MULTIPLE GRID BASED GRAPHICAL TEXT PASSWORD AUTHENTICATION

Vinothini T[1], Rajesh I[2], Kirupa Rani D[3]

[1]PG Scholar, Dept of CSE, Knowledge Institute of Technology, Salem, Tamil Nadu, India
[2]Associate Professor, Dept of CSE, Knowledge Institute of Technology, Salem, Tamil Nadu, India
[3]PG Scholar, Dept of CSE, Knowledge Institute of Technology, Salem, Tamil Nadu, India

Abstract

The system and network security is strengthened by passwords, which is a significant part of an Authentication process. Most commonly an Authentication method using either alpha-numeric password or Graphical password, which has crucial drawbacks like dictionary attacks and shoulder-surfing. The Grid based Graphical Text password Authentication have been emerged as an alternative solutions to overcome the potential vulnerabilities due to conventional schemes. Additionally, originating the "Grid Systemization and Text Enlargement Technique" for classifying a preferred theme Image. By clicking the grid on that theme Image it enlarges a next sequence of password. This method depends on "Image-Image-Alphanumeric password" and the successive mien relies on prior option. This scheme has been acquiring prominence, because of its integrity and security as well as the Grid Systemization and Text Enlargement Technique.

Keywords: *Grid Systemization & Text Enlargement Technique, Image-Image-Alphanumeric.*

---***---

1. INTRODUCTION

Since most of the system uses alphanumeric passwords for Authentication process. However, it is well familiar that the Text passwords are insecure for kind of reason. For example, dictionary attack due to choosing simple passwords in favor of prominence, easy to guess, phishing. Similarly, Graphical passwords also has few drawbacks like 1) Authentication can be guessed and succeed when the system holds too few Images. 2) shoulder surfing[1][4].

In this project work, Image-Image-alphanumeric method has been introduced to reduces all those existing drawbacks. Because, proposed scheme depends not only alpha numeric but also Graphical passwords. When user uses Graphical-Text Authentication method, users tend to choose Image password for two steps and they must also enter a Text password as final confirmation.

The main contribution of this method is to increase security and reduce the size of an Image dataset to store Images. Grid based Graphical - Text password is more efficient than other existing systems because, it ensures 2-way security (Image-Text), Images used for Authentication are classified into many grids and also it will not be suffered by dictionary attacks. The rest of this work is formulated as follows. Section II Summarizes the most recent research addressing the Graphical password system. Our proposed system and the functioning principle of grid classification techniques are presented in section III. Further enhancement and conclusion will be discussed in section IV.

2. RELATED WORK

Nowadays, Text passwords are commonly used for most of the Authentication process. In this, user has to enter their name and password. Similarly, while using Graphical passwords user has to select their name and enter an Images instead of entering Text. Graphical password schemes can be motivated by the fact that, humans can easily remember pictures than alpha-numeric; psychological studies are also proved the reality. The steps involved in Graphical password Authentication,
Step 1: On logging, user has to enter his/her name that is used when our enrollment.
Step 2: The user has to click on the particular Image, which they are preferred as a password during enrollment.
Step 3: The consequence of the click has to be the same as the user click during enrollment.
Step 4: The succession of click is acclaimed and checked with the existing dataset.
Step 5: The user is authenticated, if they enter correct Password.
Step 6: If not authenticated, the user has to inquire their Authentication process recurrently.

The Graphical password scheme has been divide into three categories. 1) Recall based scheme 2) Recognition based scheme 3) CCP (Cued-recall) method.

2.1 Recall Method

In Recall base technique, user know something. The System and the user share a confidential. User must recall and enter their password correctly to authenticate themselves into system or an application. Several methods are developed by using this technique.

