# Graphical Password to Avoid Shoulder Surfing

**Harshada Shitole[1] Priyanka Chaure[2] Pradnya Thorat[3] Ashwini Gaikwad[4] Mrs. Vrushali Sonar[5]**
[1,2,3,4]Student [5]Guide
[1,2,3,4,5]AISSMS's Polytechnic, Pune, India

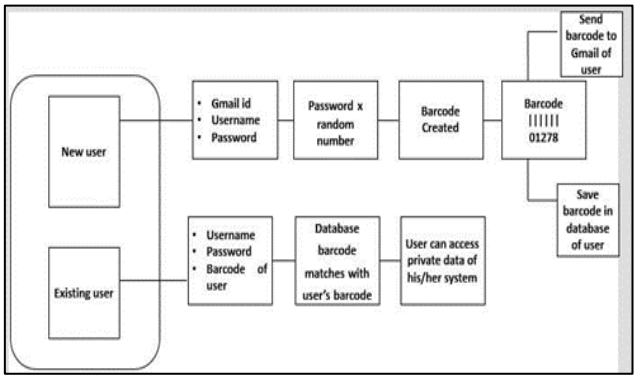
*Abstract*— The focused of this report is on Graphical password system & how can contribute to handle security problems that threaten authentication processes. Once such threat is shoulder surfing attacks which are also reviewed in this project. Computer security depends largely on passwords to authenticate the human user's from attackers. The most common computer authentication method is to use alphanumerical usernames & passwords. However there are significant drawbacks of this method. For example passwords selected by user's are easily guessed by attackers. On the other hand passwords which are difficult to remember. To overcome the problems of low security. Authentication method are developed by researchers that we used barcode image as password & also we avoid shoulder surfing using this method. In this paper we conduct a comprehensive survey of the existing graphical password techniques & provide a possible theory of our own.

***Key words:*** Graphical Password System, Shoulder Surfing, BCI

## I. INTRODUCTION

Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login. The shoulder surfing attack in an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are vulnerable to shoulder surfing, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed and each has its pros and cons.

## II. WORKING




After opening the application the login frame will be opened in that there are two types of users which is New user & Existing user. If the user is new user then the user must create their account using username & password. After creating their own username & password the Gmail id frame will be opened then after writing his/her Gmail id using special encryption algorithm the barcode will be generated & send it to user's Gmail id also this barcode stores in a database of user .Then user can write his/her private information & save it to the database. If the user is existing user then the user can login using username & password & also a barcode of user. Then after matching database barcode with user's barcode user can access his/her private data.

## III. THE BARCODES


As far back as the 1960s, barcodes were used in industrial work environments. Some of the early implementations of barcodes included the ability identify rail road cars. In the early 1970s, common barcodes started to appear on grocery shelves. To automate the process of identifying grocery items, UPC barcodes were placed on products. Today, barcodes are used for identification in almost all types of business. If barcodes are used in the business process, the processing can be automated to increase productivity and reduce human error. Whenever there is a need to identify or track something accurately, barcodes should be used. In traditional working environment, workers are required to enter an enormous amount of data into a customer database system. Instead of manually typing the customer identification number into a database of information, contained in a barcode, a data entry maybe scanned easily. This increases the automation and reduces the human error. The type of barcode to use for a particular situation depends upon:

- the actual application;
- the data encoded in the barcode;

– the printability of the barcode.

There are several different types of barcode standards for different purposes, which are called symbologies. Each type of symbology is a standard that defines the printed symbol and how a device - such as a barcode scanner - reads and decodes the printed symbol. When multiple parties or companies are involved in the ID process, industry standards are usually established. Note that the standard is not necessarily the same as the barcode symbology. If an industry standard has been established for the customer's use of barcodes, there will not be a choice in selecting the barcode symbology. Barcode standards define how to use the barcode symbology in a particular situation. For example, ISBN is a standard for labelling books and periodicals that uses the EAN-13 symbology.

| Established standard | Common use | Symbology |
|---|---|---|
| AIAG | Automotive item identification | Data Matrix |
| EA N8 EAN 13 | Items sale for Worldwide | UPC/EAN |
| MIL-STD-130L | US department of defense | Data Matrix |
| SSCC-18 | Shipping cartons | Code 128 |

The best type of the used barcode depends on the environment, requirements, application, Automotive item identificationare two types: • fonts that require encoding with use of a font tool (Code 128, UPC, Data Matrix, Code 93); • fonts that do not require encoding. Self-checking fonts (Code 39, Codabar). For fonts that require encoding such as Code 128, Data Matrix, UPC, and Code 93, a font tool must be used. A font tool is a product that is used to format data for a barcode font. This may include calculating start/stop characters, a check character, and in some cases prepare data so that it can be altered for the specified barcode symbology. It should be noted, if somebody is not a technical user or programmer, try to use self-checking barcode fonts such as Code 39 or Codabar. Self-checking fonts have checking code built-in, so there is no need to calculate check characters. Check characters are used in more dense symbologies, so the barcode scanner can verify it and reads the barcode correctly.

## IV. Related Work

### *A. Pass - Thoughts: Authenticating with Our Minds*

Author presents a novel idea for user authentication that we call pass-thoughts. Recent advances in Brain Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon "transmitting" a thought. Provided that these brain signals can be recorded and processed in an accurate and repeatable way, a pass-thought system might provide a quasi-two-factor, changeable, authentication method resilient to shoulder-surfing. The potential size of the space of a pass-thought system would seem to be unbounded in theory, due to the lack of bounds on what composes a thought, although in practice it will be finite due to system constraints. In this paper, author discusses the motivation and potential of pass thought authentication, the status quo of BCI technology.

### *B. A User Study using Images for Authentication*

Current secure systems suffer because they neglect the importance of human factors in security. Author addresses a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies on recognition-based, rather than recall-based authentication. Author examines the requirements of a recognition-based authentication system and proposes is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

### *C. The Design and Analysis of Graphical Passwords*

In this paper author propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the "memorable" passwords that, we believe, is itself a contribution.

## V. Proposed System

This paper presents the design and evaluation of graphical password which avoids shoulder surfing.

The shoulder surfing attack is an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed and each has its pros and cons.

In this paper we proposed an improved text based shoulder surfing resistant graphical password scheme by using Barcodes.

In this application we are reading & also we are generating the barcode.

Then we can use these barcode as password for most of the critical password of the user like pin, passwords, text files etc. then we can used it to avoid shoulder surfing thus providing the security to the user's most critical information.

## VI. Existing System

Most of the user uses text based password that are easy to remember.

But main disadvantage of using text based password are May attacks happened like Eavesdropping attack, Dictionary attack, Denial of service attack & so on.

To overcome disadvantage of text based password new Graphical password is used

*A. Benefits*

Provide a way of more user friendly password while increasing the level of security.

On average millions of year to break into the system. Dictionary attacks are infeasible. Reduce shoulder surfing attacks. Security of the system is very high.

## REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years,"ACMComput. Surveys, vol. 44, no. 4, 2012.
[2] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
[3] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767
[4] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.
[5] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000.
[6] Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999
[7] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[8] shoulder surfing attack", International Conference on Multimedia and Expo (ICME), IEEE.2005. 14. S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC, 2010, pp. 1–10.
[9] "Barcodes for TV Commercials". Adverlab. 31 January 2006. Retrieved 2009-06-10.
[10] http://blogs.vancouversun.com/2012/01/04/tescos-cool-qr-code-advertising-campaign/
[11] http://www.techfresh.net/keep-tabs-on-your-items-with-barcodes-scanner