Robust and Secure graphical password authentication system for multimedia data

Dr. Hetal Modi

Assistant Professor

Bhagwan Mahavir College of Computer Application

Bhagwan Mahavir University , Surat, Gujarat, IN

Abstract

The phrase “graphical password” denotes a technique of user authentication that employs pictorial information for validation purposes, as opposed to the traditional alphanumeric password. The utilization of this approach presents numerous obstacles, Memorability pertains to the ease with which a password may be recalled, while usability refers to the user-friendliness of the method. Additionally, security concerns arise due to the potential vulnerability of graphical passwords, as they may exhibit visual simplicity and susceptibility to forgery [12]. Graphical password methods can be categorized into three primary groups, which are determined by the nature of the cognitive task involved in password retrieval: acknowledgment, recall, and cued recall. The process of recognition is generally considered to be the least demanding for human memory, as it involves identifying material that has been previously encountered. On the other hand, pure recall is often seen as the most challenging task, as it necessitates retrieving information from memory without any external cues or prompts. Cued recall can be positioned between these two memory retrieval methods, since it involves the provision of a cue that serves to generate the appropriate context and activate the stored memory.

Keywords— graphical password, authentication, hack, network security ,precision, recall.

Introduction

Graphical Password

A graphical password refers to an authentication mechanism wherein users are required to select images displayed in a certain order within an interactive user interface (GUI) issue of password security. The concept of graphical passwords, initially introduced by Greg Blonder in his patent titled Graphical Passwords (United States Patent 5559961, 1996), involves allowing.

A password is a confidential piece of information utilized for the purpose of authentication. Passwords are a widely employed means of user identification in computing and communication networks. The information is intended to be exclusive to the user. A graphical password refers to an authentication mechanism wherein provided within a user interface that is graphical (GUI). Due to this rationale, the graphical password methodology is occasionally referred to as graphical authentication for users (GUA) [1]. the user to interact with certain areas of a picture displayed on the screen by means of a mouse or stylus input user is required to select the identical regions once more [11].

Research suggests that humans have a higher capacity for remembering visual information password schemes, offering both enhanced usability and improved security. The first technique pertains to recognition-based graphical authentication, while the second technique pertains to recall-based graphical authentication [7].

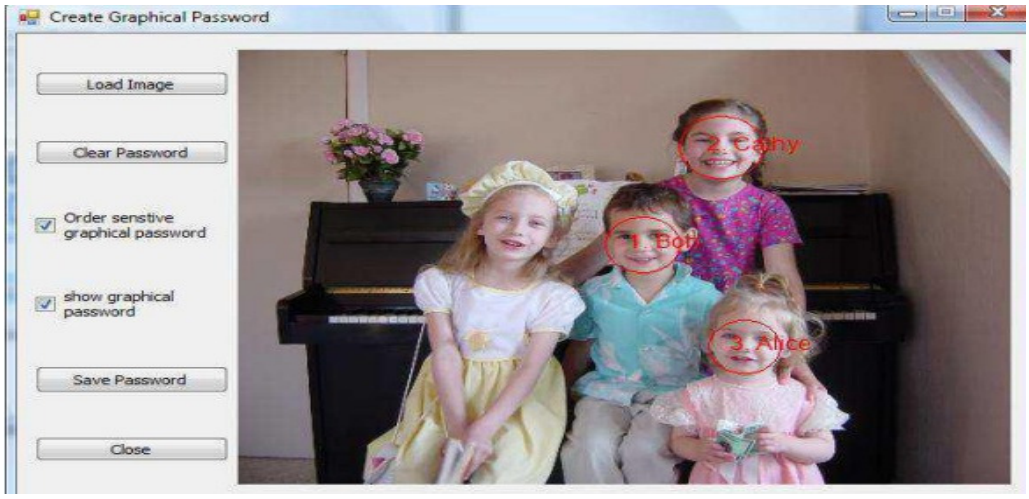

Figure 1: An example of creating a graphical password [7]

Figure 1. depicts an illustrative instance whereby a user generates a graphical password. In this instance, the user selects an image of his or her offspring by activating the "Load Image" button. Subsequently, the user proceeds to select the facial representations of the children in a sequential manner based on their respective ages, with strict adherence to the prescribed order. The user is required to input the name or nickname of the child for each designated region [3].

