AcSIS: Authentication System Based on Image Splicing

Soomaiya Hamid
Center for Computing Research,
Jinnah University for Women,
Karachi, Pakistan
soomaiya.hamid@juw.edu.pk

Narmeen Zakaria Bawany
Center for Computing Research,
Jinnah University for Women,
Karachi, Pakistan
narmeen.bawany@juw.edu.pk

Shahzeb Khan
Department of Computer Science,
FAST National University of Computer
and Emerging Sciences, Pakistan
k153005@nu.edu.pk

Abstract—**Text-based passwords are widely used for the authentication of digital assets. Typically, password security and usability is a trade-off, i.e. easy-to-remember passwords have higher usability that makes them vulnerable to brute-force and dictionary attacks. Complex passwords have stronger security but poor usability. In order to strengthen the security in conjunction with the improved usability, we hereby propose a novel graphical authentication system. This system is a picture-based password scheme which comprises of the method of image splicing. Authentication data were collected from 33 different users. The usability of the method was evaluated via a comparison between the number of correct and incorrect authentication attempts and time taken. Additionally, a comparison was made between our proposed method and a complex text-based password authentication method using the authentication success rate. Authentication using image splicing proved to be resilient to brute-force attacks since the processing of images consumes a voluminous password space. The evaluation of the usability revealed that graphical passwords were easy-to-remember, resulting in a higher number of correct attempts. The proposed method produced 50% higher success rate compared to the text-based method. Findings motivate the use of the proposed method for securing digital assets.**

Keywords-secured authentication; brute force attack; graphical authentication; picture-based authentication; image splicing; graphical passwords

I. Introduction

Secure authentication is a major concern in computerized system security. Most of the current authentication systems employ text-based passwords. In these systems, an alphanumeric string is used for preventing an unauthorized access [1]. The major issue in using alphanumeric passwords is that they are typically hard to remember as the use of a lengthy and complex password makes it more difficult to recall. Therefore, in order to make passwords more memorisable, people use short and simple passwords. This in turn leads to increase in system vulnerability as these passwords can be cracked easily using simple tools [2-4]. Various techniques [5-7] exist that can exploit the vulnerabilities present in simple passwords. Dictionary attacks are the most common type of attacks on simple passwords [8, 9]. To overcome the problem of using complex passwords, alternate methods are designed such as biometric systems [5] for secure authentication. However, they are expensive since their installation requires extra hardware. Studies prove that from the age of 62 and above finger print quality decreases [10, 11]. Therefore, biometric systems often fail to match the impressions of elderly people. Moreover, biometric systems are not applicable in all scenarios, such as during the authentication in webservers or applications. Besides all these problems, biometric passwords cannot be changed, due to which personal identification of the user is exposed. Studies have proved that human memory is good in memorizing pictures as compared to text [12-14]. Subsequently, this paper introduces an alternate solution that provides a method for secure authentication using Picture-Based Passwords. This in turn supports a suitable way to remember a complex password. Picture-based passwords come under the category of graphical authentication systems. In these systems passwords are involved with the processing of images. [15-17] Users can enter and select from the images which makes it easier than to remember passwords [18]. Besides the user point of view, graphical passwords also provide a better security against attacks. For creating secure system graphical passwords may need more clicked points to recognise [19-21].

A problem in using graphical passwords is that, the authentication requires a massive pool of images in order to make the process secure. The storage and processing of images requires huge memory size. Another problem in using graphical passwords is the extensive consumption of time taken for authentication compared to using textual passwords. Some methods use image hashes to reduce the authentication time [22-25]. Hashing is a process that modifies a password before storing it into a database. The hashing process is irreversible that makes it difficult for an unauthorized entity to steal the password from the database. An example is a graphical authentication method developed in [22]. In this method, a user is required to recognize pre-selected images in a sequence. A server stores the seeds of these images in a text file, which is a time-consuming process. Authors in [23] modified this algorithm by using an SHA-1 hash function that enabled less memory consumption and increased security. Cued click-points belong to one such technique that is based on selecting cue points on a single image for authentication. Authors in [26, 27] revealed high success rate of secure authentication using the

