CS6811 CREATIVE AND INNOVATIVE PROJECT

Enhancing QR Code Security Using Blockchain-Backed Chaotic Permutation and Share-Based Diffusion for Secure Data Transmission

First Review

Team-40

Supervisor: Dr B. Thanasekhar

Team Members:

Abhinavh P (2022503059)

Prabhakaran Arjun R(2022503003)

Buvanes Srivardan K(2022503037)

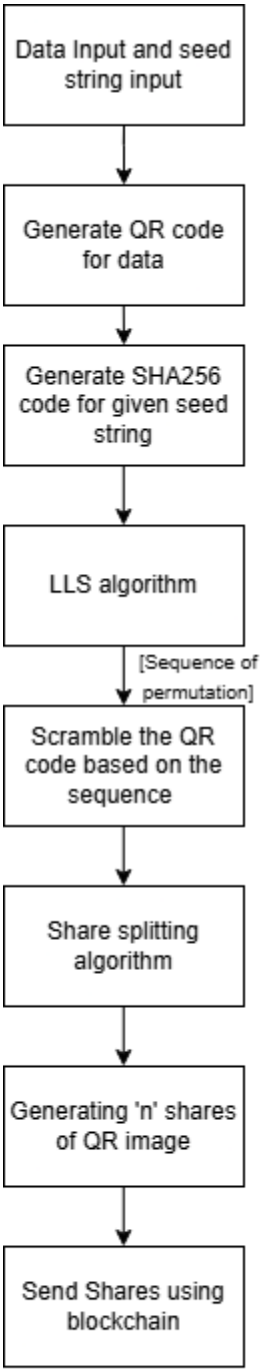
PROBLEM STATEMENT:

QR codes are widely utilized in various fields for quick and efficient information sharing. However, they are vulnerable to security threats such as information leakage, data tampering, and unauthorized access, especially during transmission and storage. Ensuring the confidentiality and integrity of QR code data in such scenarios is crucial to prevent misuse and maintain trust.

OBJECTIVE:

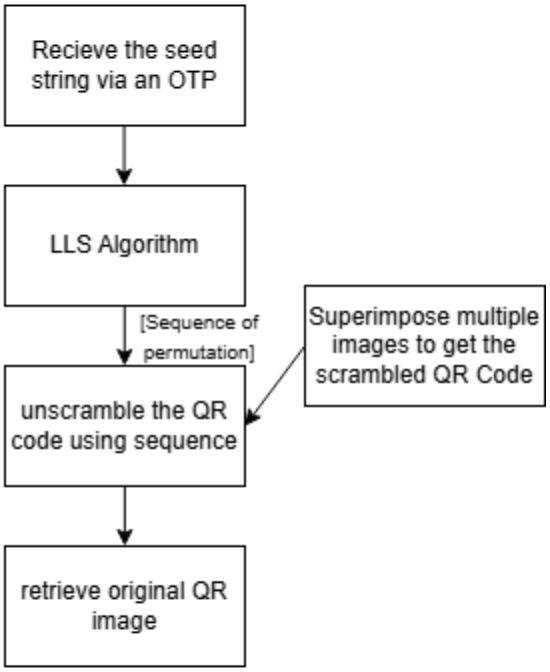
- **Secure QR Code Encryption:** Develop a cryptographic system that securely encrypts QR codes containing confidential data using block permutation and diffusion techniques to prevent unauthorized access
- **Deterministic Permutation Using Chaotic Systems:** Implement a Logistic-Sine System (LSS) and SHA-256-based key generation to generate unique yet reproducible block permutations, ensuring each encryption is highly sensitive to input changes.
- **OTP-Based Secure Decryption:** Introduce a One-Time Password (OTP) mechanism to authenticate QR code decryption, ensuring that only authorized users can retrieve the original data.
- **Blockchain-Based QR Code Verification**: Integrate a **blockchain ledger (Ethereum/Hyperledger)** to store and verify and transfer QR hashes, ensuring tamper-proof authentication and preventing QR code forgery.

