Indian Journal of VLSI Design (IJVLSID)
ISSN: 2582-8843(Online), Volume-1 Issue-1, March 2021

# Graphical Based Authentication System by Picture-Based Passwords

**Sarhad Baez Hasan**

***Abstract:*** ***In recent years, the access to computer networks and systems is mostly based on the use of conventional passwords. As the number of online internet services (requiring authentication) is increasing rapidly, the number of needed passwords is also increasing. The result is the load on user's memory to remember such increasing number of passwords that makes them to create short, simple and insecure passwords. This has a possible security risk on user's privacy. Graphical passwords have been designed to make passwords more memorable and easier; humans are more adepted at remembering images.In this paper an experimental image-based authentication system has been developed by users through authentication to online purchasing websites. This system relies on user's ability to recognize a previously seen image. A user-questionnaire has been developed before presenting the system to the users. The system has been tested in a 2-week experiment on nearly 33 MSc students in university of Portsmouth and library staff. After collecting the results, the analysis shows that the majority of the users were interested in using image-based authentication system. The project finding illustrates some results that shows the importance of the study of image-based authentication systems. For instance, the majority of users who succeeded in authenticating through using the system have created a story by using the images. This finding could define the image-based authentication as a common practical usage.***
***Keywords, Picture-Based, Graphical passwords, Text Password, Authentication techniques, Security,Attack, Random Picture***

## I.INTRODUCTION

Authentication is a vital component of most computer systems especially those which are used in e-commerce websites over the internet. The most widely used authentication methods for online websites a password-based authentication mechanism. This mechanism is easy to use and implement. However, most users find it hard to manage and remember passwords for multiple web accounts. This is because each web user has about 25 unique accounts that require passwords (Florencio and Herley, 2007). This problem causes users to adopt strategies that are easily attacked.

**Manuscript received on 05 February 2021 | Revised Manuscript received on 14 February 2021 | Manuscript Accepted on 15 March 2021 | Manuscript published on 30 March 2021.**
* Correspondence Author
**Sarhad Baez Hasan*,** Iraq-Kurdistan, Soran University, Fuculty of Science, Computer Department



For example, users write down their passwords: use the last name as the password, use the same password, and choose simple passwords such as words from the dictionaries (Gaw and Felten, 2006).All of these behaviors increase the likelihood of passwords being lost, stolen, or compromised. To address these problems, researchers came out with graphical-based authentication techniques called graphical passwords which are considered to be strong and friendly for users (Owenetal, 2005). The theory behind the graphical password system andthe idea of replacing micro-string communication with image recognition has been seen before, a skill that humans remarkably enjoy.In 1996, Blonder described a graphic password that required users to touch a predefined area of an image to steal.This method overcomes the difficulty in remembering complex passwords containing: uppercase, lowercase, special characters, and numbers such as w &oKd @ fv0. The mentioned methods above are making passwords less usable (Birgetetal, 2005).

## II.AUTHENTICATION

Authentication is a function in which the user provides credentials to the system. If the system detects this set of credits or if the credentials match a certain set of systems, the user is informed that it is allowed to have access to the certain accounts [8]. Authentication is required to allow the system to perform certain user tasks. The user must search for his services again from the system. Before a user can authenticate to the system, they must first register with the system;this step is called enrollment. Therefore, the new user must be registered in the system before through requesting the service and then confirming it.

In the basic authentication process, the user provides some valid documents like user ID and some additional information to prove that the user is the true owner of the user ID; this process is simple and easy to perform. An example of this type of authentication process is the use of a user ID and password.

**Password Based Authentication System**

This is a simple system in which the users provide their usernames and passwords to the system. If the user ID and password match the number stored in the system, then the user will be verified.A user may have multiple accounts on multiple computers.

He/she has to remember a lot of passwords. The research on human cognitive ability has generated a great deal of knowledge about what one can remember [3].
For example, domain names are used instead of IP addresses, and phone numbers are included in snippets for easy recall. It has also been proven that people can save images more easily than text.

**Biometric Based Authentication System**

Biometrics is the use of statistical analysis to identify individuals by their biological or physiological characteristics which is appeared as one of the key aspects of new safety systems.Using biometrics can prevent issues that occur in traditional security systems where users reuse information such as passwords[5]. Biometric authentication systems can be very secure and reliable, but they are expensive and require additional hardware and software.These systems are difficult to change and maintain. Using such systems of the internet may not be very complicated and comfortable.

