Securing Web Accounts Using Graphical Password Authentication through MD5 Algorithm

Siddheshwar A. Suratkar
B.E. CSE, PRPCEM, Amravati

Rahul A. Udgirkar
B.E. CSE, PRPCEM, Amravati

Pratik D. Kale
B.E. CSE, PRPCEM, Amravati

Amit A. Shelke
B.E. CSE, PRPCEM, Amravati

Mohsin H. Shaikh
B.E. CSE, PRPCEM, Amravati

Prof. D. C. Dhanwani
Prof. CSE, PRPCEM, Amravati

Abstract: Today, most Internet applications still uses traditional text based passwords for the authentication. Two conflict cases of traditional password i.e. if user choose simple password it will easy to guess by attacker. The other hand, if a password is strong then it is often hard to remember for user. Instead of a text password user will be choose graphical password scheme that uses MD5. In MD5 images that converted into binary code. Here binary code will be the password for user. Thus, graphical password is secure than existing graphical password techniques because every time user needs to enter different set of code for authentication i.e. every time new password gets generated making Dictionary attacks, Brute Force attack, and other attacks infeasible. Because of these advantages, there is a growing interest in graphical password. In addition user can use 'document sharing' feature after authentication process and also graphical passwords can be applied to workstation, web log-in applications, ATM machines and mobile device.

Keyword: *Graphical Passwords, Authentication, Web Access through Graphical Password, Graphical User Authentication, MD5 Algorithm.*

*****

I. Introduction

In now days, measure internet applications still establish user authentication with traditional text based passwords. User friendly password-based method has been on the order of security researchers for a long standing. On other hand, there are password manager programs which facilitate generating site-specific strong passwords from a single user password to eliminate the memory burden due to multiple passwords. On one hand, there are studies exploring under certain conditions of graphical passwords through as a more secure and user-friendly propositions. Research theories and experience have shown that text-based passwords are filled with both usability and security problems that make them less than worth having solutions.

Text is mentally represented as symbols which give a meaning which is associated with the text as opposed to a meaning perceived based on the form of the alphabets. Using images instead of characters will help the user to improve the security as the alphanumeric corpus size is limited. But in the case of graphical password, the size of the corpus is infinity if it is in the case of multiple numbers of images or if it is in the case of multiple points in a single image. We can select only 26 alphabets and numbers in the case of alphanumeric password, but in the case of graphical password the corpus size is not limited and that's why text password is easy to imagine or break.

According to a recent Computer world news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords.

For finding the problems with traditional username password authentication, alternative authentication methods such as biometrics have been used. Different kinds of graphical password schemes have been proposed as alternatives to text-based passwords, but in graphical password schemes the latest technique introducing for furnish more secure authentication system using graphical password authentication through MD5 algorithm.

II. Related Work

Partha Pratim Ray et al. [1] implemented the Ray's Scheme, Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices. This scheme is proposed for smart hand held devices (like smart phones i.e. PDAs, IPod, I-Phone, etc) which are more handy and convenient to use than traditional desktop computer systems.

Suchita Sawla et al. [5] has present paper on the Graphical Password Authentication System in an Implicit Manner. It is a variation to the login password scheme using graphical passwords used in an implicit manner. This Graphical Password Authentication System in an Implicit Manner is immune to the common attacks suffered by other authentication schemes.

Khan w. z. et al. [8] has present paper on A Graphical Password Based System for Small Mobile Devices i.e. proposed a hybrid system which is a combination of recognition and recall based techniques. This graphical password removes the problem of shoulder surfing and many more problem regarding to graphical password.

Jermyn et al. [9] has present paper on "Draw a Secret (DAS)", which allows the user to draw their unique password. When creating 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. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn suggested that given reasonable-length passwords in a 5*5 grid, the full password space of DAS is larger than that of the full text password space. Some further researches based on DAS were conducted.

Haichang Gao et al. [10] has proposed and evaluated a new shoulder-surfing resistant scheme called Come from DAS and Story (CDS) which has a desirable usability for PDAs. This scheme adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users to draw a curve across their password images (pass-images) orderly rather than click directly on them. The drawing method seems to be more compatible with people's writing habit, which may shorten the login time.

Wells Jason et al. [12] discussed on the topic Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication. This scheme discussed on refinement of the image generation format, size and layout and facilities. This scheme prevents the shoulder surfing attack.

III. Methodology and Algorithm

- **Registration Phase**

First user has to register by filling the credentials in the registration phase then system will allow user to log in. There is two registration phase in which first is used to fill the personal details and next second is use to select the code of respected image to set the password.

