Securing Web Accounts Using Graphical Password Authentication through Watermarking

Vinit Khetani[1]
[1]Ramdeobaba College Of Engineering, India,
Anuja Bongirwar[3]
[3]Yeshwantrao Chavhan College of Engineering, India
Jennifer Nicholas[2]
[2]Yeshwantrao Chavhan College of Engineering, India
Abhay Yeole[4]
[4]Yeshwantrao Chavhan College of Engineering, India

***ABSTRACT**: Today, most Internet applications still establish user authentication with traditional text based passwords. Designing a secure as well as a user-friendly password-based method has been on the agenda of security researchers for a long time. On one hand, there are password manager programs which facilitate generating site-specific strong passwords from a single user password to eliminate the memory burden due to multiple passwords. On the other hand, there are studies exploring the viability of graphical passwords as a more secure and user-friendly alternative.*

In this project, we propose a new graphical password scheme for accessing web accounts called "Secure Web Account Access through Recognition Based Graphical Password by Watermarking". Here user selects number of images as a password and while login user needs to enter the random code generated below each image, which has been set as a password. Here the security of the system is very high and every time user needs to enter different set of code for authentication i.e. every time new password gets generated making Dictionary attacks, Brute Force attack, and other attacks infeasible.

***Keyword:** Graphical Passwords, Authentication, Web Access through Graphical Password, Secure Web Access, Graphical User Authentication, Watermarking.*

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken.

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics, have been used.

In this project, however, we have focus on another alternative: using pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be

remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

II. BACKGROUND STUDY

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted.

The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories:

- Recognition-based graphical techniques
- Recall-based graphical techniques

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

III. EXISTING SYSTEM

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre-selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

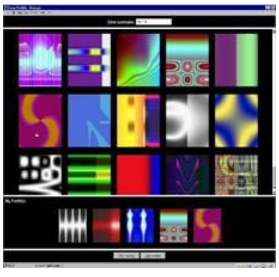

Fig 1: Random images used by Dhamija and Perrig

Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times.

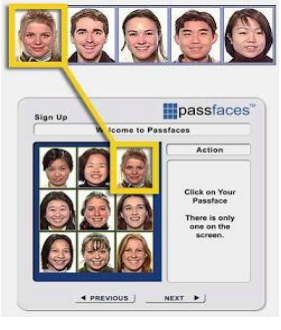

Fig 2: Example of Passfaces

Jermyn [3], proposed a new technique called "Draw- a-Secret" (DAS) as shown in figure 3 where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.

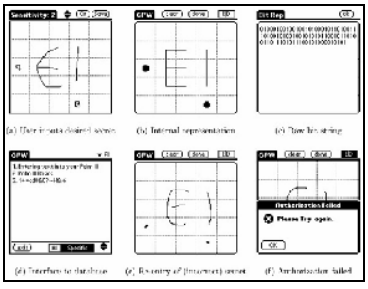

Fig 3: DAS technique by Jermyn

Haichang's [4] proposed a new shoulder-surfing resistant scheme as shown in figure 4 where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

Fig 4: Haichang's shoulder-surfing technique

IV. ATTACKS ON PASSWORD

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

a) Brute force search

The main defence against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

b) Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area.

Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

c) Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passfaces technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe's study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

d) Spyware

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

e) Shoulder surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall

based techniques are considered should-surfing resistant.

f) Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

V. WATERMARKING

Watermarking is a process of embedding a type of mark in a multimedia object i.e. images. It is similar to adding the owner's signature to the multimedia object. Much content providers use watermarking as a form of copyright protection, authenticating content, detecting unlawful editing, etc. on their multimedia objects or digital contents. The embedding process uses a secret key that determines the location of the watermark will be placed in the multimedia object or, in this case, images [6-7].

Watermarked multimedia objects are still vulnerable to attacks because digital contents can be digitally edited. They can be intentionally edited like cropping, or unintentional like gamma correction, compression or low pass filtering. This is why watermarks must be robust well designed to avoid these kinds of attacks. Whenever the content owners suspects possible occurrence of an attack, they can use the same secret key during the embedding process to check. This key can extract the watermark sequence from the embed image. If the embedded watermark and the extracted watermark do not resemble each other, then there is a possibility that the object has been attacked [8].

Therefore, to validate any image with the watermark, we can either compare the original copy with the other image (non-blinding watermarking) or use a correlation measure to detect the watermark strength of the extracted watermark (blind watermarking). The correlation measure compares the extracted with the original watermark and a statistic of the correlation process is produce to ensure the existence of the watermark [6, 8].

VI. PROPOSED ALGORITHM.

Referring to the previous section where we selected recognition out of the three categories in graphical password techniques and afterwards select the watermarking copyright technique as the proposed algorithm for image gallery security. Now we will explain the steps involved during registration and login section using this proposed algorithm.

