RESEARCH ARTICLE OPEN ACCESS

Graphical password authentication using Pass faces

Ms Grinal Tuscano*, Aakriti Tulasyan**, Akshata Shetty**, Malvina Rumao**, Aishwarya Shetty **

*(Department of Information Technology, Mumbai University, St. Francis Institute of Technology, Mumbai-103)

**(Department of Information Technology, Mumbai University, St. Francis Institute of Technology, Mumbai-103)

** (Department of Information Technology, Mumbai University, St. Francis Institute of Technology, Mumbai-103)

** (Department of Information Technology, Mumbai University, St. Francis Institute of Technology, Mumbai-103)

** (Department of Information Technology, Mumbai University, St. Francis Institute of Technology, Mumbai-103)

ABSTRACT
Authentication is one of the most important security primitive. Alphanumeric password authentication is most widely used authentication mechanism. This mechanism has been shown to have several drawbacks and is prone to various attacks such as brute force attack, shoulder surfing attack, dictionary attack. Thus to overcome the drawbacks of alphanumeric passwords, we propose Graphical passwords as an alternative to alphanumeric passwords. This is because humans tend to remember visuals better than text. This paper attempts to highlight the existing graphical Passface system, its usability features and then develop a new graphical password system that combines both graphic and texts passwords to fortify the authentication process on desktop systems.

Keywords – Security, Authentication, Graphical Password, Passfaces, Distortion.

I. INTRODUCTION

Password authentication is degrading as an authentication mechanism due to lack of memorability and security. In user authentication the process which we have to pass through is username and password. Most of the application provides knowledge based authentication which include alphanumeric password as well as graphical password. Generally, password systems are faced by problem of conflicting requirements. First is the fact that passwords should be usable and easy to remember. The second requirement is for it to be secure. In today's changing world when we are having number of networks and personal account some sort of easy authentication schema need to be provided. To combat the various security inadequacies, graphical password systems have been proposed as a possible alternative to text-based passwords, motivated particularly by the fact that humans can remember pictures better than text. Pictures are generally easier to be remembered or recognized than text [5], especially photos, which are even easier to be remembered than random pictures. Although the existing Passface method covers many usability features like easy to use, easy to memorize, easy to recognize and easy to understand [2], but there are several drawbacks with this algorithm. When a password is selected by mouse, it is very easy for the shoulder surfer attacker to observe the password. Also another research shows users tend to select faces of their own race which cause the algorithm to be guessable by attacker [5]. The aim of this study is to increase the security of Passface algorithm by creating resistance to shoulder surfing attack.

1. LITERATURE REVIEW

There are three types of user authentication: Token based, Biometric based and Knowledge based authentication, knowledge-based techniques are currently the most frequently used method for user authentication which includes text and image passwords [6]. The picture-based techniques can be further divided into two categories: recognition-based and 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 [1]. The traditional and most common authentication method employs usernames and passwords composed of alphanumeric text. This method has proven to be insecure in practice [3]. Some drawbacks of alphanumeric text

password are like forgetting the password, choosing a weak password, password stolen, etc. Moreover, alphanumeric passwords are vulnerable to shoulder surfing attack, spy ware attack and social engineering attack etc [5].

1. Shoulder surfing attack

Shoulder surfing attack refers to looking over someone's shoulder in order to obtain information such as password, PIN and other sensitive information. It is effective if the attacker can observe what the user keys in, clicks or touches. Graphical authentication is generally more vulnerable to shoulder surfing attacks than text-based passwords. Due to this reason, only a few graphical authentication methods are designed to resist shoulder surfing attack.

2. Brute force attacks

It is a simplest attack form for an authentication system where, the attacker tries to guess the correct password.

Brute force attacks have two subtypes: *Dictionary Attacks:* Here the attacker uses a dictionary of common text or graphical passwords. In the text-based password, dictionary attack creates a dictionary of memorable words such as birthdates, favorite foods, pet names, or person names as potential passwords.

