iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 3 **Issue:** II **Month of publication:** February 2015

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Towards An Efficient Graphical Password Authentication System: A Literature Survey

Akshay Patil[#1], Kiran Sankpal[#2], Zalak Shah[#3], Devendra Bhalerao[#4], Ajeet Ghodeswar[#5]
[#1,#2,#3,#4]*Department of Computer Engineering, Atharva College of Engineerin, Maharashtra, India*
[#5]*Assistant Professor, Department of Computer Engineering, Atharva College of Engineering, Maharashtra, India*

***Abstract-- Nowadays, user authentication is one of the important topics in information security. Text-based strong password scheme can provide security to a certain degree. However, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Recently, many networks, computer system and Internet-based environments try using graphical authentication techniques as their user's authentication. Here we are presenting proposed scheme as Graphical password authentication Scheme based on Color Image Gallery which is very useful for any computer related application such as web authentication, desktop &laptop logins, critical servers.***

***Keywords--- Graphical Password, Image Recognition***

## I. INTRODUCTION

A **graphical password** is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle.[2]

A graphical password is easier than a text-based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are $100^8$, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.[1]

There are two systems which are used in Graphical Password Authentication which are as follows

### *A. Recognition Based Techniques*

Fig. 1 Recognition Based Techniques

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.[1]

### *B. Recall Based*

Jermyn, et al. proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password .A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture.

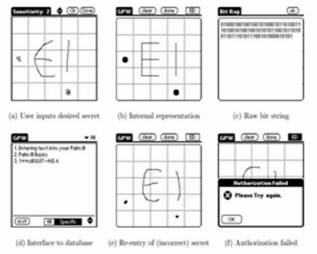


Fig. 2 Recall Based Techniques

If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space. [1]

## II. BACKGROUND

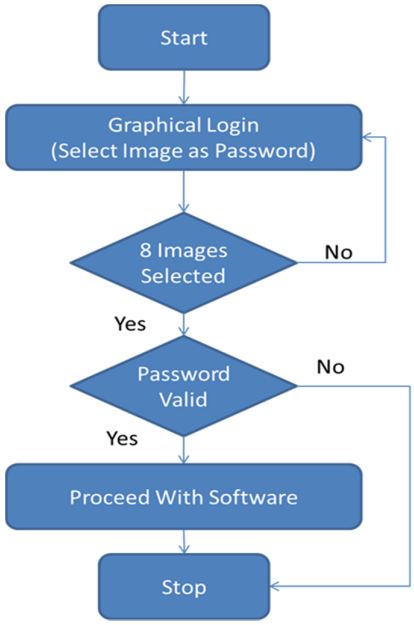
### *A. Problems with Alphanumeric Passwords*

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Decay and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall. If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords. Users typically cope with the password problem by decreasing their memory load at the expense of security. First, they write down their passwords. Second, when they have multiple passwords, they use one password for all systems or trivial variations of a single password. In terms of security, a password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering. As a result, users are known to ignore the recommendations on password choice.[2]

### *B. Why Graphical Passwords?*

Graphical passwords were originally described by Blonder (1996). In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memory of passwords and efficiency of their input are two key human factors criteria. Memorability has two aspects: (1) how the user chooses and encodes the password and (2) what task the user does when later retrieving the password. In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations

depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for arbitrary things is poor. Depending on the graphical password system, at retrieval time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known.[2]




*C. Background on Graphical Password Systems*

Here we discuss some graphical password systems based on recognition or cued recall of images. Most existing systems are based on recognition. The best known of these systems are Passfaces and Déjà Vu . Brostoff and Sasse (2000) carried out an empirical study of Passfaces, which illustrates well how a graphical password recognition system typically operates. To create a password, the user chose four images of human faces from a portfolio of faces. To log in the user saw a grid of nine faces, which included one face previously chosen by the user and eight decoy faces. The user had to click anywhere on the known face. This procedure was repeated with different target and decoy faces, for a total of four rounds. If the user chose all four correct faces, he or she successfully logged in. Data from this study suggest that Passfaces are more memorable than alphanumeric passwords. A small study of the use of Déjà Vu came to the same conclusion. With a few thousand random guesses an attacker would be likely to find the password. To increase security similar to that of 8-character alphanumeric password, 15 or 16 rounds would be required. This could be slow and annoying to the user. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in.[2]

## III. RELATED WORK

**G. Agarwal, S. Singh and R.S. Shukla** describe that the Security in the computer is largely supported by the passwords for authentication process. Also they presented that the comparison between the alphanumeric passwords and graphical password. They concluded that the main reason for adaption of graphical password is that people are better at memorizing graphical passwords than text-based passwords. Overall the current graphical password techniques are still need improvement against shoulder surfing attack and dictionary attack etc. But still these techniques are much better than the alphanumeric password techniques.[3]

**Susan Wiedenbeck , Alex Brodskiy** describe that Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create

short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. They are interested in determining the effect of the particular image used on success with graphical passwords, studying users' speed in skilled performance, and discovering what kinds of insecure password practices users invent for graphical passwords.[2]

