Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 7, July -2015

Enhancing Strength Of Graphical Password Using Image Based Textual Password

Archana Bisen[#1], Mahendra Sahare[#2], Sini Shibu[#3]

MTECH (CSE), NIIST Bhopal. Affiliated to RGPV Bhopal, M.P., India

ABSTRACT :*Graphical password is proposed as an alternative solution to text-based alphanumerical passwords. The password techniques existing currently for authentication have major issues that need to be resolved. The usual prototype uses selection of the images from the image dataset which are generated at registration phase. The major challenge here is to remember or recognize the image from the dataset. In order to increase the strength of graphical passwords a new technique is proposed which generates the password from the selection of combined text and numeric value contained in image. Thus, in this work an attempt is made further to enhance the strength of graphical passwords by using image based textual passwords.*

Keyword: *graphical password, text based scheme, authentication.*

I. INTRODUCTION

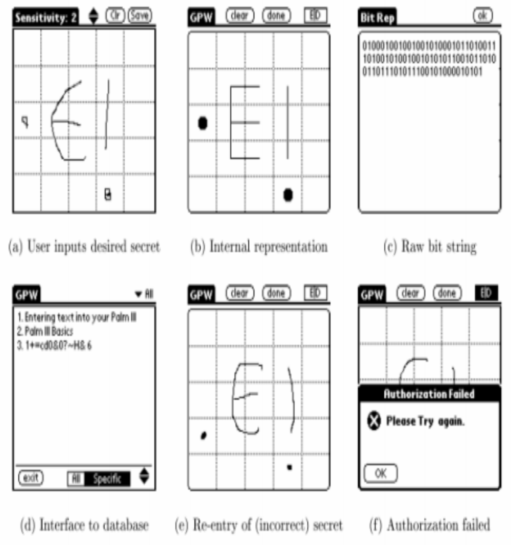
Graphical Passwords were originally described by BLONDER in 1996.A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI).For this reason, the Graphical password approach is sometimes called graphical user authentication (GUA).

Use of Graphical Password-
Web Log-in application.
ATM Machine
.Mobile device.

Why Graphical Password: Human can remember pictures better than text, Text Password is Memorable passwords easy for attackers to guess, but strong system-assigned passwords difficult for users to remember.Reusing same passwords across many accounts increases the potential impact if one account is compromised.Biometric based authentications are Expensive and inconvenient. They are Biometric information is part of a person’s identity leads to privacy concern.

II. RELATED WORK

During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size. Figure 5. A graphical password scheme proposed by Jansen,et al. [19] Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favourite image for authentication.



(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

Figure 1: Draw A secret Technique

The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their pass-images. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration. This method does not necessarily make it a more secure authentication method than text-based passwords. As shown in the studies, users' choices of picture passwords are often predictable. Allowing users to use their own pictures would make the password even more predictable, especially if the attacker is familiar with the user. Recall Based Techniques In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection.

An example of Pass faces (source: www.realuser.com) "Pass face" is a technique developed by Real User Corporation [15]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces (figure 4). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. User studies by Valentine [16, 17] have shown that Passfaces are very memorable over long intervals. Comparative studies conducted by Brostoff and Sasse [18] showed that Passfaces had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use. Their study also showed that the Passface-based log– in process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still uncertain. Davis, et al. [15] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password. Jansen et al. [19] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password .

PROBLEM FORMULATION

- Current password scheme is sometime not easy to memorized.
- Basic image password is hard to memorized sometime as it has to be chosen by the user and a image need to remember.
- Prototype execution is high and tough to remember.
- Blur images are sometime not clear to understand and recognize while registering the user.

III. PROPOSED ALGORITHM

To make Authentication technique which use text based on image set and make image authentication technique easy to memorize but hard to use by different user or robotic attacks. In order to reduce easy of use for the genuine user. we have worked on to remove blurring un-identified image problem and enhancing the system on providing clear images.In order to enhance security and user experience propose text-image based authentication algorithm. In this approach, propose a technique which is text image oriented password scheme in which nine images containing text and using which selection will provide the data containing in it. Three levels of difficulties are defined for the user registration phase, the password need to get select from the set of numeric and text values from the dataset. The final password will store in the registration time, finally user login will prompt for user to select image and select a password from the image attribute appear in combo box of password text selection.

