IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY SYSTEM USING IRIS

[1]Dr. C Usha, [2]Chandan B K, [3]Bharath Kumar M,[4] Dhanush B M, [5]Sunil M

[,2]Associate Professor, Department of Electronics and Communication Engineering, Cambridge Institute of Technology (CI Tech), Bengaluru, India

[1 ,3,4 5]Student, Department of Electronics and Communication Engineering, CITech, *Bengaluru, India*

Abstract: Graphical password authentication methods have garnered attention as an alternative to traditional text-based passwords, aiming to improve both security and usability. Nonetheless, numerous existing graphical password systems encounter usability challenges, such as poor memorability and susceptibility to various attacks. In this study, we introduce an innovative graphical password authentication approach intended to mitigate these usability issues while upholding security standards. Our approach incorporates both image recognition and user-generated patterns to establish a multi-layered authentication framework. Initially, users select a memorable image from a predefined array of categories and subsequently overlay a personalized pattern onto the chosen image. We integrate advanced image processing techniques to bolster resistance against shoulder surfing and other potential attacks. Furthermore, we conducted a usability assessment involving a diverse participant pool to evaluate the efficacy of our proposed approach. The findings indicate noteworthy enhancements in memorability and user satisfaction when compared to existing graphical password systems. In summary, our approach presents a promising avenue for enhancing the usability of graphical passwords while maintaining robust security measures.

I. INTRODUCTION

In today's digital landscape, authentication mechanisms serve as critical safeguards for protecting sensitive data and ensuring the security of online accounts. While traditional text-based passwords have long been the go-to method for user authentication, they come with a host of limitations, including vulnerability to brute-force attacks, low memorability, and susceptibility to phishing and social engineering tactics. To get beyond these obstacles, researchers have explored alternative authentication methods, with graphical password schemes emerging as promising alternatives.

Graphical password schemes offer a more intuitive and potentially more secure approach to authentication by enabling users to authenticate themselves using images, patterns, or a combination thereof, rather than relying solely on alphanumeric characters. Leveraging the human capacity for image recognition and recall, these schemes have the potential to enhance both security and usability. But even with their assurance, many existing graphical password schemes still grapple with usability challenges such as image or pattern selection and recall difficulties, susceptibility to shoulder surfing attacks, and scalability limitations.

This study addresses these issues by presenting a revolutionary graphical password authentication technique that maintains security standards while enhancing usability. Our plan aims to improve upon the drawbacks of current graphical password systems by incorporating cutting edge features and methods. In particular, we provide a multi-

layered authentication procedure that creates a robust and intuitive authentication system by combining picture recognition with user-generated patterns.

The rest of this essay proceeds as follows: In Section 2, significant advancements and difficulties in the field of graphical password authentication are highlighted in an overview of relevant work. In Section 3, we outline the design tenets and constituents of our suggested graphical password scheme and explain how it addresses usability issues while enhancing security. In Section 4, we explore the implementation details and elaborate on the assessment approach used to determine the scheme's effectiveness and usability. The results of our usability evaluation study are revealed in Section 5, which also explores the implications for the design of graphical password schemes. The work is finally concluded in Section 6, which also suggests directions for future research.

II. LITERATURE REVIEW

Table1.LiteratureReviewof Exploring Security Systems Utilizing Iris Recognition with various existing solutions

Published year	**Author Name**	**Title of the paper**	**Outcomes**
1993 [1]	Daugman	I Iris Recognition: A Method to Localize the Iris	Proposed the first working methodology on iris recognition.
1997 [2]	Wilde	An Efficient Iris Recognition Method Using Phase-Based Image Matching	Introduced a novel approach utilizing LED point source and gradient-based methods for iris recognition.
2001 [3]	Kong and Zhang	A Noise-Robust Iris Localization Method Based on Texture Segmentation	Developed a system focusing on noise disturbances and occlusions during iris segmentation.
2002 [4]	Huang et al	An Efficient Iris Recognition Technique	Described an efficient iris recognition technique using segmentation and feature extraction methods.
2005 [5]	Dorairaj et al	Iris Recognition using PCA and ICA Techniques for Non-Ideal Iris Images	Developed an algorithm for processing off-angle iris images using PCA and ICA techniques.
2014 [6]	Jan	Multi-Stage Iris Segmentation Framework	Introduced a multi-stage iris segmentation framework for localizing papillary and limbic boundaries of human eye images.
2019 [7]	Oyeniran et al	Multi-Algorithmic Technique for Iris Recognition	Proposed a multi-algorithmic technique for personal recognition using iris, employing multiple classifiers approach.