A. Registration phase

The diagram below shows the registration phase of the algorithm. The image matrix contains the password. User can select some images from the matrix as password by entering the code the corresponding image and submit to the system, for example, in the image below (Figure 5) user select selects two images as the password. But in this method the user can add own images also, but that images should be processed through the watermarking technique and put the copyright protection in the user's images.

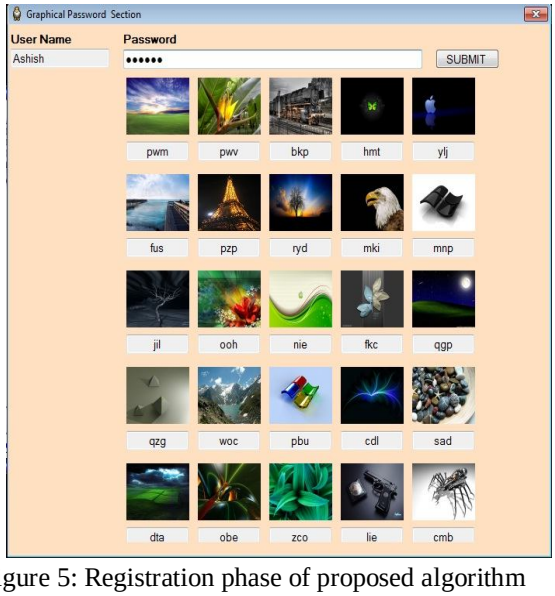

Figure 5: Registration phase of proposed algorithm

Once the user selects the preferred password, the users string will be generate. For example, a user selects two images as the preferred password with corresponding code below the image as 'mnp' & 'pbu' and these images has a watermarked code embed in the images as 1050 and 7528. Now as soon as the user enters the code in the form 'mnppbu' and click on submit button, the

algorithm will first split the password string into a string of 3 characters and will store the string in a list. Now it will check for the image on the image matrix having corresponding code as 'mnp'. Once it finds the exact match of the image, it will extract the watermarked code from the image i.e., 1050 and will store the user ID and the extracted code into the database. Same steps will be repeated for the next string also and thus completing the registration process.
The workflow of registration phase is as below:
Step1: User clicks on registration button.
Step2: In registration page, the user has to enter User ID and Select the password.
Step3: User selects the password image by entering the corresponding code generated below the image.
Step4: Algorithm checks for the match of code entered by the user and its corresponding image.
Step5: Extract the watermarked code from the image.
Step6: Store the watermarked code and the User ID into the Database.

B. Login phase

In the login section, the user first enters his username. The image matrix will be displayed which will contain same images as we had in the registration form but the position of the images will be different. Again each image will have some random characters below it. The user should recognise his password images and then enter the text corresponding to his password image in the password textbox. Now Algorithm will again split the string into sub strings of 3 characters each. Here the algorithm will then find the related images of the entered characters from the login matrix. After finding the images associated with entered characters, algorithm will extracts the watermarked data from the and checks the data with the user information in database and if the information are the same then user can login to the system, otherwise, the user need to try again. Fig 6 shows the login form.

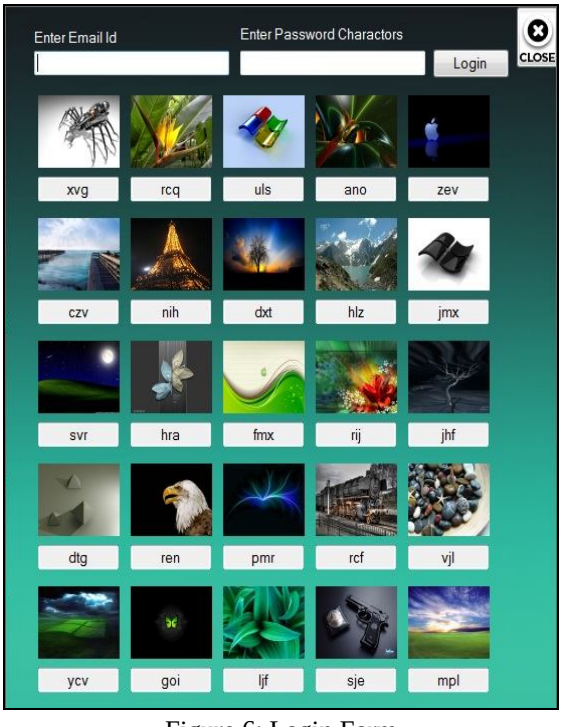

Figure 6: Login Form

The workflow of Login phase is as below:
Step1: User clicks on Login button.
Step2: In Login page, the user has to enter User ID and enter the password.
Step3: User enters the password by entering the code generated below the password image.
Step4: Algorithm checks for the match of code entered by the user and its corresponding image.
Step5: Extract the watermarked code from the image.
Step6: Checks weather the code extracted from the image selected by the user belongs to the User.
Step7: If yes, user gets Login else needs to enter the password again.

