International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

VISUAL CRYPTOGRAPHY: STRENGTHENING BANKING AUTHENTICATION WITH IMAGE PROCESSING

Shaikh Babu [1], Ahankare Anand [2], Vatse Aditya [3], Waghmare Ajinkya [4], Prof. M.P. Shinde[5]

**1.2.3.4.Last Year Student, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*

**5Profecessor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*

Abstract -In the modern age of digital technology, we introduce a cutting-edge authentication system for banking security, merging Visual Cryptography, Face Authentication, and OTP Verification. Visual Cryptography divides images into secure segments, Face Authentication confirms unique facial characteristics, and OTP Verification adds an additional layer of security. The integration of these elements creates a resilient, user-friendly security system, diminishing unauthorized access and fraudulent activities. This initiative contributes significantly to advancements in cybersecurity, enhancing the banking user experience. In the continually evolving digital banking sphere, our innovative approach ensures data privacy and combats emerging security threats.

Keywords: Visual Cryptography, Image Processing, Facial Recognition, Data Encryption, Multi-factor Authentication

1. INTRODUCTION *(Size 11, Times New roman)*

Amid the digital transformation era, online banking has become an indispensable aspect of daily life, reshaping how we manage finances with unparalleled ease and accessibility. However, this convenience comes with significant security risks due to the reliance on conventional authentication methods like passwords and PINs, which cybercriminals exploit for unauthorized access to financial data.

Our project addresses these concerns by introducing a comprehensive authentication system that integrates Visual Cryptography, Face Authentication, and OTP (One-Time Password) verification. This sophisticated system aims to enhance the security of online banking transactions and safeguard sensitive financial information.

Visual Cryptography, a burgeoning field merging computer science and cryptography, is pivotal in our approach. It involves dividing an image into multiple shares, revealing the original only when a set number of shares combine. This technique offers a secure means of storing and retrieving authentication data.

Face Authentication utilizes biometric facial attributes to confirm identity, significantly raising the bar for unauthorized access attempts.

OTP verification, a dynamic aspect of our system, adds an extra layer of security by generating single-use passwords for each transaction, minimizing risks associated with compromised authentication factors.

Our project seeks to transform the online banking security landscape by integrating these authentication methods, providing both heightened security and user-friendly functionality adaptable to evolving digital threats. Subsequent sections of this report will delve deeper into the technical intricacies and implementation of Visual Cryptography, Face Authentication, and OTP verification, showcasing their innovative potential in banking security.

.

2. LITERATURE SURVEY

[1]. Paper Name : Visual Cryptography and Image Processing Approaches for Enhanced E-Banking Transactions

Author : Kamlesh Kumar Rajput, Mrs. Madhu Lata Nirmal.

Publish Date: Sept 2022.

Information : A relatively new field of study that is gaining traction is image cryptography. Numerous strategies have been developed for cryptography over time. Images containing text or other visual information can be hidden using a variety of encryption algorithms. The term "visual cryptography" refers to the idea that the main idea behind encryption is that it may be decrypted by human vision if the right key image is used. Security has become the most important component of today's banking transaction system, notwithstanding banks' commitment to providing secure core banking services to their customers. Participation in the transaction is contingent upon the legitimacy of the users and is only permitted for those users. Banks utilise passwords, biometric,, password, and OTP-based authentication systems for this reason, but the database of the banking system is no longer secure owing to avoidable criminal activities like phishing attacks and identity theft. Intelligent hackers can retrieve biometric information about consumers from the bank's database and utilize it later to make fraudulent transactions. To prevent all of these terrible occurrences, the RSA algorithm is utilized coupled with visual cryptography and steganography approaches.

[2]. Paper Name : Haar Cascade Face detection and local binary pattern histogram face recognition based drone.

Author : K. G. Shanthi, S. Sesha Vidhya, K. Vishakha, S. Subiksha, K. K. Srija.

Publish Date: March 2022.

A common method for identifying people's faces via image processing is face recognition. Face recognition is becoming important because of the increasing population, which calls for strict security and surveillance systems. It's also important because of the modern demand for self-confirmation, fighting in rural areas, disaster aid, and other reasons. This study suggests using a face recognition-based drone for surveillance and to help the task force track illegal immigrants who go missing. An technique called Haar Cascade is used to identify faces in photos and live recordings. The Local Binary Pattern Histogram (LBPH) is a facial recognition algorithm. The drone identified people with a 98 percent accuracy rate, which has important applications.

[3].Paper Name : E-Authentication for Secure Net Banking
Author : Mitul Chauhan, Gayatri Barapatre, Amruta Ghatge, Rajashri Sabale, Pooja Sakunde

Publish Date : February 2022.