**K. Semmangaiselvi, T. Vamsidhar, Kotha Hari Chandana , B. Krishna Priyaand E. Nalina** described that Authentication, authorization and auditing are the most important issues of security on data communication. Graphical password authentication technology is the use of click on the image to replace input some characters. In the graphical password systems, we need the image big enough to ensure the security. Because of the large enough images can be cut into many enough sub-blocks to meet the users to set their passwords.[4]

**Harsh Kumar Sarohi, Farhat Ullah Khan has** conducted a comprehensive survey of the existing graphical authentication systems. a new alternative authentication method have been proposed using pictures as passwords. In our findings we can see that authentication process is slower in graphical password. Recently one of Microsoft's operating system windows 8 has used this for authentication.[5]

**Sonkar S.K., Paikrao R.L., Awadesh Kumar** Recently, many networks, computer system and Internet-based environments try using graphical authentication techniques as their user's authentication. the user is having the flexibility to select the any kind of password i.e. sequence of selecting images from gallery.[1]

**Saurabh Singh, Gaurav Agarwal** Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.[6]

**Dr. Omar Bin Zakaria, Samaneh Farmand** describe that A potential drawback of graphical password schemes is that they aremore vulnerable to shoulder surfing than conventional alphanumeric text passwords. To have a good system high security and good usability are both needed and cannot be separated. Shoulder surfing attack is under security provision. There are few proposed methods to shoulder surfing problem but they still need to be improved.[9]

**Wazir Zada Khan and Yang Xiang** describe that this scheme is proposed for smart mobile devices (like smart phones i.e. iPod, iPhone, PDAs etc) which are more handy and convenient to use than traditional desktop computer systems. some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.[10]

**Nasir Memon , Jean-Camille Birget ,** they develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. In this paper, we investigated the security of the Pass- Points graphical password scheme and the suitability of the underlying images, by providing a model that predicts the users' click points and their saliency value.[7]

## IV. OUR ANALYSIS

In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object. Our idea is inspired by this novel human ability.

### *A. Properties Expected In System :*

1) *High Availability*: Ensure business continuity with the highest levels of system availability through technologies that protect your data against costly human errors and minimize disaster recovery downtime.
2) *Performance and Scalability*: Deliver an infrastructure that can grow with your business and has a proven record in handling today's large amounts of data and most critical enterprise workloads.