2020 [8]	Oyeniyi et al |	Enhanced Iris Feature Extraction using Continuous Wavelet Transform |	Proposed an enhanced iris feature extraction method using continuous wavelet transform.

III. PROPOSED METHOD

The need for reliable and effective authentication systems is expanding across a range of industries, but investigating and assessing cryptographic hardware solutions designed for embedded systems is still vital. By conducting a thorough literature analysis, this project seeks to close this gap in knowledge by identifying, evaluating, and contrasting current cryptographic hardware implementations for embedded systems, with an emphasis on their suitability and efficacy for use in iris recognition-based security systems. This study looks at the benefits, drawbacks, and performance indicators of various approaches in an effort to offer insightful information for the creation and improvement of reliable security systems that use iris recognition technology in embedded contexts. Existing graphical password authentication systems vary in their approaches to balancing usability and security. Some systems rely solely on images or patterns chosen by users, while others incorporate additional factors such as knowledge-based authentication or persuasion techniques to enhance security. However, many of these systems still face usability challenges and vulnerabilities that can compromise their effectiveness. Our innovative graphical password authentication system revolutionizes user authentication, blending image recognition with user-generated patterns for heightened usability and security is shown in Figure 1. By harnessing human memory for images, our approach simplifies the authentication process while bolstering protection against cyber threats. It's a user-friendly, secure solution for today's digital landscape.

