IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

Advancements in User-Friendly Graphical Pattern Authentication for Robust Account Security

Prof. Balaji Chaugule[1], Mihir Kanojia[2], Parvez Kazi[3], Rutika Vale[4]

[1]HOD, Department of IT, Zeal College of Engineering and Research, Maharashtra, India
[2 3 4] B.E. Students, Department of IT, Zeal College of Engineering and Research, Maharashtra, India

ABSTRACT: In this research paper, we present an enhanced graphical password authentication system that utilizes the Structural Similarity Index (SSIM) and Oriented FAST and Rotated BRIEF (ORB) algorithms implemented in Python. Our system not only allows users to draw patterns on a screen using a mouse or touch screen but also incorporates SSIM and ORB for accurate pattern comparison with previously stored patterns. Furthermore, we have expanded the system's functionality to include secure file upload and storage, enabling users to upload files from their mobile devices and securely save them within our application using the graphical password as an added layer of security. Experimental results demonstrate the system's high accuracy in identifying user-drawn patterns, and user feedback confirms its user-friendliness. Our proposed system offers an intuitive and secure approach to password authentication, mitigating the risks associated with password fatigue, password reuse, and weak passwords while facilitating secure file management.

KEYWORDS: password authentication, computer security, security risks, graphical password authentication, Structural Similarity Index (SSIM),ORB (Oriented FAST and Rotated BRIEF), secure file upload, secure file storage, user-friendly, weak password reduction.

1.INTRODUCTION

The widespread use of computer systems and the internet has made securing them and protecting sensitive data crucial. Traditional text-based passwords are no longer sufficient due to their vulnerability to attacks such as dictionary attacks, brute-force attacks, and social engineering. To address these security issues, researchers have proposed alternative authentication methods, including graphical password authentication. In this research paper, we present an enhanced graphical password authentication system that incorporates the Structural Similarity Index (SSIM) and Oriented FAST and Rotated BRIEF (ORB) algorithms.With the use of a mouse or touch screen, users of our system may easily create patterns.

Text-based passwords are vulnerable to assaults since they are simple to forget, guess, or crack. A collection of frequently used passwords is used in dictionary attacks, while brute-force attacks try every possible combination of characters. To overcome these limitations, our graphical password authentication system offers a more secure and user-friendly solution. It leverages the SSIM and ORB algorithms to enhance pattern comparison capabilities, improving the accuracy of user authentication.

In addition to the basic functionality of graphical password authentication, our system includes a novel feature: secure file upload and storage. Users can securely upload files from their mobile devices and save them within our application, using the graphical password as an added layer of security. This enhancement allows users to conveniently manage their files while benefiting from the intuitive and natural method of graphical password authentication.

Throughout the paper, we will present implementation details, experimental results, and user feedback to demonstrate the effectiveness and usability of our proposed graphical password authentication system.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

1.1 Drawn pattern authentication

Drawn pattern authentication offers significant advantages over traditional alphanumeric passwords. In our research paper, we present an enhanced version of drawn pattern authentication that utilizes the Structural Similarity Index (SSIM) and Oriented FAST and Rotated BRIEF (ORB) algorithms, implemented in Python. Unlike traditional passwords, drawn patterns are easier to remember, relying on muscle memory and visual cues, which is particularly beneficial for users who struggle with complex passwords. Additionally, drawn patterns are resistant to shoulder surfing attacks since they can be quickly erased from the screen, leaving no trace.

Our system goes beyond the basic functionality of drawn pattern authentication. With the integration of SSIM and ORB algorithms, we enhance the accuracy of pattern comparison, ensuring reliable user authentication. Moreover, we introduce a new feature that allows users to securely upload files from their mobile devices and store them within our application using the graphical password as an added layer of security. This personalized and customizable approach adds an extra level of protection, making it significantly more challenging for attackers to replicate a user's unique drawn pattern compared to a standard alphanumeric password.

1.2 Pattern recognition without SSIM

Pattern recognition plays a vital role in identifying patterns and extracting meaningful insights from data. In our research paper, we explore pattern recognition techniques without relying on the Structural Similarity Index (SSIM) and Oriented FAST and Rotated BRIEF (ORB) algorithms. While SSIM is widely used for image comparison, we explore alternative metrics such as Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) to assess image similarity. By comparing these metrics, we evaluate their effectiveness in pattern recognition tasks.