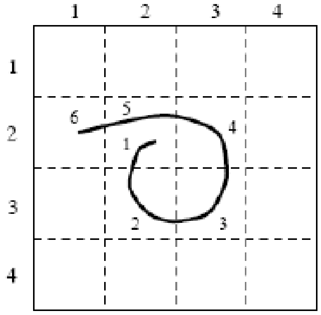


Fig -1: DAS

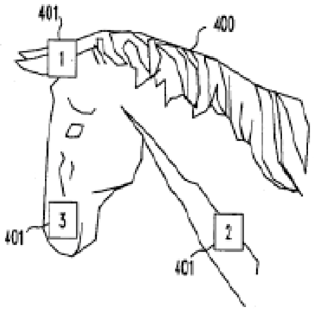


Fig -2: Blonder algorithm

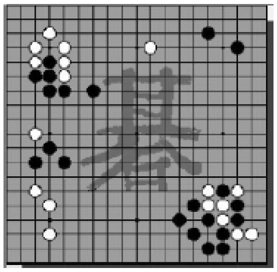


Fig -3: Pass-Go

Fig -4: Pass Doodle

2.1.1 Draw-A-Secret (DAS):

By using the mouse, users draw their password on a 2D grid. The password is composed of the grid cells that the user passes through while drawing. A drawing can contain either one continuous stroke or several strokes.

2.1.2 Blonder Algorithm:

In this algorithm, user should click several locations on that particular Image to select their password. During Authentication, the user must click those particular locations of an Image ,that is selected when their sign-up process

2.1.3 Pass-Go:

User draw their password on a grid, except that the intersections are used instead of grid squares. Visually, the user's movements are snapped to grid-lines and intersections so that the drawing is not impacted by small variations in the trace.

2.1.4 Pass Doodle:

Without using a visible grid, user has to create a freehand drawing as a watchword. The purpose of additional characteristics such as pen color, number of pen strokes, and drawing speed are suggested by the originator to add volatility to the scribble.

2.2 Recognition Method

Recognition methods are something, in which user recognize. Similarly, the user and the system share a secret. Cues are provided by the system and the user must recognize the secret. Anyone capable to perceive the secret will be able to authenticate as the primordial user. Graphical passwords where users must perceive pre-selected Images from a set of decoys decline d into this kind of group. Several methods emerged as follows,

2.2.1 Dhamija and Perrig Algorithm:

user will be asked to select certain number of Images from a set of random pictures generated by a program. Further, user will be required to diagnose the pre-selected Images to be authenticated.

2.2.2 Sobrado and Birget Algorithm:

This technique that overcome the shoulder surfing attacks. In their first method which they named ”triangle scheme”, a user needs to prefer their pass-object among many displayed object. To be authenticated, a user recommended to recognize all the pre-selected pass-object which was selected during the enrollment phase. The user requires to click inside the convex-hull which formed by the pass-object.

2.2.3 Man Algorithm:

A user selects a number of pictures as pass-images. Each pass image has several variants and each variant is assigned a unique code. During Authentication, the user is provoked with several scenes. Each scheme holds several pass-objects and many decoy-objects.

2.2.4 Jansen Algorithm:

For the password creation, a user has to select the theme first which consists of thumbnail Images. Eventually, a user has to selects and registers a sequence of the selected thumbnail photo to form password.

2.2.5 Passface Algorithm:

Based on the assumption that human can recall human faces easier than other pictures. User are requires to select the previously seen human face picture from a grid of nine faces which one of the face is the known face and the rest is the decoy faces.

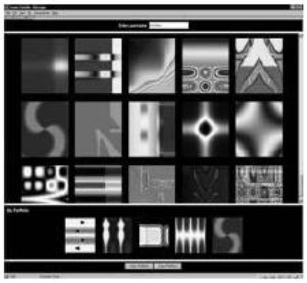


Fig -5: Dhamija and Perrig Algorithm

Fig -6: Sobrado and Birget Algorithm

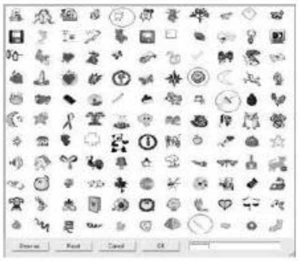


Fig -7: Man Algorithm

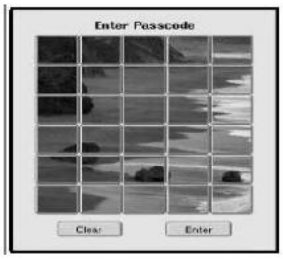


Fig-8: Jansen Algorithm

Fig -9: Passface Algorithm

2.3 Cued Recall

Cued-recall is combination of recall and recognition scheme. Thus it is more secured than other methods. In cued-recall systems, the system provides a cue to help trigger the user's memory of the password. Several method developed are,

