March-April 2020
ISSN: 0193-4120 Page No. 1420 - 1425

Change Images Password "CIP" System: A New Graphical Authentication Method

Sabah Al-Qassas[1], Wadee Al-Halabi[2], Nighat Mir[3]
[1,2,3]College of Engineering, EFFAT University, AnNazlah Al Yamaniyyah, Jeddah 22332, Saudi Arabia
[1]selqassas@effatuniversity.edu.sa, [2]walhalabi@effatuniversity.edu.sa, [3]nmir@effatuniversity.edu.sa

Article Info
Volume 83
Page Number: 1420 - 1425
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 14 March 2020*

Abstract
Alphanumeric Password is the most common authentication method for computer users. It is well known that people normally tend to choose passwords that are hard to forget and easy to remember. Moreover, they neglect the fact that passwords should be random, hard to be guessed and frequently changing. Also, passwords should not be written down or stored in a text and sent through unsecure channels. One such improvement that has been taken towards passwords is to have graphical passwords that are based on pictures rather than alphanumeric characters. Many graphical password schemas have been developed to solve the mentioned password problems. However and after the research that we have done here; none of them has managed to solve them all. In this paper we present our graphical password schema as a solution for all users' passwords problems in satisfying the requirements of having very secure password. In addition, our graphical password schema will provide the usability, reliability and availability of the user passwords. Our users will not be worry about forgetting their passwords or change them over the time. That because our passwords are easy to re-member and hard to guess and break or steal by others. Moreover, our developed pass-word schema is resistance for all kind of attacks such as brut fore, shoulder surfing and guessing attack.

Keywords**:** *Password; alphanumeric; system; CIP*

1. Introduction

As we are in the digital age, the need of security becomes one of the most important computer user's issues. That is because of the vast and widely usage of computers and networked computer systems [1]. The user uses the computer and the networks in variety of applications, logging into ac-counts, sharing and transferring different kind of data. This will require the users to secure and protect their accounts and their multiple actions. Control accesses mechanisms are used to fulfill this purpose [1]. These mechanisms work to either grant or revoke the right to access some data or per-forming some actions. Authentication methods are one of those accessibility controls. They are mostly categorized into three main categories: Biometrics-based, Token-based and knowledge-based. The first category uses physiological or behavioral characteristic to identify the user such as the user figure print, face or voice. The second one is like bank cards, key cards and PIN numbers. Knowledge-based authentication is a method that uses knowledge provided by the users to be authenticated. It has been agreed that this category is the most widely used [2]. It is generally classified into text-based and graphical-based authentications methods. Text-based authentication mechanism is considered to be the most common mechanism that has been used [3]. It only deals with alphanumeric characteristics. However, this mechanism risks the user security by having easy and short passwords. Users are commonly chose passwords which are easy to remember as well as easy to be guessed by attackers [4]. On the other side, if the user chose complex and hard passwords; unfortunately the password will be forgotten by the user due to human memory limitations [5]. Some psychological studies assumed that humans can remember pictures better than characters in which a pictures worth thousands of passwords [6].Graphical passwords schemas have been proposed to be as an alternative to text-based passwords [7]. That is to provide the most optimal secure methods and schemas for users [8]. Generally, these methods should meet the user's security requirements in any security system: Ease of use, Memorability, Effectiveness and Satisfactions as those are determined by the password features [9].

Graphical passwords have been proposed and designed to overcome the known weakness of traditional alphanumeric passwords in which user passwords become

March-April 2020
ISSN: 0193-4120 Page No. 1420 - 1425

memorable, easy to use and more secure [7,10]. Many schemas were suggested and developed to be one of the methods for graphical authentication –graphical passwords [7,11]]. All of these schemas came up to satisfy the user needs in having a secure, usable, available and reliable password. Not all of the suggested schemas managed to combine all of these features together but at least they got to have some of them to produce good graphical passwords. Security and usability were observed to be the two most important features that the users need [12] However, the remaining two features are still important too as it is good to have them all as possible. In general, graphical pass-words schemas have been commonly introduced to be either Recall-based schemas or Recognition-based schemas [10,12,13].

