International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

# A SHOULDER-SURFING RESISTANT GRAPHICAL PASSWORD SYSTEM

**Aditya Mishra[1], Rahul Jadhav[2], Shubham Patil [3]**

[1,2,3] *Student, B.E., Department of Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering & Technology, Karjat, Maharashtra, India.*

---

**Abstract -** *In order to access & help secure the system, Graphical password is an essential credential. Graphical password is a kind of a password which is an alternative mechanism to textual password in order to access the system. It is more secure than the textual password but vulnerable to shoulder-surfing attack. In this project, we have developed a system a system which is resistant against shoulder-surfing attack by using a falsification method. Hence it will confuse the hacker to capture & misuse the password.*

***Key Words***: **Graphical Password, Registration, Authentication, Shoulder-surfing attack, Falsification.**

## 1. INTRODUCTION

Authentication is the first security mechanism that can be used to prevent unauthorized access to the system. In addition, textual password (text-based password) is the most famous authentication mechanism which has been used for several years. In this authentication method, a user selects a combination of characters as his password, which is required to memorize by him. However, in order to have a secure password, the generated password must follow several requirements such as minimum 8 characters, a combination of capital and small characters, alphanumeric, using special characters, ... etc. Thus, this makes the password to be complex (e.g. "@bu*%183bDIK), which also makes difficulties for a hacker to guess (dictionary attack) or break (brute force attack) it. Similarly, the generated complex password provides this challenge for the users to memorize it for further access. Thus, the users tend to pen down their long and random passwords somewhere or take the easy passwords instead. Graphical password is an alternative authentication password which can solve the problem of remembering the complex passwords in textual password approach. In this case, several images are used to represent a user password, rather than the text. Later on, upon login to the system, a user can select or produce the same graphic image correctly for accessing to the system. Since remembering the image is easier than the text, the selected images as the password is complex as well as easy to remember by the user at the same time. Additionally, the other advantage of graphical password is to prevent stealing the passwords if a keystroke logger such as malicious software (Trojan) is installed by a hacker in order to capture the text-based passwords. In general, there are three graphical password approaches such as recognition-based, pure recall-based and cued recall based. In the recognition-based approach, the user can pick several images such as icons or symbols which he recently selected in user registration step. During the authentication process, the user is required to recognize their registration choice among a set of candidates. In the second approach, pure recall-based, the user must produce his graphical password, which he generated in registration. In this case, unlike the previous approach, the user needs to reproduce his password without any given reminder such as drawing a particular shape.

In contrast, in cued recall-based, several specific locations within an image can be selected as the graphical password. Although the graphical password method is beneficial, but shoulder-surfing attack is the main concerns in this authentication mechanism. Shoulder-surfing attack is referred to capturing the password by direct watching or recording the user's authentication session while selecting or producing the images as the password. In this project, a recognition-based graphical password technique based on the false image which is resistance to shoulder-surfing attack is suggested. In this way, the false image within the authentication step can confuse a hacker who tries to capture the password using shoulder-surfing attack.

## 2. LITERATURE REVIEW

Authentication is the first security mechanism that can be used to prevent unauthorized access to the system. In addition, textual password (text-based password) is the most famous authentication mechanism which has been used for several years.

B. Malek, M: Orozco, and A. EI Saddik, "Novel shoulder-surfing resistant haptic-based graphical password," in Proc. Euro Haptics 2006 [2]. I.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang, "Shoulder-surfing proof graphical password authentication scheme," International journal of information security, vol. 13, pp. 245-254,2014. [3].

Our System Proposal that is Graphical Password overcomes the drawbacks of textual password. Graphical password systems can be classified as either recognition-based, cued recall-based or pure recall-based. Recognition involves 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.

On contrast, pure recall is retrieval without external cues to aid memory. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage, for example, remembering a textual password that one has not written

down. Pure recall is a harder memory task than recognition. Between pure recall and pure recognition there is a different form of recollection: cued recall. An example of cued recall within graphical password systems is scanning an image to find previously chosen locations in it. Viewing the image cues the user about the locations.

This is easier than having to recall something entirely from memory (i.e. free recall), but harder than simply recognizing whether a particular image has been seen before or not (i.e. recognition).

## 3. EXISTING SYSTEM

Like other authentication methods, the graphical password consisted of two steps, registration and authentication. In the registration step, users select some images from different categories or produce a graphical image as his password. Later on, in the authentication step, he needs to select the correct images or re-draw the graphical password which is used by him in the registration step. In the following, these two steps are explained in detail.