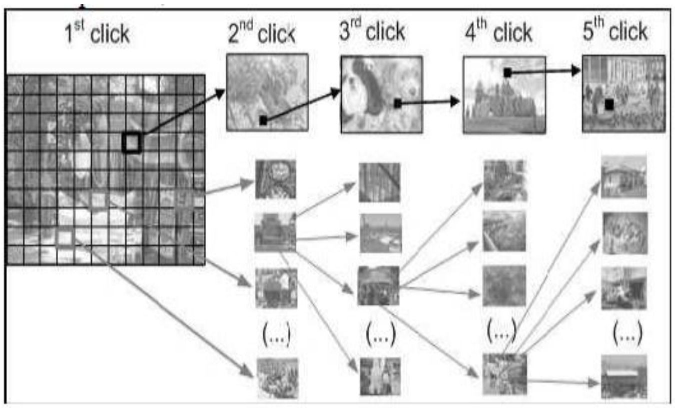


Fig -10: Cued Click Points (CCP)

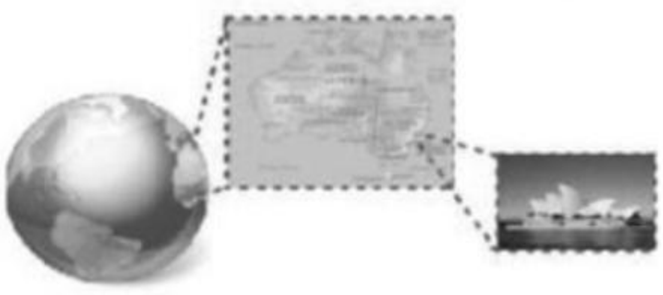


Fig -11: Implicit Password Authentication (IPA)

2.3.1 Cued Click Points (CCP):

A password comprise of one click-point per Image for a sequences of Images [4]. The succeeding Image advertised is based on the previous click-point so users can obtain immediate implicit criticism as to whether they are on the correct path when logging in.

2.3.2 Click Button According to Figures in Grid (CBAFG):

In this multiple background Images is adopted. On registration user is presented with four background Image. User should choose one or more Image from four background Image. User should choose one or more Image from four background Image.

The “n” pass-Image is displayed in turn for the user to select several cells as password by clicking the Image. After selection user choose an icon from ten icon display as starting icon. During Authentication there will be 4 background Images. If the icon is not user starting icon then user has to click any numeric button randomly and icon will change on each click. When starting icon appears user can enter password by clicking each cell.

2.3.3 Implicit Password Authentication (IPA):

This is applied in mobile banking. The bank dataset will have 100 to 200 standard questions. On registrations the user has to pick 10-20 questions from dataset and provide answer to the selected question. For each question server create an intelligent Authentication space using Image.

The answer to the question will be embedded into Image. On Authentication, the server picks one or more questions selected by user on registration time randomly .the user need to navigate the Image and click the right answer[8].

Enter the word

Fig -12: Single zoom mouse click graphical password

2.3.4 Single Zoom Mouse Click Graphical Password:

It has some features of cued recall scheme, Dhamija and Perrig scheme (recall method) and alphabetic dictionary scheme. Alphabetic dictionary add security to Authentication. In this the user has to assign an alphabet to each Image in theme Image (enlarged Image). For that selected alphabet the use has to maintain a set of word starting with the alphabet [1].

3. OUR SCHEME

In cued recall method there are sequence of Image enlargement and by clicking on that Image it contains “n” number of Images for each user [5]. Our proposed scheme has special feature that it uses multiple grid classification technique to classify a single theme Image and it uses 2 way security (Image-Alphanumeric) for its Authentication.

