbeck, et al.
Pass-Go	2006	-
Passmap	2006	Roman V. Vamponski
Background DAS (BDAS)	2007	Paul Duaphi

In Blonder scheme[8]the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as their password and they have to choose the same region following the same order to log into the system. The user must remember the "chosen click spots" and keep them secret (Fig. 4).

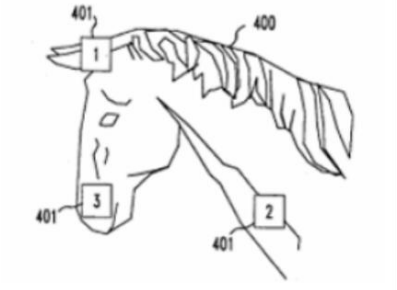

Fig. 4 Blonder scheme [1]

3) Pure-Recall Based: Pure Recall based systems which are also known as Drawn-metric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. For e.g. DAS (draw a secret), Pass-Points. Table III shows some of the algorithms which were created based on this technique.

Table III PURE RECALL BASED TECHNIQUES ORDERED BY DATE

Algorithm	**Proposed Date**	**Created By**
Draw a Secret (DAS)	1999	Jermyn Ian et al.
Passdoodle	1999	Christopher Varenhorst
Grid Selection	2004	JuaieThorpe,P.C.VanOorschot
Syukri	2005	Syukri, et al.
Qualitative DAS (QDAS)	2007	Di Lin, et al.

DAS (Draw-A-Secret) [13] scheme is the one in which the password is a shape drawn on a two-dimensional grid of size G * G as in Fig.5. Each cell in this grid is represented by distinct rectangular coordinates (x, y). If exact coordinates are crossed with the same registered sequence, then the user is authenticated.

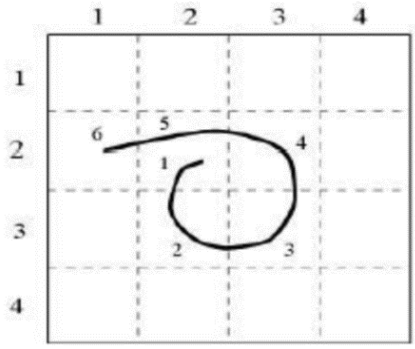

Fig. 5 DAS (Draw a secret) [1]

Pass-Pointsystem by Wiedenbeck,et al. extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used [1]. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence (Fig. 6).

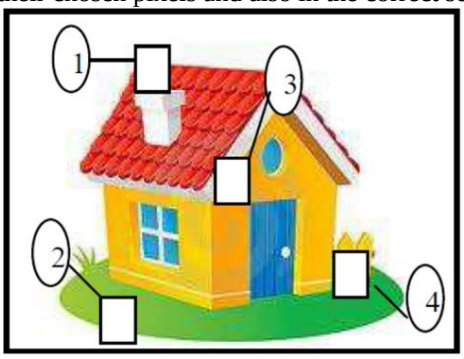

Fig. 6 Pass-point

4) Hybrid Scheme: Hybrid systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes. As hybrid systems suggest to use of multiple methods in one system, it can help to enhance the performance of the system by increasing the level of authentication.

- Textual Characters:Textual characters can be used with the combination of graphical password methods, by assigning textual characters on graphical password. We are using textual characters for recovery of images used as a password.
- Sound Signature:The sound signature allows the user to choose an audio file at runtime or use his/her voice for creating sound file. This audio file chosen from file directory or the audio file is recorded by the user and then it is associated with the graphical password and stored into the database [14]. It strengthens the security of the protected data.

At the verification level user has to provide audio file and then verifies it with the stored sound file and then shows images to the user for reading graphical password from the user, as the user is verified partially with the help of sound file. We are using this sound signature for recovery of the click points of graphical passwords.

B. Various Attacks On Graphical Passwords

Graphical passwords are not much vulnerable to attacks, so cracking the graphical passwords are difficult than text base passwords.

