*Review 2 (12/03/25)*  *Team:A19*

CREATIVE AND INNOVATIVE PROJECT [CS6611]

**Secure QR Code Transmission Using Permutation Scrambling, Share Splitting, and Private Blockchain Channels**

By Abhinavh P(2022503059) Prabhakara Arjun R(2022503003) Buvanes Srivardan K(2022503037)

**Mentor : Dr. B. Thanasekhar**

**INTRODUCTION**

Secure data transmission is a critical challenge in modern digital communication, requiring robust encryption and resilience against cyber threats. This project integrates Permutation Scrambling, AES Encryption, and Share Splitting to securely encode data into QR codes, ensuring confidentiality and integrity during transmission. By leveraging QR code-based cryptographic encoding, sensitive information is first scrambled using Logistic Sine System(LSS) algorithm, encrypted with AES for added security, and then split into multiple shares to prevent unauthorized reconstruction. These encrypted shares can be transmitted through conventional networks or securely stored and exchanged over a private blockchain, enhancing decentralization and resistance to tampering. This approach provides a highly secure, resilient, and decentralized method for transmitting confidential data, mitigating risks such as man-in-the-middle attacks, interception, or unauthorized access, making it suitable for applications in secure authentication, financial transactions, and confidential document exchange.

**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.

**LITERATURE SURVEY**

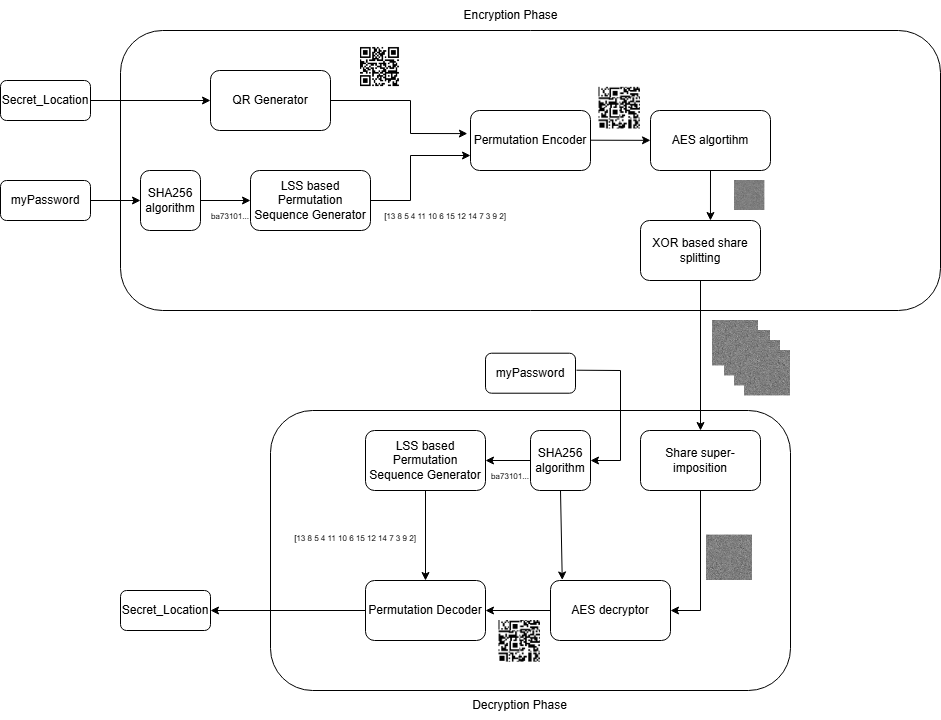
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.no** | **Title** | **Name of the Journal** | **Methodology used** | **Limitations** |
| 1 | A QR Code Used for Personal Information Based on Multi-Layer Encryption System | International Journal of Interactive Mobile Technologies (iJIM), 2023 | The paper presents a novel QR code cryptography system that utilizes a national standard code system, enhancing data security through multi-layer encryption.  Using the image's mathematical processing method, we may apply the equivalence class principle to the ordered equations of the two-dimensional code(QR), producing the desired cryptographic result. | The paper acknowledges that existing secure QR code readers have flaws and limitations, indicating that improvements are necessary to enhance security protocols.  The usability of the proposed system may not be fully addressed, which could hinder user adoption and practical application in real-world scenarios |
| 2 | A Study on the Simple Encryption of QR Codes Using  Random Numbers | Journal “*Electronics*”, 2024 | The paper proposes an encryption system for QR codes using random numbers and RC4 to enhance security against unauthorized use.  The encryption process in RC4 involves initializing an array, S, with values from 0 to 255, which is then shuffled based on a secret key using the key-scheduling algorithm (KSA), | RC4 encryption is applied to the seed values (decryption keys), but the output values are restricted to numerical characters for quick sharing. This restriction reduces the overall key space, making the system more vulnerable to brute-force attacks. |
| 3 | Sharing Multiple Secrets in XOR-Based Visual  Cryptography by Non-Monotonic  Threshold Property | IEEE Transactions on Circuits and Systems for Video Technology,  2023 | This paper introduces a multiple-secret XOR-based visual cryptography scheme (MXVCS) utilizing a novel non-monotonic threshold property, ensuring only exact kk-shadows can decrypt a secret using Boolean XOR operations.  . | The recovered secret images are reconstructed in a lossy manner, impacting their quality. This may not be ideal for applications requiring exact image reproduction, such as medical imaging or sensitive documents. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 | A Self-Authenticating Multi-Tone Secret Sharing Scheme Using Meaningful Shares for Satellite Images | IEEE Access,2024 | The proposed method employs a three-step encryption process consisting of block scrambling, pixel scrambling, and S-Box value substitution.  This layered approach enhances the confidentiality of satellite images by making it difficult for unauthorized users to decipher the original content without the keys. | Managing the keys for the (k, n) threshold system can become complex, especially as the number of participants increases. Each participant must securely store and manage their share, which can lead to potential vulnerabilities if not handled properly |