Information : Recent technological breakthroughs have led to the spread of personal computing devices, such as watches, tablets, smartphones, and eyewear. This has helped them imagine a digital future in which they may use the Internet to perform basic everyday tasks from anywhere at any time and on any device. Concurrently, developments in ubiquitous computing have spawned the idea of "smart spaces," which aim to deliver customized services to inhabitants automatically. User authentication, or confirming one's identity, is crucial in the digital era to safeguard private data kept on laptops and smartphones as well as to enable personalized services in digital spaces (such changing the temperature of the room, etc.). Recent research has shown that traditional methods of authentication, such as passwords or fingerprints, are vulnerable to hacking. As a result, scientists have created a wide range of cutting-edge techniques for user authentication in the above specified situations. In order to help direct future research in these areas, this paper offers an overview of these distinctive systems.

[4]. Paper Name :Prevention of phishing website attacks in online banking systems using visual cryptography.

Author : M. A. Snober, A. Dros, Q. A. Al-Haija.
Publish Date : December 2022.

Information : Account numbers and private passwords are two pieces of sensitive data that are frequently taken by attackers and pirate operations. They attempt to fool victims into disclosing these details. One is the counterfeiting of websites, especially those related to online banking, electronic payment services, and other websites. Those websites' users typically have lower awareness of security risks. In order to create an authentication-level protection method that restricts these phenomena, this study makes use of Visual Cryptography (VC) technology. Our suggested method would make it easier for users to discern between a legitimate website and a phishing one, especially for those who are not familiar with the cyber security industry. Considered straightforward, visual cryptography eliminates the need for convoluted encryption and decryption procedures.

[5]. Paper Name : Design and Implementation of a visual cryptography application

Author : Petre Anghelescu, Ionela-Mariana Ionescu, Marian Bogdan Bodea.

Publish Date : June 2020.

Information: An application for visual cryptography is designed and implemented in this work. After processing the original data in the form of a picture, this image will be subjected to a visual encryption technique. It will produce two to four papers that show the encryption's

outcome. By aligning them correctly and allowing the human eye to visually recognise the information, the encryption process is completed. Every encryption will provide a distinct set of results, and each encryption repetition will produce a new set.

3. SYSTEM ARCHITECTURE

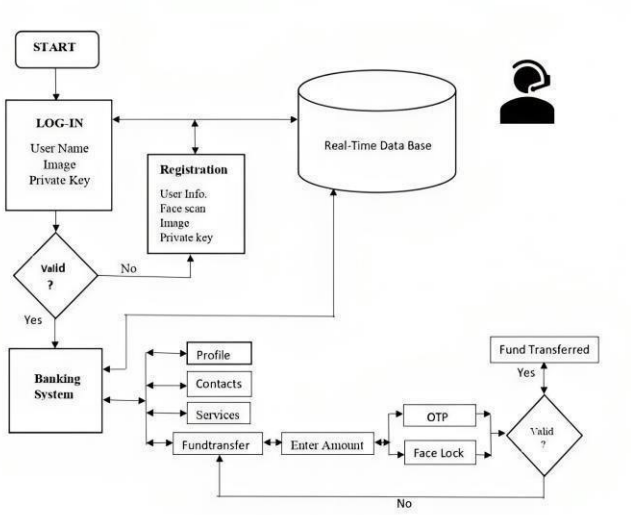

Fig. system architecture

This flowchart outlines the functionality of a banking system with real-time database integration and a face lock feature. It begins with a "START" box and concludes with a "Fund Transferred" box. Throughout the flowchart, a cylinder symbolizes the real-time database, and a Libra symbol represents the banking system. Additionally, a face icon indicates the presence of the face lock feature.

The flowchart progresses logically, depicting various stages such as financial transfers, contacts, services, profile management, loan requests, transaction requests, OTP verification, and face lock verification. Arrows connect the boxes to illustrate the flow of data and actions within the system. In total, there are 16 boxes and 17 arrows delineating the operational flow of the banking system.

4. ALGORITHMS

Visual Secret Sharing Algorithm:

The process of visual cryptography for secure authentication starts with loading the original image file, which is then converted to grayscale to simplify encryption. Two random matrices, matching the dimensions of the grayscale image, are generated to serve as encryption keys or "masks" for splitting the image.

Encryption occurs pixel by pixel: for each pixel in the grayscale image, its value is subtracted from a corresponding pixel value in the first random matrix. This difference becomes the pixel value in one share (share 1). Simultaneously, the pixel value of the second share (share 2) is obtained by subtracting the result from 255, ensuring accurate reconstruction of the original image when combined with share 1. The encrypted shares are then saved as separate images: share 1 represents the direct result of the subtraction operation, while share 2 is the complement of share 1, bolstering security by requiring both shares for image reconstruction. Additional security measures, such as share shuffling or additional encryption techniques, may be applied to enhance security and deter unauthorized access. This thorough encryption process ensures the integrity and confidentiality of visual data in authentication systems.