*1) Brute-Force Attack:*This is an attack which tries every possible combination of password status in order to break the passwords. Text-based passwords have a password space of 94^N, where N is the length of the password, ninety four is the number of printable characters excluding "space". Computationally, this attack is always successful because it checks all possible passwords in the password length; therefore users should try to select strong passwords to be more resistant to brute force attack. It is more difficult for this attack to be successful in graphical passwords than textual passwords because the attack programs must create all mouse motions to imitate the user password, especially for graphical passwords. The main item which helps in the resistance to brute force attacks is having a large password space.

*2) Dictionary Attack:*This is an attack in which the attacker starts by using the words in the dictionary to test whether the user choose them as a password or not and also to track keyboard input to crack password. The brute force technique is used to implement the attack. Since recognition based and click based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical password. This sort of attack is more successful in the textual password.

*3) Spyware Attack:*This is a special kind of attack where tools are initially installed on a user's computer and then start to record any sensitive data. The movement of the mouse or any key being pressed will be recorded by this sort of malware. All the data that has been recorded without notifying the user is then reported back out of the computer. Except for a few instances, using only key logging or key listening spyware cannot be used to break graphical passwords as it is not proved whether the movement of the mouse spyware can be an effective tool for breaking graphical passwords. Even if the mouse tracking is saved, it is not sufficient for breaking and finding the graphical password. Some other information such as window position and size, as well as timing information are needed to complete this kind of attack.

*4) Shoulder Surfing***:** It is obvious from the name of this attack, that sometimes it is possible for an attacker to find out a person's password by looking over the person's shoulder. Usually this kind of attack can be seen in a crowded place where most people are not concerned about someone standing behind them when they are entering a pin code. The more modern method of this attack can be seen when there is a camera in the ceiling or wall near the ATM machine, which records the pin numbers of users. So it is really recommend that users try to shield keypad to protect their pin number from attackers.

*5) Social Engineering Attack (Description Attack):*This is an attack in which an attacker, through interaction with one of the employees about the organization, manages to impersonate an authorised employee. This may lead the 'impersonator' to gain an identity which is the first step of his hacking process. Sometimes the attacker cannot gather enough information about the organisation or a valid user. In such a situation the attacker will most likely try to contact another employee. The cycle is repeated until the attacker manages to get an authorized identity of one of the personnel.

*6) Guessing:*It is one which allows to guess the password according likes and dislikes of person. Hence, Graphical password also can tend to predict by guessing like text based [5].

III. HYBRID GRAPHICAL PASSWORD SYSTEM

Our system uses a security system which have access through graphical password. There are mainly two types of graphical passwords. First is Recognition based system and other is Click based system. Our system is a Hybrid schemes of graphical system. The system uses Recognition based as well as Click based graphical systems. First, the user is registered by entering his name, the data is stored in the database. Next, the user have to select the images in sequential order (Picture Password) and for each image user have to click four points per image (Click-Points), so that the region of each image is selected. For assigning region use click points, certain tolerance for each click point is assigned. Additionally in our system the passwords can be recovered, in case of forgetting any identifying image or click point region of password. For this recovery option two schemes are used as textual characters and sound signature. Textual characters are used to recover the identifying images and sound signatures are used to recover click points. For each image in recognition password character is assigned by user while registering password, similarly in click based password a sound signature is assigned by recording voice to that of textual characters to recover the click points.

In our system, user have to identify the image or sequence of images in which user had chosen during selection of passwords and selecting the approximate region with respect to the tolerance provided for each image using click point method. The purpose of textual characters and sound signature associated with each image and click points is to recall the passwords. It is like the security questions used in traditional authentication methods

Our system is a hybrid system which uses both recognition based and click based methods, hence it will increase the security level and intruder cannot easily attack in it. So, our system is not easily vulnerable to various attacks like traditional systems.

A. Recognition Based Password

In recognition based user have to select the sequence of the images at registration phase. And same sequence of images user have enter while login. If the match is found between the registered sequence and the entered sequence the user is authenticated.

B.Click Based System

In click based system user have to select the click points on the images and then same have to be entered during login. In our system, we are using combination of recognition and click based system, where first image is selected and identified using recognition and later click points are used to select the region of image and entering the same during login.