| 5 | Secret Image Sharing Schemes:  A Comprehensive Survey | IEEE Access, 2023 | This paper proposes XOR-based secret image sharing methods ensure lossless reconstruction of the original secret image, making them highly reliable for secure image sharing**.**  XOR operations are computationally efficient, resulting in lower processing times compared to polynomial-based schemes, making them suitable for real-time applications | This paper does not propose any implementation of the methods proposed, only highlighting their advantages and lossless nature |
| 6 | A Construction Method of  (2, 3) Visual  Cryptography Scheme | IEEE Transactions on Circuits and Systems for Video Technology, 2023) | This paper proposes a (2, 3) Visual Cryptography Scheme (VCS) that enables sharing one or two binary secret images across three "shadows" (shares). The process involves generating shadows using optimized Boolean matrix-based encoding. | The scheme focuses on a specific case of (2, 3)-VCS, and the generalization to other (k, n)-VCS systems is suggested as future work but not addressed in the paper. This limits its immediate application to more complex access structures. |
| 7 | Cryptanalysis of Permutation-Only Image Ciphers, | IEEE Transactions on Information Forensics and Security,2020 | This paper analyzes the security vulnerabilities of permutation-only image encryption schemes and introduces a novel cryptanalysis approach based on a chosen-plaintext attack. | The cryptanalysis requires a chosen-plaintext attack, which assumes the adversary can control the input plaintexts to the encryption system. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | Distributed three-level QR codes based on visual cryptography scheme | Journal of Visual Communication and Image Representation, 2022 | This paper introduces a novel scheme to create distributed three-level QR codes combining Visual Cryptography Scheme (VCS) principles and QR code technology. The process involves encoding three levels of information—visual, public, and privacy—into shares resembling QR codes | The proposed method requires high-quality input shares for accurate recovery. Distorted or degraded photo/print-format shares may impact the effectiveness of the image distortion rectifying algorithm. |
| 9 | An Approach for Securing QR code using  Cryptography and Visual Cryptography | Ist International Conference on Computational Intelligence and Sustainable Engineering Solution, 2022 | This paper proposes a method to enhance the security of QR codes by integrating cryptography and visual cryptography. The process begins by embedding information into the QR code, followed by encrypting the QR code with a key.  The encrypted QR code is then subjected to a (k, n) Visual Cryptography (VC) scheme, generating n meaningless shares, where k shares are the minimum required to reconstruct the QR code | No practical implementation given for the (K,N) VCS scheme is given |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10 | Secure QR Code Scheme Based on Visual Cryptography | 2nd International Conference on Artificial Intelligence and Industrial Engineering, 2016 | This paper introduces a method to enhance the security of QR codes by combining Visual Cryptography with pseudo-random matrices.  The process begins by dividing the QR code (original secret image) into two meaningless "share images" using a pseudo-random matrix, which determines the pixel values of the shares | While the pseudo-random matrix plays a critical role, the paper does not discuss how to securely distribute or manage the matrix, which could present vulnerabilities if compromised. |

