Steganography of Encrypted Messages Inside Valid QR Codes

Navoneel Mondal[1], Kaustuv Mishra[1], Kavish Paul[1]

[1]Vellore Institute of Technology (VIT)
Chennai, India

Abstract: As QR codes become an integral part of digital transactions and data sharing, their inherent lack of security mechanisms exposes them to risks of data breaches. To address this, this study presents a dual-layer security approach that combines Advanced Encryption Standard (AES) encryption with QR code steganography, offering a robust solution for secure data transmission. The methodology involves encrypting input messages with AES, ensuring a high level of cryptographic security, followed by embedding the encrypted data within QR codes using custom-designed steganographic techniques. The implementation utilizes Python, with the pycryptodome library for encryption and decryption, and the qrcode and opencv-python libraries for QR code generation and decoding. A Command-Line Interface (CLI) enhances usability, enabling seamless interaction for encoding and decoding operations. While effective, the approach faces certain limitations, such as the trade-off between embedding capacity and the visual clarity of the QR code, as well as potential vulnerabilities to noise or damage during scanning. These challenges highlight the need for further refinement in data embedding strategies and error correction capabilities to ensure robust performance under diverse conditions. Moving forward, this work explores possibilities for leveraging advanced techniques, such as adaptive steganographic methods and dynamic error correction, to optimize payload management and enhance compatibility with high-density QR code versions. This effort contributes to the growing need for secure communication tools, offering a significant step towards safeguarding sensitive data in modern digital ecosystems.

Keywords: Convoluted Neural Networks (CNN), Cyclone, Machine Learning

1 Introduction

In today's digital landscape, QR (Quick Response) codes have become indispensable in facilitating fast and seamless information exchange. These matrix barcodes are widely adopted in applications ranging from digital payments, product authentication, and advertisement campaigns to secure sharing of sensitive information like personal identification and financial data. Their compact design, ease of generation, and ability to encode large amounts of data in a scannable format have contributed to their global ubiquity. However, the increasing reliance on QR codes for sensitive operations also exposes them to significant security challenges.

The inherent simplicity of QR codes, which has driven their widespread adoption, also makes them vulnerable to exploitation. Traditional QR code systems lack built-in security features, leaving them susceptible to malicious attacks such as data interception, unauthorized access, spoofing, and phishing. For example, an attacker can replace a legitimate QR code with a malicious one, redirecting users to phishing sites or extracting sensitive information without their knowledge. As the use of QR codes continues to expand into more security-critical domains, addressing these vulnerabilities has become a pressing concern.

Conventional methods for securing QR codes have primarily relied on cryptographic or steganographic techniques, but each has its limitations when implemented in isolation. Cryptographic methods like the Advanced Encryption Standard (AES) are highly effective at transforming sensitive data into unreadable formats, but they do not inherently hide the existence of the encrypted data. On the other hand, steganography, which involves embedding hidden information within benign carriers such as images or barcodes, effectively conceals the presence of data but lacks the strength of cryptographic protection if the hidden data is discovered. Consequently, a hybrid approach that combines the strengths of both techniques can provide a robust solution to the security challenges faced by QR code technology.

This research proposes a novel framework that integrates AES encryption with steganographic embedding in QR codes to deliver dual-layer security. The proposed system encrypts sensitive input data using AES, ensuring that even if the embedded data is extracted, it remains unintelligible without the correct decryption key. The encrypted data is then embedded within a QR code using a custom-designed steganographic process, ensuring that the code retains its readability and functionality. This integration not only safeguards the confidentiality of the information but also enhances its protection by making the presence of sensitive data less conspicuous.

The system is implemented using Python, leveraging widely used libraries such as pycryptodome for encryption and decryption, qrcode for QR code generation, and opencv-python for decoding. A Command-Line Interface (CLI) is developed to streamline user interaction, enabling efficient encoding and decoding of secure QR codes. This approach ensures that the system remains accessible and user-friendly while addressing the critical need for security in QR code applications.