**The Goals of System Design**

This paper aims to create a graphic-based authentication system for purchasing websites to solve security and usability issues. The proposed system will attempt to provide the following criteria:

1- Since graphic based authentication is a fresh idea and format, the required interfaces are attractive and fun. This interface makes the system more interesting for users, as well as providing a more enjoyable experience.
2- The system had to be secure enough to face mentioned security problems. In addition, the system mightbe difficult for the users to describe their passwords or write it down.
3- It has been taken into account that the interface used in this prototype is needed to be easy for users with without having experience of graphic-based authentication. The user will be helped through the registration process. Instructions should be kept simple and clear to help the user for completing the task successfully. This was the aim of the design and it is important because this application is directed to purchase websites' users.
4- The system must use cost-effective tools of operation that provide reasonable speed and meet users' needs.
5- Recognition based systems are very dependent on sight sense. Thus, the graphic-based authentication will be inaccessible by users with visual impairment.
6- Minimize the load on user's memory.

**Graphical Based Registration and Authentication System**

GBRAS is a simple authentication system that uses the image as a password [7], [9]. User sends user ID and photo to system as credentials. If the image matches the sample stored in the system, then the user verification is completed. The pictures are easy to remember; however, guessing with pictures is not an easy task. It is extremely difficult to exert brute force over such a system. The user for the first time must register in the system with all the details. User interface guides step by step. There isn'ta fundamental change in the password-based systems for the photo-based use.The system remains a simple password-based. Pictures are not stored in the system. Only hashtag values are stored; user uploads the photos. This system is also handy for internet applications.
GBRAS is designed as a security tool for testing, which can be used in the classroom to demonstrate major security mechanisms or as an access control system for any licensed applications.

## III.SYSTEM DESIGN STEPS

To reduce the complexity of system development, the design is divided into the following:

**1- Database Design**

In this phase of design, the database of the system is designed. The database contains all the data needed for the system to operate. This is user data and the images that are used for authentication.

**Table:System Database**

| Data field | Data type | Length | |
|---|---|---|---|
| USER_ID | Int | 50 | Primary key |
| First name | Varchar (50) | 50 | First name of the user |
| Last name | Varchar (50) | 50 | Last name of user |
| Email | Varchar (50) | | Email address of user |
| Username | Varchar (50) | | Name that user uses to Login |
| Sum | Varchar (50) | | Sum of the images the user has selected |

## IV.INTERFACE DESIGN

System interface is very important for the users to interact efficiently with the system. As a consequence, the interface should be clear and easy to follow. Below is a design idea for the system interface.

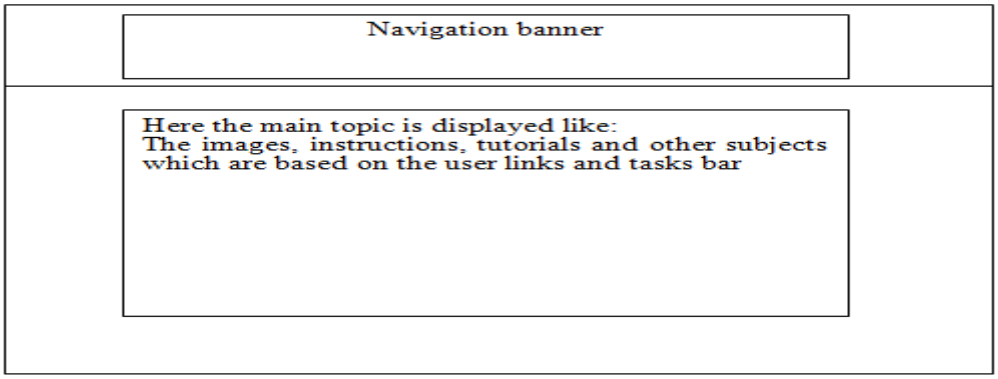


**Figure 1:System Layout**

### 2- Fetching Random Images from The Image Bank Algorithm Design

The images are randomly displayed to the user during registration and login. This means that the system cannot be attacked through observing users' selection of images. For example, if an attacker has recorded the location of images that the user has selected, then the observation will not help the attacker in logging into that account. Below is the flowchart for selecting a random image.