**ARCHITECTURE DIAGRAM:**



**MODULES**

1.QR code generation and encryption.

2.Decryption and data retrieval.

3.Transmission and evaluation metrics.

**PROPOSED WORK**

**1.QR Code Encoding**

* Input data (text) is encoded into a QR code using standard QR generation techniques.
* The QR matrix is analyzed and optimized using error correction (Reed-Solomon coding) to enhance resilience against data loss.
* The QR code is converted into a structured digital format for encryption.

**2.Permutation Scrambling Algorithm**

* A custom permutation scrambling algorithm augmented with LSS is applied to rearrange the pixel structure of the QR code, introducing an additional security layer.
* The scrambling pattern is generated based on a secret key, ensuring unique transformations per instance.

**3.AES Encryption**

* The scrambled QR matrix undergoes AES encryption, converting it into an unreadable ciphertext format.
* The encryption key is securely shared with the intended recipient via an independent secure channel.

**4.Share Splitting Mechanism**

* The encrypted QR code is fragmented using a Share Splitting Algorithm (Shamir’s Secret Sharing).
* Each fragment (or share) represents a portion of the QR code and can only be reconstructed when all shares are available.

**IMPLEMENTATION**

**MODULE-1: QR code generation and encryption**.

FUNCTION GenerateQRCode(qr\_input):

1.1 Generate QR code from qr\_input.

1.2 Save QR code as "qr.png".

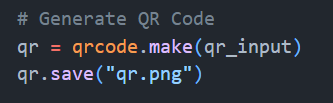
1.3 Load the QR code image from "qr.png".

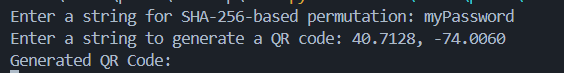
1.4 Crop the white border of the QR code.

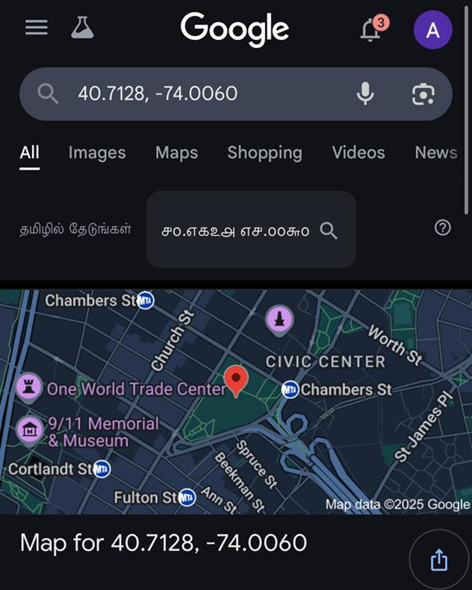
1.5 Resize the image to 400x400 pixels.