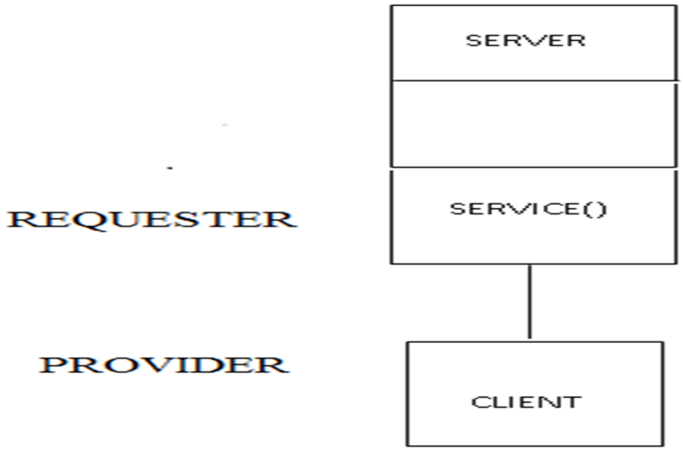



Fig. 3 Architectural Style: Client-Server Model

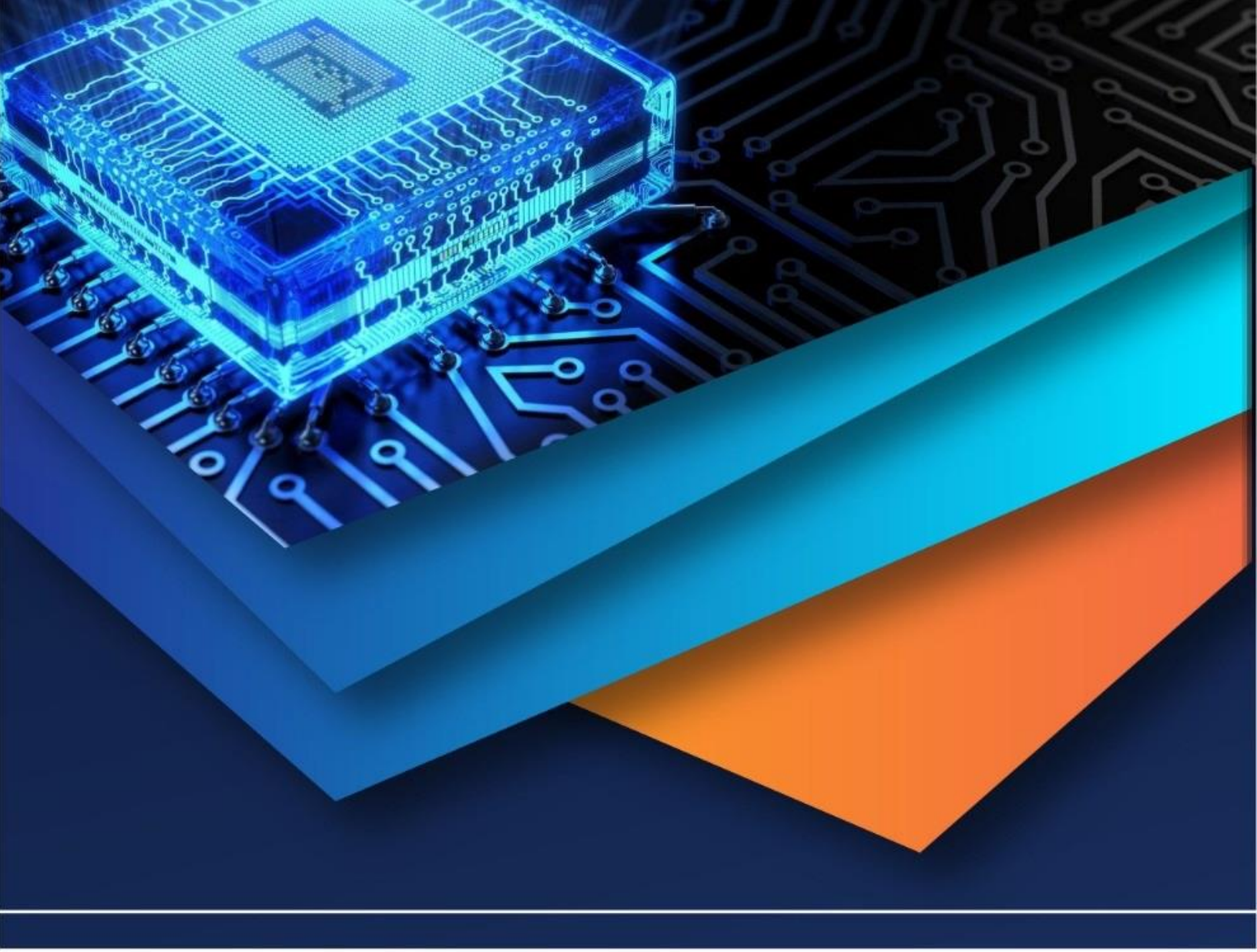
3) *Security*: Provide a secure environment to address privacy and compliance requirements with built-in features that protect your data against unauthorized access.
4) *Manageability*: Manage your infrastructure with automated diagnostics, tuning, and configuration to reduce operational costs while reducing maintenance and easily managing very large amounts of data.
5) *Developer Productivity*: Build and deploy critical business-ready applications more quickly by improving developer productivity and reducing project life cycle times.
6) *Business Intelligence*: Gain deeper insight into your business with integrated, comprehensive analysis and reporting for enhanced decision making.

## V. CONCLUSION

This research aims to study the existing graphical password schemes and to design and develop an improved graphical password scheme, to empirically test its security & usability, and to compare it with existing alphanumeric and graphical password schemes. Statics shows Graphical Passwords are difficult to crack for hackers. Here in this system we will ask user to create a graphical password by choosing 8 pictures in an particular order from a set of 50*8 pictures. Graphical password security is required to a very high security demanding software like the one we will develop, "Financial Application". All the data in Financial Application will be guarded by Graphical Password. This software can be used by any Financial Broker who wants to guard the high security financial information of his/her clients.

## REFERENCES

[01] Sonkar S.K., Paikrao R.L., Awadesh Kumar ,"Graphical Password Authentication Scheme Based On Color Image Gallery "
[02] Susan Wiedenbeck ,Alex Brodskiy "Authentication Using Graphical Passwords: Basic Results "
[03] G. Agarwal, S. Singh and R.S. Shukla "Security Analysis of Graphical Passwords over the Alphanumeric Passwords"
[04] K. Semmangaiselvi , T.Vamsidhar ,KothaHariChandana , B. Krishna Priya and E. Nalina "An Effective Secure Environment Using Graphical Password Authentication Scheme"
[05] Harsh Kumar Sarohi , Farhat Ullah Khan "Graphical Password Authentication Schemes: Current Status and Key Issues"
[06] Gaurav Agarwal , Saurabh Singh "Integration of Sound Signature in Graphical Password Authentication System"
[07] Nasir Memon , Jean-Camille Birget "Modeling user choice in the Pass Points graphical password scheme"
[08] Sonia Chiasson , P.C. van Oorschot , and Robert Biddle "Graphical Password Authentication Using Cued Click Points "
[09] DR. ROSLI SALEH , Dr. OMAR BIN ZAKARIA "Shoulder Surfing attack in graphical password authentication"
[10] Wazir Zada Khan , Mohammed Y Aalsalem and Yang Xiang "A Graphical Password Based System for Small Mobile Devices"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY