International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Implementation of Simple Text Based Shoulder Surfing Resistant Graphical Password using CAPTCHA and VRK

**Vijayalaxmi Daundkar[1], Shyam Gupta[2]**

[1, 2]Savitribai Phule Pune University, Department of Computer Engineering, Siddhant College of Engineering, Pune, Maharashtra, India

**Abstract:** ***A Higher number of security primitives depend on hard difficulties that are reasonable just by mathematical formulation. Utilization of Difficult AI problems for security has turned into a development for another worldview of security, yet still left underexplored. In this paper, we will recognizably exhibit another security primitive in view of hard AI problems, to be specific, a novel group of graphical password frameworks based on the premise of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is a mind boggling mix of Captcha and a graphical password style. CaRP tackles various security issues altogether, for example, online guessing attack, relay attack, and, if joined with double view technologies, shoulder-surfing attack. CaRP alone gets to be inefficient to keep all security, hence this paper makes a survey of the various security measures for secure password schemes and gives a clear picture of the efficiencies of the different techniques. The proposed system introduces a novel Virtual Random Keyboard and a secure intellectual OTP and LTP technique for securing the authentication at a higher level. Thus the proposed system enables user to securely login without any attack probability by multiple level security and advanced attack preventing mechanisms.***

**Keywords:** OTP, Password Attacks, Graphical Password, CaRP, Captcha, Security

## 1. Introduction

A very important aim of the security systems is to create highly cryptographic and highly non reachable techniques depending on critical mathematical formulations that are computationally intractable. Right from 1999 [4], various graphical credentials systems emerged as a challenge to the traditional login systems. With textual passwords or credentials, users try out for unsafe coping strategies, like making use of same passwords for multiple transactional accounts to avoid forgetting the passwords and avoiding memorizing different passwords for different accounts, change in security level cannot be alone addressed by the system's underlying technical security. Major issues that actually impact significantly in real life are about usability. GUI design approaches and strategies may intentionally or unintentionally sway users' tendency or behavior towards less secure transactional behaviors. Thus these powerful and most secure applications must constraint high GUI related constraints based on essential research work considering the capabilities and shortcomings of the targeted users. In pictorial passwords, human inclination for retaining visual passwords or articles will encourage the ideal determination and proper utilization of exceptionally secure and passwords that have less consistency, ceasing clients from risky practices.

## 2. Literature Survey

Previous techniques check how the attacker can predict the password by making use of offline dictionary attacks. Rather than making use of image analysis and image processing methods for determining the image hot-spots, human computation method is widely used which ensures that these tasks can be better performed by human beings as compared to computers at current moment. The points which to generate an attack (human-seeded). In general a human-seeded attack can be commonly used by the people as the pixel of choice are fist considered for attacks. Three distinct datasets are created for attacks using the dictionaries (i.e., relevant to the recent data available from the users login mechanism or login pattern, collected from various sources other than the actual target sources, where target sources are nothing but the database which actually comprises of user login credentials or passwords): few of which are based of seeded styles and others based on click patterns or click orders, and the other based on recognition of click-order styles or patterns. Once the evaluation and analysis of the both the datasets is completed, 10 fold cross validation is carried out to study the user click patterns and recognize the user passwords using this attack.

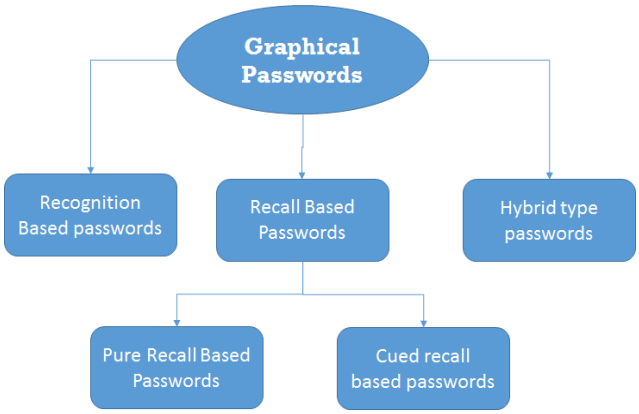


**Figure 1:** Types of graphical password methods

### A. Graphical Password

Graphical passwords are challenging techniques for authenticating by clicking on random pixels over the image themselves, rather than opting for the simple attack prone alphanumeric passwords which can be guessed easily with permutation and combination of characters [4]. There are various techniques for graphical passwords as mentioned below:

**1) Recognition Style Passwords**

In this category, under the registration process of the system, users need to select specific images of choice from large dataset of random images, icons or symbols. During login or authentication phase, challenging task of appropriately selecting and recognizing the valid images used at time of registration process must be done by user. Study and analysis was done to determine accountability of memorizing passwords and it signified that there can recall the graphical passwords even after 60 days by the most of the users [5].