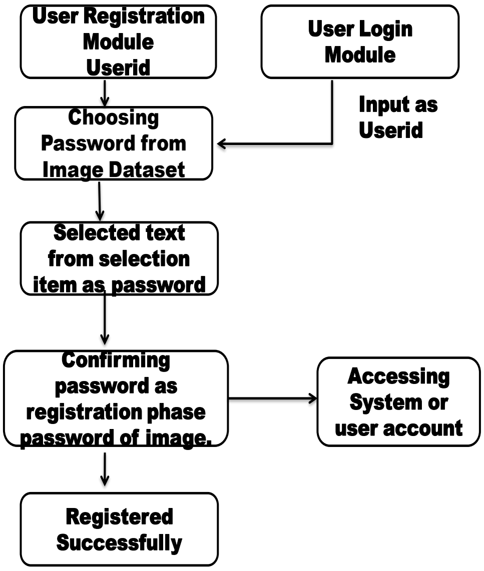

User Registration Module Userid
User Login Module
Input as Userid
Choosing Password from Image Dataset
Selected text from selection item as password
Confirming password as registration phase password of image.
Accessing System or user account
Registered Successfully

Figure2:Proposed Architecture of Experiment

<u>Algorithm Proposed:</u>

```
Input : Image dataset
Output: textual numeric password
For each(i..(1-9))
{Images are loaded into the screen set.Rotation is applied on to the image to recognize by the user.
}User click on image—loading the data on the images.
Showing them in drop down from i(1--n)
Password selection and storing in the user account.
```

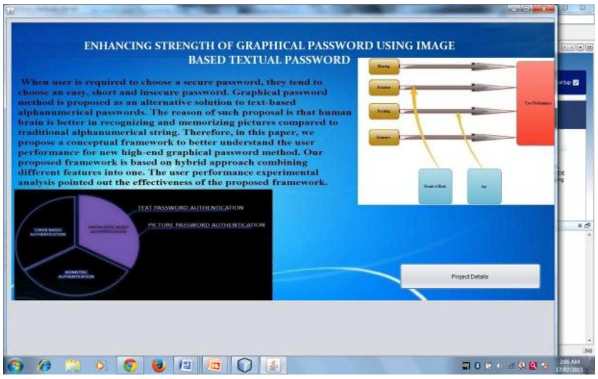
IV. EXPERIMENTAL SETUP

All the experiments were performed using an i5-2410M CPU @ 2.30 GHz processor and 4 GB of RAM running windows 7. The discussed feature selection algorithms were implemented using language Java. Proposed as well as existing feature selection algorithms were applied one by one in both the proposed framework for selection of password from different user for authentication process. At last, comparative study was prepared for both frameworks.

To estimate the performance of the system, the following formulas are used.
Computation time = Final time-initial time(in ms), Minimum time, Maximum time for authentication process.

V. RESULT ANALYSIS

Here in our research we are experimentally going to provide a simulation of Graphical password system where query will work with different type of conditions related to past behaviour of query and password system and will help to provide accurate result.
Here are the described result screen and detail discussion about the result.



ENHANCING STRENGTH OF GRAPHICAL PASSWORD USING IMAGE BASED TEXTUAL PASSWORD

When user is required to choose a secure password, they tend to choose an easy, short and insecure password. Graphical password method is proposed as an alternative solution to text-based alphanumerical passwords. The reason of such proposal is that human brain is better in recognizing and memorizing pictures compared to traditional alphanumerical string. Therefore, in this paper, we propose a conceptual framework to better understand the user performance for new high-end graphical password method. Our proposed framework is based on hybrid approach combining different features into one. The user performance experimental analysis pointed out the effectiveness of the proposed framework.

TEXT PASSWORD AUTHENTICATION
PICTURE PASSWORD AUTHENTICATION
TOKEN BASED AUTHENTICATION
KNOWLEDGE BASED AUTHENTICATION
BIOMETRIC AUTHENTICATION
Project Details

Figure 3: Simulation framework

The above screen describe about the module first before applying the appropriate visualization technique in the dataset already available taken from and performing the outlier detection technique firstly in order to simulate graphical password.