Thus in this work, a graphical based password schema is developed to enhance the security, usability, availability and reliability for users. It is an effective and innovative way to authenticate the user and create changeable passwords easily identified and known by the user because of the use of users be-longs pictures that can't be forgotten, written down or even stolen neither broken.

2. Design

2.1 CIP Data flow

Figure 1 shows the overview of the hall process of our graphical authentication method. The user has two options: either to login or sign in. if the user is a new user he should sign in and register in the system by providing a valid username, some required personal information and a folder of his belongs images. All the entered data are going to be encrypted and saved in the user database. The user now has to login. By logging in, the system will make sure of the validity of the username. Then a grid of images will be shown to the user one after another. Then the user is going to be authenticated or denied according to his selection.

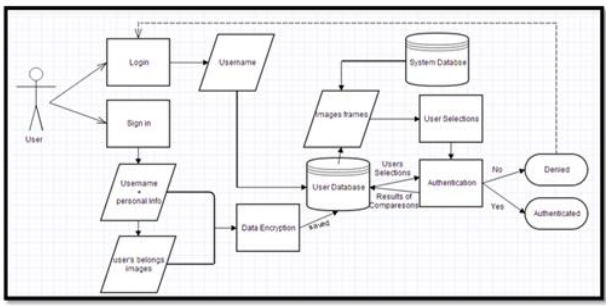

Figure 1: CIP data flow diagram

Figure 2 shows the CIP flowchart. The flow of the chart is explained as following sequences. Start A user interface will be shown to the user. If the user is a new user, then the user must sign in to be able to login later Else, the user can login by entering the username and then selects all his belongs images If the entered username and all the selected images are correct, the system will authorize the user and let him view his account. Else the user will be denied and redirected to the first interface. End

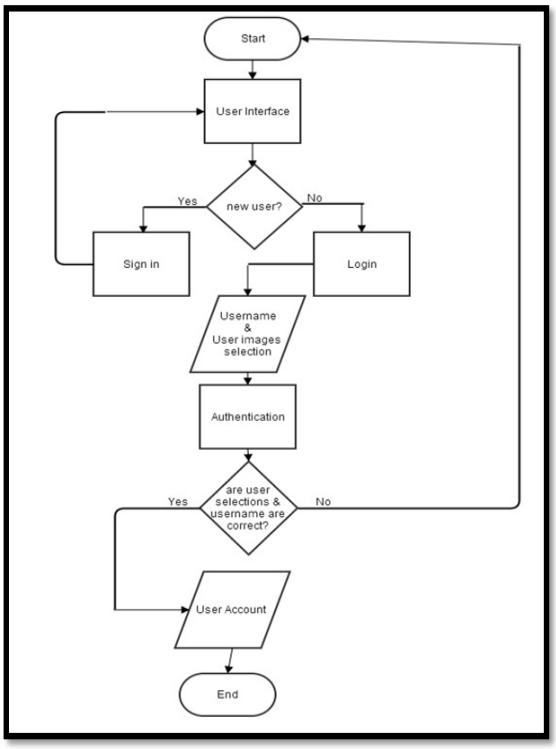

Figure 2: CIP Flowchart

Use cases are used in the system design to define the interactions between an actor on a system and the system itself, to achieve a goal. In this paper we have defined three main use cases to make the idea clearer. For user case 1, the flow is done as shown in Table 1. For user case 2, the flow is shown in Table 2. For user case 3, the flow is shown in Table 3.

