FacePattern: A New Technique for better Graphical Password

Swapnil B. Rasal[1], Gaurav S. Pawar[2], Varun D. Patel[3], Vaibhav T. Jadhav[4], Prof. R. B. Nangare[5]

[1,2,3,4] *BE Student, Computer Engineering Department, SVIT, Chincholi, Nashik, India.*
[5] *Professor, Computer Engineering Department, SVIT, Chincholi, Nashik, India.*

ABSTRACT

This concept commencing of user producing of passwords without system being providing of hints to produce passwords, the examples of pure recall technique are Draw-A-Secret technique, Grid selection, and Passdoodle. Here, we discuss two types of picture password techniques: reproducing a drawing and repeating a selection Jermyn, et al. proposed a technique, called "Draw-a-secret (DAS)", which allows the user to draw their matchless password. A user is asked to draw a simple picture on a 2D grid using a stylus or mouse. A drawing can consist of one nonstop pen stroke or preferably several strokes separated by \pen-ups" that restart the next stroke in a different cell. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is requested to re-draw the image. If the drawing touches the same grids in the same sequence, then the user is authenticated. In this type of system the brute-force attack is possible and the impact of password length and stroke-count as a complexity property of the DAS scheme. Recall-based graphical password systems are occasionally referred to as draw metric systems because users recall and reproduce a secret drawing.

Keyword : - *Graphical Password, Input, Live Video, Observation, User Study.*

1. INTRODUCTION

FacePattern is a small system that can be easily transferred from computer to computer by a simple USB stick. Its purpose is to solve a problem that really bothers many people today when they have to choose from memorizing a lot of passwords to be secure or to use every time the same one so they won't forget it but risk be found out by others. So it provides you a very secure, encrypted database where you can keep inside all your passwords, usernames, email accounts, URLs, notes without any risk for others to find them. That is because FacePattern can lock every database with only one Master Password and/or key file. There are no duplicates, anywhere in your computer, of this Master Password and/or key file so in case of lost database cannot be opened by anyone. Not even by you and that is because there is no recovery password or back door. FacePattern beside security also provides you with several functionalities in order to keep your database organized and up to date.

2. OBJECTIVES

This document includes software requirements for FacePattern, release number 1.10. FacePattern is an OSI Certified Open Source Software distributed under the terms of the GNU General Public License Version 2 or under. The system gives resolution to memorizing passwords problem. Its purpose is to keep all of the users passwords, data, email accounts, usernames and URLs stored in a very secure, encrypted database, protected by a Master Password. The system is very small so it can be easily transferred from one computer to another. It provides several functionalities on the already encrypted data and the new ones to be inserted. The database produced, is protected by a Master Password only known by its inventor with no backup if lost.

3. SYSTEM ARCHITECTURE

Graphical authentication scheme was proposed by Dhamija and Perrig based on the Hash Visualization technique. In their system, the user is requested to choice a certain number of images from a set of random pictures generated by a program. We have designed the system which will help the person to access the system using the image system will allow the person to secure the important files. Various types of images, most particularly: faces, random art,

everyday objects, and icons are used. Later, the user will be required to identify the preselected images in order to be authenticated. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The normal log-in time, however, is extensive than the traditional approach. A faintness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the procedure of choosing a set of pictures from the picture database can be tedious and time consuming for the user. Recognition-based systems, also known as cognometric systems or search metric systems. The scheme increases usability as it is easy to remember images but prone to replay attack and mouse tracking because of the use of a fixed image as a password, hence its security issues arises.

This study assessed the reliability of FacePattern in order to determine suitable thresholds for the equality of two password items in terms of the minimum number of image features they should possess and the percentage of image features that should match. As variations in token placement are inevitable with FacePattern camera-based setup, we also explored the robustness of the system with rotated input images. Finally, we assessed the uniqueness of feature-based password items.

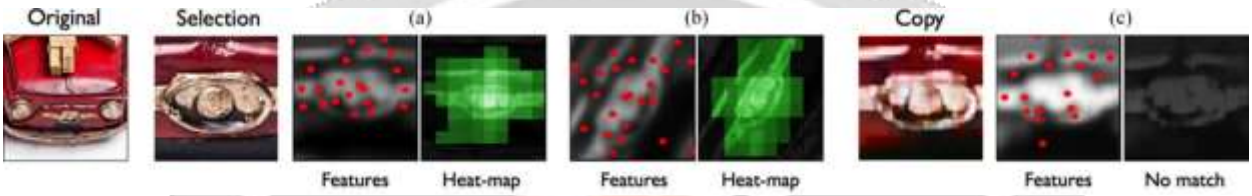

Figure 1: Feature heatmap generated by testing the match between a selected area its transformations (rotation or translation) with the same image or a downgraded copy. Light colored zones in the heatmap indicate a match (white is 100% match). (a) Translated (b) Rotated (c) Translated.

Five source images were selected based on the image categories with highest success rate in prior work. They depicted cars, a mural, toys, a statue, and a human face. These images were displayed on a Samsung Galaxy S-II mobile phone with a screen resolution of 480 * 800 pixels and each image was preprocessed to match this screen resolution. We placed a 110-pixel square NyARToolkit fiducial marker in the center of each image to enable accurate detection of its angle relative to the FacePattern camera. Four selection points were also marked on the image with a 110-pixel circle and labeled with numbers from 1 to 4. The selection points were chosen in a pilot study where eight users (two females, aged between 20 and 25 years) choose four passwords items on the selected images and entered them into the FacePattern system five times. We chose prominent distinctive points from among the selections in these sessions either those that were frequently chosen or, if there was substantial variation in the points selected by users, one of the items at random. An example of one of final images used in the study can be seen in Fig. 2. The experimental task involved users selecting these marked points in order. The use of predetermined and clearly marked selection points ensured the results were not influenced by issues such as memorability.