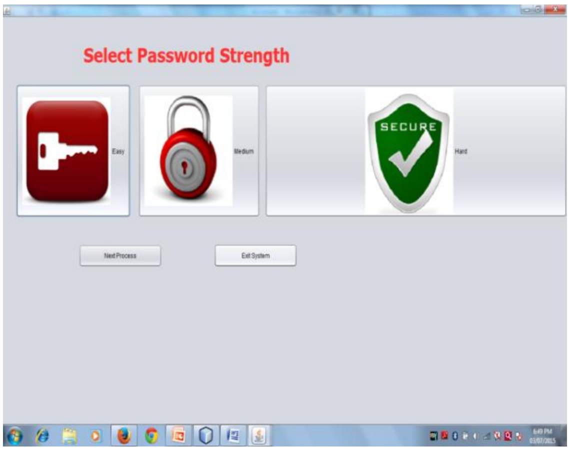


Figure 4: Medium Selection

Figure describe about the difficulty level selection three different medium of password.

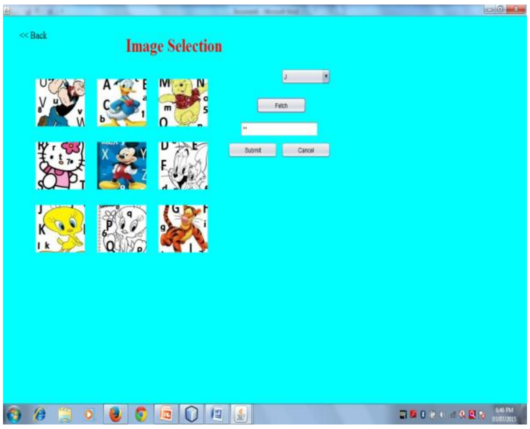


Figure 5: Password Selection from Image then Text

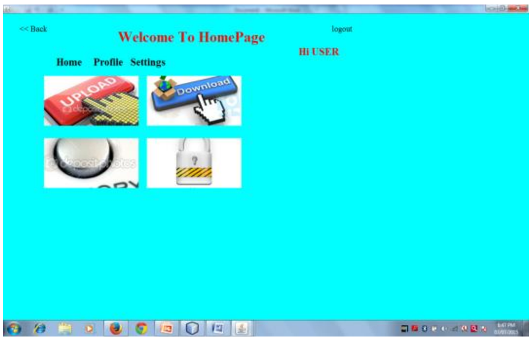


Figure 6: Operation performing

Various operation we can provide and can be applicable once we perform the authentication success on the proposed technique. Here we

have demonstrated our work in various respects and observed the result and measure the results based on the experiment performance we have observed and notified that Proposed Text based Graphical technique can be more better when we are using Authentication technique before applying the application process technique, while dealing with the secure system before the user can draw the things. Performance Measures Computation Time

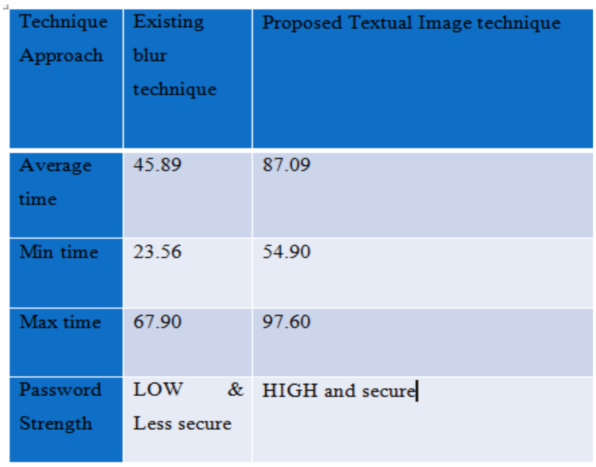
A training time of a dataset in Javais computed with the help of start and end time class variables defined in the tool and here as we load the dataset and verifies the eligibility and taking their features for consideration or not is the time taking process to identify and to load the images and selection of password comes under training time of a dataset, extracting the properties and making them in process format is training time.

Average Time

A Average time is the time of process we calculate and obtain the various average of multiple attempts from different id is made to get authenticate.

Observation:

In result analysis here is the system tolerance detail I have applied some random click and observed my best analysis result.



Technique Approach	Existing blur technique	Proposed Textual Image technique
Average time	45.89	87.09
Min time	23.56	54.90
Max time	67.90	97.60
Password Strength	LOW & Less secure	HIGH and secure

Table 1: Statically analysis of obtained result

- Password Strength

The capacity of password to get access grant while trying for multiple time and providing access to the graphical password environment to the wrong user.Password strength comes under weak password when we talk about.

- Computation time

Timing which it take to process the complete scenario.

