A graphical password authentication system

Dolase Dadasaheb Gowardhan[1], Prathmesh Narayan kamble[2], Aman Akil Shaikh[3], Ade Vikas Shahu[4]
[1,2,3,4]*Shri Chhtrapati Shivaji Maharaj college of Engineering, nepti*

***Abstract*— Authentication is a technique for granting users access to system objects based on their individuality. If the code matches, the procedure is completed, and the user is given permission to access the system. Text-based password schemes adhere to standards including being at least 8 characters long, using a combination of upper- and lower-case letters, and using numerals. Due to the limitations of the human brain, users struggle to remember complex passwords over time and frequently forget them. The same password is frequently used by users for all types of accounts. Therefore, there is a high likelihood that other accounts will also be compromised if one is. In addition, using a simple text-based password may make it more vulnerable to attacks and invasions. As a result, this project has added graphical password authentication using the passpoints system. A model is used to determine the places that users are most likely to click while creating graphical passwords in the authentication process for graphical passwords utilising the passpoints scheme. Since users are already familiar with textual graphical password schemes, the intended scheme's operation is straightforward and simple to understand. Finally, because it is simple to remember and challenging for others to decipher, this graphical password scheme will make it simpler for users to complete their authentication process.**

***Keywords* – Authentication, Password, Security, Graphical Password, Pass Points, Authentication.**

I. INTRODUCTION

Physical security safeguards people and physical property against criminal behaviour; cyber security safeguards computer systems, back-end systems, and end-user applications as well as the data they hold. Its objective is to prevent hackers, nefarious insiders, and other people from accessing, damaging, disrupting, or altering IT systems and applications.

Alphanumeric passwords are a traditional, out-of-date, and widely used form of authentication. Practically speaking, the standard method is a dangerous system. For instance, if a user doesn't use a strong password, the attacker may use a password that is simple to decipher. A user is permitted to use the same password across many devices or websites. Regular users are exposed as a result of all of these features. And during authentication, one of the crucial security points, the user actively bears responsibility for the security of their personal data. Dictionary and brute force assaults are potential outcomes when employing an antiquated, traditional password method.

A. Motivation

Because usability decreases as password strength grows, the text-based solution cannot accomplish the goal. It ensures that the system's usability and security are both preserved without requiring us to give up either of these requirements.

II. RELATED WORK

William Stallings and Lawrie Brown., "Computer Security: Principle and Practices."[1]. Interest in education in computer security and related topics has been growing at a dramatic rate in recent years. This interest has been spurred by a number of factors, two of which stand out: 1. As information systems, databases, and Internet-based distributed systems and communication have become pervasive in the commercial world, coupled with the increased intensity and sophistication of security-related attacks, organizations now recognize the need for a comprehensive security strategy. This strategy encompasses the use of specialized hardware and software and trained personnel to meet that need.

Susan Wiedenbecka,, Jim Watersa, Jean-Camille Birgetb , Alex Brodskiyc, Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", [2] Finally, the actual evaluation of PassPoints reveals its advantages and disadvantages. Users using graphical passwords could make a good password fast and easily, but it took them longer and required more tries to memorise their passwords than users of alphabetic passwords. Over the course of six weeks, graphical users and alphanumeric users both retained their passwords, however graphical users continued to take longer to type their passwords. When it came to how simple, quick, and enjoyable their password system was, graphical users had

perceptions that were comparable to those of alphanumeric users.

Robert Morris and Ken Thompson., “Password security: a case history”, [3] UNIX is arguably more secure than most systems when it comes to password security. In the absence of careful consideration from subject-matter specialists, using encrypted passwords seems to be adequately secure.

Making an attempt to hide even encrypted passwords is worthwhile. An "external security code" is a requirement on some UNIX systems that users must enter when phoning in but before logging in. If this code is updated on a regular basis, someone with an outdated password will probably be unable to access it.