In our proposed system, Graphical-Text Authentication is done in the basis of Image-Image-alphanumeric. There are 3 steps to be considered for their Authentication.
1) The user has to select one Image as a theme Image. The theme Image will be classified into many number of grids using “Grid Systemization Technique”. By Clicking, any grid on that pre-selected theme Image, it enlarges another theme Image depend upon our pre-selection.
2) For every grid on that first theme Image, we are setting individual theme Image for its enlargement. An Image that is enlarged at second, also classified into multiple grids.
3) By clicking the grid of second theme Image, it enlarges an Input Text box containing “Enter Password”. This box shows that we should enter our Text password that is used when our registration.

Selection of one root path from multiple paths make this method as an efficient. Finally, the user can be authenticated When they will select Graphical as well as Text passwords correctly. Let us evaluate the Graphical- Text Authentication in the basis of three steps(Image-Image- Alphanumeric).

A Figure III represents that, a single theme Image can be used for an entire system of process and it uses Grid Systemization and Text Enlargement Technique. The system can be implemented using the following five stages. 1. User registration process 2. Picture selection process 3. Grid systemization of picture 4.Login process 5. Final Authentication

3.1. User Registration Process

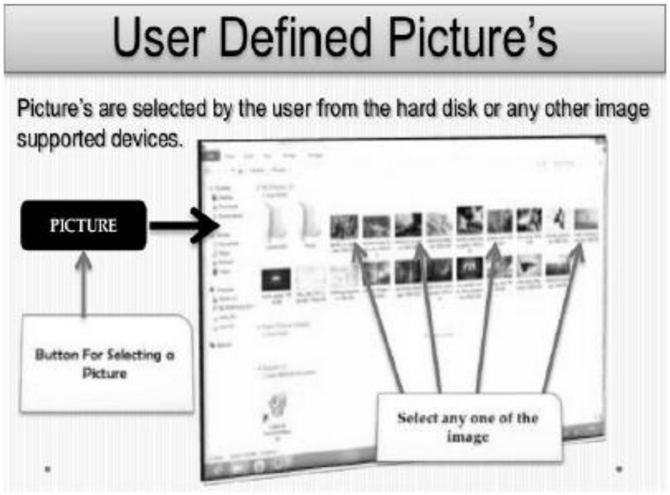
During registration process user has to provide their username and they should specify their passwords for entering into the system. Password is the sequence of 3 steps. Our system uses Image-Image-Alphanumeric category as password. During login process user should enter the specific sequence of password to enter into the system. It includes,

- Entering username
- Setting password sequence

3.2. Picture Selection Process

During picture selection process, picture for password is selected for next sequence of modules. There are two types of picture selection.

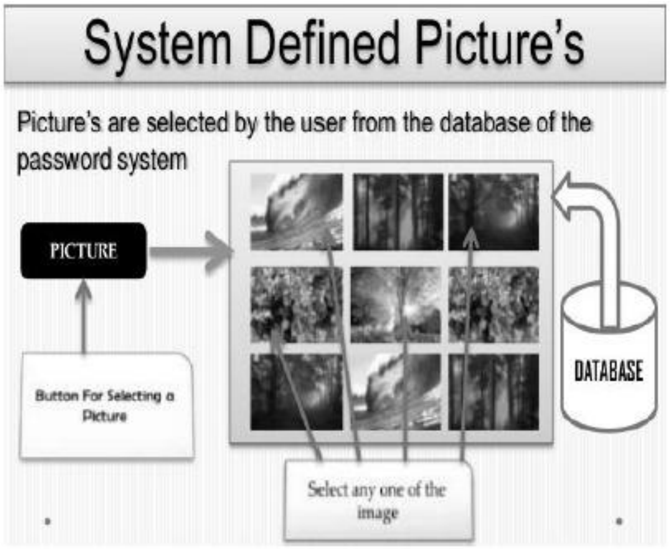
3.2.1 User Defined Picture


User Defined Picture’s

Picture’s are selected by the user from the hard disk or any other image supported devices.