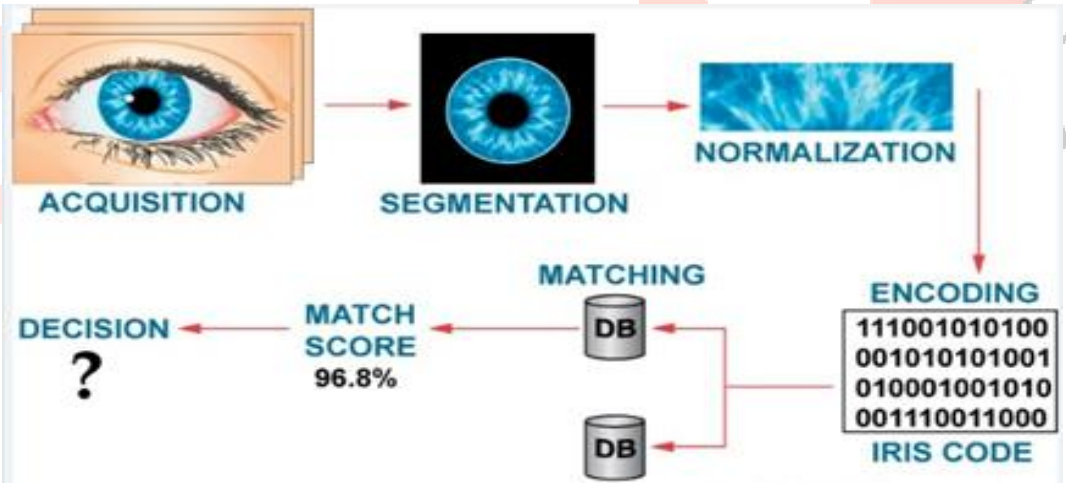


Figure 1: Block diagram of Proposed method

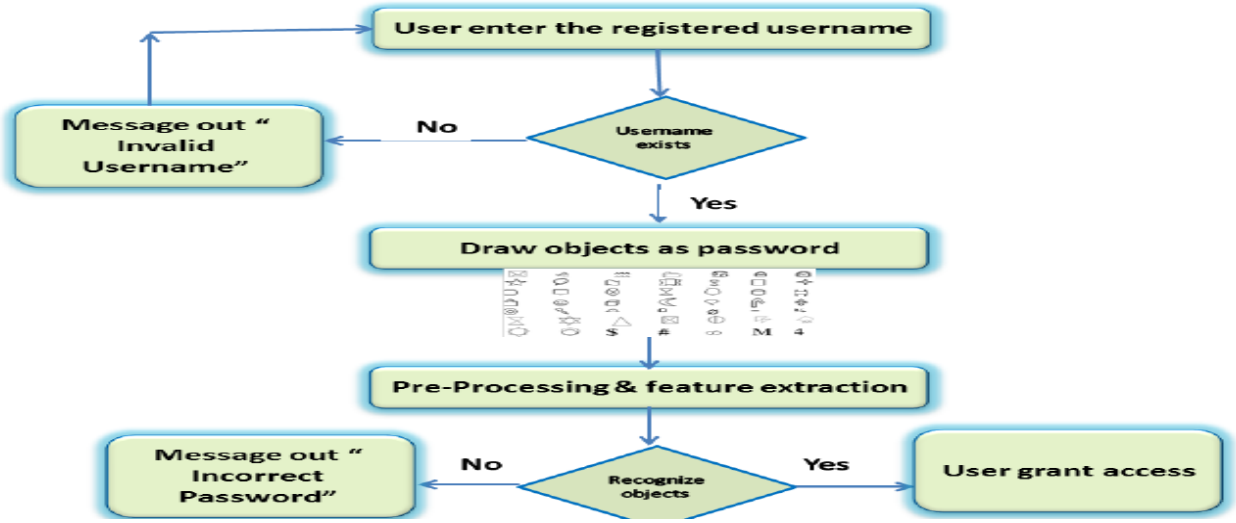


Figure 2: Flow chart of Proposed method

This flowchart depicts a graphical authentication system shown in Figure 2 where users draw some kind of a shape to log in. There are other graphical password systems where users click on specific points on an image in a specific order to log in

The flowchart illustrates the process a user undergoes to log in to the system. Here's a breakdown of the process:

1. The user enters their registered username.
2. The system validates the username. If the username is invalid, an error message is displayed.
3. If the username is valid, the system prompts the user to draw the registered graphical password.
4. The system pre-processes and extracts features from the user-drawn pattern.
5. The system then compares the extracted features with the stored template (which is the correct graphical password for the user).
6. If there is a mismatch, the system displays an "incorrect password" message.
7. If there is a match, the system grants access to the user if there is a match, the system grants access to the user

We harness the power of the Daugman algorithm for precise iris segmentation, complemented by a suite of essential Python libraries: Django and HTML/CSS for frontend development, SQL for database management, and TensorFlow, NumPy, Pandas, Matplotlib, and Scikit-learn for diverse tasks ranging from iris recognition to data preprocessing and visualization.

The use case diagram and the system's comprehensive design are both improved by the class diagram. The actors identified in the use case diagram are categorized into a number of related classes by the class diagram. There are two types of relationships that can exist between the classes: "is-a" relationships and "has-a" relationships. It's possible that every class in the class diagram can perform certain functions. The "methods" of the class refer to these features that it offers. Aside from this, any class could possess some "attributes" that make them distinct.

According to the Unified Modeling Language (UML), a use case diagram is a particular kind of behavioral diagram that is produced from and defined by a use case study. Its objective is to provide a graphical summary of the functionality that a system offers in terms of actors, use cases (representations of their goals), and any interdependencies among those use cases. A use case diagram's primary goal is to display which actors receive which system functionalities. It is possible to illustrate the roles of the system's actors.