**2) Pure Recall-Based Technique:**

In this process, the accurate login passwords have to recall by users without a single provision of getting a hind or clue from the login system. Although this technique is a most convenient and easy method to login, but it emphasizes on remembering the user passwords which is a tedious task.

**3) Cued Recall-Based Technique:**

Under this technique, availability of hints for logging in to the system is provided by the system. Such hints provide users with additional support to re generate during login process. This paradigm is quite equivalent to the techniques which is recall based but it is recall along with cueing.

**B. One Time Password Methods**

A one-time password (OTP)[7] is a phenomenon making use of a alphanumeric or only numeric codes for authenticating user for current session in progress. OTPs overcome the shortcomings of the static traditional alphanumeric passwords which can be hacked and remembered by attackers as well. The major advantage of the OTPs over traditional passwords is that they cannot be reused once it has been used for the logon process. This implies that even a high graded attacker who can somehow record the OTP, which had been used for previous transaction of login in to the service, cannot forge the system or cannot login to the system, since it will not be long time valid for transaction. OTPS also have an additional feature of random and irregular patterns which are hard to memorize and therefore cannot be predicted for future use.

## 3. Proposed System

The proposed system is a robust and dynamic security system that allows user to secure the transactional credentials and the way to login to the system using the latest and innovative techniques. The proposed system is a multilevel highly attack resistant to shoulder surfing and password guessing attacks. Graphical password approach additionally gives the superior throughput as compared to previous alphanumeric credentials thereby making the login systems secure. The proposed system implementation comprises of below mentioned workable modules:

**A. Captch as a Graphical Password(CARP)**

The Carp technique is a predefined graphical password scheme which makes use of non-alphanumeric artifacts for creating the passwords which ensures that the person while trying to login is to the system is in front of the system. In CaRP technique user, while registration, is provided with a random set o images of which user is supposed to select any 3 to 5 images as a selected image for authentication. But the authentication process does not end over only image selection, once all the images are selected, these selected images are displayed in the sequential manner for recording the user pixel clicks as a password which comprises of an 'x' coordinate and a 'y' coordinate. The pixels are recorded in a sequence and encrypted using a secure encryption module i.e. SEM module which uses a novel technique of cryptography for encryption. When the encrypted pixel values are recorded for all the selected images, user registration is completed with provision of an alphanumeric password for second level authentication mechanism of virtual Random Password. The algorithm used by SEM module i.e. Secure Encryption Module with encryption and decryption example is explained below:

Advanced encryption using whole number

**4) Encryption**

Step 1: (Actual Data Encryption)

Let the transmitted message be "SECURITYTECH". Then find ASCII equivalent values of the above all characters.

S E C U R I T Y T E C H
83 69 67 85 82 73 84 89 84 69 67 72

Step 2: Now with these numbers perform the addition of the above digits of the whole number as follows:

```
   83 69 67 85 82 73 84 89 84 69 67 72
(+) 3  7  1  9 49  1 27 343  1  3  7  1
-------------------------------------------------------
   86 76 68 94 131 74 111 432 85 72 74 73
```

Step 3: Then, convert from above array to a matrix form as follows:

$$A = \begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix}$$

Step 4: Now, consider an matrix of encoding:

$$B = \begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{bmatrix}$$

Step 5: Then, multiplication of matrices (B X A) are perform as follows:

$$C = \begin{bmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{bmatrix}$$

After multiplication, we get encrypted data which is,

858,4566,28458,1273,7339,47545,3442,22252,151258,807, 4347,27399

The above values are the encrypted mode of original information.

