Array-based Graphical Password Authentication

Ritu P Simha*, Sri Nithya S**, Sneha P K***, Rabichith**** and Surekha Borra*****
*-****UG Student, Department of ECE, K.S. Institute of Technology, Bangalore, Karnataka, India
ritu.simha@gmail.com
*****Professor, Department of ECE, K.S. Institute of Technology, Bangalore, Karnataka, India
borrasurekha@gmail.com

Abstract: Rapid growth in the technology, has led the computer and information security a most challenging task. Traditional methods provide security by means of text-based passwords, which are easy to crack. This paper presents a graphical password method in which the authentication of the user is based on the recognition of pictures in an array. The proposed method is user friendly and is robust to shoulder surfacing attacks. Hence the proposed method is more secure than existing methods.

Keywords: Graphical Password; Shoulder Surfacing; Authentication; Recognition-based Approaches.

Introduction

Over years, passwords are the foremost used techniques for distinctive user authentication in communication systems and laptop. Typically, passwords are strings of digits or letters. Such alpha-numeric passwords have the disadvantage of being arduous to recollect. Alpha numeric passwords are prone to a lot of attacks like brute-force, shoulder-surfacing, dictionary attacks, guessing, and spyware. A good authentication system is expected to meet the following requirements:

- Ease of recollection of passwords.
- Ease of execution of authentication protocols.
- Use of random passwords and must be arduous to guess.
- Provision to frequent change the passwords.

The current authentication methods are divided into three main areas as mentioned below:

Token based authentication [1]: It involves the use of key card, bank cards and smart cards. In order to enhance the security, many of these techniques use knowledge based authentication. Examples include ATM cards which are generally used with a PIN number.

Biometric based authentication [2]: Iris scan, facial recognition and finger prints fall under the technique of biometrics. Though these authentication systems highly secure, they are not largely adopted as they are slow and expensive.

Knowledge based authentication [3]: These are the mostly used authentication systems, and are mainly text and picture based. Yet another way of classification depends on whether the passwords can be recalled or recognized.
In Recognition-Based techniques a group of images are selected during the registration phase, wherein they are later recognized and re-identified during authentication phase. Techniques include Jensen method[4], Color login method and Image pass method [5].

In Recall-Based techniques: a group of images are selected during the registration phase, wherein they are later reproduced during authentication phase. Techniques include: Exact-match and Elastic Approaches. In contrast to Exact-match approaches, the Elastic approaches have some flexibility thereby allowing the user to reproduce the patterns with fine variability. The recall based techniques are further divided into two main categories:

Pure Recall-Based technique: A type of Recall-Based technique in which the user is not given a clue to recall any password. Few examples of this technique are:

Passdoodle technique: A type of design taken in writing is usually a text which is drawn onto the touch sensitive screen using the stylus. The users have the ability to remember the textual kind of password, i.e., the Passdoodle written or drawn by them. But on the other hand, they tend to forget the order in which the doodle is made. They are more interested in the doodles made by the other users and they end up entering the log-in details of other users. This is sensitive to guessing, spyware and shoulder surfing attacks.

Draw-a-Secret (DAS) technique: Here a user can draw on a 2D grid of size A×A where rectangular co-ordinates (x,y) is used to represent each cell. The touch grid's values are to be stored by the authentication system and reproduced by the user in the same order of drawing. The users have no time constraints to draw their password. While this technique results in huge password space, the users are poor at remembering and reproducing the order in which the password was made. There are times where the user chooses a delicate password that is sensitive to attacks like graphical dictionary and replay attack.

Signature technique: In this technique, user uses mouse to draw a signature which acts as password. This technique has an advantage as the signatures cannot be forged or remembered.

Cued Recall-Based technique [4]: In this system, the user remembers the password using a clue that is registered during a phase of registration. This method helps the user by providing clues to remember the password. Hence, it is advantageous compared to pure recall based technique. Few examples of this technique are:

Blonder technique: In this technique predefined images with their respective regions are displayed for the user to click and select some points on the image in a sequence. Since the number of click points are less, the password should have around ten plus clicks for adequate security and these regions needs to be readily identifiable such as cartoons.

Passpoints technique: This is a method described to overcome the drawbacks of Blonder technique. Here natural image is displayed to the user to remember the click points.
Section 2 presents a survey on recall based graphical authentication techniques. Section 3 presents the proposed array-based graphical password authentication system. Section 4 analyses the practicality of the defined system and section 5 concludes paper.