Corresponding author: Soomaiya Hamid

cued click-points based on a two week recall study. Authors in [28] used distinct shape, color, and type of images from a predefined set to authorize a user. Authors in [29] also used color code authentication. In [28, 30] a user had to recognize previously selected images from a set of random images for logging into the system. Authors in [31] proposed an alignment based graphical password system to authenticate a user. They used a spin wheel that was rotated by the user until a combination of images was achieved. Real User Corporation developed an algorithm called “Passface”, which was enhanced in [32, 33]. This method worked by matching a sequence of face images and random face images. However, the passwords were predictable since image sequences were obvious. A similar method was developed in [27]. In this method, a user had to recognize a pre-selected object between 1000 crowded objects in a picture. A downside of this method was that, the log-in process was too slow. In order to quicken the log-in process, an assisted graphical password method was proposed that used approximation of pre-selected locations in a picture [18]. The idea was further extended into a ‘PassPoint’ system 35] who calculated the amount of tolerance around each chosen pixel for authentication.

The paper introduces a novel approach for secure authentication using picture-based passwords along with the cue-point technique. The method generates a combination of a large set of images that is used as a password for authentication. The log-in speed is enhanced using SHA-1 hashing and image splicing.

II. System Overview

This paper proposes a picture-based password scheme which is flexible because the solution accepts any type of picture, e.g. nature images, paintings or daily life pictures. The block diagram of the proposed system in Figure 1 shows the entire work-flow of the system.

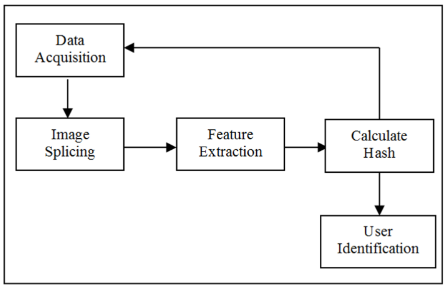


Fig. 1. A schematic diagram of the picture-based authentication system

First time registration process has two phases. In the first phase, a screen is presented to the user where the user is required to enter a user name and a unique pin code. In phase 2, the user is required to upload an image on the system. The system divides the image into 500 slices in a 20x25 grid. In this paper each slice is termed as a “cue point”. The user is then required to select a single cue point out of the 500 slices. Hash code is computed for the selected cue point and stored in the database. The image uploading and cue point selection process is repeated five times in order to complete the registration process. In the authentication phase, the user is authenticated by the username and the pin code added during phase 1 of the registration. After successful authentication, all five images are presented to the user, one by one, where the user is required to select the cue points chosen before. After successful registration of conventional username and pin code, the system performs the steps as shown in Figure 1, to complete the picture based registration process which is described in the following sub sections.

A. Data Acquisition

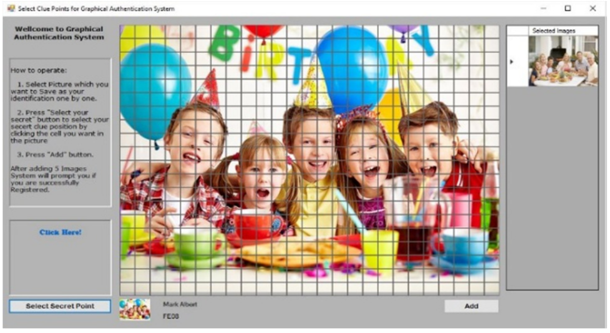
This system requires images from the user as an input. In the first step, system prompts the user to upload five images of his/her own choice in five consecutive steps (the system supports jpeg, gif or png formats). In each step, the uploaded image is saved by the system for further processing. This image is presented to the user at the time of authentication. The images for initial testing are used from the open source image databases MorgueFiles [36] and Shutterstock [37].