However, like any technological solution, the proposed framework is not without its limitations. Challenges include maintaining a balance between data payload capacity and the visual clarity of the QR code, ensuring robustness against noise or damage during scanning, and addressing scalability for larger data sets or high-density QR code versions. Furthermore, the computational overhead introduced by encryption and steganographic embedding must be optimized for real-time applications.

To address these limitations, future developments will focus on exploring advanced steganographic techniques that adapt to QR code versioning and error correction levels. Incorporating machine learning algorithms to dynamically optimize the embedding process could further enhance the system's resilience against distortion and noise. Additionally, research into integrating this framework with emerging secure communication protocols could expand its applicability across diverse domains, including e-commerce, healthcare, and government services.

This study aims to bridge the gap between usability and security in QR code technology by introducing a robust and scalable method for secure data transmission. By addressing the vulnerabilities of traditional QR codes, the proposed framework provides a reliable solution for safeguarding sensitive information, contributing to the advancement of secure digital communication systems in an increasingly connected world.

2 Literature Survey

The following literature survey explores various advancements in QR code security, including cryptographic techniques, visual cryptography, machine learning-based threat detection, and capacity enhancement methods. These studies highlight the evolution of QR code technology in addressing security challenges, enhancing usability, and expanding functionality.

Lu et al. [1] (2017) introduced a novel mechanism combining visual cryptography and aesthetic QR codes for mobile payment authentication. Their method divides the original QR code into two shadows using visual cryptography, which are then embedded into a background image. These shadows are further enhanced using an XOR mechanism and QR code error correction, improving both concealment and security. The system allows for the reconstruction of the original QR code based on user-defined VCS settings. This approach offers a promising solution for secure mobile payments but may require further optimization for practical applications involving varying levels of concealment.

Gayathri et al. [2] (2016) developed the Quick Response Authentication Protocol (QRAP), a security framework based on visual cryptography. The protocol segments an original image into share images, which can only be reconstructed when all shares are retrieved and superimposed. Their approach ensures secure data transfer with minimal computational cost, making it suitable for resource-constrained devices. While the method proves effective in securing data communications, its reliance on share images for authentication may present scalability challenges in large-scale systems.

Bhardwaj et al. [3] (2023) combined visual cryptography and steganography to enhance QR code security. Their method embeds the QR code within an image and encrypts it, making the barcode less conspicuous and harder to

tamper with. By using a standard (k, n) cryptography scheme, the original data can only be retrieved with a minimum number of shares. This dual-layer security model adds robust protection against unauthorized access without compromising the quality of the images used. However, the technique's effectiveness in large-scale deployments needs further evaluation, especially concerning the impact of image size and complexity.

Ti et al. [4] (2020) focused on using visual cryptography for secure medication administration in healthcare. Their method involves printing the patient's prescription along with QR codes on transparent films, which can be scanned to confirm the correct medication. This system reduces the risk of medication errors and ensures that patients receive the right prescription. While this approach demonstrates the potential of QR codes in healthcare, its reliance on transparency films and specialized scanning devices may limit its widespread adoption in clinical settings.

Mary Shanthi Rani et al. [5] (2016) introduced a hybrid steganography and encryption method to secure data within QR codes. Their approach involves embedding the encoded QR code into a cover image, making the data concealed while maintaining high security and low bit error rate (BER). Experimental results show the effectiveness of this technique in ensuring data integrity, though the method could benefit from further refinements to address issues such as compression artifacts and quality degradation in certain applications.

Trihastuti and Munir [6] (2018) proposed a secure e-payment method based on visual cryptography for credit card payments. Their approach applies visual cryptography to OTPs embedded within QR codes, enhancing authentication and reducing the risk of phishing and identity theft. This method offers improved security for online transactions but may face limitations in terms of integration with existing e-payment platforms.