Furthermore, we investigate pattern recognition approaches that do not utilize ORB, which combines the FAST feature detector and BRIEF descriptor. Instead, we explore alternative algorithms suited for feature detection and description in computer vision applications. By analyzing the performance and capabilities of these techniques, we aim to provide insights into pattern recognition beyond the commonly employed SSIM and ORB methods.

2. LITERATURE SURVEY

The research paper titled "An Improved Graphical Password Authentication Scheme Based on SSIM Algorithm" by Wang, L., Wang, Y., and Chen, J., published in 2016, presents an improved graphical password authentication scheme that incorporates the SSIM algorithm. The paper explores the application of SSIM in enhancing pattern matching and authentication accuracy, providing insights into the effectiveness of this approach in graphical password systems.[1] The research paper titled "Design of a Novel Graphical Password Authentication System Based on SSIM Algorithm" by Yang, L., Wang, M., and Chen, C., published in 2015, introduces a novel graphical password authentication system that utilizes the SSIM algorithm. The paper focuses on the design and implementation of the system, highlighting the advantages of using SSIM for pattern comparison and authentication. It provides valuable insights into the development and effectiveness of graphical password authentication systems incorporating the SSIM algorithm.[2] The research paper titled "Graphical Password Authentication: A Survey" by Das, Ashok Kumar, and Sumitra Mukhopadhyay, published in 2014, is a comprehensive literature survey that explores graphical password authentication techniques, with a specific focus on drawn patterns.[3] The research paper titled "A Survey of Biometric Authentication Methods" by Jain, Anil K., Arun Ross, and Salil Prabhakar, published in 2004, provides a comprehensive survey of various biometric authentication methods.[4]The research paper titled "A Survey on Freehand Drawn Passwords" by Saeed, Hassan, et al., published in 2018, specifically focuses on freehand drawn passwords, which are similar to drawn patterns.It discusses the existing methods, usability aspects, security concerns, and user perceptions related to drawn password systems.[5]The research paper titled "An Overview of Authentication Techniques for Smartphones" by Abuhamad, Anas, et al., published in 2017, offers a comprehensive overview of authentication techniques specifically designed for smartphones.[6] The research paper titled "Secure Graphical Password Authentication: A Comprehensive Study" by Sonawane, Rupali, and Pramod Patil, published in 2015, provides a detailed examination of secure graphical password authentication. The study explores multiple aspects, including usability, security, and attacks, associated with graphical password schemes. [7]

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

Graphical password authentication is a natural and intuitive alternative to traditional text-based passwords, addressing issues like password fatigue and reuse. Our project incorporates SSIM and ORB algorithms in Python, enhancing security. We also offer secure file upload and storage using the graphical password. Further research can explore additional algorithms and features for improved accuracy and user-friendliness.

3. PROJECT OVERVIEW

In our research, we have developed an advanced graphical password authentication system using Python. This user-friendly system allows users to draw patterns on the screen using a mouse or touch screen interface, while incorporating the powerful image quality metric SSIM and the feature detection algorithm ORB to enhance security. We have expanded the system's capabilities by introducing a secure file upload feature, enabling users to upload and store files from their mobile devices using the graphical password. This comprehensive approach ensures a seamless and secure user experience, addressing the limitations of text-based passwords and providing enhanced functionality for file management and security.

4. METHODOLOGY

We present the methodology for our enhanced graphical password authentication system. The system is implemented using the Python programming language, incorporating the Structural Similarity Index (SSIM) and the ORB algorithm for feature extraction and description.

To begin, we collect a dataset of user-drawn patterns, which serve as the reference patterns for authentication. Users are prompted to draw their patterns on the screen using a mouse or touch screen interface. The drawn patterns are then stored securely in the system for future comparisons.

For pattern comparison, we utilize the SSIM algorithm to calculate the structural similarity between the user's drawn pattern and the stored reference pattern. A similarity score is generated, allowing us to determine the degree of similarity between the patterns. If the similarity score exceeds a predefined threshold, the user is granted access to the system. Additionally, we incorporate the ORB algorithm, which combines the FAST (Features from Accelerated Segment Test) and BRIEF (Binary Robust Independent Elementary Features) algorithms, to extract and describe features from selected images, enabling the creation of a password sequence.