1.6 RETURN processed QR code image.

END FUNCTION







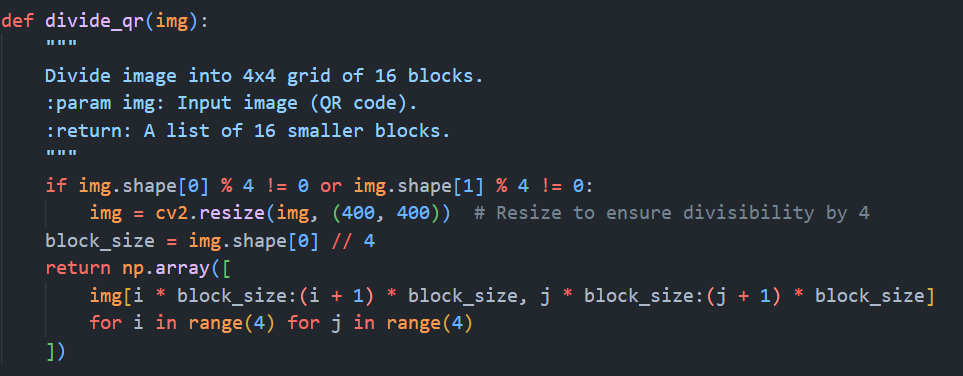
FUNCTION DivideQRCode(img):

2.1 Ensure img dimensions are divisible by 4. If not, resize to 400x400.

2.2 Divide img into 4x4 grid → 16 blocks.

2.3 RETURN list of 16 blocks.

END FUNCTION



FUNCTION GeneratePermutation(sha256\_input, n):

3.1 Convert sha256\_input into a floating-point seed.

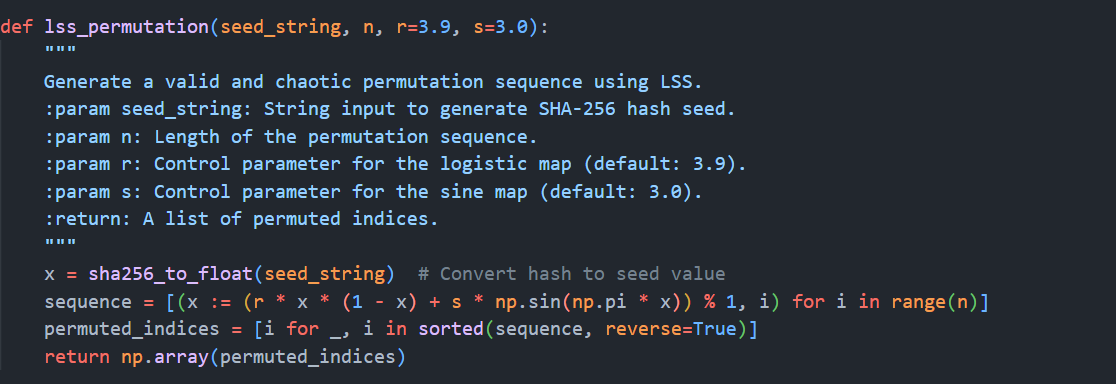
3.2 Initialize logistic-sine system (LSS) with control parameters r=3.9, s=3.0.

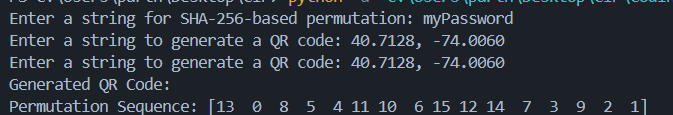
3.3 Generate chaotic sequence using LSS.

3.4 Sort sequence in descending order → Extract permutation indices.

3.5 RETURN permutation indices array.

END FUNCTION



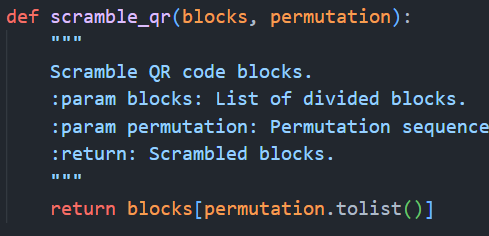


FUNCTION ScrambleQRCode(blocks, permutation):

4.1 Rearrange blocks according to permutation indices.

4.2 RETURN scrambled QR code blocks.

END FUNCTION



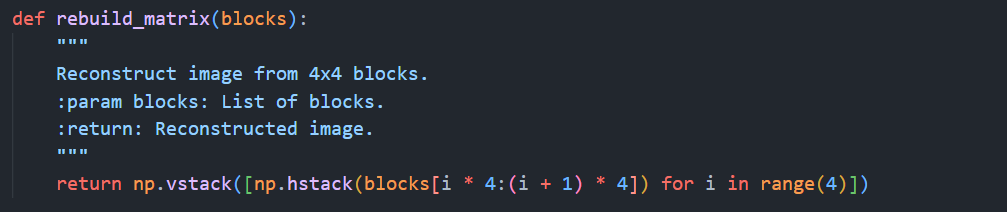


FUNCTION RebuildMatrix(blocks):