Related Works

A good amount of work has been done in this area, and they have come up with brilliant ideas. One of them involves choosing large number of images from a folder or briefcase of images. This is known as the challenge response scheme. In order to log-in, the user must complete several challenges and stages in which he will have to choose one image out of several decoy images as password. It has an advantage of simply viewing the displayed images and choosing the known, as it completely relies on the recognition memory. When different users try their hands on the same image or password, security reduces as the entropy of the system goes down. Three challenge response systems are discussed in this section.

PASSFACES [6]:

This system is based on the recognition based approach which has been explained in the introduction above. This is based on the known assumption that humans have more visual memory than text-based recognition. The log-in uses four rounds of tasks or challenges. Every challenge involves a set of nine images, with only one legitimate image on which the user need to click to move to next challenge and further authentication. The Passfaces system is analyzed later by Brostoff and Sasse and showed that it leads to login failure rate was 4.9 percent. The result of this study also showed that Passfaces are more memorable than alpha-numeric type of passwords. Although it has this advantage, Passfaces has a more dangerous disadvantage wherein the attacker has 1-in-9 chances to get the password right. With few numbers of guesses, the attacker discovers the password. To increase security, many phases needs to be used which can be time consuming and very slow.

DÉJÀ VU [7]:

Déjà vu system of graphical password authentication is akin and almost analogous to the Passfaces system of graphical authentication. This system uses random images/photographs. The log in can be achieved in just one round wherein the user must select five images from the 25 images which occur simultaneously on the screen. The remaining 20 images are decoy images. The user should be careful not to click or select on any of the decoy images, following which the log in fails. A parallel study like the one for Passfaces was carried out for this method which consisted of comparison between déjà vu, alpha-numeric password and numeric PINs. The conclusion of this study yielded 5% failure rate for the numeric PINs and 10% failure rate for alpha-numeric passwords. Déjà vu method revealed that it requires a minimum of 30 seconds for log-in which is not favourable as it reduces the efficiency of the authentication.

VIP [8]:

The VIP system of authentication is commonly used in PINs and ATM cards. It is basically a kind of a graphical PIN. The VIPs were less error-prone than the alpha-numeric passwords. This system failed when the same category images were used as they were confusing a distractor image. (Eg: The "trees" category). This system has less password space. The efficiency of the visual PIN scheme was different for the 3 versions which ranged nearly from 6 to16 seconds in contrast to the 3 seconds taken by the numeric PINs.

Two other challenge response schemes are proposed by **Dhamija and Perrig [9],** and **Haichang's et al. methods [10].** The study of all these systems show that passwords created using challenge-response scheme is more advantageous for users to remember over time. But, most of the challenge response approaches are not resistant to shoulder surfing attack.

Proposed Array-based Graphical Password Authentication System

Rows and columns have always been the basics of mathematics and design. Using this simple yet efficient concept, a novel array-based graphical password authentication system is presented in this section. This method is based on the identification of the location of the selected image from a grid of decoy images displayed at anytime. The location of the image in the grid helps in building the password as a numeric code. The procedure of the proposed system contains two phases: Registration phase and the Login phase which are shown in Fig. 1 and Fig. 2.

Registration phase

- User creates their ID or username.
- The user ID is registered and in order to set up the password, a number of images appear on the screen.
- The user selects four images in sequence from the number of images that are presented to him/her.
- The images that are selected by the user along with their order information, is maintained by the system as password.

Login phase

- During the log-in phase, the user enters his/her log-in ID or username and the system will immediately fetch the user ID login vector.
- The system then displays an array of images, which includes the images the user has selected during the registration phase.
- The position of the image, that is, the row and the column of the user's image are typed in the space that is provided.
- The position of four images is entered in sequence in four displays, which forms the password for the user.
- If the entered position and order has the correct image sequence, then the user gets authenticated through the login. If not, he gets another chance to enter the password, failing which the system will block the user from logging in for a small period.

Implementation

Four images shown in Fig. 2 are chosen during the registration phase by the user. These 4 images in the same sequence are stored as a password in the database. They will be displayed in random rows and columns along with other decoy images as an array of images on the screen during log-in phase after entering a valid user name as shown in Fig. 3. The author has to recall his password images and enter their row and column numbers in the same sequence to form a temporary eight digit number. The authentication system verifies the images provided by this set of row and columns in sequence and with the images and their order which is in the user database.

