

GRAPHICAL PASSWORD SECURITY BY USING LIVE OBJECT

Auti Mohini¹, Auti Sayali², Jadhav Pratiksha³, Gadge Meghana⁴

¹ B.E. Student, Computer, SGOI-COE, Maharashtra, India

² B.E. Student, Computer, SGOI-COE, Maharashtra, India

³ B.E. Student, Computer, SGOI-COE, Maharashtra, India

⁴ B.E. Student, Computer, SGOI-COE, Maharashtra, India

ABSTRACT

This paper is a new graphical password scheme. This increases the security. User can set the password in the form of image. User presents this image to a system camera and then enters their password as a sequence of selection on live video of object. In existing system cloud data storage and its access is done by using text password which is combination of numbers, characters and special symbols that why these password are the easily guessable and easy to hack. Because of this drawback we are propose to a new solution and that is graphical password security. In that we are going to use the image processing concept for login purpose. To achieve that goal we store one sample image of object and password as the part of that image.

Keywords: Feature extraction , Loci metric Password Schemes, Multifactor Authentication Schemes, Live object, PassBYOP, Physical tokens, click points, Security

1. INTRODUCTION

Now a day's security is important issue. Text password is most useful authentication method. But it has many security usability related problems. Authentication is a process of identifying whether a particular individual or device should be allowed to access a system or not. Text password requires to remembering it and recalling at time of login operation. It is use to provide security to system & resources. User authentication is most important for providing security. It provides accountability & access control to user. There are various types of authentication systems in market. In that text password that is alphanumeric password. This password are easy to remember & easy to use. But if this password is too short then, it easily guess by attacker & if password is strong it is hard to remember. To solve the problem which occurred due to text password i.e. easily guess & difficult to remember. The market was provide a technique OTP (One Time Password). OTP passwords provided by token devices are very expensive. Another proposed solution is to use Graphical password. In which graphical images are used to provide security. But graphical password has some disadvantages that are shoulder surfing attack and intelligent guessing. Such attack are more powerful because of area selected by user on image is observed or guess by attacker.

2. PROBLEM STATEMENT

Design a system which provides a better authentication to cloud. Traditional system uses text, numeric or some pattern passwords which is not the good way. Because by using the shoulder surfing techniques anyone may guess the passwords. To overcome this problem we will introduce the new way to unlock the cloud account which is the object detection technique.

3. EXISTING SYSTEM

Password is used to user authentication. It is used to prove identity or access approval to gain access to a resource. Two conflicting requirements of alphanumeric passwords-

1) Easy to remember

2) Hard to guess

4. PROPOSED SYSTEM

Now a days security is very important issue in terms of cloud computing. To authenticate the system text passwords are mostly used. But it has many security & usability related problems.

Basically Authentication is a process of identifying whether a particular individual or device should be allowed to access a system or not. Text passwords are easy to memorize & recall it at the time of access a system. To address this issue, we proposed a new technique "Graphical Password Security by Using Live Object". Graphical password system is a technique that depends on selecting click points on image. This technique resistance to brute force attack and shoulder surfing attack. Such attacks are more powerful because attacker can easily hacked a system.