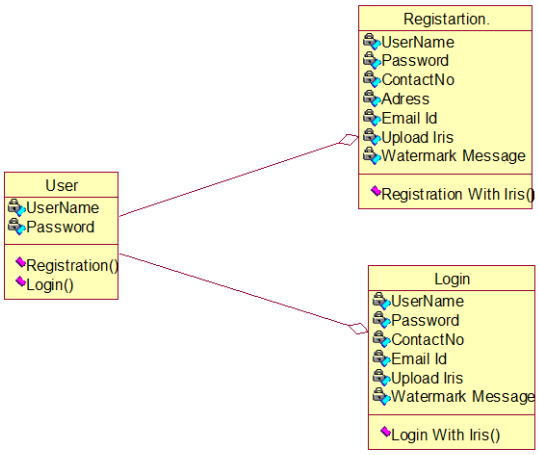


Figure 3: Class Diagram

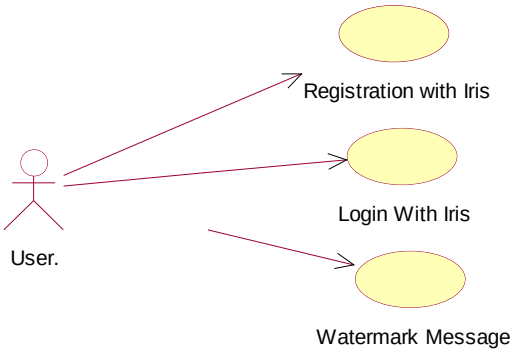
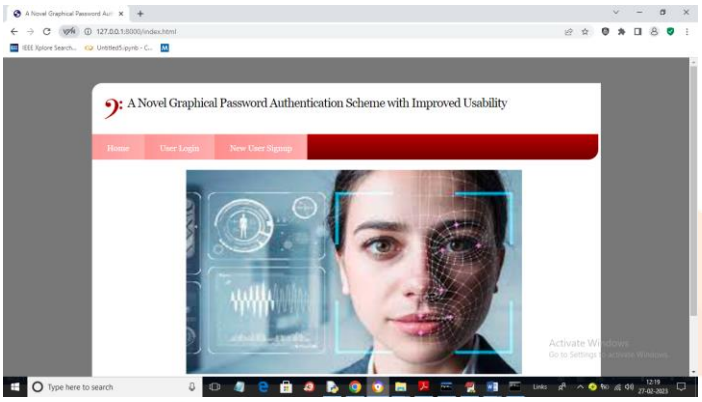


Figure 4: Use case Diagram

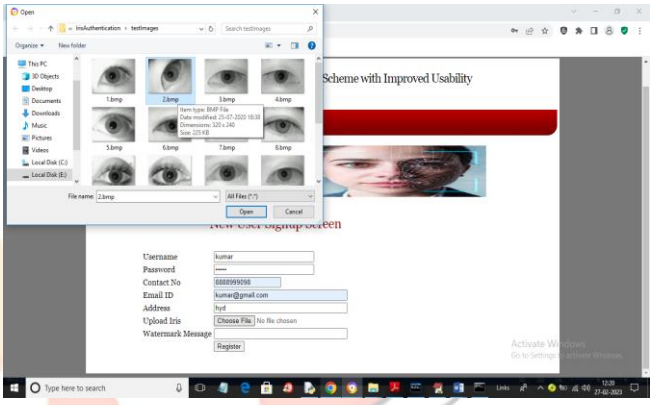
SOFTWARE USED

Python Django Framework: The project's backend development will make use of the Python Django framework. A comprehensive collection of tools for developing web applications is offered by Django, including capabilities for URL routing, database administration, and authentication.
Frontend: The system's frontend user interface will be constructed using HTML and CSS. Web pages are structured by HTML, with styling and layout provided by CSS.
SQL for Databases: Structured Query Language, or SQL, will be utilized to administer databases. It will make it possible to store and retrieve user data, such as authentication credentials and iris data.
TensorFlow: For iris recognition and authentication, TensorFlow, an open-source machine learning framework, will be used. It is appropriate for iris identification applications because it provides tools for creating, honing, and implementing machine learning models.
NumPy: Numerical calculations and array processing will be performed using NumPy, a core Python library for scientific computing. In order to handle iris data, it offers effective data structures and functions for working with multidimensional arrays.
Pandas: Iris data pretreatment and analysis will be done using Pandas, an open-source data analysis and manipulation package. It provides strong functions and data structures for analyzing, transforming, and cleaning datasets.
Matplotlib: The iris data and analysis outcomes will be visualized using Matplotlib, a Python charting library. For the purpose of producing educational visuals, it offers an extensive variety of plot styles and customization choices
Machine learning: The machine learning techniques for iris recognition will be implemented using Scikit-learn, a Python machine learning package. It provides tools for selecting and evaluating models in addition to a variety of supervised and unsupervised learning algorithms.