5.1 Stack blocks row-wise to reconstruct a full image.

5.2 RETURN reconstructed scrambled QR image.

END FUNCTION



FUNCTION EncryptAES(data, aes\_key):

6.1 Initialize AES-256 cipher in CBC mode with random IV.

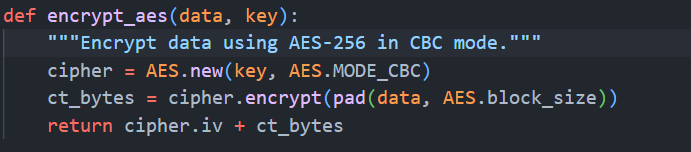
6.2 Apply PKCS7 padding to data.

6.3 Encrypt padded data using AES cipher.

6.4 Concatenate IV + ciphertext.

6.5 RETURN encrypted data.

END FUNCTION





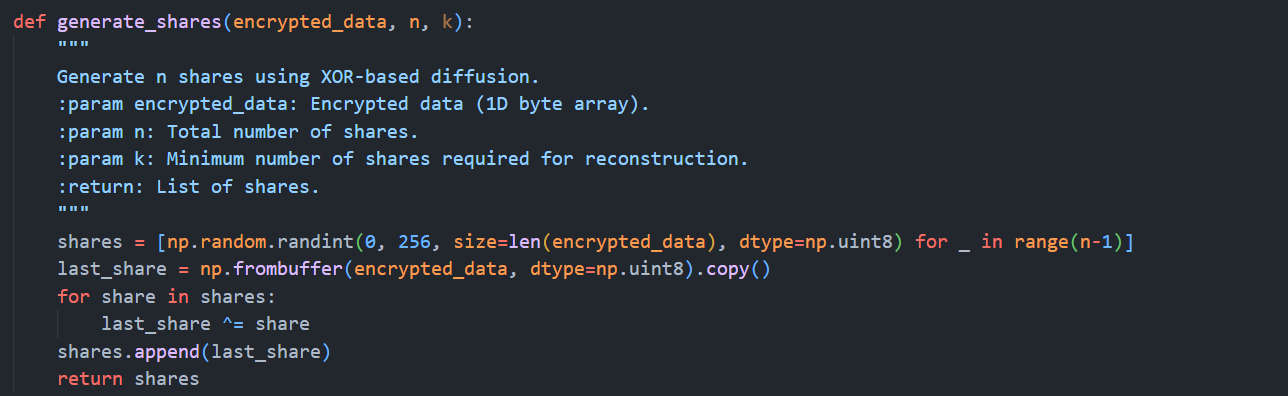
FUNCTION GenerateShares(encrypted\_data, n):