Guessing Attacks: The attacker here tries possible passwords related to the user. Such as, birth date, English name, phone number, combination of two elements etc. To defend against brute force attacks the system should have a sufficiently large password space to make it impractical.

3. Spyware

There are several types of spyware including hijackers, key loggers etc. Spyware collects information entered by the user. With graphical passwords, it is more difficult to conduct spyware based attacks because it is harder to copy mouse motions exactly. Combinations of Passfaces and text may be especially resistant to spyware.

A graphical based password is one promising alternatives of textual passwords. The motivation for graphical authentication is that people remember images better than text [3]. Pass face algorithm was created in 2000, with the idea of using pictures of human faces in order to validate the identity of user [7]. 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 [1]. Because of these (presumed) advantages, there is a growing interest in graphical password.

2. PREVIOUS WORK

In conventional Graphical Password Authentication, 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. 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 [4]. The technique is based on the assumption that people can recall human faces easier than other pictures [1]. A potential drawback of this system is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Also it is easily predictable since people tend to choose images that are more attractive.

Security Features of Graphical Passwords:

Different graphical password schemes have different techniques to reduce the effectiveness of known attacks [8]. It is considered good practice to have security features in authentication to favor better security over usability. However, building a balance between usability and security can be difficult. It might be a particular graphical password technique has higher usability but less security or higher security with low usability. For example increasing the picture library would provide a larger password space, but leads to longer login time due to crowdedness during authentication. Combining several security features should increase the security level. For instance, implementing decoys, randomly assigned, and random characters could make it harder for the observer to obtain login session during shoulder surfing activity surfing [6]. In addition the location of the images can be randomized and not the same for every authentication phase. Limited login attempts block user access to the login page after several unsuccessful login attempts.

3. PURPOSE

The proposed mechanism focuses on providing more powerful secure authentication mechanism. System goes through several phases before creating a password and while logging into the system such as image selection, image distortion, text association and finally password generation. At the time of login, one correct image from a 3X3 grid is identified. Grid shows up one correct image and eight decoy faces and shuffles faces for every attempt. Only upon identifying correct image and entering text associated with it, user gets access to the system.

Security Features of Graphical Passwords:

Different graphical password schemes have different techniques to reduce the effectiveness of known attacks [8]. It is considered good practice to have security features in authentication to favor better security over usability. However, building a balance between usability and security can be difficult. It might be a particular graphical password technique has higher usability but less security or higher security with low usability. For example increasing the picture library would provide a larger password space, but leads to longer login time due to crowdedness during authentication. Combining several security features should increase the security level. For instance, implementing decoys, randomly assigned, and random characters could make it harder for the observer to obtain login session during shoulder surfing activity surfing [6]. In addition the location of the images can be randomized and not the same for every authentication phase. Limited login attempts block user access to the login page after several unsuccessful login attempts.

II. SYSTEM DESCRIPTION:

1. DESIGN:

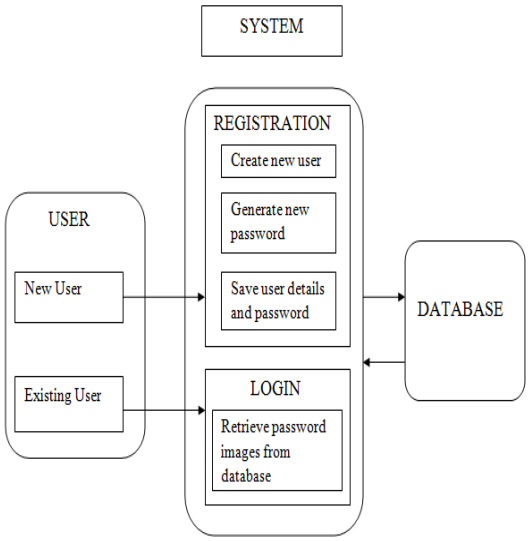


Fig. 1.Architectural Diagram of the proposed solution

2. DESCRIPTION:

In Password creation phase, user is given two options; user can either provide images of their choice or can select images from system database. In either of the choice user is required to provide three images.