B. Image Splicing

Once an image is uploaded to the system, a two-dimensional array of Bitmap type is initialized. The size of the array is kept 20x25 which is capable of holding 500 objects of Bitmap type. The height and width of each bitmap is calculated. Each bitmap is represented by *B* with height of *Bh* pixels and width of *Bw* pixels. The total height *Ih* of an input image *I* is the sum of heights of all bitmaps as shown in (1). Similarly, the total width of bitmap is calculated as the width of all bitmap images, equal to the width *Iw* of the input image *I* as shown in (2). After the bitmap size calculation the uploaded image is mapped to the array of bitmaps where a portion of the uploaded image of height *Bh* and width *Bw* is stored in each Bitmap B. These bitmaps are placed in a matrix as shown in Figure 2.

$$I_h = \sum_{i=0}^{19} B_h \qquad (1)$$

$$I_w = \sum_{i=0}^{24} B_w \qquad (2)$$


Select Clue Points for Graphical Authentication System

Wellcome to Graphical Authentication System

How to operate:

1. Select Picture which you want to Save as your identification one by one.

2. Press "Select your secret" button to select your secert clue position by clicking the cell you want in the picture

3. Press "Add" button.

After adding 5 Images System will prompt you if you are successfully Registered.

Mark Albert
FE08

Fig. 2. Sliced grid view of the user's selected image

C. Feature Extraction

The most important feature, cue point selection, is extracted at this step. Cue point is a part of the original user uploaded image which has been sliced by the system in the previous step of image splicing and is now selected by the user as a part of password from the grid shown in Figure 2. This single slice of the picture is used to authenticate the user on a recall technique. When the user clicks on the cue point, the system processes it transparently. Therefore no change appears on the screen so the people around are unable to look at the selection in a glance. Without selecting the cue point, the user is unable to proceed further. After selecting the cue point user clicks the Add button as shown in Figure 2, to complete the round. Then, a preview of the selected pictures is shown in selected images section so that the user can see a list of pictures he/she had selected. This step is repeated in all 5 rounds. If the user quits before completing the 5 rounds, the system will terminate the registration process and delete the incomplete data. After successful registration, the user can authenticate by only selecting cue points from the pictures that were added at the registration time.

D. Hashing

To make the system more secure, user input data is encrypted with hashing algorithms making it impossible to decrypt, in case of an unauthorized entity getting access to the database. In this system SHA-256 algorithm is used which has 2256 possible combinations. In the user registration process, once the user selects the cue point, the system computes the hash of the selected cue point using the secure hashing algorithm SHA-256 to ensure the security of user information stored in the database. SHA 256 generates a 128-bit key which helps increasing the key size for secure authentication. In the authentication phase the user selects the cue point on a recall-based technique. All images are presented to the user iteratively where he/she has to select that cue point which was selected at the time of registration. Then the hash is computed and the system proceeds to the next round. When all 5 rounds are completed, hashes are compared with the database records.

E. User Identification

At the start of the authentication process, the user is required to provide the name and unique pin code added at the time of registration. Once the conventional username and pin code verification is completed, the user is presented with all the images added at the time of registration. Subsequently, the user is asked to select the cue points that were selected at the time of authentication. Each image hash of the selected cue points is computed using SHA-256 and is compared with the hash value already stored in the database. On successful match of hashes, the user is authenticated by the system. In case of a hash mismatch, the session is terminated by the system, declaring an unauthorized access and the authentication window is closed. Figure 3 shows the complete working model of the system.

III. EXPERIMENTAL SETUP

To perform our experiments a laboratory environment was created where people were asked to register themselves into the system for later authentication. An evaluator monitored how people were interacting with the system. This system was evaluated for different age groups, where the majority of the testing data set was acquired from 20-40 year old users who were the students of computer science department of FAST National University of Computer and Emerging Sciences and Jinnah University for Women.