Flowchart:



Encryption and transfer

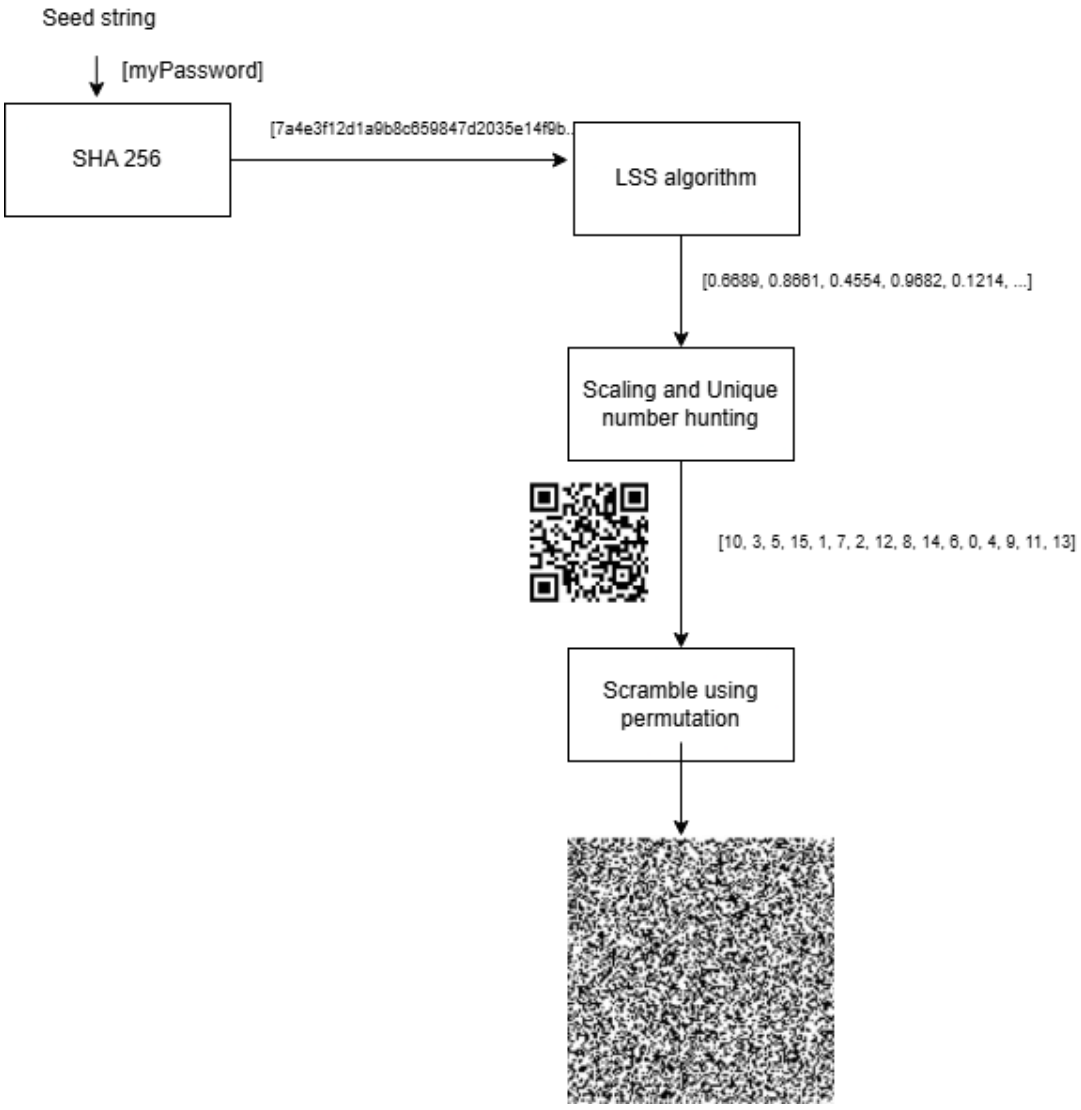
Fig. 1



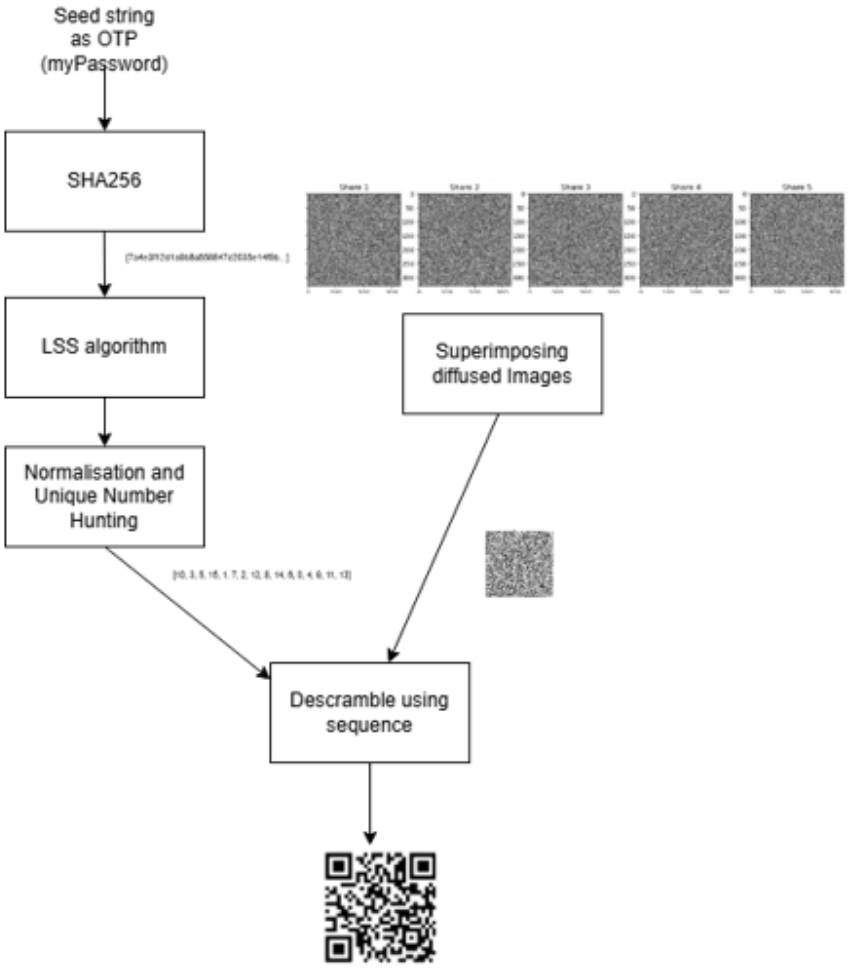
Decryption Stage

Fig. 2

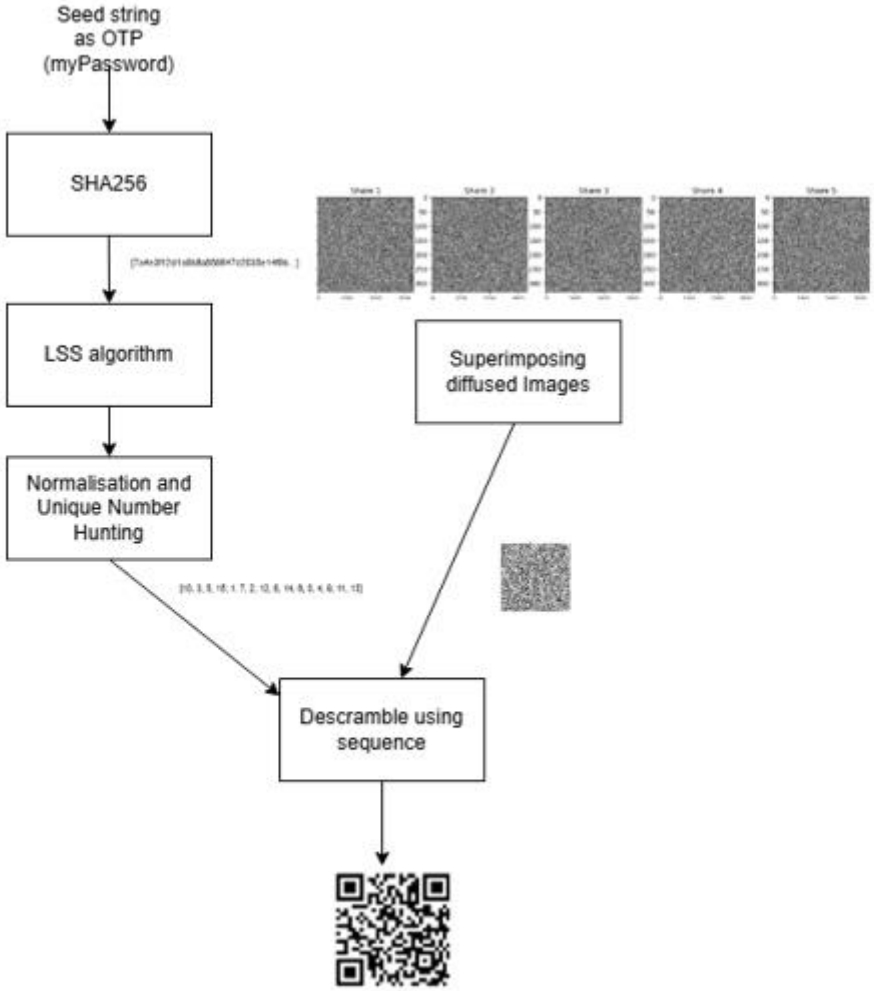
Permutation Block Scramble Process:



Diffusion-into-parts Algorithm:



Decryption Process:



ENHANCEMENT:

- The given diffusion techniques to secure the image during transfer are all either weak to attacks or incur large over-head in terms of time, thus a new diffusion technique is employed.
- The diffusion-by-parts technique only consists of algorithms to split an image into two noisy counterparts, this project extends upon than concepts to split into multiple noise images.

PROPOSED WORK:

The proposed system is a secure QR code encryption and transmission framework designed to protect confidential data by splitting the QR code into multiple