Table 1: Use case 1: Sign in

Function Name	Sign in
Actors	New user and System
Input	Username, user belongs images folder, personal info
Output	Registered user
Description	By clicking on the sign in button; a new user is able to register in the system by providing a valid username and images folder with some required personal info. After that the user will be able to login to the system and view his account.
Expectation	**Uploading 22 images (minimum)** Registering with a unique username that never exists before

Table 2: Use case 2: Login

March-April 2020
ISSN: 0193-4120 Page No. 1420 - 1425

Function Name	Login
Actors	Registered user and System
Input	Username and selected images
Output	User Authenticated or user denied
Description	By clinking on the login button; the registered user has to enter the username and able to see the grid of images created by the system. Then, the user is going to click on the identified images that appear on all the viewed frames.
Expectation	Entering a right user name Selecting all user belong images that the user have uploaded during the registration phase.

Table 3: Use case 3: User image selection

Function Name	User image selection
Actors	Registered user and system
Input	Click events
Output	User Authenticated or user denied
Description	The user is going to click on all viewed belongs images.
Expectation	The user may click on only one image in a frame The user may click on more than one image in a frame The user may not click on any image in a frame

2.2 CIP Architectural design

The CIP architectural design consist of two data based which area system database and user database. One is to save the user information (username and images folder) as the other database is going to be use to save all the random distracter images.

2.3 CIP System Prototype

In this work, the authors used the Windows Application in Visual Studio 2010 to design and implement the prototype. The developed prototype has following components.1. System images: a set of random – distracter- images. 2. System database that store the system images. 3. A database that stores all the users belongs images along with their usernames. Table 4 shows the CIP tools used for this prototype development

Table 4: CIP Tools

Operating system	Windows xp/7
Browser	Internet Explorer, Google Chrome
Tools	Visual studio professional 2010
Language tools	ASP.NET , C# , CSS, JavaScript
Database language	SQL
Cryptography	Rijndael Cipher
Supporting tools	Gliffy

2.4 Database

CIP is dealing with a database to store users' data. All the registered users' data are stored in "DatabaseUSER.mdf" database file in visual studio 2010. This data-base has only one table "Registered Users". Data string connection contains a collection of parameters to establish the connection with the database through the applications. To provide more security to CIP system, a Rijndael Cipher has been used to en-crypt some data in the database. The encryption has been applied on the most important columns in the database which are: username and path name of the user images. The encryption and decryption code has been written in a separated class in c# language in which the methods of encryption and decryption are called whenever they are needed. The system will show up random number of frames and pictures each time the user logs in. The minimum number of the system's frames should be not less than 7 frames and the maximum is 12.

2.5 The Pseudo-code of Authentication Method Algorithm

The pseudo code of the authentication method algorithm used in this work is stated as follow.
Start
Enter username
Username validation
If username is not valid; then show error message "invalid username"
If username is valid; then direct the user to the password page
If "Start" button is clicked: "numberOfTotalFrames" random number will be generated
When the page is loaded
Start
RandomPlacesIndex random number is generated to be from 1 to 12
RandomPlacesIndex is assigned to each imageButton
"numberOfAllImages" integer random numbers is generated to be from 1-12
"numberOfRandomImages" integer random numbers is generated to be from 5 -12
"numberOfUserImages" integer random numbers is generated to be from
1- numberOfRandomImages
If statements to prevent the duplication of "numberOfRandomImages" selected
If statements to prevent the duplication of "numberOfUserImages" selected
Finish function () to check if numberOfFrames== numberOfTotalFrames
End

March-April 2020
ISSN: 0193-4120 Page No. 1420 - 1425

If Next button is clicked_
Start
Increment "numberOfFrames"
Loop to select and assign random images to images buttons according to "num-berOfRandomImages"
Loop to select and assign user random images to images buttons according to "numberOfUserImages"and assign user images names to a system string "a" array
End

Figure 3 and Figure 4 shows the pseudo code of the authentication method.