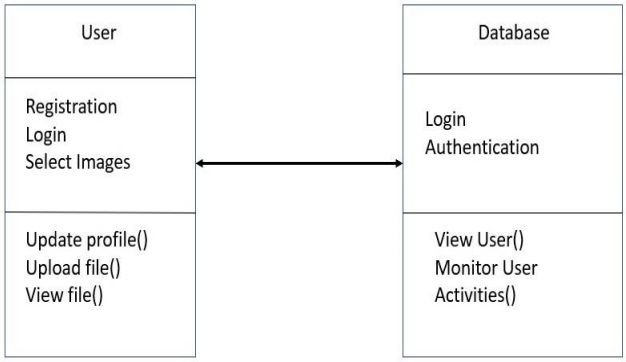


**Fig -1**: Class diagram of the process

### 3.1 REGISTRATION

Since registration is the first step, each user needs to input his full name, email address and username. In addition, he requires to select minimum 5 and maximum 8 image categories from giving options. After the information is submitted to the database, selecting graphical password process will start. In this case, a user can select one image from each category per page, depends on the length of his password (minimum 5 and maximum 8 pages) but this selection must be done by typing the alphanumeric character, which is attached to each image. In addition, the alphanumeric characters which belong to each image and the position of images in each category are selected to be randomized. This can make the proposed method to be robust against key logger as well as shoulder surfing attack at the same time. Similarly, selecting one image from each category will be continued till the last category. Hence, a sequence of images as a graphical password will store in the database. The registration flowchart is shown in figure.

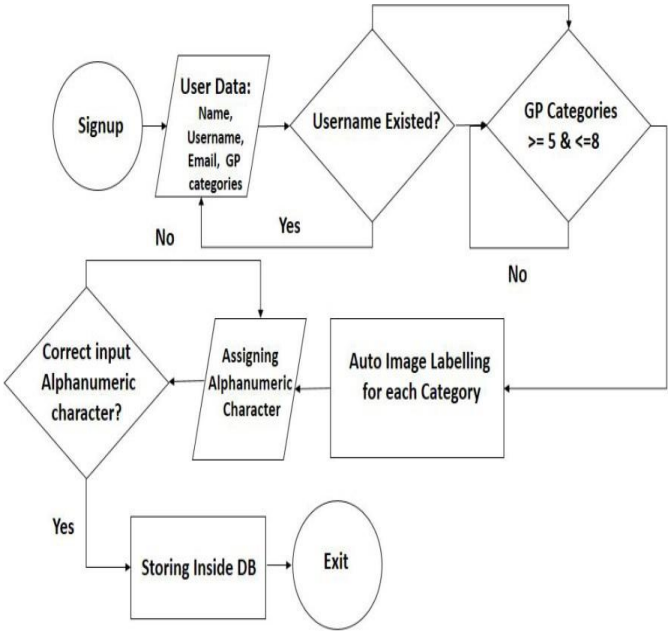


**Fig -2**: Registration Flowchart

### 3.2 AUTHENTICATION

In the authentication (login) page, a user needs to provide the correct username first. Afterward, the system will retrieve the image categories which selected by the user in the registration step. Since the process of selecting images as a password is similar to the registration step, the user will type the alphanumeric character, which is attached to each image.

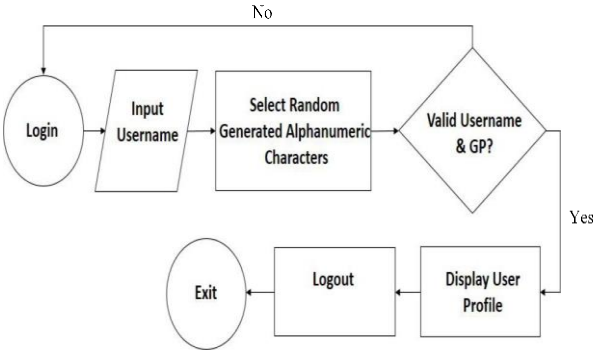


**Fig -3**: Authentiation Flowchart

## 4. PROPOSED SYSTEM

Like existing system our proposed system also consist of two steps that is first is registration and then is authentication.