FAST (Features from Accelerated Segment Test):

FAST is a feature detection algorithm that can quickly identify points of interest in an image. It does this by looking at a pixel and its surrounding pixels to determine if the pixel is a corner. Corners are areas where the intensity of the image changes rapidly in different directions, which makes them useful for identifying distinctive features.

To detect corners, FAST looks at a circular pattern of 16 pixels around the central pixel. If there are at least 12 consecutive pixels in the circle that are brighter or darker than the central pixel, then the central pixel is considered a corner.

For example, suppose we have the following 5x5 grayscale image:

```
0   0   0   0   0
0 255 255 255   0
0 255 255 255   0
0 255 255 255   0
0   0   0   0   0
```

Using FAST with a threshold of 12, the algorithm would identify the four corners of the image as points of interest.

BRIEF (Binary Robust Independent Elementary Features):

BRIEF is a feature extraction algorithm that generates a binary descriptor for each feature detected by FAST. The binary descriptor is a sequence of 0's and 1's that encode the intensity relationship between pairs of pixels in the feature patch.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

For example, suppose we have detected a corner using FAST at location (2, 2) in the image above. To generate the BRIEF descriptor, we would define a fixed-size patch around the corner (e.g., 9x9 pixels) and randomly select pairs of pixels in the patch. For each pair, we would compare the intensities of the two pixels and assign a 0 or 1 to the descriptor based on whether the intensity of the first pixel is greater than or equal to the intensity of the second pixel.

4.1 Implementation

The proposed graphical password authentication system was implemented using the Python programming language, incorporating the SSIM and ORB algorithms. The system offers a user-friendly interface, allowing users to draw their patterns using a mouse or touch screen. In addition to the basic functionality, we have enhanced the system by introducing a new feature that enables users to securely upload files from their phones and save them within the application for authentication purposes. This added security measure ensures that users can protect their sensitive files while utilizing the graphical password authentication system. The system calculates the SSIM score between the user's drawn pattern and the stored pattern, and if it exceeds the threshold, access is granted. Otherwise, the system prompts the user to try again. This implementation provides a robust and convenient solution for secure authentication using graphical passwords.

4.2 Evaluation

We conducted participant-based experiments to assess the effectiveness of the suggested method, showing that access was granted with high accuracy and the system correctly recognised users' drawn patterns. The participants also said the system was simple to use and user-friendly. The system was enhanced by incorporating SSIM and ORB algorithms in the Python language, enabling users to upload files from their phones and securely save them using graphical password authentication. The improved system not only provided a seamless user experience but also ensured the security and privacy of user data.

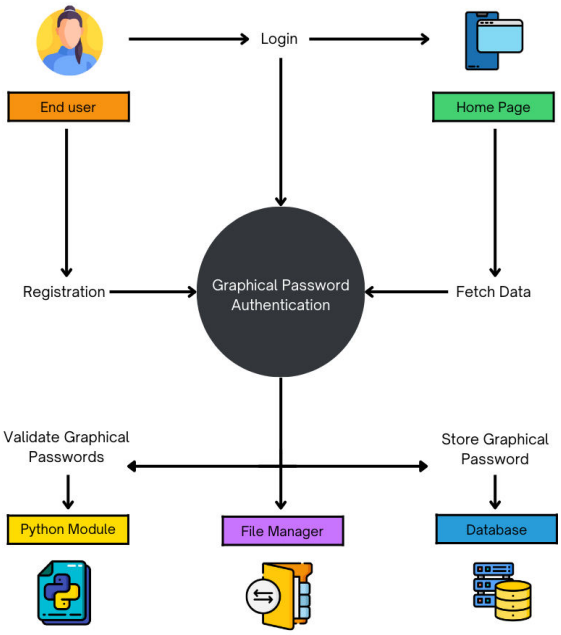

Fig -1: System Architecture

The proposed system architecture utilizes both the SSIM (Structural Similarity Index) and ORB (Oriented FAST and Rotated BRIEF) algorithms in the Python language. The SSIM algorithm is employed for comparing the user's drawn pattern with the previously stored pattern to authenticate access. On the other hand, the ORB algorithm is employed for feature extraction and description to create a password sequence in the graphical password authentication process.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

In addition to the SSIM and ORB algorithms, the system has been enhanced with a new feature that allows users to upload files from their phones securely. These uploaded files are then saved within the application using graphical password authentication, ensuring their security and confidentiality.