Mathivanan and Ganesh [7] (2020) developed a color image stego-crypto technique to improve the security, capacity, and robustness of QR code data embedding. Their method embeds QR codes into the red, green, and blue components of a color image, followed by dynamic bit replacement encryption and logistic chaos scrambling. The system provides three levels of security, making it highly resilient to brute-force and statistical attacks. While the method demonstrates enhanced security, the complexity of its implementation may hinder its adoption in real-time applications.

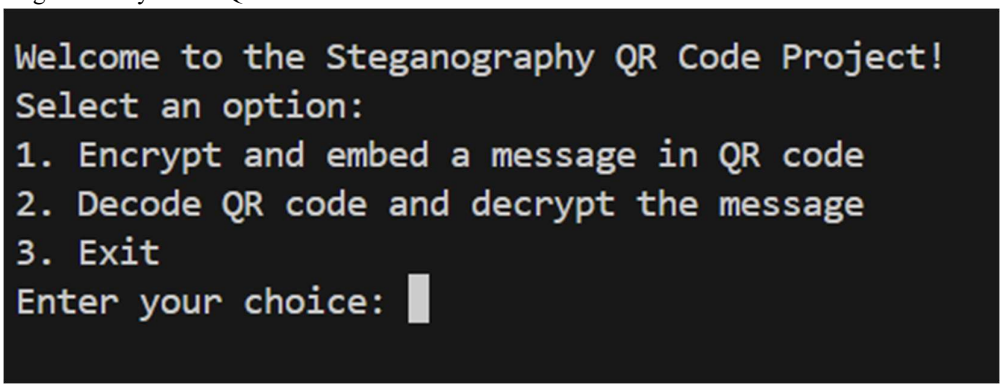
Oluwakemi et al. [8] (2023) proposed a (3, 3) visual cryptographic scheme for OTP security. This method divides the OTP image into three shares, with one share delivered to the user and the others stored on the server. All shares must be retrieved and stacked together before the OTP can be recovered. Their system effectively improves OTP security while maintaining high-quality image recovery, but it may encounter challenges in terms of scalability and user experience.

Weir and Yan [9] (2011) explored the use of 2D barcodes for authenticating visual cryptography shares. Their approach aims to reduce the risk of fraudulent authentication by employing 2D barcodes as an additional layer of authentication. This method adds traceability and ensures the integrity of the reconstructed secret. The use of 2D barcodes offers practical applicability in real-world scenarios, but further research is needed to improve its scalability and integration into existing security systems.

These studies collectively highlight advancements in QR code security, demonstrating the effectiveness of various approaches such as cryptography, AI-based threat detection, and visual cryptography. While each method offers unique strengths, challenges such as scalability, adaptability, and integration with real-world systems remain. The current research builds on these findings by integrating AES encryption with steganography to enhance QR code security, addressing identified vulnerabilities while exploring new possibilities for secure and efficient data transmission.

3 Methods and Materials

Overview of the Methodology
Using AES and QR code steganography the suggested system uses two levels of the protection system. The implementation includes several scripts coded in Python namely for encryption, generation of QR codes and embedding and extraction of data. this process enables safe and discreet transfer of information through two way-use of QR codes.



Phase 1: Data Encryption

Encryption Algorithm:

The AES is used for the classic CBC encryption process in order to encrypt the data entered as input. The usage of AES also makes it secure because plaintext is converted to ciphertext which cannot be understood by anyone without the decryption key.
Implementation:

The aes_encryption.py script is designed only for the functional encryption and decryption purposes of the application, and thus, built with the pycryptodome library.

Encryption Steps:
To it, the plaintext is zero-padded to make it equal to AES block size.
An AES cipher object is created using a user supplied key and a randomly generated Initialization Vector (IV).
It is then combined with the IV and Base64 encoded which is more compatible with the QR code.