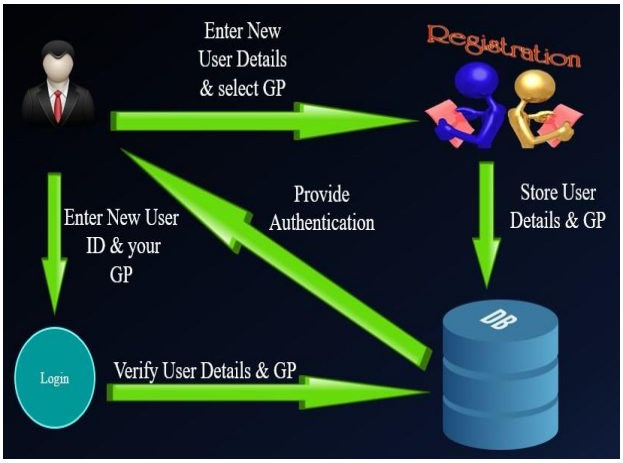


**Fig -4**: System Architecture

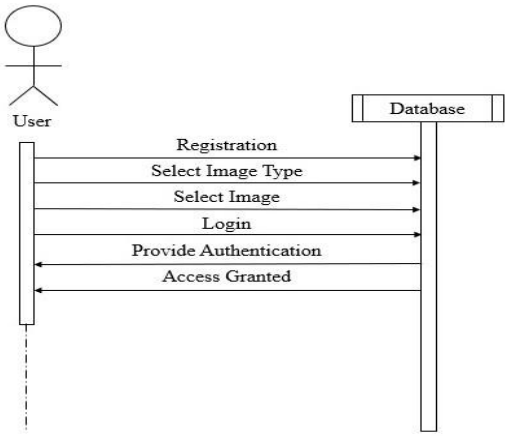


**Fig -5**: Sequence diagram of the process

### 4.1 REGISTRATION

The registration step is as same which is explained in existing system without any change. That is in registration step users select some images from different categories or produce a graphical image as his password. In which users select images from a category of 5 or 8 image categories from the options. After the information is submitted to the database, selecting graphical password process will start.


**Fig -6**: Typing image from the football (desired) category.

### 4.2 AUTHENTICATION

In our proposed system in order to provide more security to the existing authentication methods, in each page where all images within each category are shown, the false image (not my password) is added automatically. This image can be replaced with one of the images in each category. Since the user is aware of the selected image in each category, if the known image is available, he can pick out the correct image, otherwise, he takes the false image. In order to make the process to be more complex for the attacker, a random category will be added between selected categories. In this example, since the pet category was not selected by the user as part of his password in the registration step, he must select the false image to ignore this category. However, this category can be considered as the real image category by an attacker who watches the user authentication process, since the user selected an image from this category. After the graphical password will be validated, then the system will automatically direct the user to the appropriate web page (user profile). To this end, it can prevent shoulder-surfing attack by pretending that the selected image (false image) is one of the images that user selected as his password.

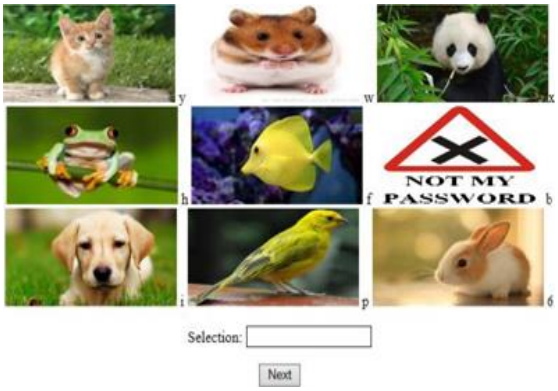


**Fig -7**: Typing false image as a password from random category

## 5. PROBLEM DEFINITION

Graphical passwords introduce us to a whole new form of authentication. The most common form of authentication used today is the used of alphanumeric texts and this form of authentication has been proven to be prone to several forms of attacks such as guessing, social engineering, spywares, dictionary attacks, shoulder surfing and even hidden cameras. It can be frustrating to keep up with all the passwords since it is not a recommended that someone uses one password for more than one account or computer program or device.

One of the main problems graphical passwords tend to solve is the problem of a user using a weak password so that he/she won't forget it and at times when users are encouraged to use strong passwords, they tend to use it for all their accounts and also users keep their passwords where

attackers can access because of the fact that they don't want to memorize it. Since it is easier to remember pictures than text, graphical passwords tend to enhance security and at the same time make it easier for the user to use.