System uses distortion technique in Distortion phase to distort received or the provided images. This distortion of images is carried out by using filters. System then displays both the distorted and original images to the user; so that it is easier for user to mentally associate the distorted images. User is also required to enter some random text for each of these images. Both original and distorted images along with the text are saved or preserved in database.

During Authentication phase, only valid user is or will be granted access to the system. The system will ask the user to identify one out of three user entered images from the grid containing one correct image and 8 decoy faces and also entering the associated text. User gets only two attempts to identify correct images from the grid and to enter the associated text of the image. The system shuffles the images in the grid every time the user logs in to the system.

3. WORKING:

The system requires the user to start the Graphical Password Authentication application. System goes through Registration phase, Password Creation phase and Authentication phase.

In Registration phase, user selects 'Register' option from displayed Homepage. He can register to the system by proving required details. Entered details will then be validated and user name will be verified against availability.

In Password creation phase, three images provided by user are distorted using distortion technique. The original and distorted images along with the text are then saved or preserved in database.

During log-in phase, user gives username. Valid users are shown grid of distorted images. The user then has to identify the correct distorted image and then enter the text associated with that image .This procedure is carried out 3 times and on entering the correct data user gets access to the system. User gets exactly three attempts to enter correct username and password into the system.

III. USER INTERFACE DESIGN:

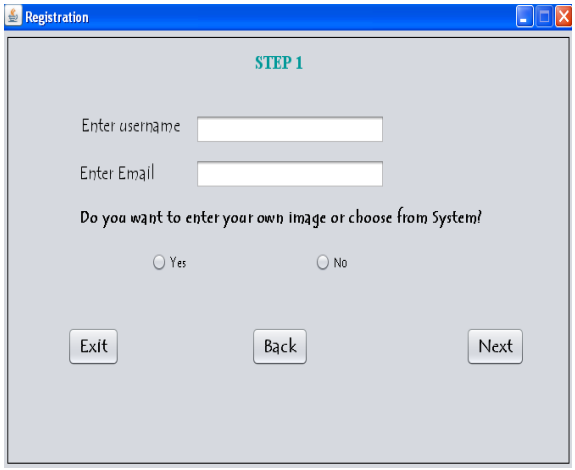


Fig .2.Interface Design for Registration Screen

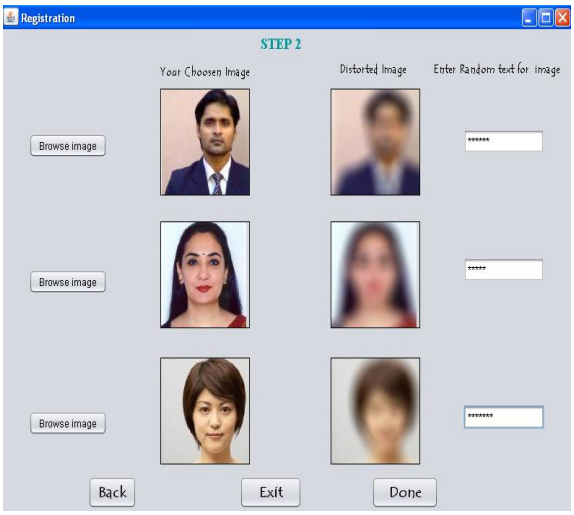
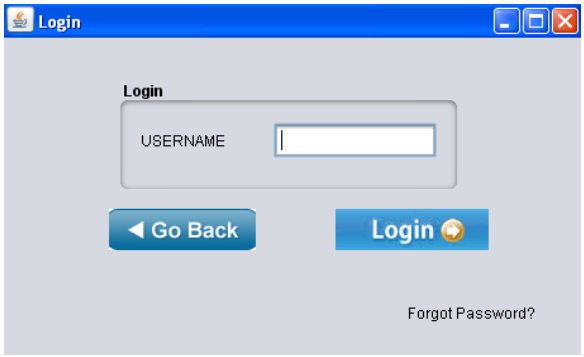