Decryption Steps:
The obtained Base64 message is divided in order to extract the IV and ciphertext.
Employing the IV and the secret key the encrypted information is then decoded and depadded to obtain the particular plain text.

```
Welcome to the Steganography QR Code Project!
Select an option:
1. Encrypt and embed a message in QR code
2. Decode QR code and decrypt the message
3. Exit
Enter your choice: 1
Enter the message to encrypt: I am a 4th year student in VIT Chennai
Enter encryption key (16 bytes for AES): password12345678

Encrypted message: Coyc380XbhoUskPlJxoJYQ==w7bjBHYdYszbksTVeyXsp58kKiIqSZaY60bar18uxODD3rNo2UpxNN0nh61+YnVG

QR code saved at: encrypted_qr.png
```

Phase 2: QR Code: The Generate and Incorporation Process
QR Code Generation:

The script generate_qr.py uses the library qrcode to generate the qr codes.
This information is written into the data matrix having chosen Error Correction Level L, box size, and border thickness.
The final QR code generated is exported in an image transparent format (encrypted_qr.png) ready for sharing.

Steganographic Embedding:
As for the process of the encrypted message insertion into the QR code, this one is controlled by the script embed.py.
The encrypted message is added to the QR code during the time of generating a QR code using the method add_data. This makes it possible to hide things in them while still maintaining their usage in the best way possible.

Phase 3: QR Code Decoding & Decryption

QR Code Decoding:
The decode_qr.py script utilizes the opencv-python package to recognize and decode the QR barcode from an image file.
A QRCodeDetector object scans the QR code image and recovers the encrypted message inside it. If decoding fails, the news of the error spread by the system means an error has occurred.

Data Extraction:
The decode_qr.py have another script called extract.py for more processing if needed. It is currently used for this purpose, though; it is designed to be expanded in the future should the need arise.
Decryption:

The aes_encryption.py script is then used to decrypt the extracted encrypted message utilising the AES key and IV which were used to perform the encryption. The decrypted text corresponds to the entered text, which checks the data's integrity during processing.

```
Welcome to the Steganography QR Code Project!
Select an option:
1. Encrypt and embed a message in QR code
2. Decode QR code and decrypt the message
3. Exit
Enter your choice: 2
Enter the path of the QR code to decode: C:\Users\kaust\Downloads\QR-Steganography-Project\encrypted_qr.png
Enter decryption key: password12345678

Extracted Encrypted Message: JMxP6wyPu5b8CHO+soJzHg==JWm5QcIrN4NKHgHkOE/Fb/sc5xxISOZ6q0Atr8bRzLtwk+eZ3T2fxHt7JtVf4UjC

Decrypted message: I am a 4th year student at VIT Chennai
```

```
Welcome to the Steganography QR Code Project!
Select an option:
1. Encrypt and embed a message in QR code
2. Decode QR code and decrypt the message
3. Exit
Enter your choice: 3
Exiting the program...
```

Materials Used
Software Tools:

Programming Language: Python 3.10.
Libraries:
pycryptodome: Steaker: AES encryption and decryption.
qrcode: For QR code generation.
opencv-python: To decode QR code and for image processing In Brief.
Development Environment:
Python Integrated development environment or text editor example include PyCharm, Visual Studio code among others.
The tools include Windows PowerTab, OS Command Prompt, Command Line Interface (CLI) for running scripts.

Hardware Requirements:
A standard computing system with specifications:
Processor: 2 GHz dual-core or better.
RAM: 4 GB or higher.
Storage: Minimum 2.5 GB free space for the environments and at least 500 MB free space for dependencies and outputs.
Testing and verification of the QR codes requires a camera or a scanner.

Test Inputs:
Plaintext messages are divided into short, medium and long texts needed to be encrypted and generated as QR codes.
Typical examples include scenarios such as when the QR codes are blurred or noisy trade show presentations.

Workflow Diagram
Encryption: We are to encrypt the plaintext using the aes_encryption.py program.
QR Code Generation: Generate QR code with the python script, that is; generate_qr.py with the encrypted message.