parts and applying a permutation scrambling technique. This ensures that even if an attacker intercepts the QR code, they cannot reconstruct it without the correct scrambling order and all necessary shares. The system comprises four main components:

● **QR Code Splitting Using a Share Splitting Algorithm**: The QR code is divided into multiple shares using a secure share splitting algorithm, ensuring that the QR cannot be reconstructed without collecting all the required parts.

● **Permutation Scrambling for Additional Security**: A Logistic-Sine System (LSS) and SHA-256-based key generation are used to determine a unique permutation order, scrambling the QR code blocks in an unpredictable manner.

● **Reconstruction and Unscrambling at the Receiver's End**: The receiver must first gather all required shares to reassemble the QR code. Once reassembled, the system reverses the permutation scrambling using the correct LSS-generated key, restoring the original QR code.

● **User-Friendly Secure Transmission System**: A GUI or mobile app is developed to facilitate QR code splitting, transmission, and reconstruction, ensuring a smooth and secure user experience.

.

ALGORITHM:

Module 1: QR Code Splitting & Permutation Scrambling

Objective: Develop the block-based scrambling algorithm by:

1. Splitting the QR code into smaller blocks (4×4 grid).
2. Generating a deterministic permutation order using a SHA-256-based Logistic-Sine System (LSS).
3. Rearranging blocks according to the permutation to scramble the QR code.

Module 2: Secure Decryption with OTP & AES Encryption

Objective: Implement secure QR code decryption, adding AES-256 encryption and OTP-based authentication.