4.1 Architecture of proposed system:

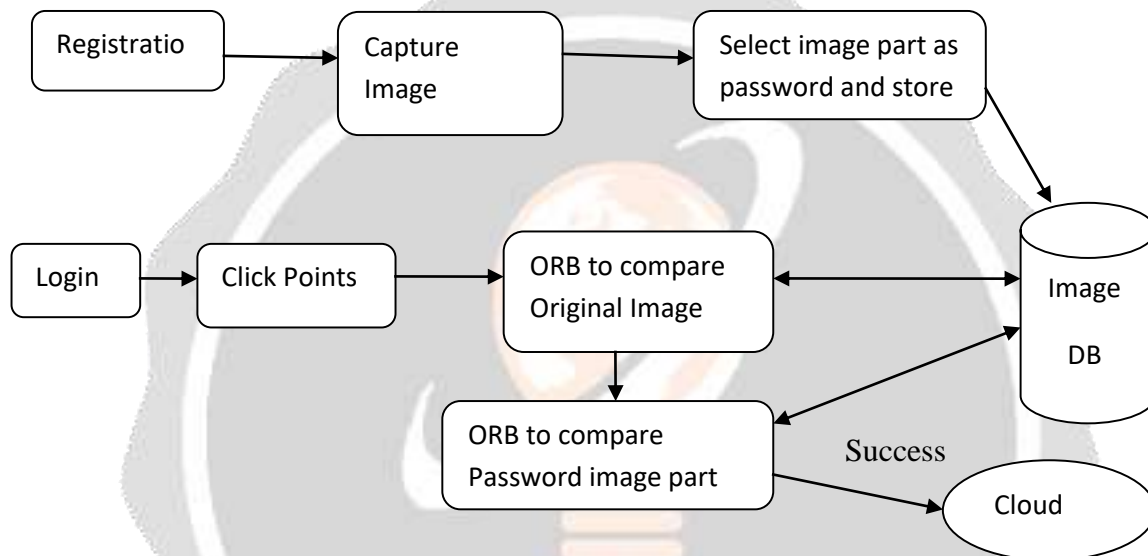


Fig 4.1.1: Block diagram of proposed system.

In this, we use live object detection technique to authenticate the system. User present live object to a camera & select the click points as a portion of an image. Highly distinctive features extracted from this live object & click points are saved in database & used as a password.

At the time of login user again gives live object and sequential click points. The extracted features from this live object and click points are match with stored features in database. We have set some threshold value to match extracted features. If features are match then successful authentication to cloud otherwise authentication denied.

5. ALGORITHM

ORB is used for object matching. As compare to SIFT (Scale Invariant Feature Transform) and SURF (Speeded up Robust Features) this algorithm is efficient and faster. ORB is a combination of FAST key point & BRIEF descriptor.

We use two different algorithm:

1. BRIEF descriptor. (Binary Robust Independent Elementary Features)
2. FAST algorithm. (Features from accelerated segment test)

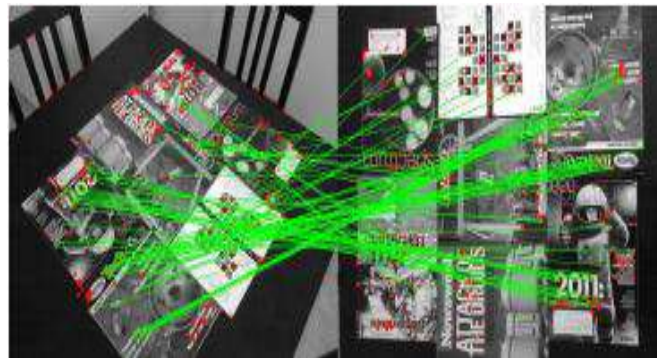


Fig 5.1: Object matching using ORB

5. EXPERIMENTAL RESULT

At the time of registration participants were first given an introduction to the system and its operation. Each condition started with the *creation phase* in which the user set a four-item password by selecting points on the displayed image.

Performance measures used during the login phase of the study included: the mean time taken to enter the full set of four password items during successful authentication trials, the number of repeated trials required to setup the original password, the number of errors and resets that occurred during the study, and the number of features and matching score for each entered password item.

If any selection contained less than 0.7, users were prompted to make another selection.

Existing system	Proposed system
In existing system we use text password and graphical password.	In proposed system we use graphical password with multiple click points.
Static images are used.	Dynamic images are used.
Dictionary attack and Shoulder surfing attack are able to hack password.	Dictionary attack and Shoulder surfing attack are not able to hack password.



Fig: 5.1. Select click points and match.