Fig -13: User Defined Picture

3.2.2 System Defined Picture



System Defined Picture's

Picture's are selected by the user from the database of the password system

PICTURE

Button For Selecting a Picture

Select any one of the image

DATABASE

Fig -14: System Defined Picture

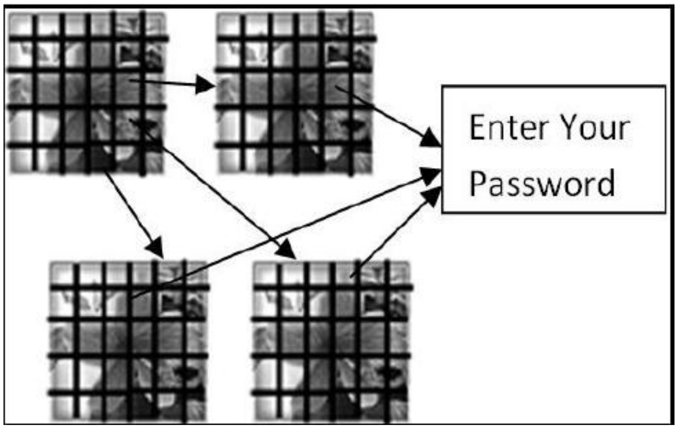


Fig -15: Multiple Grid Based Graphical Text Password Authentication

3.3. Grid Systemization of Picture

Picture can be classified into multiple grids using grid systemization technique. It includes,

- Setting clickpoint's of grid as password
- Picture enlargement
- Text enlargement

3.4. Login Process

Login process includes 3 steps authentication (Image-Image-Text). User should visit their sequence of steps for logging into the system. It includes,

- Username selection
- Grid selection from pictures
- Text selection

3.5. Authentication Process

Final authentication process includes verification of 3 steps passwords. If the user enters their 3 steps of passwords in a correct manner then they are allowed or authenticated into a system.

4. RESULTS AND DISCUSSION

In this project work, both graphical and text passwords has been used to provide better security and also graphical passwords are used in terms of multiple grids instead of using simple images. Using Grid Systemization & Text Enlargement Technique, images are classified into 5x5 grids. User has to select one grid among 25 grids. It improves the performance by providing 3 levels of authentication. The three levels are Image-Image Alphanumeric. If the user selects the wrong sequence in any of the three levels of authentication, the system will not enter into the application. So, this project work improves the performance and increases the security compared to existing methods. Using Visual C# .Net, this project is implemented and executed. The results of this work improves the performance and security.

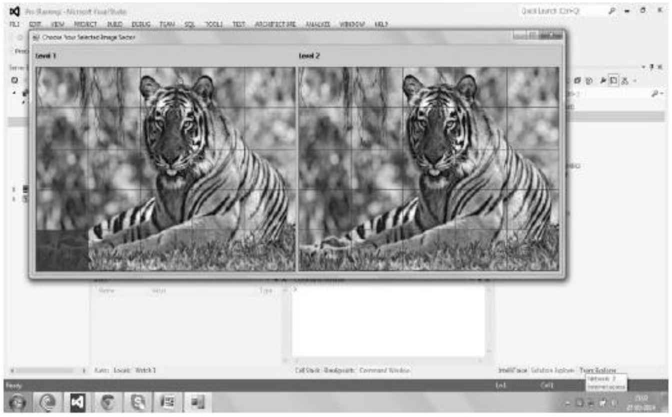
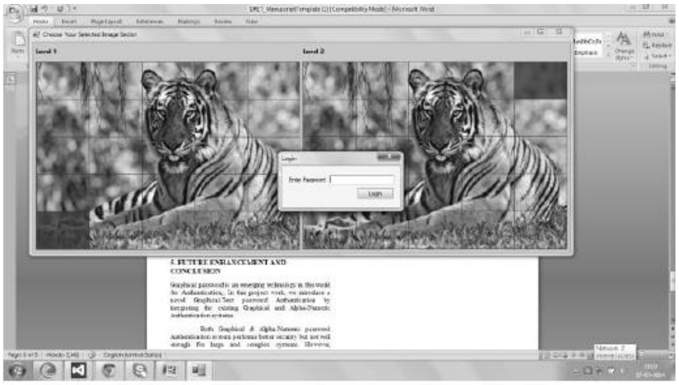