The workflow of registration phase is as below:

Phase 1:

Step 1: User clicks on registration button.

Step 2: In registration page, the user has to enter personal details like name, mobile no, city and email id.

Step 3: User click on submit and next page will be open.

Phase 2:

Step 1: User enter username and search for image he want to select. Now user will select code of three images and click on submit.

Step 2: Now program will divide string into three parts and check whether the user input code is correspond to image or not. If yes program search for corresponding image and MD5 Algorithm will generate binary code for the image.

Step 3: Store the generating binary code as password and the username into the Database.

Following detail description contains flowchart of proposed system

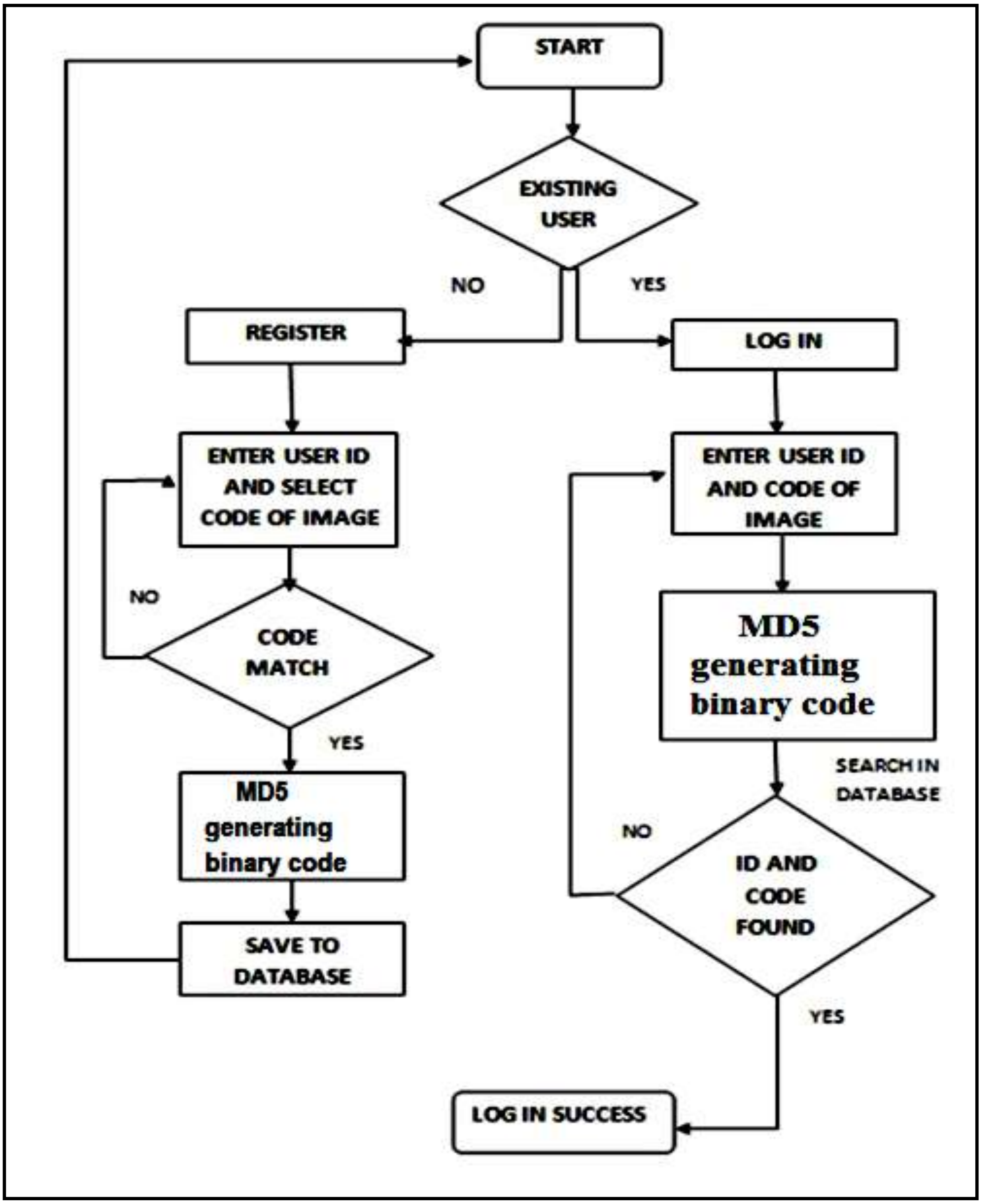

Figure 1: Flow Chart of Proposed System

- **Algorithm : MD5**

In the below figure 3.2 MD5 Algorithm Structure where we selected recognition out of the three categories in graphical password techniques and afterwards select the MD5 Algorithm copyright technique as the proposed algorithm for image gallery security. Now we will explain the steps involved during registration and login section using this proposed algorithm.