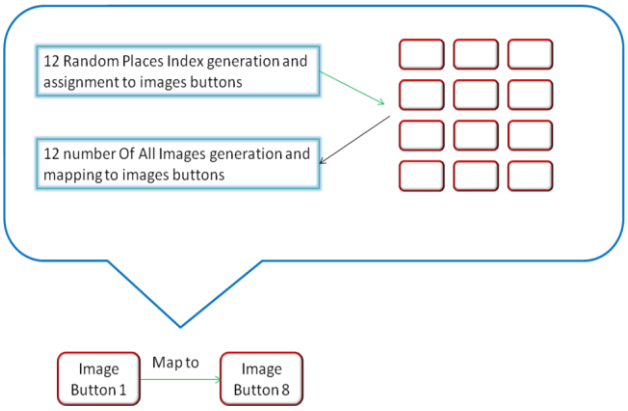

Figure 3: Pseudo code of the authentication method

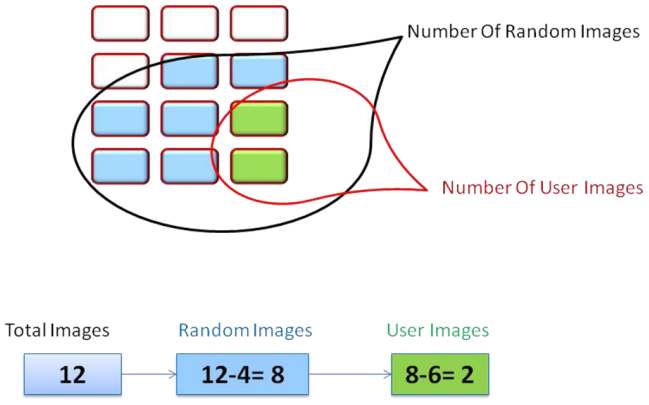

Figure 4: Pseudo code of the authentication method

2.6 Web Forms

CIP consists of four main web form pages which are: Home page, Registration page, username login page and password login page. The Home page is a page where the user can read some information and take a general idea about CIP. It also has an option to direct the user to register in the system. Figure 5 shows the CIP Home page.

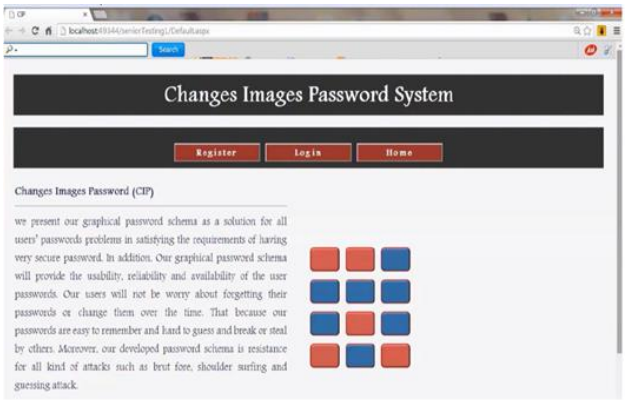

Figure 5: CIP Home Page

2.7 System Design (Master page & CSS)

ASP.NET master page and CSS allow the creation of a consistent layout for the pages in the system. A single master page was used and defined a CSS file to be applied on the system.

2.8 System's main events and functions:

All the web forms created have two files: HTML with ASP.NET markup file and C# code behind file. The first is to handle the client side events as the second is to handle the server side controllers. Because we were using ASP.NET many ASP controllers have been used in the project such as: buttons, image buttons, update panel, grid view, textboxes and labels. Some of these controllers carry a code be-hind. As well as, the project main events were: buttons clicks and page loads. In addition some user defined functions were very important to use such as: finished, encryption and decryption functions. The following lines will show in details the most important functions, part of codes and events in CIP System.

3. Testing and Validation

The developed system has been tested. The testing methods were

1. **Unit Testing:** all the pages of the system have been tested in separate case to make sure that the code of the page is working well and effecting the others.
2. **Functionality Testing:** all the functionalities of the system are working as it was expected.
3. **GUI Testing:** all the graphical user interface in all pages was tested and all the results were as required.
4. **System Integration Testing:** all different parts of the system was able to communicate with each other.

Figure 6 shows the screenshot of the testing output.