Fig -16: Selecting grids from level 1



4. FUTURE ENHANCEMENT AND CONCLUSION

Fig -17: Selecting grids from level 2 and entering Text Password

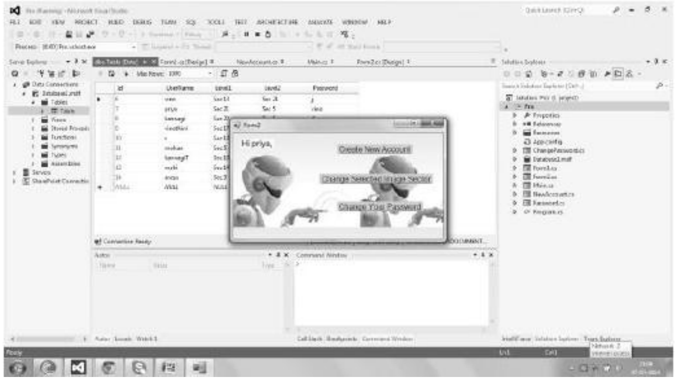

Hi priya,

Fig -18: User Authentication Successful

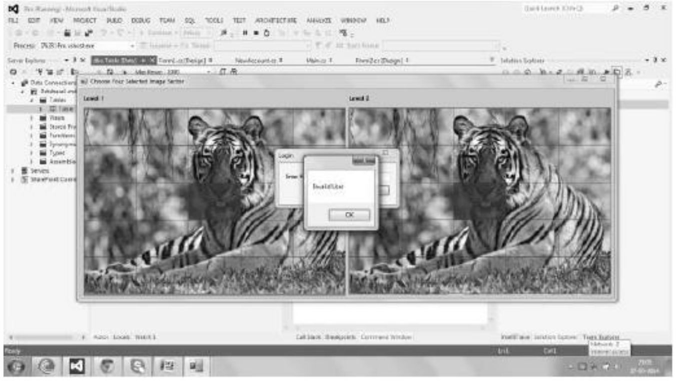

Choose Your Selected Image Sector
InvalidUser

Fig -19: Invalid user because of wrong selection of password sequences

5. FUTURE ENHANCEMENT AND CONCLUSION

Graphical password is an emerging technology in this world for Authentication.. In this project work, we introduce a novel Graphical-Text password Authentication by integrating the existing Graphical and Alpha-Numeric Authentication systems.

Both Graphical & Alpha-Numeric password Authentication system performs better security but not well enough for large and complex systems. However, Graphical/Text Authentication has many drawbacks like dictionary attacks, shoulder surfing & phishing. Therefore, we try to integrate the features present in the Graphical as well as Text password Authentication. This can be achieved with the help of Grid classification technique and it also adapted to these extended applications

REFERENCES

[1]. Merin Sebastiian, Biju Abraham Narayamparambil, "A New Approach For Instigating Security Using single Zoom Mouse Click Graphical Password" International Journal of Communication Network Security ISSN:2231-1882, Volume-1,Issue-4,2012.

[2]. P.Golle and D.Wagner, "Cryptanalysis of a Cognitive Authentication Schemes", IEEE Symposium on Security Conference.

[3]. S.Wiedenbeck, J.Waters, J.C.Birget, A.Brodskiy and N.Menon, "Authentication using Graphical passwords: Basic results", Human-Computer Interaction International(HCII 2005),Las Vegas,NV,2005.

[4]. Sonia Chiasson, P.C.Van Oorschot and Robert Biddle, "Graphical password Authentication using cued click points",12th European Symposium On Research In Computer Security(ESORICS),2007.

[5]. Jinhua Qiu, Xiyang Liu, Licheng Ma, Haichang Gao and Zhongjie Ren,"A Novel Cued-recall Graphical password Scheme", International Conference on Image and Graphics page949-956, Washington,2011

[6]. G.S.Owen, X.Suo and Y.Zhu,"Grphical passwords: A Survey", in Computer Security Applications Conference,21st annual,5-9Dec,2005.

[7]. Haichang Gao,Xiyang Liu,Sidong Wang,Honggang Liu and Ruyi Dai,"Design and Analysis of a Graphical password scheme", International conference on Innovative Computing Information and Control ICICIC,2009.

[8]. Sadiq Almuairti and Parakash Veeraraghavan, "IPAS:Implicit Password Authentication Systems", in workshop of International Conference on Advanced Information Networking and Applications, Singapore.2011.