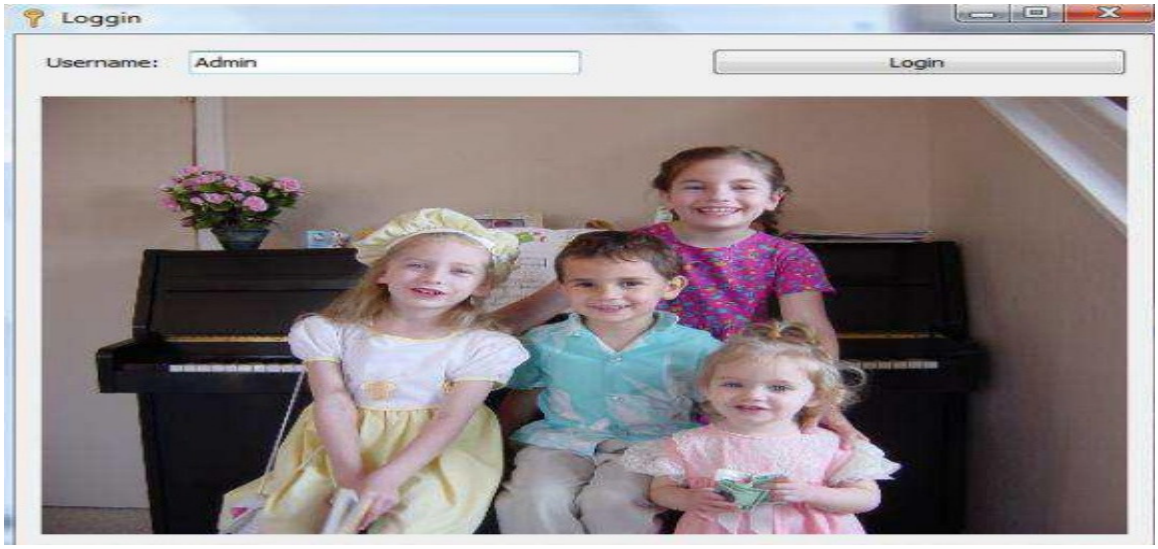

Figure 2: Login Screen [3]

Sr no.	Paper title	Author name	Summary	Limitation
1	**An Eye Gaze-driven Metric for Estimating the Strength of Graphical Passwords based on Image Hotspots**	**Argyris Constantinides, Marios Belk, Christos Fidas, Andreas Pitsillides,ACM2020**	The eye gaze-driven metric evaluates graphical password strength by analyzing users' eye movements to identify image hotspots. By determining which areas attract the most attention, this approach assesses password vulnerability and guides the creation of stronger, more secure passwords by avoiding predictable selections	The eye gaze-driven metric's limitations include the need for specialized eye-tracking hardware, potential variability in user attention patterns, and difficulty in accurately modeling complex visual stimuli. It may also overlook non-visual cognitive factors affecting password choice, leading to inconsistent strength assessments across different users and contexts.

			based on visual attention patterns.	
2	**Shoulder surfing: From an experimental study to a comparative framework**	**Leon Bošnjak, Boštjan Brumen, ARXIV2019**	The study explores shoulder surfing, a security risk where attackers visually obtain sensitive information. Through experiments and comparative analysis, it assesses different authentication methods' vulnerabilities. Findings highlight the need for enhanced security measures and offer a framework for evaluating the resilience of authentication systems against shoulder surfing threats.	The study's limitations include a controlled environment that may not replicate real-world scenarios, a limited sample size that affects generalizability, and potential bias in participants' awareness of being observed. Additionally, it primarily focuses on common authentication methods, potentially overlooking emerging technologies and innovative security solutions.
3	**On the Accuracy of Eye Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords**	**Argyris Constantinides, Marios Belk ,Christos Fidas, Andreas Pitsillides, RESCHRCH GATE 2019**	This study evaluates eye gaze-driven classifiers' effectiveness in determining image content familiarity within graphical passwords. By	Eye gaze-driven classifiers for predicting image content familiarity in graphical passwords face limitations such as variable gaze patterns among users, potential privacy concerns,