C. Textual Characters

In text based approach user have to select the textual characters for each image followed by each image of recognition based password. Textual characters will be used to recover the images used as password.

D. Sound Signature

Sound signature is used to recover the click points used for selecting region, it is nothing but to choose a small sound file for each click. It will be used for each click point followed by click based system.

In our system, Recognition and click based methods are used for authentication, whereas textual and sound signature methods are used for recovery of passwords. Let's consider the stepwise procedure for our system.

- First user has to enter user id and then have to register picture password by selecting the sequences of images in specific order.
- Next step to select the area of each image by selecting four co-ordinates by using click points and then to assign textual characters to each image.
- Then, assigning sound signature by recording voice associated with textual characters for each click points.
- Selecting textual characters and sound signature corresponding to each image and each click point respectively for recovery of passwords.
- At login phase, user has to enter the registered password as selecting the images along with the specified region by using click points for all registered images in sequence.
- After selecting the right sequence of the both password user is able to login successively.
- If user is not able to recall the graphical password, then user can use the recovery option of passwords by using textual characters and sound signature.

E. Registration flow of our system:

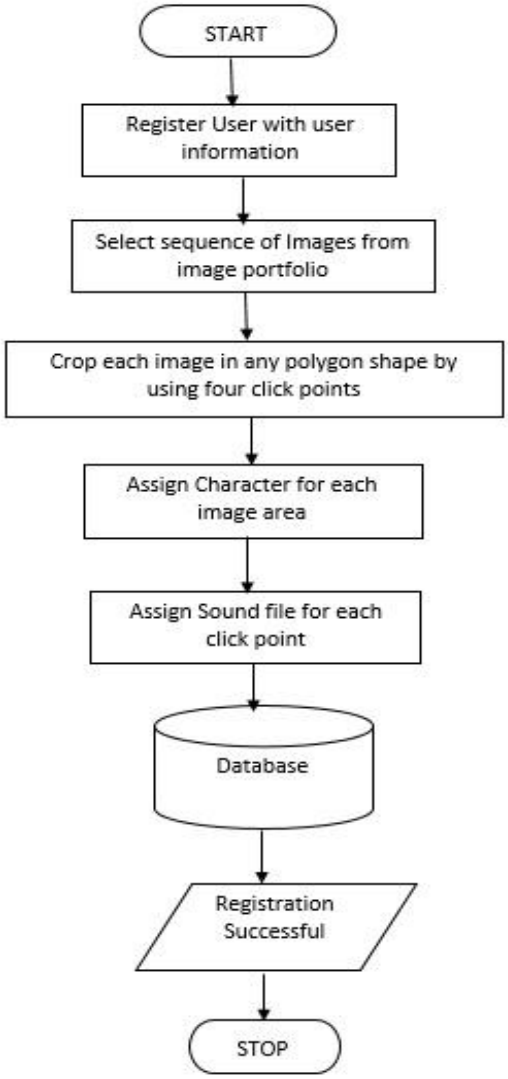