Daniel V. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security ”, [4] Good fences make good neighbours," as the saying goes. On a Unix system, many users also claim that they "don't need a solid password" since they "don't care who sees my files." Unfortunately, keeping data unsecured is not the same as leaving accounts open to attack. The data stored in the unprotected files is all that is at risk in the latter scenario, but the entire system is at risk in the former. Your home's front entrance is an invitation to the regrettably commonplace low-morale individuals, even if you only secure it with a cheap latch. The same is true for accounts that are susceptible to password cracking attacks.

Eugene H. Spafford., “Observing reusable password choices”, [5] In this essay, the design of a password collector was presented. The collector has provided some interesting design issues despite being created to facilitate investigation of a new password screening technique. To securely save obtained passwords for future analysis, the collector employs a public-key technique. The instrumented systems are not under any apparent danger during the collection operation. The method employed could be adapted to other contexts and readily expanded to gather additional data.

Sigmund N. Porter. “A password extension for improvedhuman factors”,[6] We utilise a reasonably big keyspace (64 bits) and a very long "passphrase" (up to 80 characters) to enhance both the difficulty of guessing passwords and also the simplicity of remembering passwords. The word is entered into the key and hashed, and it is then saved in encrypted form. One-way encryption is a necessary component of the hashing. Given the phrase's length, one would anticipate both the hashed and the original phrase to have a sizable keyspace. Since the owner finds meaning in the term, it ought should be simpler to remember.

XiaoyuanSuo, Ying Zhu, and G. Scott Owen,“Graphical passwords: A survey”,[7]The use of graphical passwords as an alternative to conventional text-based passwords has gained popularity during the past ten years. We have undertaken a thorough analysis of the graphical password approaches that are currently in use in this work. The two types of graphical password methods currently in use are recognition-based and recall-based methods.

Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud,“Is a picture really worth athousand words? exploring the feasibility of graphicalauthentication systems”,[8]In order to utilise visual memory for user authentication in self-service technologies, this research revealed a user-centered approach to the creation of cognometric mechanisms. Our experience has shown that designing an effective authentication method is a challenging process since it necessitates taking into account and balancing a number of crucial factors in order to achieve the highest levels of security and usability. No "miracle solution" exists, and the tension between these two goals occasionally seems insurmountable. This paper's contribution is the definition of a few variables that may impact the usability and security of graphical authentication techniques.

Siva Janakiraman, Karunya Sri V S, ChathuryaPulluri, SundararamanRajagopalan, K Thenmozhi, and RengarajanAmirtharajan, “Numerical Password via Graphical Input – An Authentication System on Embedded Platform”,[9] The system suggested in this paper enables the user to use graphical passwords while storing and authenticating them using hexadecimal numerical passwords. It is not necessary to store the pixel values for the selected block when LFSR is used to randomise the image matrix blocks during the authentication phase. In this strategy, increasing the picture matrix's dimension can increase the number of password combinations that are conceivable. As a result, the suggested technique works well for highly secure graphical password authentication for embedded devices with constrained memory resources.

Sung-Shiou Shen, Tsai-Hua Kang, Shen-Ho Lin,& Wei Chien, “Random Graphic User Password Authentication Scheme in Mobile Devices”[10] the self-developing keypad lock app's graphical user interface, which launches when the user tries to unlock the screen. To start, the placement of each digital button on the screen is chosen using a random number generator method that

generates random numbers. The user must think about the password sequence and the shortest route based on the location of each of the digital buttons on the screen, for instance, if the user password is set to "168". The app programme gives 1-2 redundant toleration digitals analysing mechanisms for the convenience of users, even if it is designed to determine the quickest path and password sequence. In other words, the sequence "1968" is the precise graphic user password.