C. Account Lock-Out

If an unauthorised user attempts to login into an account and enters incorrect password for 3 times then the account will be locked out. Not only this, if the computer has a webcam, it will take a snap of the intruder.

D. Account Recovery

In the account recovery section, genuine user needs to enter the registered email ID. User will receive an OTP (one time password) on the mail. To activate the account user need to enter this code in the verification

section. Now after the account gets activated genuine user can see the snap of intruder.

E. Secure Web Account Access

This is the module, for which we have proposed the authentication system, i.e., to provide secure access to the web accounts such as Gmail, Facebook, etc. For this, user needs to enter the authentication credentials of the web accounts to be secured as shown in Fig. 6.

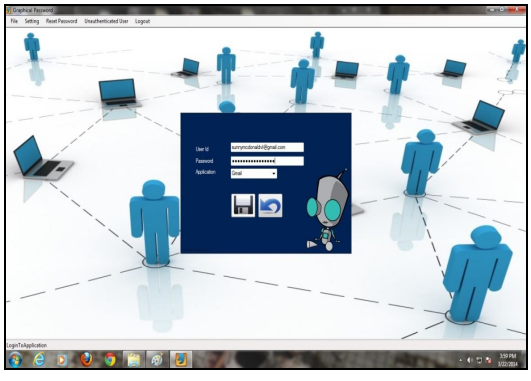

Figure 6: Storing Credentials

Then for accessing the account user just needs to click on the Web Account to be accessed. The application will directly open the web account by passing the authentication credentials as shown in Fig 7 & Fig 8. It will prevent the web account from Phishing and Keylogger kind of attack.

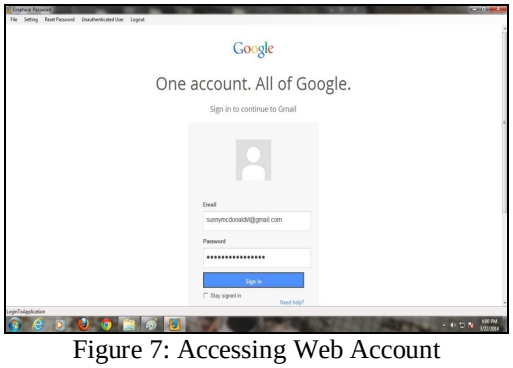

Figure 7: Accessing Web Account

VII. CONCLUSION

In information security, user authentication is the most critical of all the elements. Researches made between 1996 to 2011 has shown that people tend to remember combinations of geometrical shapes, patterns, colours and textures better than alphanumeric characters that are meaningless to the user. This proves that graphical password is a more desirable alternative to alphanumerical passwords. In this paper in the beginning, we presented the recognition based algorithm type of graphical password. Since there is no proper evaluation framework for GUA algorithms until now, we focus on attacks of graphical password algorithms and evaluate all recognition based algorithms. Then, after explaining the watermarking techniques and schemas, this is a new graphical password algorithm that uses watermarking techniques and random character set to provide stronger security against Password Cracking attacks and shoulder surfing attack. Finally, we evaluated this proposed algorithm and its working for securing the web account access.

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] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing"
[5] Kumar, M., et al., Reducing Shoulder-surfing by Using Gaze-based Password Entry, in Symposium On Usable Privacy and Security (SOUPS). 2007: Pittsburgh, PA, USA.
[6] Zheng-ding, L.T.Q., *The Survey of Digital Watermarkingbased Image Authentication Techniques*, in *IEEE, ICSPOP Proceedings*. 2002.
[7] Zheng, D., Y. Liu, and J. Zhao, *A Survey of RST Invariant Image Watermarking Algorithms*, in *IEEE CCECE/CCGEI, Ottawa, May*. 2006.
[8] Luis P´erez-Freire, P.C.n., Juan Ram´on Troncoso-Pastoriza, and Fernando P´erez-Gonz´ale, *Watermarking Security: A Survey*. Springer-Verlag Berlin Heidelberg, 2006.
[9] Gao, H., et al., Analysis and Evaluation of the ColorLogin Graphical Password Scheme, in Fifth International Conference on Image and Graphics(ICIG). 2009, IEEE. p. 722 - 727
[10] Lashkari, A.H., et al., Shoulder Surfing attack in graphical password authentication. International Journal of Computer Science and Information Security, 2009. 6(9).
[11] Biddle, R., S. Chiasson, and P.C.v. Oorschot, Graphical Passwords: Learning from the First Generation. 2009: Ottawa, Canada.
[12] Dunphy, P., J. Nicholson, and P. Olivier, Securing Passfaces for Description. 2008.
[13] Sandouka, H., A. Cullen, and I. Mann, Social Engineering Detection using Neural Networks, in 2009 International Conference on CyberWorlds 2009, IEEE.
[14] al, A.A.G.e., Network Attacks, in Network Intrusion Detection and Prevention: Concepts and Techniques, Springer Science, Business Media.