Fig. 7 Registration flow of our system

F. Login flow of our system:

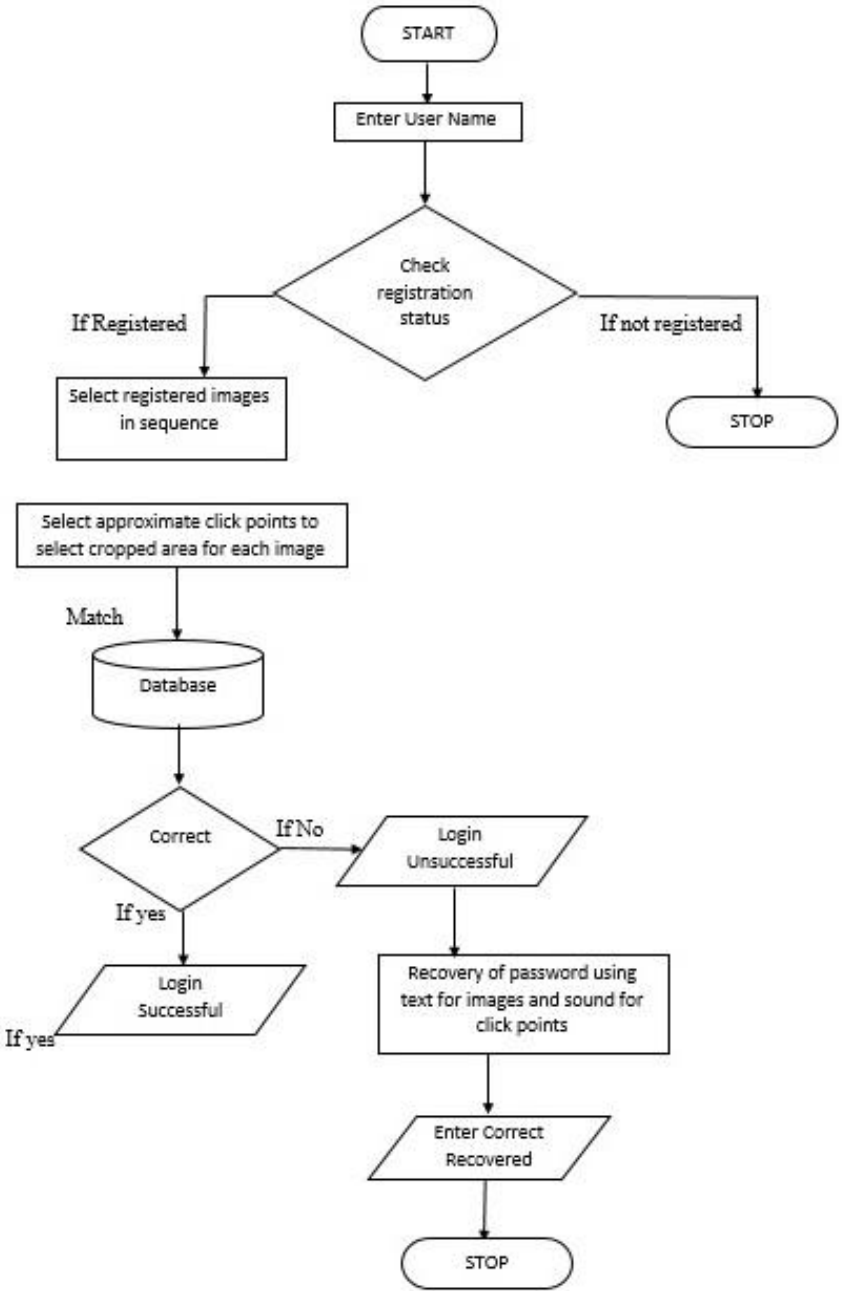

Fig.8 Login flow of our system

IV. IMPLEMENTATION AND RESULTS

We began analyzing the performance of the system based in terms of security, so that the system should not be vulnerable to any of the attacks mentioned above in section 2.2. We used matlab version 7 for implementing our system. For identifying the sequence of images we used the indexing with unique image id. For identifying the region of images we used correlation algorithm and for click points we used co-ordinates of (x, y) axis. Mainly the system is subdivided into four parts as:

A. Registration

Creating user profile with user details, this information is used to identify the user. Later, registering the password in sequence along with the recovery data in the form of text and sound file.

B. Login

In login part, user has to enter the registered password, which is matched with database. If match is found then user gets access to the system.

C. Recovery password

If user fails to login into system, user can recover the passwords. For recovering the passwords, user should have knowledge about the textual characters assigned for each images and sound file recorded for each click points.

D. Methodology

Consider, in our image grid we have 16 images, say I1-I16. Out of which four images are selected as password. These four images be I1-I4.

I1 = (P11, P12, P13, P14)
I2 = (P21, P22, P23, P24)
I3 = (P31, P32, P33, P34)
I4 = (P41, P42, P43, P44)

Here, I1 – I4 are the sequence of four images selected as password. And P11 – P44 are set of sixteen click points, four click points per image.

