COGNITIVE GRAPHICAL PASSWORD BASED ON RECOGNITION WITH IMPROVED USER FUNCTIONALITY

Mozhdeh Sarkhoshi and Qianmu Li

Nanjing University of Science and Technology, Nanjing, Jiangsu, China

ABSTRACT

The fact that photos and graphics are more easily recalled by humans than text led to the proposal that visual passwords may be a viable alternative to text passwords in certain situations. User-friendliness characteristics of existing models are based on graphical password recognition, and the introduction of a new model that is related to the specifications and features of ISO standard usability and to the specifications and features of general usability specifications and features is being considered. Once these criteria and characteristics and sub-components of usability had been compared, additional usability features that could be included into the new graphical password model provided were discovered. There was a presentation of the graphical password model, which was separated into two sections, which included new users and current users. A questionnaire was used to evaluate the usability features and applicability of the prototype system after it had been implemented as a prototype system. After this step, the system was implemented as a prototype system and its evaluation and evaluation through a questionnaire was used to evaluate the usability features and applicability of the prototype system. Then there will be user input on the whole system, as well as the outcomes. The characteristics and specifications of the usability of the visual password prototype will be gathered and examined in this study. All of the percentages collected in this publication in connection to the findings and results from the point of view of usability are such that it is possible to conclude that the new visual password system is acceptable in its current form.

KEYWORDS

Graphic password, authentication, usability.

1. INTRODUCTION

In today's world, authentication methods, of which passwords are the most significant component, are extensively employed. As soon as the system determines that an input has the right username and password, the user is prompted to go through the authentication procedure. Users must initially register in order to be granted access to the system, and they must remember the username and password they created during the registration process in order to log in each time they wish to use it. Being aware of a user's password and username are the only things that can confirm their identity. Text passwords are often the sole method by which users are authenticated while accessing a network system. This approach is used by many networks, computer systems, and Internet settings today to verify their users' identities. Unfortunately, many passwords may be readily guessed or broken, making them vulnerable to attack. There are several and well-documented downsides of using this strategy [1].

Instead of using text-based passwords, visual encryption methods have been created as a replacement for them. As a result, picture codes have the potential to be more secure and reliable

David C. Wyld et al. (Eds): SIPP, NLPCL, BIGML, SOEN, AISC, NCWMC, CCSIT - 2022
pp. 17-24, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.121302

than earlier text codes since they govern the capacity to quickly detect and recall the image. Text-numeric coding has long been known to have a flaw, and this system is meant to solve that flaw. The premise that people recall images more readily than letters and numbers, and the concept that a picture is worth a thousand letters are both supported by certain research conducted by psychologists and software businesses. The fact that photographs and graphics are more easily recalled by humans than text led to the suggestion that visual passwords may be a suitable alternative to text-based passwords.

It is an authentication and validation system that operates on a graphical password interface, which allows users to pick certain photographs in a specified sequence using a visual password. Computer systems are routinely run under the control of an authentication system that relies on characters such as usernames and passwords. These sorts of systems have been known to include significant vulnerabilities; for example, users often use a basic password that may be quickly guessed by others. To be honest, it's tough to remember a password that's both safe and difficult to guess. Today, this approach is used as the authentication strategy for the vast majority of computer systems, whether they are network-based or host-based. A lot of people are already aware of the risks involved with this strategy. An assault linked to (Dictionary Attack), which is used by hackers to get access to numeric alphabetic passwords, is one of the most popular attacks in this field of study. However, there is no doubt that this form of assault is a very successful strategy. Because it just takes a short amount of time to figure out the password. Other disadvantages of utilizing this strategy include the same difficulty in learning and remembering passwords, since studies have shown that just a few kinds of passwords are simple for users to remember, as a result of which people often create and use the same passwords for all of their accounts [3]

As previously stated, the graphical password authentication system is a viable alternative to the numerical alphabetical form of password authentication. Specifically, this approach has been presented to remove the usual shortcomings and vulnerabilities of the primary methodology (numerical alphabetic technique).It is also possible that this technique will be better appropriate for producing passwords that are both more secure and more memorable for users. Users may recall photos more quickly than numeric alphabetic letters, according to one of the primary assumptions in this field. The other hypothesis is that images are worth thousands of dollars, according to the other hypothesis. These theories have been put to the test by the code, software firms, and some study in the area of psychology. Computer systems must meet certain security standards in order to function properly, which is particularly crucial given the proliferation of threats in this field. It's true that scientists and security professionals have long been concerned with the safety of computer systems, digital assets, and humans. However, security has been seen as a technological matter of considerable importance to date, and concerns have emerged in this respect. Users have resorted to passive or active usage of security technology in a variety of situations. Understanding may be vital in passive applications; nevertheless, in addition to active applications, consumers want additional usability elements as well as security-related solutions in passive apps. For example, they need characteristics such as expertise and mastery, simplicity of operation, ease of recall, contentment, and efficiency, among others.