			analyzing users' eye movements, the research aims to predict how familiar users are with specific images, enhancing password security by identifying patterns that might indicate predictable password choices and vulnerabilities.	environmental lighting conditions affecting accuracy, high computational cost, and difficulties in handling involuntary eye movements, which may affect prediction reliability.
4	**Development Status and Prospects of Graphical Password Authentication System in Korea The user's text is already academic and does not need to be rewritten.**	**Gi-Chul Yang, ISSN2019**	The graphical password authentication system in Korea is currently evolving, focusing on enhancing security and user experience. Despite its advantages over traditional passwords, challenges remain, such as usability, security vulnerabilities, and implementation costs. Future prospects include integrating biometric elements and improving technology to address	The graphical password authentication system in Korea faces limitations, including susceptibility to shoulder surfing attacks, memory burden on users due to complex patterns, vulnerability to pattern prediction, higher implementation costs compared to traditional passwords, and challenges in balancing security with user convenience and accessibility across various devices.

			these issues effectively.	
5	**Enhancing the Security of FinTech Applications with Map-Based Graphical Password Authentication**	**Weizhi Menga,Liqiu Zhub, Wenjuan Li,Jinguang Hand, Yan Lie ,ELSVEIR 2019**	It uses geographical locations as passwords, making them harder to guess and resistant to common attacks. This approach improves user engagement and security, balancing ease of use with robust protection against unauthorized access.	Map-based graphical password authentication for FinTech applications faces limitations such as the potential for shoulder surfing attacks, difficulties in remembering complex map locations, high susceptibility to phishing, increased cognitive load on users, and challenges in ensuring compatibility with various devices and screen sizes, impacting usability and security.

Problem definition

- **Vulnerability to Attacks:** Graphical passwords are susceptible user's interactions.
- **Predictability:** Users often choose predictable patterns or images, making it easier for attackers to guess the password through pattern recognition techniques.
- **Implementation Complexity:** Developing and deploying graphical password systems require more complex algorithms and higher computational resources compared to traditional text-based passwords, posing challenges for developers.
- **User Memorability Issues:** While graphical passwords are designed to be more memorable, users may still struggle to recall complex or abstract graphical patterns, leading to frequent password resets and frustration.

- **Device Compatibility:** Ensuring compatibility across various devices and screen sizes can be challenging, affecting the usability and accessibility of graphical password systems.
- **Phishing Vulnerability:** Graphical passwords can be vulnerable to phishing attacks if users are tricked into revealing their password sequence on malicious platforms or interfaces.
- **Cognitive Load:** Users may experience increased cognitive load when creating and remembering intricate graphical passwords, which can impact the overall user experience and willingness to adopt the system.

Performance Metrics

The majority of the time, performance metrics like Accuracy, Precision, Recall and F1 Score can be used to determine how well our proposed model is performing.

Comparison			
Factors	**Text-based Image (Captcha Image)**	**Shape Based Image (Car image)**	**Color-Based (Abstract Color Image)**
Accuracy	0.8185	0.9998	1
Sensitivity	0.7875	1.0	1
Specificity	0.8306	0.9998	1
Precision	0.9092	1.0	1
Recall	0.7875	1.0	1
F-Measure	0.8728	-	-
G- Mean	0.8103	1.0	1

Table 1: Performance Metrics

Proposed System

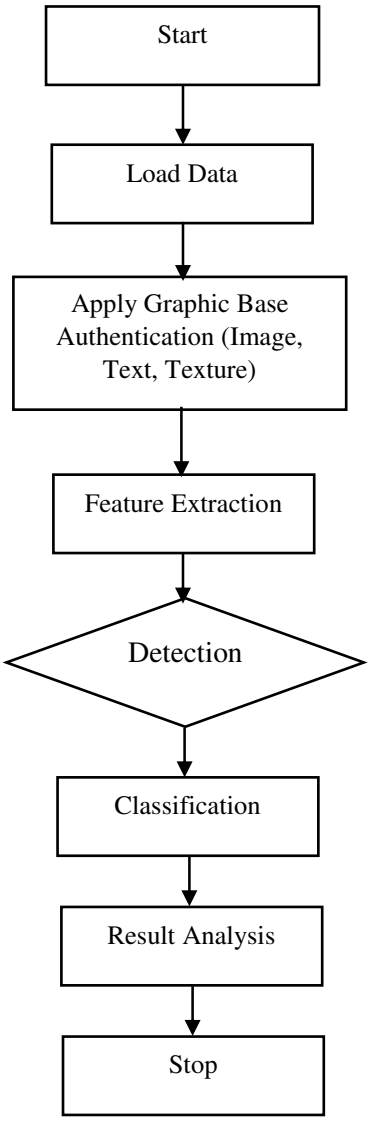

Figure 3: Flow of Proposed System

Algorithm Steps

- **Initialize User Input:** The algorithm begins by capturing the input provided by the user through an interface, which is then stored for processing.