III. PROPOSED METHODOLOGY

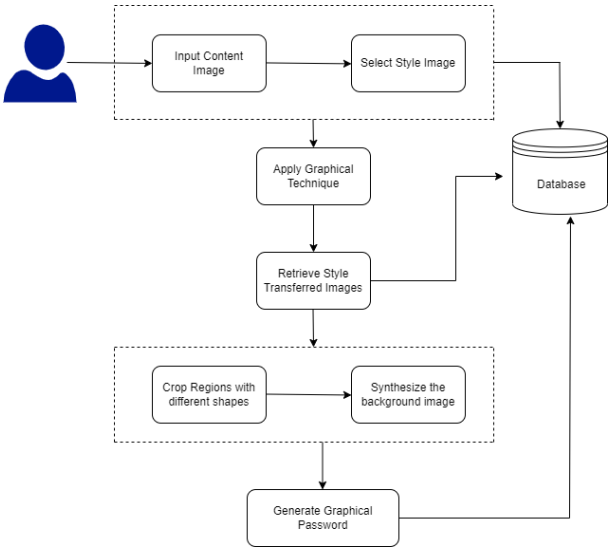


Fig. System Architecture

Algorithm1: Crop an Image(I, left, top, right, bottom)
Input: image I, rectangle with corners (left, top) and (right − 1, bottom − 1)
Output: cropped image I' of size new − width × new − height

1. new − width ← right − left
2. new − height ← bottom − top
3. I' ← AllocateImage(new − width, new − height)
4. for(x', y') ∈ I'do
5. I'(x', y') ← I(x' + left, y' + top)
6. return I'

Mathematical Model

Content Image Selection and choose convolution layer for feature maps: Given a chosen content layer l, the content loss is defined as the Mean Squared Error between the feature map F of our content image C and the feature map P of our generated image Y.

$$\mathcal{L}_{content} = \frac{1}{2}\sum_{i,j}(F_{ij}^{l} - P_{ij}^{l})^2$$

Calculate Gram-matrix for style image: Calculate the **Gram-matrix**(a matrix comprising of correlated features) for the tensors output by the style-layers. The Gram-matrix is essentially just a matrix of dot-products for the vectors of the feature activations of a style-layer. If the feature map is a matrix F, then each entry in the Gram matrix G can be given by:

$$G_{ij} = \sum_{k} F_{ik}F_{jk}$$

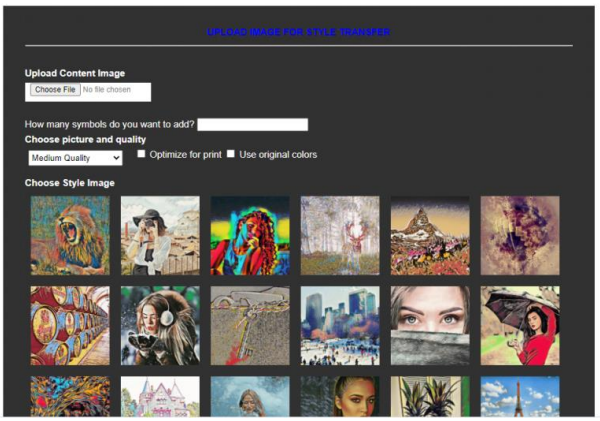
The loss function for style is quite similar to out content loss, except that we calculate the Mean Squared Error for the Gram-matrices instead of the raw tensor-outputs from the layers.

$$\mathcal{L}_{style} = \frac{1}{2}\sum_{l=0}^{L}(G_{ij}^{l} - A_{ij}^{l})^2$$

The total loss can then be written as a weighted sum of the both the style and content losses.

$$\mathcal{L}_{total} = \alpha\mathcal{L}_{content} + \beta\mathcal{L}_{style}$$

IV. RESULT AND DISCUSSION



V.CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.

REFERENCES

1. William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.
2. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63:102–127, July 2005.
3. Robert Morris and Ken Thompson. Password security: a case history. Communications of the ACM, 22:594–597, November 1979.
4. Daniel V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. In Proceedings of the 2nd USENIX UNIX Security Workshop, 1990.
5. Eugene H. Spafford. Observing reusable password choices. In Proceedings of the 3rd Security Symposium. Usenix, pages 299–312, 1992.
6. Sigmund N. Porter. A password extension for improved human factors. Computers Security, 1(1):54 – 56, 1982.
7. Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.
8. Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.
9. Real User Corporation. The science behind passfaces, June 2004. 10. G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.