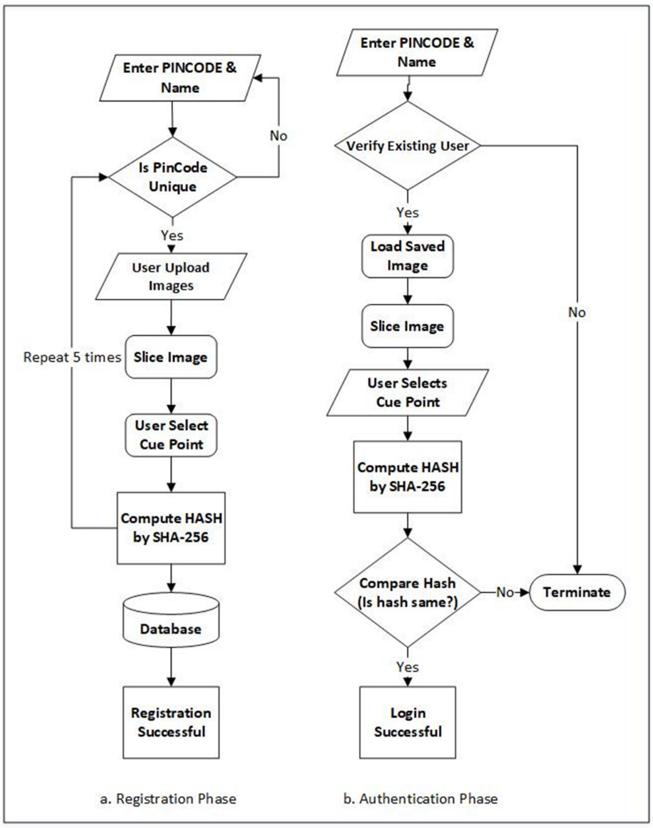


Fig. 3. Proposed system work flow: (a) The registration phase for a new user. (b) The steps required for authentication into the system.

IV. TESTING AND RESULT ANALYSIS

The proposed methodology suggests that, on an input of one picture, the system created 500 sub images (slices), which made 500 possible cue points of that particular picture. The system required 5 pictures with 500 slices of each picture. At the authentication phase if the hash of cue points was compared at every round, the possible combinations become 5x500=2500 which is very small to protect the authentication from brute force attacks. Therefore, the hash was compared after the completion of all 5 rounds. This technique made the system more powerful because it made 5005 possible combinations that resulted in Tens of Trillions values which constitute a huge data set for an attacker to predict the password. The proposed system was tested by a group of people (20 to 40 years old), in lab environment. Users selected pictures and performed registration and authentication process by following the rules which were learned before the testing session. Instructions were also provided on the system's screen. Users were asked to register and authenticate to the system. Each user had to make ten attempts while the time taken in the authentication process was recorded. Only the authentication time was recorded as the registration is an one-time activity. The success rate was also recorded. The data of correct and incorrect attempts were collected and it was found that alphanumeric passwords were less memorable than graphical passwords. According to the results shown in Table I, a higher rate of incorrect attempts was noticed in alphanumeric passwords and a lower rate of zero incorrect attempts was found regarding graphical passwords. This proves that users found graphical passwords more convenient to remember. Users were excited about the system and took this survey as playing a game in order to examine their memory strength. Some users used few techniques to remember the tiles (slices) while some used the attraction points of the pictures. Only a few of them were those who were tired of remembering the cue points in the beginning attempts of the survey.

TABLE I. INCORRECT ATTEMPT COMPARISON

Incorrect Attempts	Alphanumeric Authentication	Graphical Authentication
all	8	4
zero	12	22
half	1	1
three	2	2
two	3	2
one	7	2

It is a fact that whenever a new system is proposed in the market, people find it difficult to adopt it in the beginning, but later on, they get impressed by the new approach and ultimately adopt it [3]. For the comparative study we designed an alphanumeric password system with hard restrictions to obtain a strong password and asked users to try some new passwords. In the strong password credentials we accepted at least 10 characters long combination passwords comprising of 1 numeric digit, 1 uppercase letter, 1 lowercase letter and 1 special character. We noticed that the majority of the users used password structure like Username1234+ or Username@1234. They derived an easier way to break the combination password rules and to memorize it. When a user types his/her username in password and 1234 digits, the password becomes more guessable and can be affected by social engineering attacks. From the comparative study, we found that graphical authentication process took a little longer time than the alphanumeric password process. According to the results of this research, graphical authentication took 13 seconds in average while alphanumeric authentication took 11.9 seconds. Note that the alphanumeric scheme is well-known and the most commonly used process for authentication and that the graphical authentication process proposed in this paper was definitely new to the users.

These observations reveal that although graphical authentication took a little more time, it also provided a highly secure password space which provided greater chances to memorize a strong password as compared to the text based password method. These findings support the studies which reported that pictures have a high tendency to be memorized by the human brain.