This report focuses on graphical password authentication and the different forms commonly used today. It also highlights the advantages graphical passwords have over text based passwords and the forms of attack you can be prone to while using graphical passwords. Because of increasing threats to computer systems, there is great need for security requirements. Security practitioners and researchers have made studies in protecting systems, individual users and digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem, and the system user was not factored into the equation. Users interact with security technologies either passively or actively. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions and usability solutions such as: ease of use, memorability, usability, efficiency, effectiveness and satisfaction.

Nowadays there is an increasing recognition that security problems are also fundamentally human-computer interaction issues (Dourish, P 2004 and Patrick et al 2004). Authentication is the process of determining whether a user should be allowed access to a particular system or resource. Conventional passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost.

As a result, passwords are still dominant and are expected to continue toremain so for some time as an authentication process (Coventry et al 2003, Jain et al 2000 and Brostoff et al 2000).

Conventional passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit Brown et al. 2004, Dhamija et al 2000, Feldmeier et al. 1990, Klein et al 1990, Morris et al.1979 and Sasse et al. 2001). The "password problem," as formulated by Birget (2005), arises because passwords are expected to comply with two conflicting requirements, which is passwords should be usable and ease to remember, and the user authentication protocol should be executable quickly and easily by humans and passwords should be also secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

## 6. SECURITY MEASURES


**Fig -8**: Falsification

Security is an essential concept to any system being developed. It certainly keeps unauthorized users or else hackers from maliciously exploiting the system.

Likewise, in our project we have taken a measure to protect our system. As described earlier we have introduced a method called as falsification to prevent shoulder-surfing attacks. Falsification is nothing but adding a false image in the authentication step in order to confuse the hacker. This image can be replaced with one of the images in each category. Since the user is aware of the selected image in each category, if the known image is available, he can pick out the correct image, otherwise, he takes the false image. In order to make the process to be more complex for the attacker, a random category will be added between selected categories.

In the above example, since the basketball team category was not selected by the user as part of his password in the registration step, he must select the false image to ignore this category. However, this category can be considered as the real image category by an attacker who watches the user authentication process, since the user selected an image from this category.

After that the password will be validated and user will be directed to the desired page. This will prevent shoulder-surfing attack since the false image selected by the user is not the actual password and in turn will confuse the hacker.

## 7. CONCLUSIONS

The graphical password is an alternative authentication system, which can be based on a selection of graphical images as the password to access to the system. It has been developed to make the passwords to be more memorable and secure.

In this project, a suggested graphical password method is similar to the Pass Faces approach but it provides this opportunity to remember the images. Since a grid of 9

human faces, for example, is used in Pass Faces approach, this may confuse the user to remember the selected faces in the registration step. In contrast, since the user needs to remember his favourite categories such as football team or car and also each image within each category, the suggested graphical password is simple in term of remembering the images. In addition, this approach can increase the security of the system since the alphabet, the image, as well as the category sequence are randomizing every single time that the user requires to login to the system. Additionally, the alphanumeric character which are located close to each image in 9 grids are typed by user instead of using mouse to select the graphical password. Moreover, a false image can be useful in order to make the authentication to be more complex for the attacker.

## ACKNOWLEDGEMENT

I take the privilege to express my sincere thanks to Prof. P.A. Ghonge, Principal, Y.T.I.E.T, Bhivpuri road and Prof. Vaishali Londhe, Head, Department of Computer Engineering, Yadavrav Tasgaonkar College of Engineering, for providing the much-needed support.

I wish to express my wholehearted appreciation and deep sense of heartfelt gratitude to my guide Prof. Nilima D. Nikam, Professor, Department of Computer Engineering, Yadavrav Tasgaonkar College of Engineering for his generous help, excellent guidance, lucid suggestions and encouragement throughout the course of this work. His concrete directions and critical views have greatly helped me in successful completion of this work.

I am also thankful to all those who helped directly or indirectly in the completion of this work.

## REFERENCES

[1] Andrew Lim Chee Yeung*, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal, Vahab Iranmanesh* (Department of Computing and Information Systems Faculty of Science and Technology Sunway University Bandar Sunway, Malaysia, 2015).

[2] B. Malek, M: Orozco, and A. EI Saddik, "Novel shoulder-surfing resistant haptic-based graphical password," in Proc. Euro Haptics 2006.

[3] I.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang, "Shoulder-surfing proof graphical password authentication scheme," International journal of information security, vol. 13, pp. 245-254,2014.

[4] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in Proceedings of the Seventh Symposium on Usable Privacy and Security, 2011, p. 6.

[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, 2006, pp. 177-184.