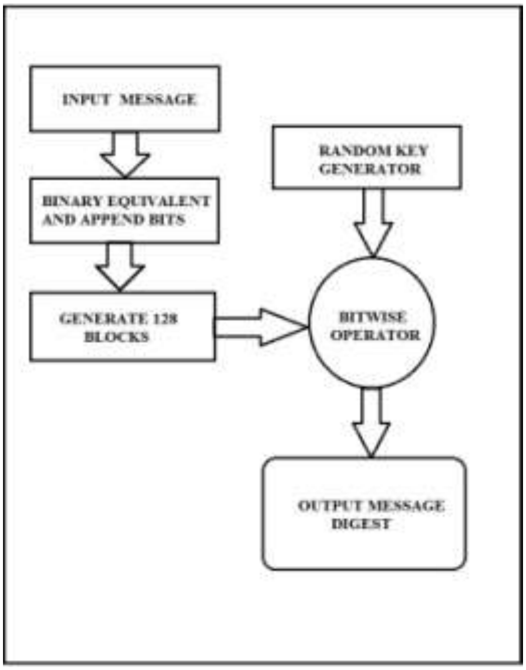

Figure 2: MD5 Algorithm Structure

For convenience, we describe the algorithm through the following five steps:

- Add padding bits behind the input message

This step is to elongate the initial message and make its length be congruent to 448 mod 512. First, a single bit “1” is appended to the message. Then a series of “0” bits are appended so that

- Length(the padded message) ≡ 448 mod 512

For example, suppose the initial message has 1000 bits. Then this step will add 1 bit “1” and 471 bits “0”. As another example, consider a message with just 448 bits. Since the algorithm doesn’t check whether the initial length is congruent to 448 mod 512, one bit “1” and 511 bits “0” will be appended to the message. Therefore, the padding bits’ length is at least one and at most 512. Add a 64-bit binary-string which is the representation of the message’s length. Please pay attention to the meaning of the 64-bit binary-string. You shouldn’t regard it as first 64 bits of the initial message. It is indeed the binary representation of the length of the initial message. For example, suppose the message is 1000bits long. Its 64-bit binary representation would be 0x00000000000003E8. If the message is very long, greater than 264, only the lower 64 bits of its binary representation are used.

- Initialize four 32-bit values

These four 32-bit variables would be used to compute the message digest. We denote them by A, B, C, D. Their initial values are:

A = 0x67452301

B = 0xEFCDAB89

C = 0x98BADCFE

D = 0x10325376

- Compress every 512-bit block and Generate the 128-bit output that we needed. This is all process how MD5 algorithm works and provides a desired output as a password of user.

IV. Result and Discussion

In result analysis phase of propose system i.e. graphical password authentication scheme on recognition-based techniques and for better security than existing system purpose uses MD5 algorithm. These propose system provides a desired result to the users.

These are the some common techniques designed by the researchers. Based on these researches we prepare the comparison report between alphanumeric and graphical passwords against the following points.

- **Password Learning**

After selecting a password, users practiced their password to learn. In the analysis of 15 users learning password process below table 1 shows the how many users learn and login time enter correct input submissions and incorrect input submissions. Users continued to input the password until the criterion was met. In study out of 15 alphanumeric password authentication participants, 9 users had correct inputs submissions and 6 users had incorrect input submissions for login time. In the analysis of existing graphical based password authentication out of 15 users, 12 users had correct inputs submissions and 3 users had incorrect input submissions for login time. Finally in analysis of proposed system graphical password authentication out of 15 users, 14 users had correct inputs submissions and 1 user had incorrect input submission for login time. According to these data we analyze that the easy to understands and learning of propose system graphical password authentication is better than alphanumeric password and existing graphical based password.

Table 1: Number of Participants Making Incorrect Password Submission in the Learning Phase

Authentication Schemes	Users	Correct Input	Incorrect Input
Text Based Password	1 to 15	9 Users	6 Users
Existing Graphical Based Password		12 Users	3 Users
Proposed System		14 Users	1 Users

- **Time Requirement**

The time requirement shows the requirement of time for generating the passwords. The average time for generating the time for three types of authentication schemes i.e. text based password, existing graphical based password and proposed system graphical passwords in seconds. The graph shows the comparison result between text based password and proposed system graphical password. The results are based on the calculation done for the three retention values as in table 2.