V. CONCLUSION AND FUTURE WORK

In conclusion, a graphical password technique was developed for user authentication. Our findings suggest that this system had improved the capability of remembering complex passwords in terms of pictures. A user had to memorize only five points in five images and the system automated these five images into tens of trillions combinations. This huge set of combinations made it harder for brute force attacks to crack a password. This paper also provided a comparative study of the effectiveness of the proposed system. According to the results, the graphical authentication process has 50% more success rate than the text-based password method. The proposed system provides secure authentication using images and eliminates the use of textual passwords. Capitalizing the ability of humans to remember images, this system has the advantage over textual passwords in terms of remembering complex passwords in the simplest way. Future work includes using a dynamic number of slices per image. It can be suggested that 100 or 50 slices will not make the system vulnerable for brute force attack. This will increase cue point dimensions which helps users who are not eligible to remember small cue points and do not have a need of high security. This might decrease the number of image-slices but still the number of possible combinations will be enormous. The system can be enhanced by adding a module to prevent it from shoulder surfing attack for which fake pointers could be used with different colors for confusing the attacker. An analysis on big data and picture resolution is also required, to analyze its effects on hash function or brute force attack. The system can be further modified by the addition of a password recovery feature.

REFERENCES

[1] S. Xiaoyuan, Z. Ying, G. S. Owen, “Graphical Passwords: A Survey”, 21st Annual Computer Security Applications Conference, Tucson, USA, December 5-9, 2005

[2] D. Florencio, C. Herley, “A Large-Scale Study of Web Password Habits”, 16th International Conference on World Wide Web, Banff, Canada, May 8-12, 2007

[3] J. Yan, A. Blackwell, R. Anderson, A. Grant, “Password memorability and security: Empirical results”, IEEE Security and Privacy, Vol. 2, No. 5, pp. 25–31, 2004

[4] C. Kuo, S. Romanosky, L. F. Cranor, “Human Selection of Mnemonic Phrase-Based Passwords”, Second Symposium on Usable Privacy and Security, Pittsburgh, USA, July 12-14, 2006

[5] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication”, Proceedings of the IEEE, Vol. 91, No. 12, pp. 2021–2040, 2003

[6] A. K. Jain, K. Nandakumar, A. Nagar, “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing, Vol. 2008, Article ID 579416, 2008

[7] C. Roberts, “Biometric attack vectors and defences”, Computers and Security, Vol. 26, No. 1, pp. 14–25, 2007

[8] M. D. Amico, P. Michiardi, Y. Roudier, “Password Strength: An Empirical Analysis”, IEEE INFOCOM, San Diego, USA, March 14-19, 2010

[9] A. Narayanan, V. Shmatikov, “Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff”, 12th ACM Conference on Computer and Communications Security, Alexandria, USA, November 7-11, 2005

[10] S. K. Modi, S. J. Elliott, “Impact of Image Quality on Performance: Comparison of Young and Elderly Fingerprints”, 6th International Conference on Recent Advances in Software Computing, West Lafayette, USA, 2006

[11] S. K. Modi, S. J. Elliott, J. Whetsone, H. Kim, “Impact of Age Groups on Fingerprint Recognition Performance”, IEEE Workshop on Automatic Identification Advanced Technologies, Alghero, Italy, June 7-8, 2007

[12] A. Paivio, T. B. Rogers, P. C. Smythe, “Why are pictures easier to recall than words?”, Psychonomic Science, Vol. 11, No. 4, pp. 137–138, 1968

[13] M. H. Erdelyi, J. Becker, "Hypermnesia for pictures: Incremental memory for pictures but not words in multiple recall trials", Cognitive Psychology, Vol. 6, No. 1, pp. 159–171, 1974

[14] C. L. Grady, A. R. Mcintosh, M. N. Rajah, F. I. M. Craik, "Neural correlates of the episodic encoding of pictures and words", National Academy of Sciences, Vol. 95, No. 5, pp. 2703–2708, 1998

[15] S. Nasiri, M. T. Sharabian, M. Aajami, "Using combined one-time password for prevention of phishing attacks", Engineering, Technology & Applied Science Research, Vol. 7, No. 6, pp. 2328-2333, 2017