**5) Decryption:**

Step 1: (Original data Decryption) Perform the encoding matrix inversion

D= $B^{-1}$

$$D = \begin{bmatrix} -7/24 & 1/3 & -1/24 \\ \frac{1}{56} & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{bmatrix}$$

Step 2: Now perform multiplication of decoding matrix and the encrypted data matrix i. e. (D X C), as follows:

$$D \times C = \begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix}$$

Step 3: Then transform above result as given below

86 76 68 94 131 74 111 432 85 72 74 73

Step 4: Now, Subtract Armstrong numbers from the digits as follows:

86 76 68 94 131 74 111 432 85 72 74 73
(-) 3 7 1 9 49 1 27 343 1 3 7 1
---
83 69 67 85 82 73 84 89 84 69 67 72

Step 5: From the above ASCII equivalent obtain the characters

83 69 67 85 82 73 84 89 84 69 67 72
S E C U R I T Y T E C H.

**C. Virtual Random Keyboard (VRK)**

Virtual Random Keyboard is a novel technique for securing the login systems from shoulder surfing attacks. All the credential based systems are likely prone to shoulder surfing attacks. The virtual random keyboard VRK makes authorized users feel ensured for entering the password and hiding it or making a googly for those peeping in while entering your credentials. VRK is a Virtual On-screen Keyboard having all numbers and characters displayed on it but with an innovative approach to shuffle the characters on the keyboard buttons in a random pattern so as to distract the shoulder surfing attacker and hiding the characters being pressed. Working of VRK is as explained below:

1) Initialize the virtual keyboard to QWERTY keypad.
2) Accept the first character as numeric character considering it as length of password only, so as to avoid exposing the first character of the actual password.
3) On first character click, call random function over 26 characters and 10 digits for shuffling of the keyboard layout.
4) Display the randomized characters on the virtual keyboard keys.
5) For every consecutive click, call random function till submit buttons clicked.
6) Store the entered characters as user entered password and pass it for authentication using username and password.

**D. OTP LTP Authentication (OLA)**

Many banking applications for authenticating the user and securing the transactions make use of One Time Passwords (OTPs) to verify the transacting user and ensuring the valid user doing transaction. But the traditional approach can be hacked if the users SIM card is hacked and the OTP SMSs are retrieved by the attackers in between i.e. if the OTP is eavesdropped. So to secure the OTP system, an additional process of involving the Long Term Passwords for authenticating the users have been proposed in this system thereby making the attacker's task more difficult as compared to traditional OTP ways. During User registration process using Carp, a user gets a secure LTP i.e. Long Term Password which is a simple 4 digit number like an ATM Pin. Once the user registers successfully, this LTP is delivered to registered mail id of user for using it in for further transactions. Once the user receives the LTP over the mail, and tries to login to the system and successfully passes the first two levels of authentication i.e. CARP and VRK , the OTP is delivered to users mobile number. Similar to LTP, this OTP is also a 4 digit number. But the innovation to OTP's use is a research part applied in the proposed system. The OTP is not entered as it is, instead the OTP is arithmetically computed with LTP previously sent over mail id , and the new number obtained by post performing the arithmetic operation is used as a secure pin to validate the authorized user.

The generation of LTP and OTP is as mentioned below:

1) The OTP and LTP generation functions is provided with length of OTP and LTP to be generated.[Note: OTP and LTP both will be of same length, in proposed system length is kept as 4 digits.]
2) The random function is provided with the limits for each digit from 0 to 9.
3) The random function is called for n number of times where n is length of OTP.
4) The Once n number of random numbers are created, the numbers are concatenated to form a 4 digit OTP.
5) The LTP is generated using the same technique and drafted as mail to the corresponding user mail id.

**E. System Architecture**

The system architecture comprised of 5 major blocks including the user, the server, the SMTP client, the SMS client, and the Application for logging in. The SMS client and email clients are connected via server to the clients for communicating the LTP and OTP to the clients. The overall flow and proposed system's architecture is mentioned in the below figure: Fig 2.