1. Generate OTP and derive encryption key (SHA-256)
2. Encrypt the QR data using AES-256
3. Send the encrypted QR & OTP securely
4. Receiver enters OTP to decrypt QR and reverse scrambling

Module 3: Blockchain-Based QR Code Authentication & GUI

Objective: Integrate blockchain verification and build a user-friendly interface for secure QR transfer.

1. Store QR hash & transaction details on blockchain (Ethereum/Hyperledger).
2. Verify QR integrity upon decryption using blockchain.
3. Develop a GUI for easy encryption & decryption.

Evaluation Metrics

Security Metrics

- **Share Reconstruction Security**
  - Ensure that reconstruction is only possible when the required number of shares is available.
  - Validate that missing or incorrect shares prevent successful reconstruction**.**
- **Resistance to Attacks**
  - Test resistance against brute-force attacks attempting to guess the correct permutation order.
  - Perform histogram analysis or edge detection to ensure that scrambled QR codes do not reveal meaningful patterns.

Performance Metrics

- **Encryption Time (ms)**
  - Measure the time taken to split the QR code, generate the permutation key, and apply the scrambling algorithm.
- **Decryption Time (ms)**
  - Measure the time required to reconstruct the QR code by gathering all shares and reversing the scrambling process.
- **QR Code Readability After Reconstruction**
  - Ensure that the decrypted QR code can be successfully scanned without errors.

Image Quality Metrics

- **Peak Signal-to-Noise Ratio (PSNR)**
  - Compare the reconstructed QR code with the original to measure distortion.
  - Higher PSNR values indicate better reconstruction quality.
- **Structural Similarity Index Measure (SSIM)**
  - Evaluate the perceptual similarity between the original and reconstructed QR codes.
  - SSIM values close to 1 indicate near-perfect reconstruction.

Functional Test Cases:

Testcase	Expected Outcome
Test different passwords for scrambling	Different passwords generate completely different permutations
Attempt to scan a scrambled QR code	Scanner fails to recognize the scrambled QR code
Attempt decryption with the wrong password	Reconstruction fails, preventing unauthorized access
Reassemble QR code with missing shares	Reconstruction is unsuccessful due to missing information

Security Test Cases:

Testcase	Expected Outcome
Brute-force attack on permutation order	Reconstruction should be computationally infeasible
Histogram and edge detection analysis	Scrambled QR code should not reveal meaningful patterns
Test QR code alteration and tampering	System detects tampering and rejects reconstruction

Performance Test Cases:

Testcase	Expected Outcome
Encrypt a large QR code (1024×1024 pixels)	Encryption and decryption time remains within an acceptable range
Measure PSNR between original and reconstructed QR	PSNR remains above a threshold indicating low distortion
Measure SSIM between original and reconstructed QR	SSIM value remains close to 1, indicating minimal loss

LITERATURE SURVEY:

Source	Objectives	Methodology	Limitations
[1]	To develop a fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and image diffusion.	Employ block permutation techniques and diffusion techniques for encryption of images.	The diffusion techniques used in the proposed work incur large overhead, impractical for real time applications.
[2]	To develop a share-splitting scheme to split the image into noisy shares for a QR code.	Utilise the usage of probability and pixel manipulation to induce noise in such a way that it doesn't affect overall image integrity of the QR code.	This system limits itself to splitting an image into two noisy counterparts, which is very limited. Also, it includes no practical implementation.
[3]	To implement the share splitting algorithm with probability and pixel manipulation.	Utilize Python libraries such as QRCODE, CV2 and HASHLIB to implement the diffusion technique.	Efficiency may vary based on the number of shares being split.
[4]	To implement PSNR (Peak Signal to Noise Ratio) and SSIM (Structured Similarity Indexing Method) to measure the integrity of recovered QR code.	Analyse and use PSNR and SSIM formulas to sent and received QR code image.	The proposed paper does not give any insights into how binary coloured (black and white) images may be studies under these metrics.
[5]	To develop a diffusion technique over the existing Permutation only block scrambling technique.	Implement the diffusion algorithm as the share-splitting algorithm using pixel manipulation.	The chosen diffusion method can add overhead to the entire project, having a possibility of making the application slow.
[6]	The paper presents a modern method for detecting web phishing using Visual Cryptography (VC) and Quick Response (QR) codes, focusing on secure One Time Password (OTP) distribution	The method involves generating two meaningful shares from a secret image, which are stored on separate servers to enhance security.	The proposed method relies heavily on the security of the two separate servers. If either server is compromised, the security of the entire system could be at risk, as a hacker could potentially access one meaningful share and attempt to decode the secret image with other means
[7]	The paper proposes a general threshold progressive visual secret sharing (PVSS)	The secret image is shared among n shadow images, and the recovery process utilizes the human visual	The proposed method does not split the shares as meaningful and meaningless.