7.1 Generate (n-1) random share matrices of same size as encrypted\_data.

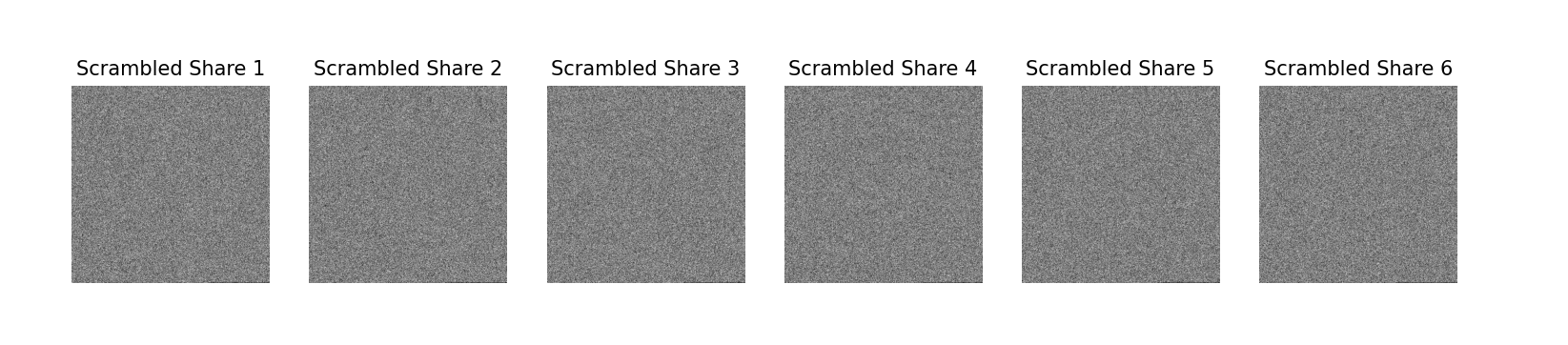
7.2 Compute last share as XOR of all previous shares and encrypted\_data.

7.3 RETURN list of n shares.

END FUNCTION







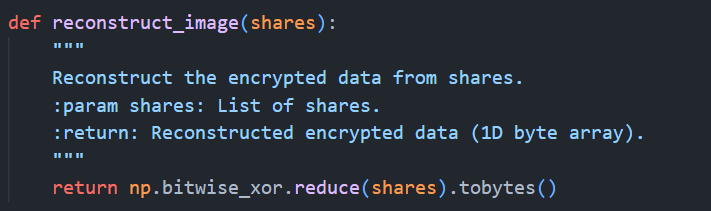
**MODULE-2: Decryption and data retrieval.**

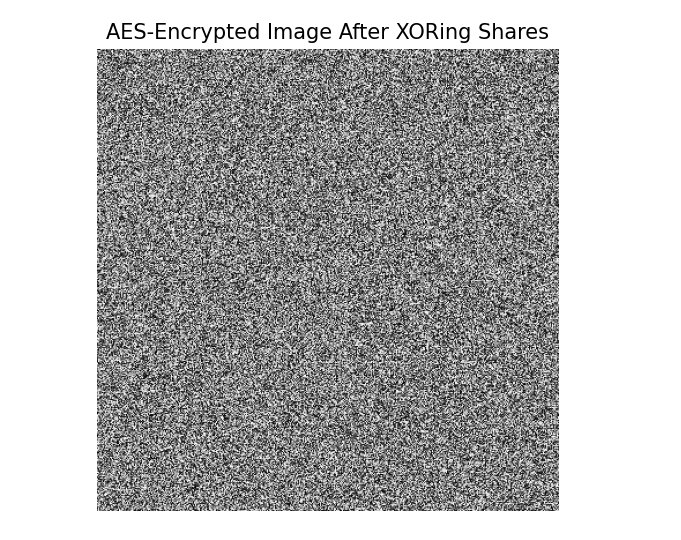
FUNCTION ReconstructFromShares(shares):

8.1 XOR all received shares together.

8.2 RETURN reconstructed encrypted data.

END FUNCTION





FUNCTION DecryptAES(encrypted\_data, aes\_key):

9.1 Extract IV from first 16 bytes of encrypted\_data.

9.2 Extract ciphertext.

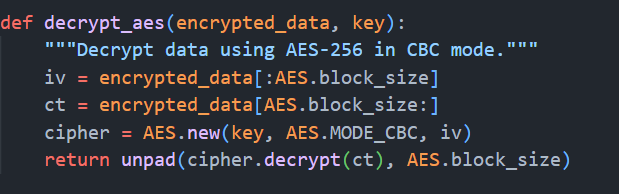
9.3 Initialize AES-256 cipher with IV and aes\_key.