- **Validate Input Data:** The algorithm checks if the user input meets the required criteria. If the input is invalid, an error message is generated, and the process is halted.
- **Process Input:** Upon successful validation, the algorithm processes the input by applying predefined rules or logic relevant to the system's functionality.
- **Database Access:** The algorithm interacts with the database, either retrieving necessary data or storing processed information as required.
- **Generate Response:** Based on the processing and database interaction, the algorithm generates an appropriate response.
- **Deliver Output:** The final step involves sending the generated response back to the user interface, where it is presented as feedback or result, completing the algorithm's execution

Results and Discussion

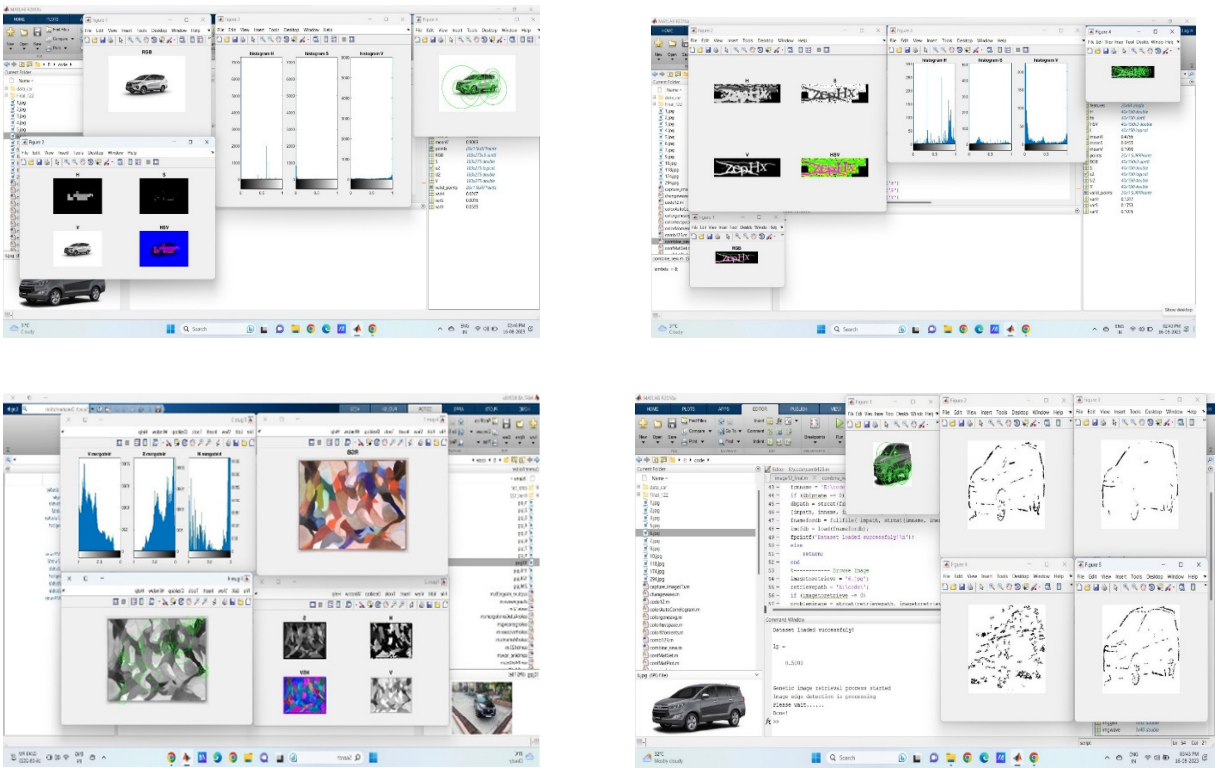

Figure 4: a) Histogram of Color, text and shape-based Image

b) Edge Detection in text, color and Shape based Image

Conclusion

Graphical password systems present a promising alternative to traditional alphanumeric passwords, offering significant advantages in terms of security and user experience. By leveraging the human brain's superior ability to recognize and recall images over text, these systems provide a more intuitive and memorable authentication method. The proposed model, incorporating dynamic image grids, multi-layered images, and pattern obfuscation, addresses key security challenges such as shoulder surfing, pattern recognition, and phishing attacks.