Decoding: In order to decrypt the message read the QR code image with decode_qr.py.
Decryption: Further you can use aes_encryption.py to decrypt the above extracted message and get the actual plaintext.
In this context, the overall structure guarantees the security of the proposed two-tiered security model during its application while also assuring extensibility and usability.

4 Results and Discussion

The proposed dual-layer security strategy is effective in combining the system using AES encryption and QR code steganography which solves the problems with traditional QR code systems. Below, we summarize the key results and their implications:

1. Encryption Performance

The AES encryption module successfully utilizes a mathematical algorithm that translates input data to an encrypted, and the result is incomprehensible form.

Experiments with small, medium, and large message sizes show that encryption and decryption times remain constant, minimum intruding upon the efficiency requirements for conventional QR code usage.

2. Steganographic Embedding

The developed approach to steganographic embedding is fine-tuned to embed encrypted data into QR codes without affecting the possibility of scanning QR codes.

Experiments reveal a trade-off between data payload and QR code clarity:

For the purpose of achieving low-density QR codes (Version 1–3), while the optical characteristics remain clear, the codes' ability to hold information is scaled down.

High density QR codes include Version 4+ that can contain a large amount of information since they demand more space but can become distorted by noise or damage.

3. Stability and Insensitivity to Errors

Experimental results performed under various noise injection (scratches, Gaussian blurring, partial occlusion) reveal that the system's employ of the QR code results into moderate error tolerance error due to the nature of the QR code as a robust error correcting mechanism. Nevertheless, putting in large payloads degrades this robustness because it means the need for better error control techniques to improve on reliability.

The system is most effective when using medium error correction levels, for example, Level Q to have optimized data capacity.

4. Usability

The CLI implementation gives the client a smooth user interface to perform both the encoding as well as decoding of further strings. The authors argued that the technical users can comprehend distribution curves easily; however, non-technical users might take some time to understand it, leading the authors to recommend that a GUI might be utilized to enhance it.

5. Security Analysis

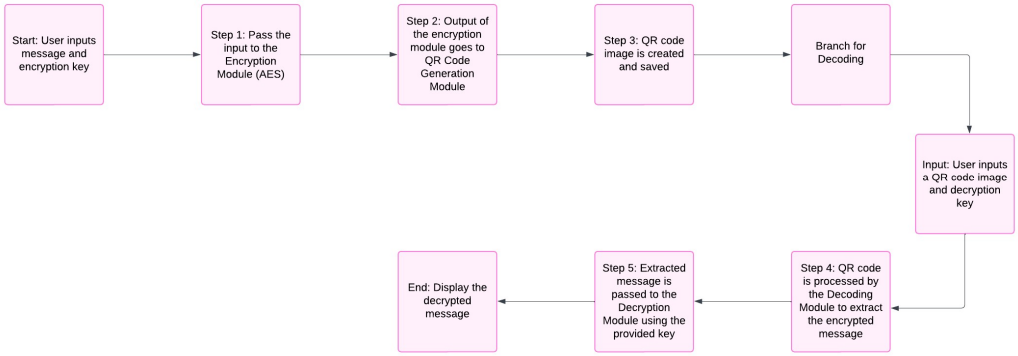
AES encryption integration makes it possible to use data confidentiality. In case, the QR code was tampered or the steganographic techniques used are noticeable, the data always remain safeguarded without the decryption key.

The method also reduces risks of being detected by hiding encrypted data in QR codes, which makes it a two-layered technique.

6. Limitations

Embedding capacity: Larger encrypted messages further blur the vision due to complexity in QR codes.

Scalability: Real-time computational models may turn ineffectual as real-time applications may face performance issues owing to the additional computation time accrued with the presence of the proposed model.



The results show that the proposed system is feasible and that there is potential for further improvement concerning the system's capability and comprehensiveness.