Figure 4 is displayed during the login phase to the user after typing his user name. Note that the images of the user are displayed in a random fashion on the screen. It is seen that the first password image is at the location 1x5. Therefore, the digits to be entered for this image are 15. The same procedure is followed for other 3 images to obtain the authentication digit sequence 14224352. One more variant of this proposed idea is to name the rows using alphabets and the columns are numbers, or vice versa. For example, let the rows be a, b, c, d, e, from left to right respectively. Then, our password would be A5B2D3E2.

The proposed system provides a good defense against the brute force and guessing attacks as it has a good combination of both test-based and picture-based password. It is difficult to guess the password by the user by trying a million combinations. The problems of guessing the password is completely eradicated as the images are jumbled during every log-in. The number of combinations in which a single image can be jumbled every login is 25, for a grid of 5x5. This grid can be made large to improve security. The new password gets generated for every trial increasing the security of the system. The probability of guessing the password will be comparatively low. The size of every image is a thumbnail size. At every log-in, the position of images will vary along with the decoy images. So, the intersection images which are used as a session password will also vary. Also because of the randomization of password in the steps, the attacker can get confused if he is trying to memorize the password details. In this way, our system is strongly resistant to shoulder surfing attack.

The shoulder surfing attack is comparatively low compared to the existing system or keeping into account of only using the graphical password system without combining it with the text-based password.

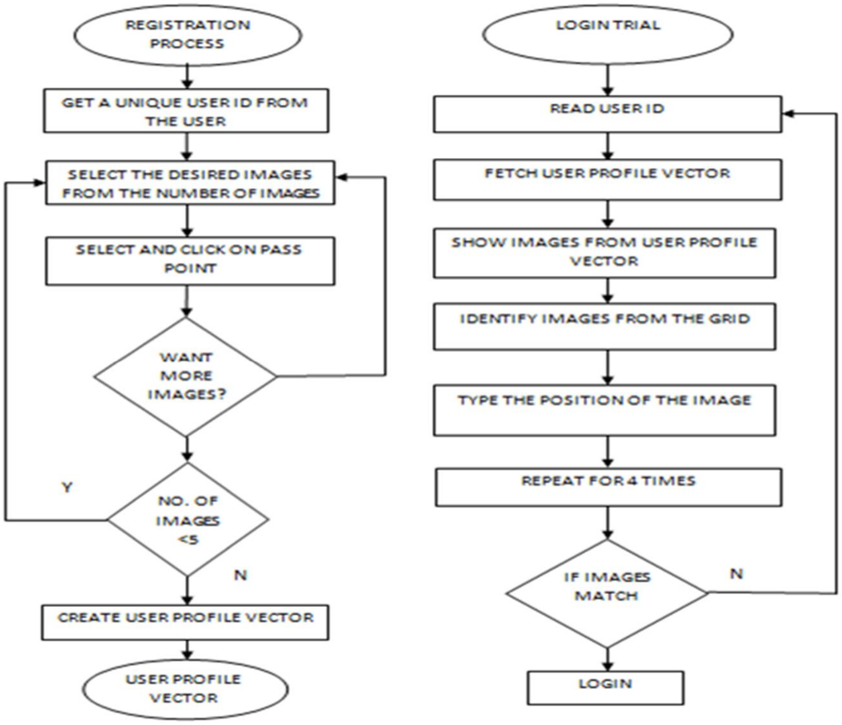
REGISTRATION PROCESS
GET A UNIQUE USER ID FROM THE USER
SELECT THE DESIRED IMAGES FROM THE NUMBER OF IMAGES
SELECT AND CLICK ON PASS POINT
WANT MORE IMAGES?
Y
NO. OF IMAGES <5
N
CREATE USER PROFILE VECTOR
USER PROFILE VECTOR
LOGIN TRIAL
READ USER ID
FETCH USER PROFILE VECTOR
SHOW IMAGES FROM USER PROFILE VECTOR
IDENTIFY IMAGES FROM THE GRID
TYPE THE POSITION OF THE IMAGE
REPEAT FOR 4 TIMES
IF IMAGES MATCH
N
LOGIN