March-April 2020
ISSN: 0193-4120 Page No. 1420 - 1425

Figure 6: Successful Authenticating Result testing

4. Data Collection and User Evaluation

The study was conducted after the system full implementation and testing. We had 20 participants. The participants had to listen to an introductory session on CIP system and how they can use it. After that the participants are allowed to use the system by registering and logging in. A total of 17 were females from Effat University not majoring computer science. As 3 of the participants were males individuals. The age of all participants was between 20- 28. The purpose of the study was to:

1. Evaluate the usability of the scheme if deployed in a real environment.
2. Evaluate the user interactions and number of wrong logging in

Table 5 summarizes the result of data collection. Based on Table 2, it was observed that only 30% had a previous experience with graphical password. 90% of the participant had a successful login from first try. In addition, 100% output was shown for image remembrance. Finally, 80% of the participants have stated the desire to reuse the system again and 20 % has stated not to reuse this image type password identification.

Table 5: Results of Data Collection

No. Of Participants	20
Experience with graphical passwords	30%
Successful login from first try	90%
Remembered all images	100%
Likes to use the system again	80%

5. Conclusion

This study has proposed a patent idea for a graphical password schema that solves user passwords problems. The proposed password system has combined all the password requirements: security, usability, reliability and availability. We have managed to enlarge the password space in which any simple try of breaking our password will take huge time due to its huge probability. We also have managed to randomize the process of showing and selecting the images by having all the system elements as variables changing in each log in time. By doing this we are going to get new and changeable password for each process. In the same time; it becomes easier for the user to re-member his password (images) because these images are related to the user as they are impossible to be forgotten. By implementing this idea we are protecting the user and providing a very high secure solution for him. We manage to introduce a novel and original method of using Graphical password that we are sure, it will never be forgotten, and can never be copied. We offered a totally new method of implementing a high secured way of using graphical password, which can join all different method of passwords. Different applications may find our method is more convenient for them. Our proposed solution will create transparency or system independence which is one of the most important non-functional requirements of modern information systems.

References

[1] Gelbstein, E., & Kamal, A. (2002). *Information insecurity: a survival guide to the uncharted territories of cyber-threats and cyber-security* (Vol. 1). United Nations Publications.

[2] Rabkin, A. (2008, July). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In *Proceedings of the 4th symposium on Usable privacy and security* (pp. 13-23). ACM.

[3] Feng, D., & Lin, D. (2005). Information Security and Cryptology: First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings (Vol. 3822). Springer Science & Business Media.

[4] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553-567). IEEE.

[5] Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., ... & Egelman, S. (2011, May). Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). ACM.

[6] Stobert, E., & Biddle, R. (2013, July). Memory retrieval and graphical passwords. In *Proceedings of the ninth symposium on usable privacy and security* (p. 15). ACM.

[7] Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 19.

[8] Hu, W., Wu, X., & Wei, G. (2010, October). The security analysis of graphical passwords. In *2010 International Conference on Communications and Intelligence Information Security* (pp. 200-203). IEEE.

[9] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 1-12). ACM.

[10] Eljetlawi, A. M., & Ithnin, N. (2008, November). Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on* (Vol. 2, pp. 1137-1143). IEEE.

[11] Andriotis, P., Tryfonas, T., & Oikonomou, G. (2014, June). Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 115-126). Springer, Cham.

[12] Sarohi, H. K., & Khan, F. U. (2013). Graphical password authentication schemes: current status and key issues. *International Journal Of Computer Science Issues (IJCSI)*, *10*(2 Part 1), 437.

[13] Hussain, A., Razak, H. A., & Mkpojiogu, E. O. C. (2017). The perceived usability of automated testing tools for mobile applications. *Journal of Engineering Science and Technology*, *12*(Special Is), 89–97.

[14] D.K. Jayaram (2019). Hyper-Mino Spectral Efficiency Augmentation Techniques in 5G. *IIRJET*, 4(4), EC-04-EC-09.