9.4 Decrypt ciphertext.

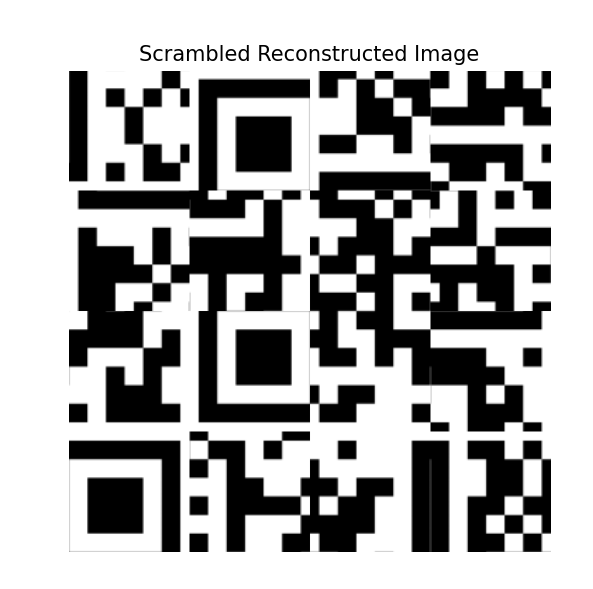
9.5 Apply PKCS7 unpadding.

9.6 RETURN decrypted data.

END FUNCTION







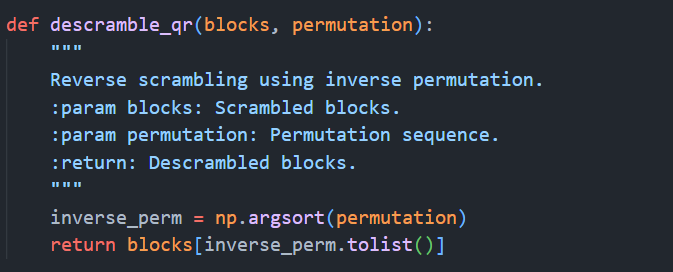
FUNCTION DescrambleQRCode(blocks, permutation):

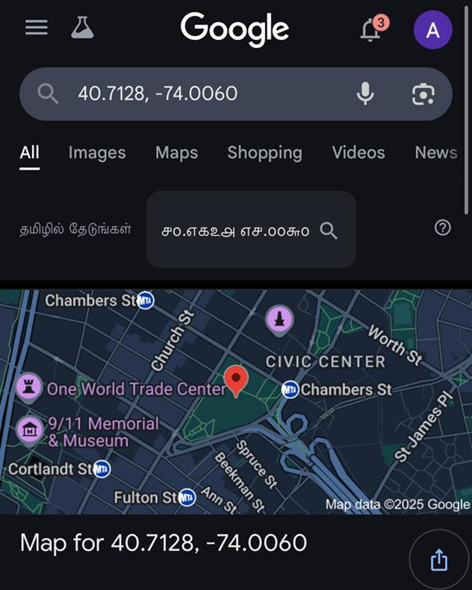
10.1 Compute inverse permutation.

10.2 Rearrange blocks according to inverse permutation.

10.3 RETURN descrambled QR code blocks.

END FUNCTION





**MODULE-3: Evaluation Metrics**

FUNCTION EvaluateQR(original\_qr, reconstructed\_qr):

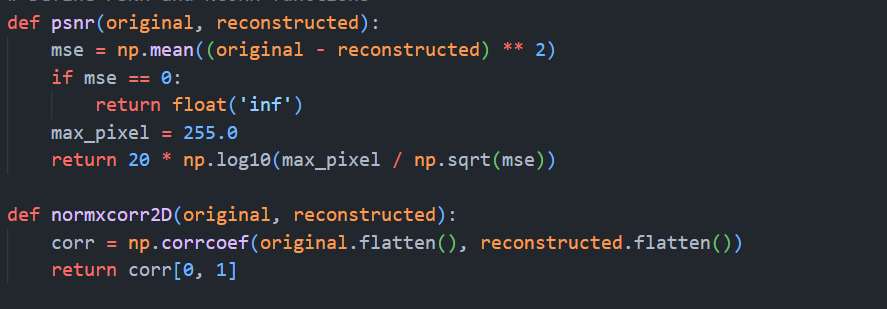
11.1 Compute Peak Signal-to-Noise Ratio (PSNR).