Fig.1. Flow of the registration and login phases

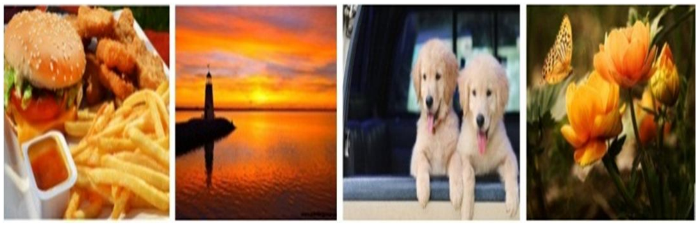

Fig. 2. Sample images chosen during Registration phase

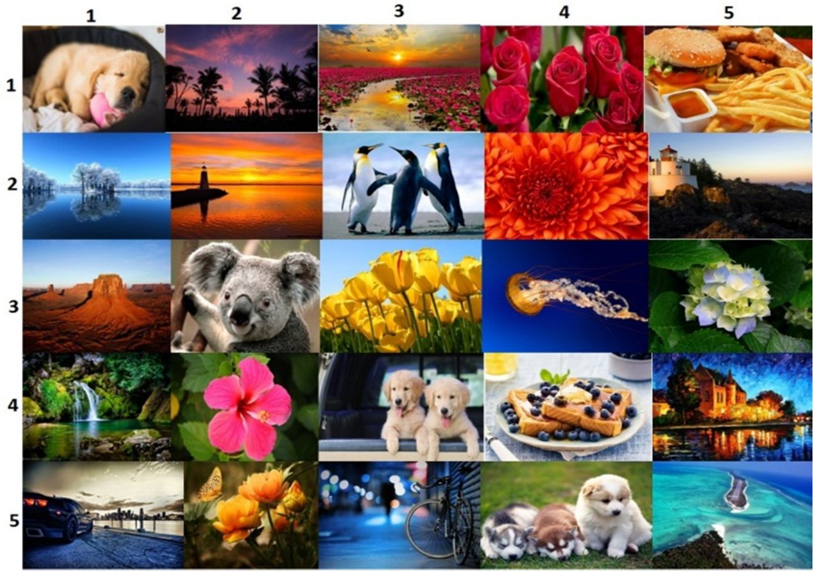

Fig. 3. Sample grid of images displayed during Login phase

Table 1. Comparison of Techniques

Description	Passface system [6]	Déjà vu system [7]	Proposed system
Shoulder surfacing, brute force and guesswork	Maximum	Maximum	Hardly exists
Watermarking	Needed	Needed	Not needed
Permutations and combinations of password generated	Less	Very less	More
Stages of security	One	Two	More than 4

Conclusion

Password ensures that the computer or information can be accessed by those who have been granted right to view or access them. Graphical password systems are introduced as an alternative to traditional passwords so as to ease the job of humans in remembering them. In this paper, a graphical password system is presented for authentication purposes. The method involves choosing images from an array of images by entering the corresponding rows and column numbers as a numerical data to be verified in the database with password images chosen by the user during the registration phase in a specific order. The system is more human friendly with increased levels of security. This method of authentication is an effort to develop security innovations with people in mind. The method is a hybrid approach that combines images and numbers for improving security and resistance to attacks. The randomization of images strongly helps in additional security. This system can be used for web account access, be it social media accounts, bank accounts or company security logins. It can also find its applications in smart phones and home security systems.

References

[1] Das, Anupam, et al. "The Tangled Web of Password Reuse." NDSS. ,14, 2014, 23-26.

[2] He, Debiao, and Ding Wang. "Robust Biometrics-Based Authentication Scheme for Multiserver Environment", IEEE Systems Journal, 9, 3, 2015, 816-823.

[3] Patil, Kailas I., and Jaiprakash Shimpi. "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices" International Journal of Innovative Technology and Exploring Engineering (IJITEE) , 2013, 2278-3075.

[4] Jensen, Wayne, Serban Gavrila, and Vladimir Korolev. "Picture Password: A Visual Login Technique for Mobile Devices." NISTIR 7030 (2003).

[5] Mihajlov, Martin, Borka Jerman-Blazič, and Marko Ilievski. "Imagepass-Designing Graphical Authentication for Security." , 7th International Conference on Next Generation Web Services Practices (NWeSP), 2011, 262-267.

[6] Brostoff, Sacha, and M. Angela Sasse. "Are Passfaces more usable than passwords? A field trial investigation.", People and Computers XIV—Usability or Else!. Springer London, 2000, 405-424.

[7] Dhamija, Rachna, and Adrian Perrig. "Deja Vu-A User Study: Using Images For Authentication." , USENIX Security Symposium, 9, 2000.

[8] De Angeli, Antonella, et al. "Is A Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems." International Journal of Human-Computer Studies, 63,1, 2005, 128-152.

[9] Perrig, Adrian, and Dawn Song. "Hash Visualization: A New Technique to Improve Real-World Security." International Workshop on Cryptographic Techniques and E-Commerce. 1999.

[10] Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010, October). A new "Graphical Password Scheme Resistant to Shoulder-Surfing". International Conference on Cyberworlds (CW), 2010, 194-199.