Determining the authentication process is a procedure that decides whether or not a user is permitted to access a given system or piece of information. Despite the fact that passwords are still frequently used today to authenticate individuals, there are other options available, such as biometric systems and smart cards, that may be used instead.

Using these options, on the other hand, has a number of drawbacks. Biometrics involves a wide range of security concerns, many of which are connected to privacy; on the other hand, smart cards need a unique PIN in order to prevent them from being misplaced.

Consequently, passwords are still the primary method of authentication. A variety of shortcomings of traditional passwords are related to their usability, and these shortcomings are directly related to security difficulties. Users that are unable to choose secure passwords make the authentication procedure dangerous and provide possibilities for attackers to get access to credentials [4].

It is believed that passwords will be able to deal with two required requirements that are in conflict and conflict, and one feature that is extremely significant is that users will be able to passwords. There are various issues with passwords. Authentication processes must be conducted swiftly by users, but passwords must be safe, for example they must be secure, random and difficult to guess. Passwords must also be changed on a regular basis and in a secure manner. Users' preferences should evolve over time and not be the same for all of their accounts. They should also not be entered and kept in text files.

Utilitarian design is critical in the creation and development of an aesthetically pleasing graphical password system that also fits the demands and expectations of its users. ISO 241-11 defines usability as the degree to which a product may be utilized by individual users to accomplish their specified objectives in an effective and efficient manner, as well as adequately, in the appropriate area of application. Several academics have carried out investigations to propose new algorithms or enhance existing algorithms with the goal of boosting security and usability since the first graphical user authentication system was introduced by Blonder. Unfortunately, the majority of graphic password researchers have not paid attention to usability aspects. In most cases, researchers investigate graphical password security solutions, focusing on the probability of passwords failing during the authentication process, as well as user satisfaction and system operational aspects, among other things.

Do not put anything in it (especially the simplicity of remembering passwords). A critical topic to consider is the implementation of an entirely new graphical password system that offers a variety of interesting usability features.

2. DIAGNOSIS-BASED TECHNIQUES

Most articles from 2000 to 2015 have described that the methods available for diagnostic techniques are five designs. In the following section, existing methods will be reviewed and their strengths and weaknesses will be studied.

2.1. PASS FACE ALGORITHM

According on the idea that the human face is easier to recall than other photographs, Real User created a technology called Pass Face in 2002, which is now widely used. It is possible to pick images of previously seen people with this solution, which offers choices that prompt the user to select photos of previously seen people. When consumers have selected all four of their face photographs, the procedure is complete. Results of earlier research have indicated that users can remember their passwords more readily when using this approach as opposed to the text password method [6], despite the fact that it takes a longer time to login to the system when using this method.

In this approach, the user's gender, race, and face beauty are the three criteria that influence the choice of trend, allowing the selections to be predicted in advance of time. Although optional assignment makes the password more forgettable, it is given as a modification to make it more memorable. Other shortcomings of this technique are related to the processing time required. The

registration component of the Pass Face algorithm is the most time-consuming phase for users, resulting in a lengthier overall validation and authentication time than with a text password, according to the algorithm.

2.2. Already Seen Algorithm

This approach, which was first used in 2000 and reported by Lashkari and Farmand (2009), is given as a vast collection of photographs, some of which are random, and users are asked to choose a certain number of them from the collection. The photographs that were previously picked must be identified later on in order to verify the user's identity. When compared to text passwords and PINs, the login time is much longer, and 90 percent of users have been successful in this approach throughout the validation process, while other ways have only been successful in 70 percent of cases [7].

Some of this technique's shortcomings are discussed as follows. With traffic congestion and several photographs being given by the server, processing time will be prolonged; ii) Despite the fact that this solution has a lower password space, it will be more secure. The password formed is difficult to remember, iii) while the server must analyze documents pertaining to many users, picture selection is a time-consuming procedure, and iv) the overall time necessary to construct the password is prohibitively expensive. The time required for a text password is 25 seconds, but the time required for this strategy is 60 seconds.

2.3. Triangle Algorithm

This approach is based on the Shoulder-Surfing problem's graphical password-based solution. The system displays a number of items associated with passwords, and the user picks an area made by him. For instance, the system may show three items and the user may choose three things associated with the password, resulting in the formation of a triangle. By clicking on the inside of the invisible picture, the user may confirm. This technique is performed with the icons in various places on the screen [8]. Researchers recommend doing this technique numerous times to eliminate the chance of unintentional connection by clicking or rotation. As a result, the method's sluggish connecting procedure might be considered a significant shortcoming.