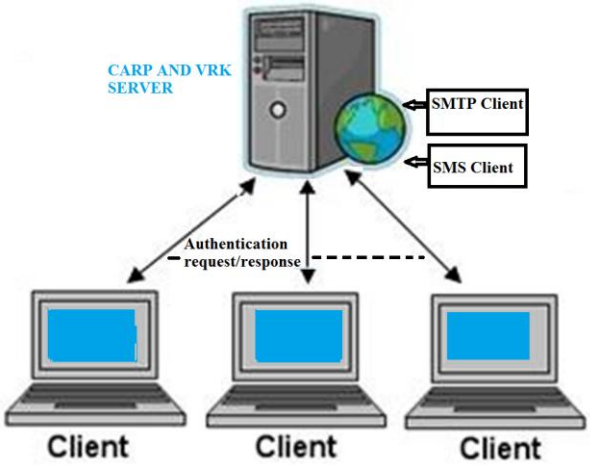


**Figure 2:** Proposed System Architecture

## 4. Mathematical Model

The mathematical formulation of the proposed system can be done on the basis of Deterministic Finite Automata (DFA) and Context Free Grammar (CFG) to represent the entities and the various transitions taking place between the entities.
The DFA for the proposed system comprised of 5 major components as mentioned below:
S = {∑, ƛ, δ, ψ, F}
Where,
∑ is combination of alphanumeric password being entered through virtual random keyboard.
ƛ is a Random secure OTP and LTP generation system which on every new login creates a new OTP.
δ represents the operation or transitions being performed for bringing the project from one state to another.
Ψ are the sequential click points clicked for Carp authentication of the system
F is the final state of the proposed system which depicts the output if the proposed system.

The proposed system states are as mentioned below:
q0- input accepting state
q1- user authentication using login id
q2- user authentication using virtual random keyboard
q3- user authentication using sequential click points clicked
F- validate verification code
The proposed system goes from one state to another state as follows:
q0→q1 where → user authentication using login id.

$$\delta_{q0 \to q1} \text{(user authentication using loginid)}$$

q1→q2 where →user authentication using virtual random keyboard.

$$\delta_{q1 \to q2} \text{(user authentication using virtual random key}$$

q1→q3 where → compress encrypted file.

$$\delta_{q3 \to q4} \text{(user authentication using sequential click points clicked)}$$

q2, q3→F where → validate verification code.

$$\delta_{q2 \to F} \text{(validate verification code)}$$

## 5. Experimental Results

After the working of the proposed system the level of security being achieved will be incomparable to any existing security system as it's a multilevel system combining innovative and novel techniques for user security to avoid the attacks for shoulder surfing and password guessing attacks. The additional OTP and LTP along with VRK technique provides an additional edge for making the system secure and authenticating the users in an innovative way.