[16] D. Virmani, P. Girdhar, P. Jain, P. Bamdev, "FDREnet: Face detection and recognition pipeline", Engineering, Technology & Applied Science Research, Vol. 9, No. 2, pp. 3933-3938, 2019

[17] R. Rasras, Z. Alqadi, M. Rasmi, A. Sara, "A methodology based on steganography and cryptography to protect highly secure messages", Engineering, Technology & Applied Science Research, Vol. 9, No. 1, pp. 3681-3684, 2019

[18] G. E. Blonder, Graphical Password, U.S. Patent 5,559,961, 1996

[19] W. Meng, F. Fei, L. Jiang, Z. Liu, C. Su, J. Han, "CPMap: Design of Click-Points Map-Based Graphical Password Authentication", IFIP International Conference on ICT Systems Security and Privacy Protection, Poznan, Poland, September 18-20, 2018

[20] C. Katsini, C. Fidas, M. Belk, G. Samaras, N. Avouris, "A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication", International Journal of Human–Computer Interaction, available at: https://www.tandfonline.com/doi/full/10.1080/10447318.2019.1574057

[21] L. N. Tiller, C. A. Angelini, S. C. Leibner, J. D. Still, "Explore-a-Nation: Combining Graphical and Alphanumeric Authentication", International Conference on Human-Computer Interaction, Orlando, USA, July 26-31, 2019

[22] R. Dhamija, A. Perrig, "Deja Vu: A User Study Using Images for Authentication", 9th USENIX Security Symposium Paper, Denver, USA, August 14-17, 2000

[23] A. E. Dirik, N. Memon, J. C. Birget, "Modeling User Choice in the PassPoints Graphical Password Scheme", 3rd Symposium on Usable Privacy and Security, Pittsburgh, USA, July 18-20, 2007

[24] D. Weinshall, S. Kirkpatrick, "Passwords You'll Never Forget, But Can't Recall", Extended Abstracts on Human Factors in Computing Systems, Vienna, Austria, April 24-29, 2004

[25] A. Perrig, D. Song, "Hash Visualization : A New Technique to improve Real-World Security", International Workshop on Cryptographic Techniques and E-Commerce, 1999

[26] S. Chiasson, P. C. V. Oorschot, R. Biddle, "Graphical Password Authentication Using Cued Click Points", 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007

[27] S. Chiasson, E. Stobert, A. Forget, R. Biddle, P. C. V. Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Transactions on Dependable Secure Computing, Vol. 9, No. 2, pp. 222–235, 2012

[28] R. Mahey, N. Singh, C. Kumar, N. Bhagwat, P. Verma, "Graphical Password Using an Intuitive Approach", in: International Conference on Intelligent Computing and Applications , pp. 153–161, Springer, 2016

[29] S. Agrawal, A. Z. Ansari, M. S. Umar, "Multimedia Graphical Grid Based Text Password Authentication: For Advanced Users", Thirteenth IEEE International Conference on Wireless and Optical Communications Networks, Hyderabad, India, July 21-23, 2016

[30] D. H. Dhandha, P. Chandresh, "Enhancement of password authentication system using recognition based graphical password for web application", International Journal of Advanced Research in Computer Science, Vol. 8, No. 5, pp. 1135–1139, 2017

[31] A. Danish, L. Sharma, H. Varshney, A. M. Khan, "Alignment Based Graphical Password Authentication System", 3rd International Conference, Computing for Sustainable Global Development, New Delhi, India, March 16-18, 2016

[32] F. Towhidi, M. Masrom, A. A. Manaf, "An enhancement on passface graphical password authentication", Journal of Basic and Applied Scientific Research, Vol. 3, No. 2, pp. 135-141, 2013

[33] S. Brostoff, M. A. Sasse, "Are Passfaces more usable than passwords? A field trial investigation", in: People and Computers XIV-Usability or Else!, pp. 405-424, Springer, 2000

[34] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, Vol. 63, No. 1-2, pp. 102-127, 2005

[35] A. Bertolino, "Software Testing Research: Achievements, Challenges, Dreams", Future of Software Engineering, Minneapolis, USA, May 23-25, 2007

[36] https://morguefile.com/

[37] https://www.shutterstock.com/