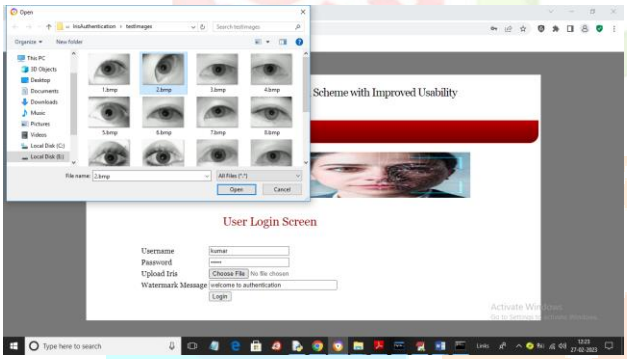
IV. RESULTS AND DISCUSSION



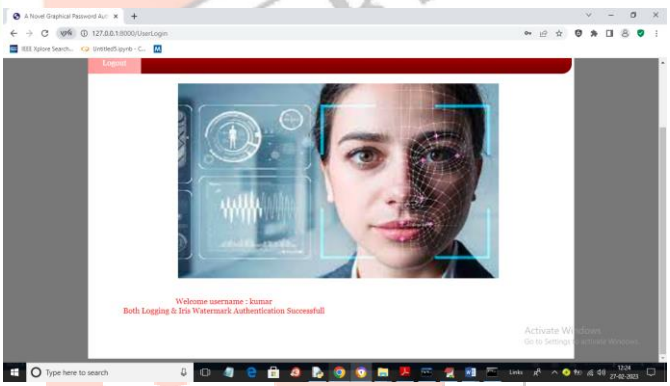
Home page



New User Signup



User login



Authentication successfull

Users create a new account by providing their credentials, such as username, password, and email address. This process might also involve entering additional information like contact details . Once registered, users can access the application by entering their username and password. This verifies their identity and grants them access to the app's features.After logging in, users can create and post messages for other users to see. This functionality allows users to interact and share information on the platform.

V. CONCLUSION AND FUTURE SCOPE

We have built a revolutionary graphical password authentication strategy that offers enhanced security and greater usability, which is a significant improvement in authentication systems. Users who are frustrated with traditional password systems can now enjoy increased security without losing simplicity. Its success is largely due to its usage of user-selected photos, which offer a simple and memorable identification mechanism. Additionally, the scheme's usability lowers cognitive burden and errors during the authentication procedure itself. Cryptographic approaches, among other security measures, help to reduce common dangers such as brute force attacks. This multi-layered strategy represents a significant advancement in authentication technology by guaranteeing user accounts stay safe even from highly skilled attacks.

Enhance Usability: Conduct user studies to gather feedback on the graphical password scheme's interface. Iterate design based on user preferences and behaviors, exploring alternative graphical elements or interaction paradigms for improved intuitiveness.
Improve Security: Investigate advanced cryptographic techniques to enhance resistance against attacks. Perform security analyses and penetration testing to identify and address vulnerabilities. Integrate biometric authentication for added security layers.

Explore Multi-Factor Authentication (MFA): Integrate graphical passwords with biometrics, one-time passwords, or hardware tokens for MFA systems. Research seamless integration mechanisms and optimize the balance between security and usability.

Investigate Emerging Technologies: Explore decentralized identity systems, zero-trust architectures, or blockchain-based authentication for novel authentication approaches. Stay innovative to shape the future of authentication and security in the digital age.

REFERENCES

1. Daugman, J. (1993). Iris Recognition: A Method to Localize the Iris. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(9), 1148–1161.

2. Wilde, R. (1997). An Efficient Iris Recognition Method Using Phase-Based Image Matching. Proceedings of the IEEE, 85(9), 1348–1363.

3. Kong, Y., & Zhang, H. (2001). A Noise-Robust Iris Localization Method Based on Texture Segmentation. Pattern Recognition Letters, 22(5), 479-486.

4. Huang, Y., Wang, L., & Sun, T. (2002). An Efficient Iris Recognition Technique. Pattern Recognition Letters, 23(12), 1289-1298.

5. Dorairaj, S., Jain, A. K., & Ross, A. (2005). Iris Recognition using PCA and ICA Techniques for Non-Ideal Iris Images. Proceedings of the International Conference on Biometrics: Theory, Applications, and Systems, 3873, 700-709.

6. Jan, T. (2014). Multi-Stage Iris Segmentation Framework. International Journal of Pattern Recognition and Artificial Intelligence, 28(01), 1450003.

7. Oyeniran, O. A., Adebayo, A. A., & Oladipo, O. M. (2019). Multi-Algorithmic Technique for Iris Recognition. International Journal of Electrical and Computer Engineering (IJECE), 13(3), 1023-1030.

8. Oyeniyi, D., Alabi, B. O., & Adetunmbi, A. O. (2020). Enhanced Iris Feature Extraction using Continuous Wavelet Transform. International Journal of Pattern Recognition and Artificial Intelligence, 34(01), 2050002.