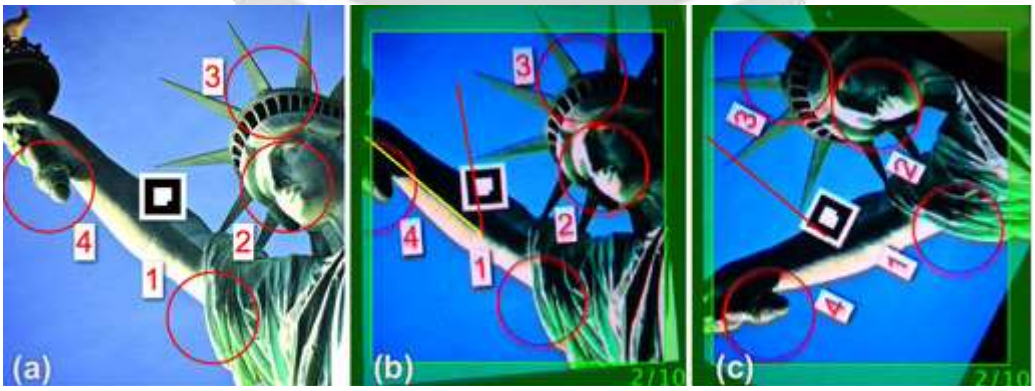

Figure 2: (a) One of the five images used in the feasibility study. Colored lines showing the required and current angular orientation. (c) Image after the token has been rotated to match the required orientation.

4. ADVANTAGES AND DISADVANTAGES

4.1 Advantages

- Better than existing system.
- High Security.
- No sensors required.
- Low Cost.
- No Maintenance.
- Used at Military Area.
- Bank Locker.
- High Privacy Maintained.

4.2 Disadvantages

- Programming is Very Complex.

5. CONCLUSIONS

User authentication is a fundamental component in most computer security contexts. In our paper we proposed a simple graphical password authentication system which provides the more secure authentication than the text password scheme. We described the system operation with implementation of PCCP and trying to implement SHA Algorithm for folder security. PCCP tool such as PCCPs viewport (used during password creation) cannot be exploited during an attack. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember. Better user interface design can influence users to select stronger passwords. The PCCP technique and Secure Hash Algorithm provides an environment in which the folder will be in safe condition. While encrypting the folder, it will be converted into zip file and then encrypted, which will not allow entering any viruses and making damage to the files present in the folder. It will be one of the safe mechanisms for folder security.

6. ACKNOWLEDGEMENT

We take this opportunity to express our hearty thanks to all those who helped us in the completion of the paper. We express our deep sense of gratitude to our guide Prof. R. B. Nangare, Asst. Prof., Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi for his guidance and continuous motivation. We gratefully acknowledge the help provided by him on many occasions, for improvement of this project report with great interest. We would be failing in our duties, if we do not express our deep sense of gratitude to Prof. S. M. Rokade, Head, Computer Engineering Department for permitting us to avail the facility and constant encouragement. Lastly we would like to thank all the staff members, colleagues, and all our friends for their help and support from time to time.

7. REFERENCES

[1] A. Adam, M. Sasse, “Users are not the enemy," Commun. ACM, vol. 42, pp. 40-46, 1999.
[2] M. Adham, A. Azodi, Y. Desmedt, I. Karaolis, “How to attack two-factor authentication internet banking," 17th International Conference Financial Cryptography, pp. 322-328, 2013.
[3] F. Aloul, S. Zahidi, W. El-Hajj, “Two factor authentication using mobile phones," Procedure Computer System Application, pp. 641-644, 2009.
[4] R. Biddle, S. Chiasson, P. van Oorschot, “Graphical passwords: Learning from the first twelve years," ACM Computer Survey's, vol. 44, no. 4, pp. 19, 2012.
[5] S. Chiasson, E. Stobert, A. Forget, R. Biddle, P. C. Van Oorschot, “Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE Transaction Dependable Secure Computers, vol. 9, no. 2, pp. 222-235, March/April 2012.
[6] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni, M. P. Scipioni, M. Langheinrich, “Back-of-device authentication on smartphones," SIGCHI Conference Human Factors Computer System, pp. 2389-2398, 2013.

[7] B. Dodson, D. Sengupta, D. Boneh, M. S. Lam, "Secure, consumer friendly web authentication and payments with a phone," 2nd Int. ICST Conf. Mobile Computer, Application, Services, pp. 17-38, 2010.
[8] K. M. Everitt, T. Bragin, J. Fogarty, T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," SIGCHI Conference Human Factors Computer System, pp. 889-898, 2009.
[9] A. Gelman, J. Hill, M. Yajima, "Why we (usually) don't have to worry about multiple comparisons," J. Res. Educ. Effectiveness, vol. 5, no. 2, pp. 189-211, 2012.
[10] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," SIGCHI Conference Human Factors Computer System, pp. 1107-1110, 2010.