Fig. 3.Interface Design of the original Image with the distorted Image



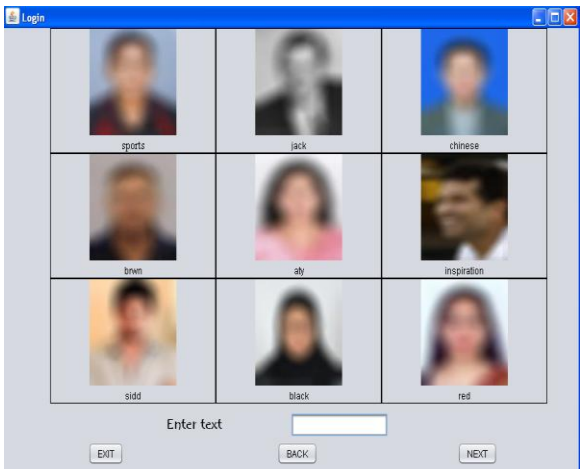


Fig .4.Interface Design for Password Login

IV. CONCLUSION

There is a growing interest in using pictures as passwords instead of alphanumeric passwords. The main reason for using Graphical passwords is they can be easily recalled. In this paper, we have proposed two step graphical password authentication system which is based on Passfaces. In order to make our system user friendly and at the same time difficult to crack ,we have combined images along with text .The original images taken by the user are vulnerable to individualized educated guess attacks if users have a good amount of information about the users. Moreover, even in the case when the attacker does not have any information about the users, the attackers can make better guesses than random guesses based on contextual information of the original photos .In contrast, when distorted photos are used as authentication images, attackers cannot make better guesses than random guesses even with good amount of knowledge about the target users. The Distortion Technique can mitigate the risk of the collective educated guess attacks using the Biases in users' choices of authentication images. Currently, we are working on the System Evaluation and hope our paper can prompt research in new techniques to improve security systems.

Acknowledgements

We hereby take the privilege to present our project report on "**Graphical Authentication of passwords using Passfaces**". We are very grateful to our Project Supervisor **Ms. Grinal Tuscano** for contributing her valuable moments in the Project from her busy and hectic schedule right from the Project's inception. Being after us like a true mentor and a great academic parent.

We are very thankful to Ms. Grinal Tuscano whose guidance and support was an immense motivation for us to carry on with our Project. She has been a constant source of inspiration to us. Her suggestions have greatly contributed for the betterment of our project.

Our special thanks to the Head of Department Mr. **Pramod Shanbhag**, staff members and lab assistants for their co-operation.

REFERENCES

[1] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen ,"*Graphical Passwords: A Survey*", Department of Computer Science,Georgia State University,Dec-2005,IEEE

[2] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "*Graphical Password Authentication"-Cloud securing scheme*," IEEE 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[3] Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee ,"*Security in Graphical Authentication*", International Journal of Security and Its Applications Vol. 7,No. 3, May, 2013

[4] Gaurav A.,Saurabh S.,Ajay I., "*Analysis of Knowledge Based graphical password authentication*" IEEE 2011 International

Conference on Computer Science and education.

[5] Sacha Brostoff & M. Angela Sasse "*Are Passfaces More Usable Than Passwords? A Field Trial Investigation*",Department of Computer Science, University College London

[6] Ayannuga Olanrewaju O., Folorunso Olusegun, "*Graphical-text Authentication of a window-based application*", 2011 International Journal of Computer Applications.

[7] Farnaz Towhidi, Maslin Masrom, Azizah Abdul Manaf, "*An Enhancement on Passface Graphical Password Authentication*", Journal of Basic and Applied Scientific Research 2013.

[8] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig," *Use your illusion: secure authentication usable anywhere*", In Proceedings of Usable privacy and security, Aug.2008.