(I1, I2, I3, I4) = (T1)
(P11, P12 ….. P44) = (S1)

Here, T1 = Set of textual characters assigned for each image.
S1 = Sound file assigned for click points.
So, vector (I, P, T, S) are stored into database for particular user who is registered on system.
Where, I = (I1 – I4)
P = (P11 – P44)
T = Textual Characters
S = Sound File

Here, vector (I, P) is used for authentication. When user wants to login in to system, then input vector (I, P) is matched with database vector (I, P).

The purpose of vector (T, S) is to recall the vector (I, P) from database, when user is unable to input correct vector (I, P). But user must be aware of vector (T, S) used during registration.

E. Results

Table IV shows various attack to which authentication system is vulnerable, so particular solution for each attack has described. It also shows our hybrid system is solution to all the attacks discussed in Table IV.

Table IV PERFORMANCE OF SYSTEM WITH RESPECT TO ATTACKS

Attacks	**Vulnerability**	**Particular solution**	**All in one solution**
Brute force	For short length password	Selecting large passwords	Our hybrid system
Dictionary	Trace keyboard input	Recognition method (mouse)	Our hybrid system
Guessing	Guessing easy passwords	Selecting stronger passwords	Our hybrid system
Spyware	Trace mouse input	Hybrid method	Our hybrid system
Shoulder surfing	Shoulder movement	Recognition method	Our hybrid system

V. CONCLUSIONS

In this paper, we present hybrid system which is combination of recognition and click based system. Our system also provides facility to recover passwords by using textual characters and sound signature. In spite of slower registration, our system deals with efficient security. Combination of recognition and click based methods makes system stronger so that it cannot be attacked by intruders easily. So our system is efficient where daily transactions are not necessary and demands stronger security system where time is not much concerned.

ACKNOWLEDGMENT

A very warm gratitude to my guide for providing their help and guide for completion of work which is very appreciable.

REFERENCES

[1] Almulhem, A.; Comput. Eng. Dept., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia,"A graphical password authentication system", IEEE, FEB 2011.
[2] XiaoyuanSuo ; Dept. of Comput. Sci., Georgia State Univ., Atlanta, GA; Ying Zhu; Owen, G.S, "Graphical passwords: a survey", IEEE, DEC 2005.
[3] Eljetlawi, A.M.; Fac. of Eng., Univ. of Tajoura, Tripoli, Libya," Graphical password: Existing recognition base graphical password usability", IEEE, March 2010.
[4] WazirZada Khan, Mohammed Y Aalsalem and Yang Xiang, School of Computer Science, University of Jazan, "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[5] AshwiniFulkar, UchitaSawla, Zubin Khan AndSarang Solanki, "A Study Of Graphical Passwords And Various Graphical Password Authentication Schemes", Volume 1, Issue 1, 2012.

[6] *Ali Mohamed Eljetlawi, NorafidaBt.Ithnin, "Graphical Password: Usable Graphical Password Prototype", Journal of International Commercial Law and Technology Vol. 4, Issue 4, 2009.*

[7] Dhamija R. and Perrig A. (2000) In Proceedings of the 9th USENIX Security Symposium.

[8] Blonder G. (1996) In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961.

[9] Jansen W., Gavrila S., Korolev V., Ayers R. and Swanstrom R. (2003) NISTt NISTIR 7030.

[10] Real User Corporation (2007) PassfacesTM, http//:www.realuser.com.

[11] *Brostoff S. and Sasse M.A. In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.*

[12] *Davis D., Monrose F. and Reiter M.K. (2004) Proceedings of the 13th USENIX Security Symposium. California.*

[13] Davis, D., Monrose, F., and Reiter, M. K. 2004. On User Choice in Graphical.

[14] VikramVerma, Shilpi Sharma, "Authentication System with Graphical Security and Sound Signature", International Journal of Computer Applications,Volume 66, No.5, March 2013.

[15] *P.Elamathi, S.Saranya, E.Elamathi, "Implementing Authentication Providers Using Image And Sound Signature" 2013.*

[16] *Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.*