Table 2: Time in Seconds for Generating of Password

Authentication Schemes	Parameter	Mean R1 (SD)	Mean R2 (SD)	Mean R3 (SD)
Text-Based Password	Average Time for generating the password (second)	13.01	9.87	17.87
Existing Graphical Based Password		21.23	16.98	23.65
Proposed System		18.40	14.84	20.22

- **Number of attempt to remember password**

  The graph figure 3 below shows the alphanumeric passwords take many attempts to remember the passwords but proposed system graphical passwords are very likely to remember the passwords. These graphs are generated with the records given in figure 3.

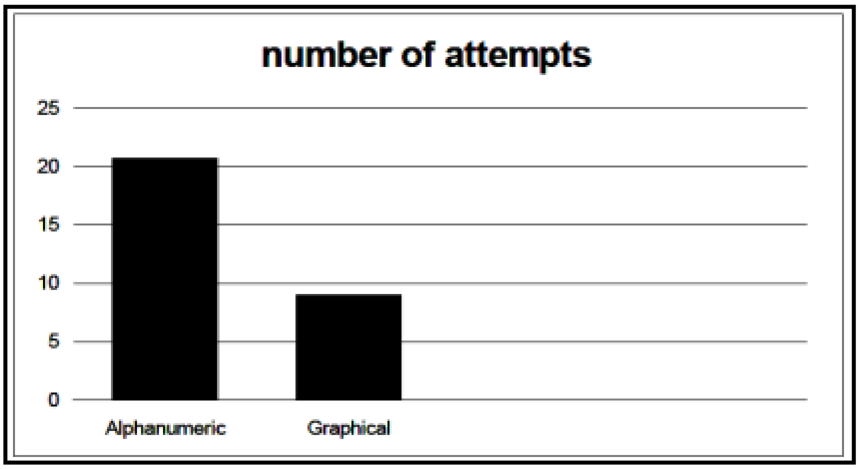

Figure 3: Graph for Number of Attempt to Remember Password

V. Conclusion

The system for securing web accounts using graphical password authentication through MD5 is implement successfully. It can be conclude that, this system overcome the drawback of previous existing system like user don't have to remember the difficult text based password, problems of attacks like shoulder surfing and dictionary attacks. It is user friendly authentication scheme which can be used by all the types of user very easily. The system takes slightly more time than other system but in measure of security it is better than existing system. It also provides the feature of file sharing among multiple users by single click.

References

[1] P. P. Ray, "Ray's scheme: Graphical password based hybrid authentication system for smart hand held device," *Journal of Information Engineering and Application,* vol. 2, no. 2, 2012.

[2] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system*".* *International Journal of Human-Computer Studies,* 63 (1-2): 102-127, 2005.

[3] Ali Mohamed Eilejtlawi, "Study and development of a new graphical password system", May 2008.

[4] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords, *School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada,* Vol.5, ACM CCS'09, November 9–13, 2009.

[5] Z. K. Suchita Sawla, Ashvini Fulkar and S. Solanki, "Graphical password authentication system in an implicit manner," *International Journal of Cryptography and Security,* vol. 2, no. 2249-7019, pp. 27-29, 2012.

[6] F. Towhidi, M. Masrom and A. A. Manaf, "An enhancement on Passface graphical password authentication," *Journal of Basic and Applied Scientific Research,* vol. 2, no. 2, 2013.

[7] S. Chiasson, P.C. van Oorschot, and R. Biddle. "Graphical password authentication using Cued Click Points". In European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[8] Khan. W. Z., Aalsalem. A. Y., Xiang. Y. (2011), A graphical password based systems for mobile devices. *International Journal of Computer Science and Issues*, Vol. 8, Issue 5, No. 2, 145-154.

[9] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical passwords" *in Proceedings of USENIX Security Symposium,* Vol.42, August 1999.

[10] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing" Vol.5.

[11] Berson, Thomas A. "Differential Cryptanalysis Mod 232 with Applications to MD5". *In European Symposium on Research in Computer Security (ESORICS),* Vol.2, pp. 71–80. ISBN 3-540-56413-6, 1992.

[12] Wells Jason, Hutchinson Damien and Pierce Justin Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management Conference, 58.

[13] R.Dhamija and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[14] 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.

[15] K. Renaud and E. Smith. Jiminy: "Helping user to remember their passwords". Technical report, *School of Computing, University of South Africa,* 2001.