2.4. Picture Password Algorithm

This method is related to a graphic password scheme proposed by Sobrado and Birget, which is based on a visual password. Basically, this algorithm is designed for mobile devices such as PDAs. Password selection in this method is done using small photos in the form of themes provided in the form of cats and dogs or the sea and the beach. Therefore, users can be authenticated by identifying the viewed photos and touching them in the appropriate sequence using a stylus pen. Once the user can authenticate, he or she may change what theme or password. Researchers have also suggested that this process be repeated several times in order to minimize the possibility of connection in a random click or rotation mode [9].

Weaknesses: While this algorithm is provided with specific and specified photos, there will actually be a limited space to choose the password. In other words, as the researchers examining the algorithm have noted in their study, a numeric password is generated when each image represents a number of consecutive options. On the other hand, the selected sequences are shorter than the text passwords. One of the solutions offered to expand the password space created by using this solution is more complex and forgettable for users.

2.5. Story Algorithm

According to the Story algorithm, which was established in 2004, the user selects a set of photographs and is then tasked with identifying the required inventory from a collection of photos and images. These photographs depict locations, items, or people. To assess the users' ability, a series of nine photographs is supplied and the user is requested to choose four of them, while also providing a sequential component to aid with memory. The technology encourages that users construct a narrative to link their photographs and images [10]. According to the Monotheistic and Denominational Study (2009), users often forget their Story passwords and commit common blunders. Thus, in comparison to the validation of the Pass Face algorithm, the greatest shortcoming of this approach is the difficulty of recalling photographs.

3. PROPOSED METHOD

In this article, we propose a new model with high security for mobile. In this design, it consists of 6 dice, each dice containing 6 numbers from 1 to 6. Figure 1 shows the proposed scheme in this article. For example, suppose the suggested password is 1, 2, and 3, respectively. The user must move from dice to number 1 and swipe to dice number 2 and finally swipe to number 3.

Figure 1. proposed Cognitive graphical password

To set the password by the user, according to Figure 2, there are six dice with 6 numbers in front of the user. The user can select any combination of numbers from 1 to 6 and swipe in order. For example, suppose that the 1356 password is selected by the user and swipes from 1 to 3, then to 5, and finally to 6, respectively. This password is taken as a template in the publication. Figure 3 shows an example of entering the wrong password and two examples of the correct password.

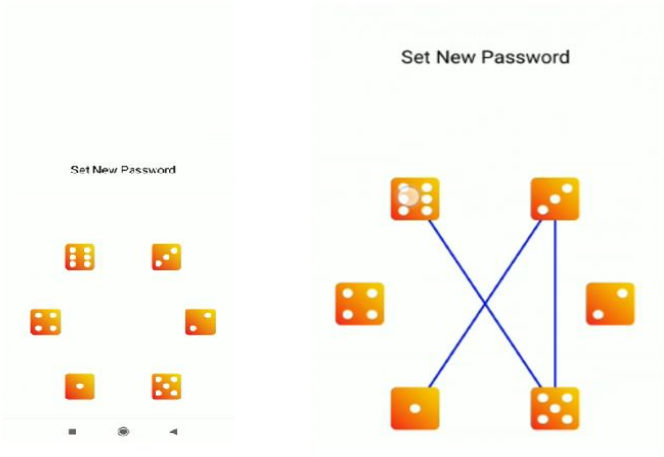

Figure 2. How to set a password in the proposed pattern

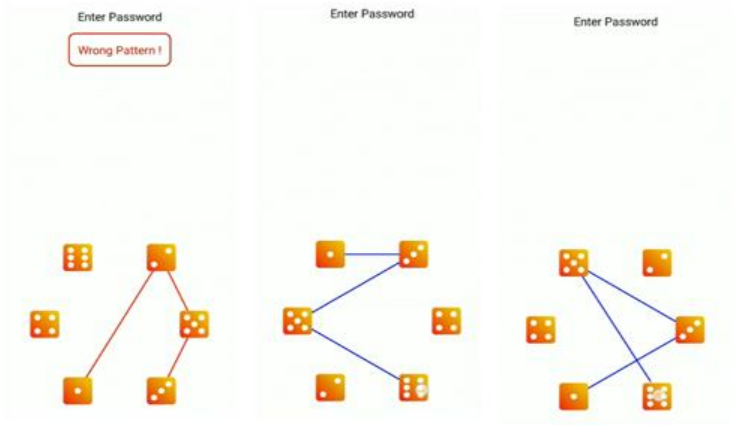

Figure 3. wrong and correct pattern

4. TESTING AND EVALUATION

The suggested system, a graphical password authentication mechanism, is assessed and tested by individuals who have used and tested it. Additionally, they will respond to questions in an online questionnaire designed to evaluate the system's usability qualities. The assessment plan that was created includes some information on the users. The participants are a group of 40 individuals, 15 of whom are female and 25 of whom are male. The participants were between the ages of 24 and 40.The participants were chosen as system users who accessed the system throughout the registration procedure and subsequently chose to connect. Finally, they answered to the online questionnaire's questions in order to provide a more detailed evaluation of the proposed system's usability qualities.