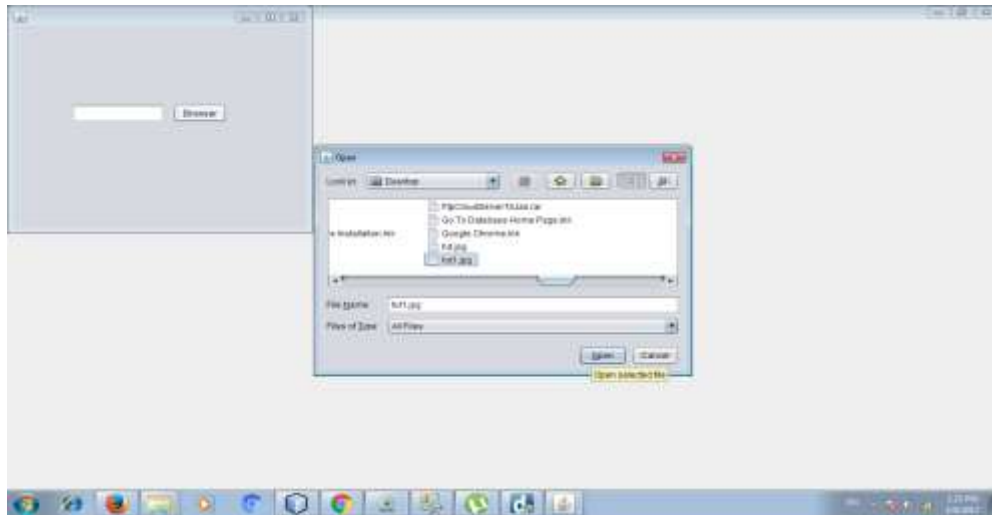


Fig 5.2: Perform cloud operation.

4. CONCLUSION

In traditional password system Dictionary attack and Shoulder surfing attack are possible. We conclude that, our system provide secure authentication to cloud. It vanish the shoulder surfing attack. It resistance to brute force attack & guessing attack.

5. ACKNOWLEDGEMENT

The authors would like to thank computer department HOD Prof. Shimpi M.R and Prof. Deokar M.S, Prof. Ingale S.E. in Samarth Group of Institutions, Belhe (Bangarwadi) Savitribai Phule Pune University for their kind support and assistance during the course of this research.

REFERENCES

- [1] Dhananjay Garud, Dr. S.S. Agrawal " A Review: Face Liveness Detection" in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 1, January 2016.
- [2] Dmitri Bitouk, Neeraj Kumar, Samreen Dhillon, Peter Belhumeur, Shree K. Nayar" Face Swapping: Automatically Replacing Faces in Photographs", 2015.
- [3] G. Akhila Goud, B. Hemanth,"Face Recognition using Edge Detection of Layer", IJSRSET,VOL 1,2015.
- [4] Fei Zuo Peter H. N. de, "Real-time Face Recognition for Smart Home Applications".
- [5] Hu Han, Brendan F. Klare, Kathryn Bonnen, Anil K. Jain, "Matching Composite Sketches to Face Photos: A Component-Based Approach," in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 1, JANUARY 2013.
- [6] V. Bhusari " Graphical Authentication Based Techniques" in International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.
- [7] Iranna A. M., Pankaja Patil, "Graphical Password Authentication Using Persuasive Cued Click Point", International Journal of advanced research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[8] Iranna A. M.,Pankaja Patil,"Graphical Password Authentication Using Persuasive Cued Click Point" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013

[9] Raikoti Sharanabasappa, Sanjaypande M. B "Real Time Multiple Face detection from Live Camera, a Step towards Automatic Attendance System" International Journal of Computer Applications (0975 8887), Volume 45 No.4, May 2012.

[10] Priti C. Golhar, Dr. D.S. Adane " Graphical Knowledge Based Authentication Mechanism". International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[11]Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski, "ORB: an efficient alternative to SIFT or SURF" 2010.