**Figure 3:** Pre Login check Page

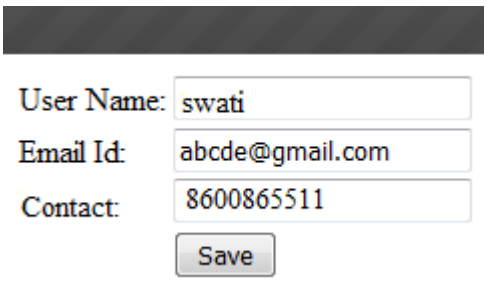


**Figure 4:** New User Registration Page

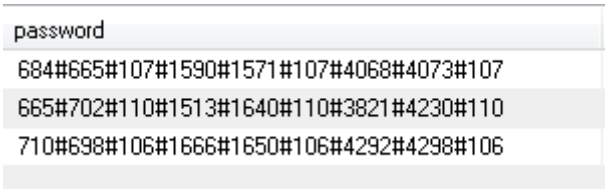


**Figure 5:** Encrypted password in database

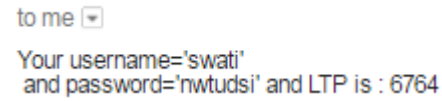


**Figure 6:** LTP and password mail

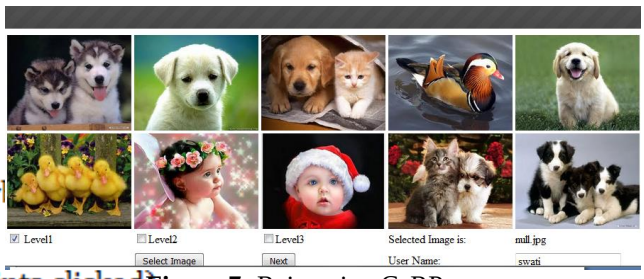


**Figure 7:** Reistration CaRP page

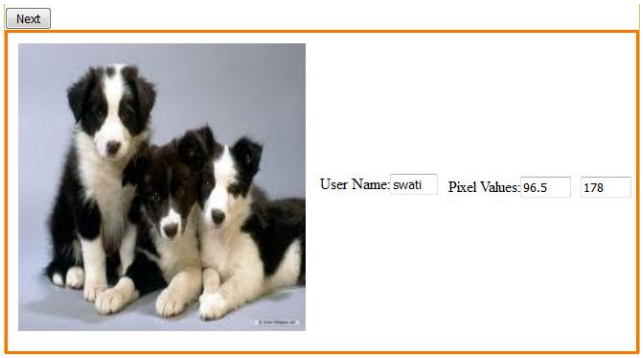


**Figure 8:** Pixel Click Page for registration

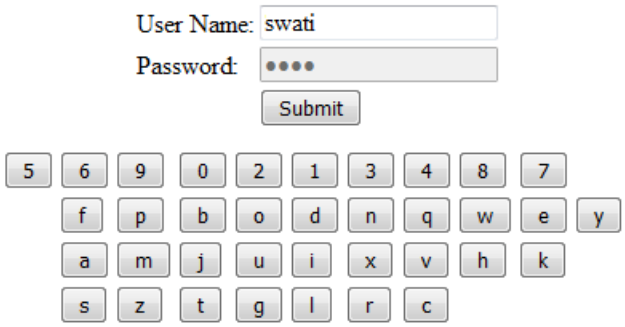


**Figure 9:** Shuffling of VRK on character press

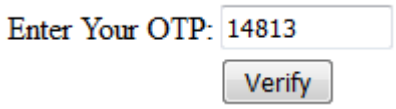


**Figure 10:** LTP OTP addition verification

## 6. Conclusion

Thus it can be concluded from the above results of the proposed system that this security system will make the revolution in the field of credential login system or online login systems. The proposed system will make the online transactions secure upto greater extent. The use of VRK, OTP and LTP and newly proposed Graphical password technique highly secure the user authentication process and avoid malicious users from accessing the system without three level security bypass.

## 7. Acknowledgment

I would like to take this opportunity to express my profound gratitude and deep regard to my guide Prof. Shyam Gupta for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.He was the one who never let my moral down and always supported me through my thick and thin. He was a constant source of inspiration for me and took utmost interest in my project. He motivated me to give me best and encouraged me to think on our own.

## References

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, “Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems”, IEEE transactions on information forensics and security, vol. 9, no. 6, june 2014.
[2] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, “Graphical passwords using images with random tracks of geometric shapes,” 2008 Congress on Images and Signal Processing. 2008.
[3] K. Renaud and E. Smith. Jiminy: “Helping user to remember their passwords”. Technical report, School of Computing, Univ. of South Africa, 2001.
[4] H. Zhao and X. Li, “S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme”, in 21st International Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, 2007, pp. 467-472.
[5] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.
[6] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in clickbased graphical passwords,” J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.
[7] E.Kalaikavitha, Juliana gnanaselvi, “Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology” , Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 14-17.
[8] Viju Prakash, Alwin Infant, S. Jeya Shobana, “Eliminating Vulnerable Attacks Using One-Time Password and PassText – Analytical Study of Blended Schema”, Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, Nov. 2010. © 2010 UniCSE, ISSN: 2219-2158.
[9] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using hard AI problems for security,” in Proc. Eurocrypt, 2003, pp. 294–311.
[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in Proc. ESORICS, 2007, pp. 359–374.
[11] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.

## Author Profile

**Vijayalaxmi Daundkar** received the B.E. and Pursuing M.E. degree in Computer Science and Engineering from Siddhant College of Engineering,Pune, India.

**Prof. Shyam Gupta** received the B.E in Computer Science and Engineering from Jiwaji University, Gwalior. M.Teach degree in Computer Science and Engineering from Rajiv Gandhi Technical University (RGTU) Bhopal. Currently working as a Assistance Professor in Siddhant College of Engineering, Sudumbare, Pune,