One of the primary benefits of graphical passwords is their potential to enhance security through complex and unpredictable password patterns. By implementing techniques such as user-specific salting, time-based authentication, and multi-factor authentication, this model ensures that unauthorized access is considerably more difficult, providing a robust defense against common attack vectors. Moreover, the use of adaptive user interfaces and memory aids helps maintain user convenience without compromising security, catering to a diverse range of users across different devices and platforms.

In conclusion, graphical password systems have the potential to significantly enhance the security landscape by providing a more secure, user-friendly, and innovative approach to authentication. By addressing current limitations and continuously evolving the technology, graphical passwords can offer a viable and effective solution to meet the increasing security demands of today's digital world. With further development and widespread implementation, graphical password systems can pave the way for a more secure and user-centric authentication future.

References

[1] Argyris Constantinides, Marios Belk, Christos Fidas, Andreas Pitsillides, An Eye Gaze-driven Metric for Estimating the Strength of Graphical Passwords based on Image Hotspots, ACM 2020.

[2] Leon Bošnjak, Boštjan Brumen, Shoulder surfing: From an experimental study to a comparative framework, ARXIV2019

[3] Argyris Constantinides, Marios Belk ,Christos Fidas, Andreas Pitsillides, On the Accuracy of Eye Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords, RESCHRCH GATE 2019.

[4] Gi-Chul Yang, Development Status and Prospects of Graphical Password Authentication System in Korea The user's text is already academic and does not need to be rewritten.ISSN2019.

[5] Weizhi Menga,Liqiu Zhub, Wenjuan Li,Jinguang Hand, Yan Lie , Enhancing the Security of FinTech Applications with Map-Based Graphical Password Authentication, ELSVEIR 2019.

[6] S. Vaithyasubramaniana, A. Christyb D.Lalitha, "Two factor Authentication for Secured

Login Using Array Password Engender by Petri net", ELSEVIER, 2015.

[7] Neha Singh, Nikhil Bomanwar, "Improved Authentication Scheme Using Password Enabled

Persuasive Cued Click Points", IEEE, 2015.

[8] Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle,

"Comparison of Graphical Password Authentication Techniques", International Journal of

Computer Applications, 2015.

[9] Andrea Bianchi, Ian Oakley, and Hyoungshick Kim, "PassBYOP: Bring Your Own Picture

for Securing Graphical Passwords", IEEE, 2015.

[10] Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally, "Graphical Password-Based User

Authentication with Free-Form Doodles", IEEE, 2015.

[11] Pooja Jaiprakash Kulkarni, Dr. G. M. Malwatkar, "The Graphical Security System by using

CaRP", IEEE, 2015.

[12] Swaleha Saeed, M. Sarosh Vmar, "A Hybrid Graphical User Authentication Scheme", IEEE,

2015.

[13] Liew Tze Hui, Housam Khalifa Bashier, Lau Siong Hoe, Goh Kah Ong Michael, Wee Kouk

Kwee, "Conceptual Framework for High-End Graphical Password", IEEE, 2014.

[14] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, “Graphical Password Authentication”, IEEE, 2014.

[15] Longyan Gong, Jingxin Pan, Beibei Liu, Shengmei Zhao, “A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords”, ELSEVIER, 2013.

[16] Sadiq Almuairfi, Prakash Veeraraghavan, Naveen Chilamkurti, “A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices”, ELSEVIER, 2013.

[17] Uma D. Yadav, Prakash S. Mohod, “Adding Persuasive features in Graphical Password to increase the capacity of KBAM”, IEEE, 2013.

[18] M.Arun Prakash, T.R. Gokul, “Network Security-Overcome Password Hacking Through Graphical Password Authentication”, IEEE, 2011.

[19] John Charles Gyorffy · Andrew F. Tappenden · James Miller, “Token-based graphical password authentication”, Springer, 2011.

[20] Wei Hu, Xiaoping Wu, Guoheng Wei, “The Security Analysis of Graphical Passwords”, IEEE, 2010