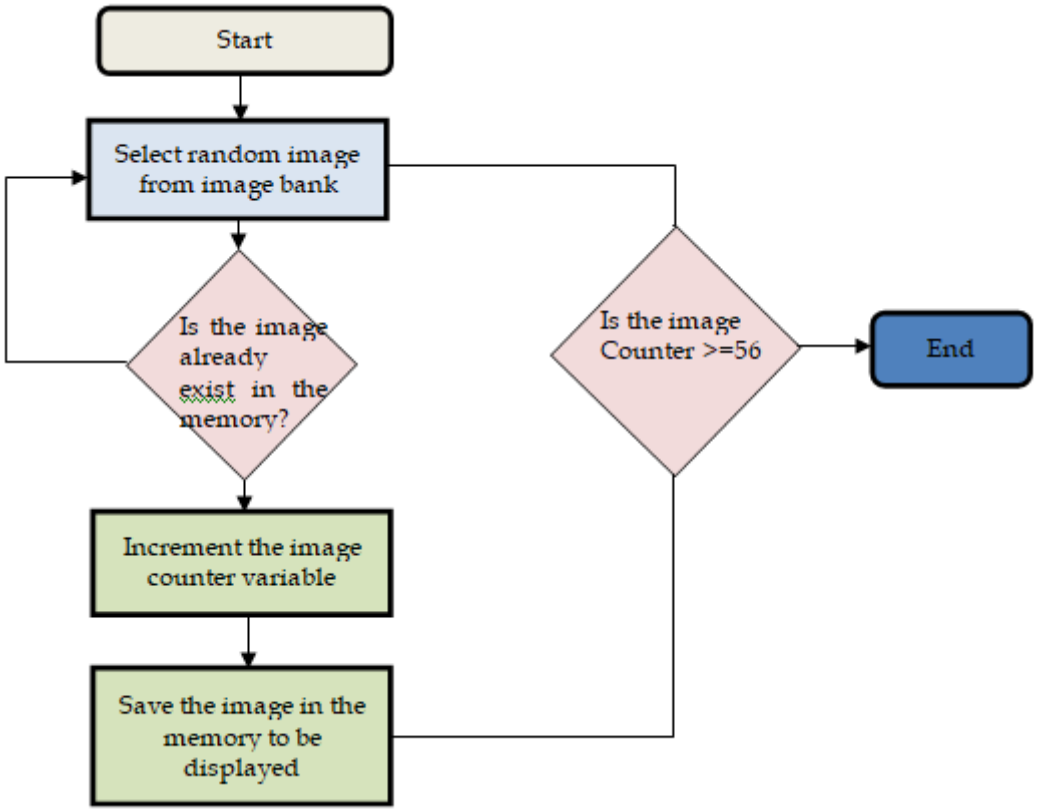


**Figure 2:Fetching Random Images Algorithm**

## V.BROWSING PLAN

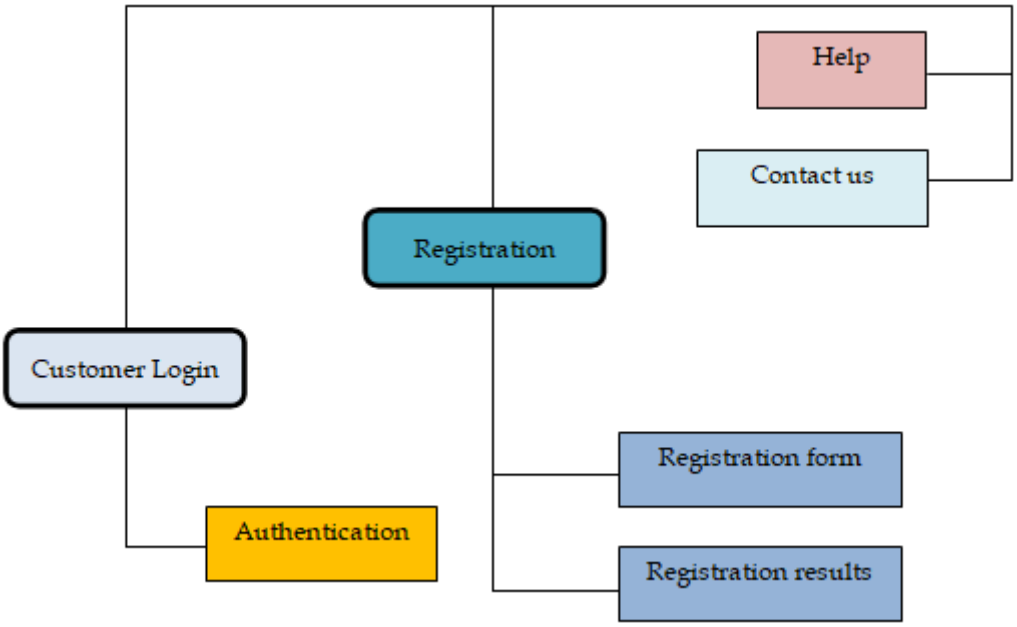


**Figure 3: Browsing Plan**

**Randomization of The Image Positions**

The system randomly varies the location of images within the challenges-set. This would help the system for avoiding attacks by observing users' responses and attempts to reselect them at later times. I.e, if an attacker observes users' selections at the first three images on the right of first row in the challenges-set and then selects another one which is appeared on the bottom left corner, then such observation and even memorization of the locations would not assist the attacker in breaking into that user's account. In other words, one attack that this technique is intended to fight is the keystroke logging attack.

## VI.CONCLUSION

The survey participants are required to select four images at the registration stage as their password. The use of four images as a password aims to accomplish a balance between system usability and security. Choosing less than four images as a password could satisfy the usability requirement, but it may represent a security risk.Whereas choosing six or seven images as a password could be a good option for a secure system, but it may overload user's memory and affect the system usability

## REFERENCES

1. Muhammad Ahsan, Yugang Li (2017). Graphical Password Authentication using Images Sequence, International Research Journal of Engineering and Technology.
2. N.K. Sreelaja and N.K. Sreeja (2016), An image edge-based approach for image password encryption, Security and Communication Networks.
3. Adams, A., &Sasse, M. A. (1999). USERS ARE NOTTHE ENEMY. Retrieved July 29, 2009, from University College London Department of Computer Science.