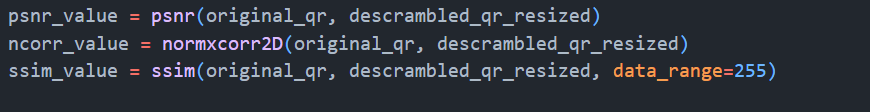
11.2 Compute Normalized Cross-Correlation (NCORR).

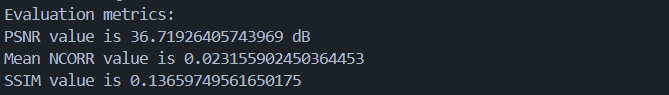
11.3 Compute Structural Similarity Index (SSIM)

11.3 RETURN PSNR, NCORR and SSIM values.

END FUNCTION

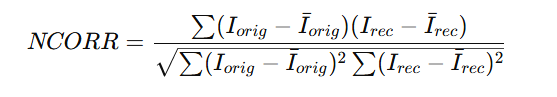




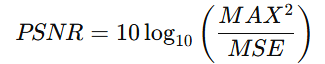


**EVALUVATION METRICS**

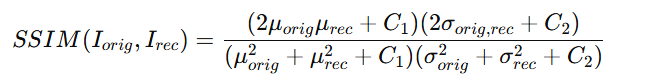
1. **Normalised Cross Correlation**
   1. NCORR Measures the similarity between the original and reconstructed QR codes

**

1. **Peak-Signal-To-Noise Ratio**
   1. Measures the difference between the original and reconstructed QR codes in terms of pixel intensity distortion.
   2. Higher PSNR means better quality (less distortion).



1. **Structural Similarity Index (SSIM)**
   1. Compares luminance, contrast, and structure between images.
   2. More sensitive to human visual perception than PSNR.



**CONCLUSION**

By leveraging cryptographic techniques such as AES-256 encryption and QR code scrambling, this project ensures secure and tamper-resistant data transmission. The integration of permutation scrambling and QR code share splitting enhances confidentiality, making unauthorized reconstruction significantly more difficult. Reassembling the original QR code through systematic decryption and reconstruction techniques enables reliable data retrieval while maintaining security. Therefore, this approach contributes to advancements in secure communication, reinforcing the robustness of encrypted QR-based data transfer systems.

**REFERENCE:**

[1] Haroon Rashid ,Hammood Al Dallal and Wijdan Noaman Marzoog Al Mukhtar, “*A QR Code Used for Personal Information Based On Multi-Layer Encryption System* ”, *Int. J. Interact. Mob. Technol.*, vol. 17, no. 09, pp. pp. 44–56, May 2023.

[2] Okubo, I.; Ono, S.; Kim, H.-W.; Cho, M.; Lee, M.-C. “*A Study on the Simple Encryption of QR Codes Using Random Numbers*.” Electronics 2024, 13, 3003.

[3] X. Wu, N. An and Z. Xu, "*Sharing Multiple Secrets in XOR-Based Visual Cryptography by Non-Monotonic Threshold Property*," in IEEE Transactions on Circuits and Systems for Video Technology,

[4] S. Sharma, S. Shivani and N. Saxena, "*A Self-Authenticating Multi-Tone Secret Sharing Scheme Using Meaningful Shares for Satellite Images*," in IEEE Access, vol. 12, pp. 101563-101591, 2024,

[5] S. Saha, A. K. Chattopadhyay, A. K. Barman, A. Nag and S. Nandi, "*Secret Image Sharing Schemes: A Comprehensive Survey*," in IEEE Access, vol. 11, pp. 98333-98361, 2023,

[6] P. Li, J. Ma, L. Yin and Q. Ma, *"A Construction Method of (2, 3) Visual Cryptography Scheme*," in IEEE Access, vol. 8, pp. 32840-32849, 2020,

[7] A. Jolfaei, X. -W. Wu and V. Muthukkumarasamy, "*On the Security of Permutation-Only Image Encryption Schemes*," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 235-246, Feb. 2020,

[8] Zhengxin Fu, Liguo Fang, Hangying Huang, Bin Yu,”*Distributed three-level QR codes based on visual cryptography scheme*,”,Journal of Visual Communication and Image Representation,Volume 87,2022,

[9] 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)

[10] 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)