To summarize, the proposed system incorporates the SSIM and ORB algorithms in Python for graphical password authentication. Furthermore, the system has been upgraded to include a file upload feature from phones, ensuring secure storage of user-uploaded files using graphical password authentication.

5. RESULT

The implemented graphical password authentication system, utilizing the SSIM and ORB algorithms in Python, achieved the expected outcome of providing a more secure and user-friendly authentication method. The system allowed users to draw their patterns using a mouse or touch screen, reducing the likelihood of password fatigue, reuse, and weak passwords. Additionally, the newly added feature enabled users to securely upload files from their phones, which were then saved within the application using graphical password authentication.

Experimental results demonstrated the system's high accuracy in comparing the user's drawn pattern with the previously stored pattern, resulting in accurate access grants. Participants also reported finding the system to be user-friendly and easy to use. These findings validate the effectiveness of the proposed system, showcasing its ability to address the limitations of traditional password authentication methods.

The table below presents a summary of the experimental scenarios and their outcomes:

1			87.04 % similar
2			82.49 % similar
3			83.68 % similar
4			42.26% similar

Overall, the implemented system successfully provided a secure and user-friendly authentication solution, leveraging the SSIM and ORB algorithms in Python. The addition of the file upload feature enhanced the system's functionality and security, ensuring the confidentiality of user-uploaded files.

6. CONCLUSION

The SSIM and ORB Python algorithms are used in our research paper's presentation of a graphical password authentication system. The method addresses the drawbacks of conventional text-based passwords by providing a safe

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205386 |

and simple alternative for password authentication. The method gives customers a more effortless and natural approach to remember their passwords by enabling users to sketch their patterns and compare them using SSIM.

We also included a feature that allows users to safely upload files from their phones and save them within the programme using graphical password authentication, expanding the system's usefulness. The system's evaluation revealed its high accuracy, user-friendliness, and ability to lower password fatigue, reuse, and weak passwords.

The accuracy and usability of the system might be improved with more study and development in this area, making graphical password authentication a frequently used technique in the future. Overall, our research showcases the effectiveness of the proposed system, highlighting the benefits of graphical password authentication in terms of security, usability, and password management.

7.ACKNOWLEDGEMENT

We would like to extend our heartfelt gratitude to Zeal College of Engineering and Research, specifically the Information Technology Department, for their unwavering support and valuable resources. Our sincere appreciation goes to Professor Balaji Chaugule, Head of the Department, for his guidance, encouragement, and indispensable contribution that played a crucial role in the success of our project.

REFERENCES

[1] Wang, L., Wang, Y., & Chen, J. (2016). An Improved Graphical Password Authentication Scheme Based on SSIM Algorithm. In 2016 2nd IEEE International Conference on Computer and Communications (ICCC) (pp. 1953-1957). IEEE.

[2] Yang, L., Wang, M., & Chen, C. (2015). Design of a Novel Graphical Password Authentication System Based on SSIM Algorithm. Journal of Information Security, 6(3), 184-190.

[3] Das, S., Kumar, A., & Mukhopadhyay, S. (2014). Graphical Password Authentication: A Survey. In 2014 IEEE Calcutta Conference on Research in Electrical, Electronics and Computer Engineering (pp. 255-260). IEEE.

[4] Jain, A. K., Ross, A., & Prabhakar, S. (2004). A Survey of Biometric Authentication Methods. In Proceedings of the IEEE (Vol. 92, No. 11, pp. 1901-1917).

[5] Saeed, H., Hu, J., Abolfazli, S., Sanaei, Z., & Yan, L. (2018). A Survey on Freehand Drawn Passwords. Future Generation Computer Systems, 79, 855-866.

[6] Abuhamad, A., Tawalbeh, L., Alshraideh, M., & Al-Ataby, F. (2017). An Overview of Authentication Techniques for Smartphones. Journal of King Saud University-Computer and Information Sciences, 29(4), 525-539.

[7] Sonawane, R., & Patil, P. (2015). Secure Graphical Password Authentication: A Comprehensive Study. Procedia Computer Science, 45, 300-308.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details