	construction method that extends traditional (2, n) PVSS schemes to (k, n) thresholds without pixel expansion	system, allowing for the secret to be reconstructed without the need for cryptographic computations	Also, it does not account for any practical implementation
[8]	The paper presents a novel symmetric cryptography technique based on the Caesar cipher, aimed at enhancing secure data communication over network	Instead of using a traditional symmetric key, the sender transmits a hash code that generates the symmetric key for the receiver to decrypt the message	The method is weak because the Caesar cipher is easily breakable, and using SHA-256 is better as it provides irreversible, collision-resistant hashing for stronger security.
[9]	This paper proposes two new visual cryptography schemes using color XOR to enhance secure image transmission	The first scheme generates meaningless shares, while the second produces meaningful shares and the second scheme modifies shares into color QR codes, allowing for complete restoration of the secret image	The limitations of this method include increased complexity, color inconsistency issues, and vulnerability to noise, whereas black-and-white QR codes are better due to their higher contrast, easier scanning, and lower risk of decoding errors.
[10]	The paper systematically examines security risks in blockchain technology, focusing on popular systems like Ethereum and Bitcoin	Implement a distributed storage system (like IPFS), a smart contract platform (such as Ethereum or Hyperledger), and cryptographic hashing (e.g., SHA-256) to securely store, verify, and reconstruct the QR code shares on the blockchain	The paper does not specify practical implementation of the given technology and only discusses security concerns.

REFERENCES:

1. Chai, X., Gan, Z., & Zhang, M. (n.d.). “A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion.” *Springer Science+Business Media New York 2016*
2. Bhardwaj, C., Garg, H., & Shekhar, S. (2022). “:An Approach for Securing QR code using Cryptography and Visual Cryptography.” *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES).*
3. Xiaohe Cao, Liuping Feng, Peng Cao and Jianhua Hu “Secure QR Code Scheme Based on Visual Cryptography” *2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE2016)*
4. Sara, U., Akter, M. and Uddin, M.S. (2019) “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study.” *Journal of Computer and Communications, 7, 8-18*
5. Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy, "*Cryptanalysis of Permutation-Only Image Ciphers*," IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 236-242, Feb. 2016.
6. A. Kute, S. Kadam, et al., "Modern Method for Detecting Web Phishing Using Visual Cryptography (VC) and Quick Response Code (QR code)," *Int. Journal of Engineering Research and Applications*, vol. 5, no. 1, Part 3, pp. 01-05, Jan. 2015.
7. Xuehu Yan & Shen Wang & Xiamu Niu., “Threshold progressive visual cryptography construction with unexpanded shares” *Ms. Ashvini Kute et al Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 5, Issue 1(Part 3), January 2015, pp.01-05*
8. S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, "A Novel Approach of Symmetric Key Cryptography," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343*.
9. Pan, J. S., Liu, T., Yang, H. M., Yan, B., Chu, S. C., & Zhu, T. (2022). “Visual cryptography scheme for secret color images with color QR codes.” *Journal of Visual Representation, 82, 103405. 288 Communication and Image*
10. Xiaoqi Li , Peng Jiang , Ting Chen. Xiapu Luo , Qiaoyan Wen., “A survey on the security of blockchain systems” *Future Generation Computer Systems 107 (2020) 841–853*