4. Chapman, D. (2005). PRINCIPLES AND METHODS OF DATA CLEANING. Retrieved August 23, 2009, from Global Biodiversity Information Facility.
5. Chiasson, S., Biddle, R., & Oorschot, P. v. (2007). A Second Look at the Usability of Click-Based Graphical Passwords. Rerieved August 28, 2009, from CyLab Usable Privace and Security Laboratory.
6. Daniel, N. (n.d.). On Secure Knowledge-Based Authentication. Retrieved July 17, 2009, from Official home of the point system.
7. Dhamija, R., &Perrig, A. (2000). Déjà Vu: A User Study Using Imagees for Authentication. Retrieved August 14, 2009, from Harvard school of engineering and applied sciences.
8. Go lofit, K. (2007). Picture Passwords Superiority and Picture Passwords Dictionary Attacks. Retrieved August 13, 2009, from Machine Intelligence Research.
9. Matya, V., &Riha, Z. (2002). BIOMETRIC AUTHENTICATION-SECURITY AND Usabilty. Retrieved August 14, 2009, from Faculty of Informatics Masaryk University.
10. Project, T. A. (2009). Authentication, Authorization, and Access Control. Retrieved August 13, 2009, from the Apache HTTP Server Project.
11. Suo, X. (2009). A DESIGN AND ANALYSIS OF GRAPHICAL PASSWORD. Retrieved August 23, 2009, from Georgia state University.
12. Wiedenbeck, S., Birget, J. -C., &Brodskiy, A. (2005). Authentication Using Graphical Passwords: Basic Results. Retrieved August 17, 2009. From Rutgers University.
13. Xu, F. (2008). Short-Term Memory in EFL listening Comprehension. Retrieved August 20, 2009, from Canadian Center of Science and Education.
14. Towseef A., Vakeel A., Israrul H., (2017) Monisa N., Graphical Password Authentication, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.6, June- 2017, pg. 394-400