Haar-Cascade Algorithm:

The Haar Cascade Algorithm is fundamental to face authentication systems, employing a systematic approach to detect and recognize faces in images or video streams. Initially, a pre-trained Haar cascade classifier, comprising a hierarchical series of classifiers, is utilized to identify potential facial regions by scanning the input image or frame using a sliding window technique. Within each window, the algorithm assesses features like edges and texture variations using Haar-like features, comparing them against predetermined thresholds to identify facial characteristics. Through a cascade of classifiers, non-facial regions are progressively filtered out based on feature characteristics, enhancing the accuracy of face detection. Upon passing through all cascade stages, a face candidate yields bounding box coordinates indicating the detected face. This robust and efficient approach enables real-time face detection across various conditions, serving as a foundational framework for advanced face authentication systems in security, surveillance, and human-computer interaction domains.

5. RESULTS

This proposed system is built to provide the secure authentication for the various systems. The system uses the visual cryptography technique to encrypt the image and Haar- Casacade algorithm for the purpose of face authentication. This system helps the users for doing registration and login without the need of remembering the passwords.

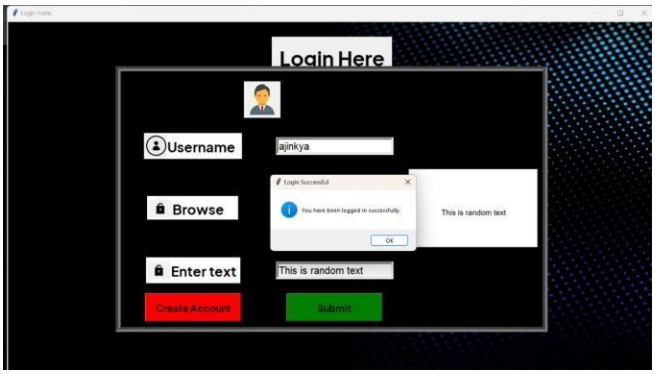

fig 2. Result

Fig 3. Result

6. CONCLUSION

In summary, the team has executed an impressive implementation of visual cryptography for financial authentication. The integration of facial identification, OTP verification, and image processing has resulted in a robust solution that emphasizes user-friendliness while enhancing security measures. Leveraging techniques like steganography and watermarking further enhances data secrecy. Meanwhile, face authentication and OTP verification serve as formidable barriers against unauthorized access, ensuring the integrity of banking transactions. While there's more work to be done, this achievement establishes a strong foundation for future advancements in financial security. The project is poised for a promising future, brimming with opportunities for further growth and development..

7. FUTURE SCOPE

1. Biometric Enhancements: Advancing biometric capabilities beyond facial recognition, such as integrating fingerprint or iris scanning, to bolster authentication processes.

2. Machine Learning Integration: Incorporating machine learning algorithms to improve the system's ability to detect and respond to emerging security threats in real-time.

3. Multi-channel Authentication: Implementing multi-channel authentication methods, such as combining SMS verification with app-based authentication, for added security layers.

4. Block-chain Technology: Exploring the potential of block- chain technology for transaction verification and data integrity, enhancing security and transparency in banking operations.

5. Continuous Cyber Threat Monitoring: Developing robust systems for continuous monitoring of cyber threats to promptly identify and mitigate potential security risks

8. REFERENCES

[1] E – Authentication for Secure Net Banking Mitul Chauhan1, Gayatri Barapatre, Amruta Ghatge , Rajashri Sabale4 , Pooja Sakunde. Computer Science and Engineering Vol.10, Issue.1, pp.15-18, February (2022) E-ISSN: 2320-

[2] Design and implementation of a visual cryptography application. Petre Anghelescu; Ionela-Mariana Ionescu; Marian Bogdan Bodea

[3] Visual Cryptography and Image Processing Approaches for Enhanced E-Banking Transactions: A Survey. Dogo Rangsang Research Journal UGC Care Group I Journal ISSN : 2347-7180 Vol-12 Issue-09 No. 02 September 2022.

[4] Haar Cascade Face Detection and Local Binary Pattern Histogram Face Recognition based drone. K G Shanthi; S Sesha Vidhya; K Vishakha; S Subiksha; K K Srija; R Srinee Mamtha 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 295-298, doi: 10.1109/ICACCS54159.2022.9785051.

[5] "Prevention of phishing website attacks in online banking systems using visual cryptography," M. A. Snober, A. Droos and Q. A. Al-Haija, 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 2022, pp. 168-173, doi: 10.1049/i