Participants tried to utilize the proposed authentication system by requesting the formation of a new user account and signing in after requesting the establishment of a new user account, as shown in the table below. As shown in the table below, the findings indicate that although all participants established their application accounts readily and without difficulty, they had divergent beliefs about how to connect to the system, as shown by their responses to the online questionnaire. The findings indicated that on the second day, 25 users successfully logged in on

their first try, 12 users successfully logged in on their second attempt, and just three users successfully logged in on their third attempt. On the third day, 20 users successfully logged in on their first try, 15 users received a success message on their second attempt, and 5 users successfully logged in on their third attempt. Table 1 contains all of the findings.

Table 1. Users trying to log in

	Create the user name and password			attempts to Enter the system		
	Attempt1	Attempt2	Attempt3	Attempt1	Attempt2	Attempt3
Day one-Creation	33	5	2	No need to enter the system		
Day2	No need for creation			25	12	3
Day3	No need for creation			20	15	5

Categories related to the structure of the questionnaire

Questionnaire review is the selected method, or in other words, the selected tool to verify the claims (objectives) of the research in terms of improving the usability characteristics of the graphic coding authentication system. 21 questions in 8 categories, which included some questions about the general information of users and the prototype of the system, as well as the usability features of the proposed system, formed the questionnaire form. The designed questionnaire, which included 21 questions in 8 different categories, can be seen in Appendix A.

1- General information
2. User comments
3. Evaluate the whole system
4. Evaluate the ease of use of the feature
5. Evaluate the simplicity of feature creation
6. Evaluate the simplicity of remembering a feature
7. Assess the simplicity of feature learning
8. Evaluate the outline

Finally, after analyzing all the answers, it is possible to realize that most of the system users have favorable feedback on all the usability features of the proposed method and also in evaluating the whole prototype of the system. All results are presented in Table 2.

Table 2. Results of the questionnaire analysis

Categories	Percentage
Evaluation of whole system	79.75 %
Easy to use	86.66 %
Easy to create	74.5 %
Easy to memorize	85 %
Easy to learn	81 %
Screen design	74.5 %

CONCLUSION

Based on the results in Table 2, this questionnaire explained that most users in general expressed their satisfaction with the usability features proposed in the proposed method and also with the whole prototype of the system as well as the visual design and outline. Have . The evaluation of the whole graphic password method had a percentage of 79.75%, which is very desirable, and it was determined that the system is generally acceptable to the participants in the dissertation testing and evaluation.

There was a variety of percentages between 74.5% to 86.66% in the usability characteristics of the proposed system. The highest percentage, which is equal to 86.66, is related to the simplicity of using the feature, which shows that the participants are satisfied with the simplicity of evaluating the system. The simplicity of creating a graphic password in the proposed design was 74.5%, so this favorable percentage showed that users created their password easily without any difficulty. Remembering the chosen password Despite 85% positive feedback showed that users can easily remember their passwords, due to the special features used in the design of this proposed design. 81% is related to the percentage of ease of learning the system, so this part of the questionnaire shows how easy it is to learn to use this system. The visual design of the proposed design and its overall design showed good results despite a positive feedback of 74.5%.

REFERENCES

[1] S. Komanduri and D. R. Hutchings, "Order and entropy in picture passwords," in Proceedings of graphics interface 2008, 2008, pp. 115-122.
[2] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in Cyberworlds (CW), 2010 International Conference on, 2010, pp. 194-199.
[3] H. L. Arash, A. Abdul Manaf, and M. Masrom, "Security evaluation for graphical password," 2011.
[4] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: applying recognition to textual passwords," in Proceedings of the Eighth Symposium on Usable Privacy and Security, 2012, p. 8.
[5] Z. Erlich and M. Zviran, "Authentication methods for computer systems security, "Encyclopedia of information science and technology 2nd ed, vol. 1, pp. 288-293, 2009.
[6] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords? A field trial investigation," in People and Computers XIV—Usability or Else!, ed: Springer, 2000, pp. 405-424.
[7] R. Dhamija and A. Perrig, " D´ej`a Vu: a user study using images for authentication," presented at the Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, Denver, Colorado, 2000.
[8] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, an electronic Bulletin for undergraduate research, vol. 4, p. 2002, 2002.
[9] W. Jansen, "Authenticating mobile device users through image selection," The Internet Society: Advances in Learning, Commerce and Security, vol. 1, pp. 183-194, 2004.
[10] D. Davis, F. Monrose, and M. K. Reiter, "On User Choice in Graphical Password Schemes," in USENIX Security Symposium, 2004, pp. 11-11.