Graphical analysis:

We have also observed and plotted a bar graph to represent our result analysis part:

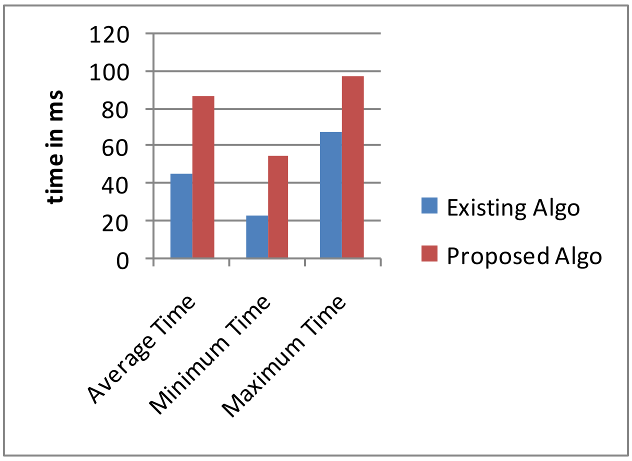


Figure 7: Bar chart presentation

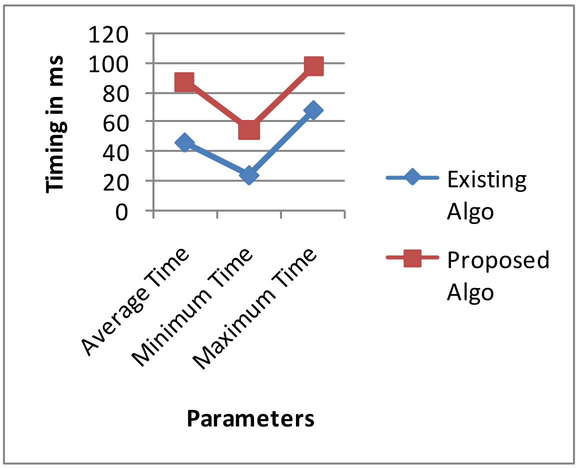


Figure 8: Graphical Line graph of Result Obtained

Working on text based graphical algorithm such as our proposed technique authentication will be efficient and easy to visualize and in order to make it more easy for user to use, such outlier technique will be efficient to use.

VI. CONCLUSION

In this paper we have discussed various techniques and our proposed technique model presented by our research. We have observed the result using various computation time of registration and login process where we find it at level best. As per our observation the proposed technique is performing and taking long computation time and also it removes the previous shoulder surfing problem associated with the current algorithm. Our result observed in statically and graphical presentation where it clearly provide us the accurate result of our proposed technique. A combine approach of graphical selection and then a text password based on object perform best and hence the approach is better to use in authentication process in real time. Our future work will be to perform the proposed approach on web or a model cloud technique for authentication process.

REFERENCE

[1]. Jalan Ayer Keroh Lama, "Conceptual Framework For High-End Graphical Password", 2014 2nd International Conference on Information and Communication Technology(ICoICT).

[2]. Yi-Lun Chen, Wei-Chi Ku , "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme", 2013 IEEE 2nd International Symposium on Next Generation Electronics.

[3]. HarmeetKaur , "Hybrid Scheme: Two Factor Authentication using Graphical password with Pass point scheme in Cloud computing", IJET-2013.

[4]. C Singh1 , L Singh, " Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[5]. S. Singh, and G. Agarwal, "Integration of Sound S signature in Graphical Password Authentication System", IJCA January 2011.

[6]. Fatehah M.D.,MohdZalishamJali,&Wafa M.K., "Educating Users to Generate Secure Graphical Password Secrets:An Initial Study" 2013 IEEE 5th Conference on Engineering Education (ICEED) 978-1-4799-2332-8/13

[7]. Gurav,S.M. Gawade,L.S.;Rane,P.K.; Khochare,N.R.Gawade, L.S., "Graphical Password Authentication",2014 IEEE international conference on electronic systems, signal Processing and Computing Technology.

[8]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a grapgical password system", International Journal of HumanComputer Studies, Vol.63, pp.102-127. (2005)

[9]. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.

[10]. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[11]. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int"l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[12]. Robert Biddle, Sonia Chiasson, P.C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years", Carleton University - School of Computer Science, Technical Report TR- 11-01, January 4, 2011.

[13]. P.C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," J. Computer Security, vol. 19, no. 4, pp. 669-702, 2011.

[14]. P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.

[15]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[16]. T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[17]. T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[18]. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[19]. W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004