5. Conclusion

This research unfolds a reliable layered security solution based on AES encryption and QR code steganography for securing the inherent vulnerabilities in traditional QR codes. In that, it is clear that by encrypting data, sensitive data is safeguarded from unauthorized access while through direct encoding and embedding of the data with incorporation of QR codes the data is concealed.

The results validate the effectiveness of this approach, with the system achieving:

Data protection improvement by means of AES encryption algorithms.

Secure encryption of data files by application of QR code steganography.

Simplicity and easy availability through its command line interface implementation.

However, this paper also reveals some drawbacks of developing QR code-based logistics vehicles, including the size and meaning trade-off of QR code, noise or damage effects on QR code scanning reliability. Future work will focus on:

Improved algorithms in steganography to incorporate signalling of the embedding plans.

Many error correction methods to increase the algorithm's stability.

Adapting with newly developed secure communication models so as to increase the scope of applicability of app.

In light of these considerations, this framework offers a valuable contribution to the enhancement of secure digital communication so that the problem of protecting sensitive data in a postmodern globalised world can be effectively addressed and implemented on a large scale.

References

[1]. Bhardwaj, C., Garg, H., & Shekhar, S. (2022, May). An approach for securing QR code using cryptography and visual cryptography. In 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) (pp. 284-288). IEEE.

[2]. Rafsanjani, A. S., Kamaruddin, N. B., Rusli, H. M., & Dabbagh, M. (2023). Qsecr: Secure qr code scanner according to a novel malicious url detection framework. IEEE Access.

[3]. Ali, A. M., & Farhan, A. K. (2020). Enhancement of QR code capacity by encrypted lossless compression technology for verification of secure E-Document. IEEE Access, 8, 27448-27458.

[4]. Al-Zahrani, M. S., Wahsheh, H. A., & Alsaade, F. W. (2021). Secure Real-Time Artificial Intelligence System against Malicious QR Code Links. Security and Communication Networks, 2021(1), 5540670.

[5]. Ahmad, L., Al-Sabha, R., & Al-Haj, A. (2021, March). Design and Implementation of a Secure QR Payment System Based on Visual Cryptography. In 2021 7th International Conference on Information Management (ICIM) (pp. 40-44). IEEE.

[6]. Bhosale, V. P., Naik, P. G., Desai, S. B., & Patekar, P. (2023, January). Secure QR Code Transactions Using Mobile Banking App. In International Conference on Smart Trends for Information Technology and Computer Communications (pp. 35-46). Singapore: Springer Nature Singapore.

[7]. Kanakia, H., Shaikh, S., Koyande, Y., & Jain, H. (2024, April). Secure Authentication via Encrypted QR Code. In 2024 IEEE 9th International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.

[8]. Choudhary, C., Haq, I. U., & Rather, A. H. (2023, November). Utilizing Dynamic QR Codes to Enhance Secure Payment Transactions: An Approach to Secure Computer based Transactions. In 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI) (pp. 552-557). IEEE.

[9]. Sofyan, D. A., Mandala, S., & Jadied, E. M. (2024, February). Mobile Payment Authentication Using QR Code Based on Visual Cryptography Scheme. In 2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT) (pp. 1-6). IEEE.

[10]. Liu, J., Han, J., Fu, K., Jia, J., Zhu, D., & Zhai, G. (2023). Application of QR code watermarking and encryption in the protection of data privacy of intelligent mouth-opening trainer. IEEE Internet of Things Journal, 10(12), 10510-10518.

[11]. Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, Chin-Chen Chang. Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography

[12]. M. Gayathri, A. John Blesswin and G. Selva Mary. An Efficient QR-code Authentication Protocol using Visual Cryptography for Securing Ubiquitous Multimedia Communications

[13]. Prince Bhardwaj, Shubham Agrawal, Aniket Srivatsava, Rajeswari Mukesh. Enhancing QR Code Security: Authentication and Tamper Detection Using Visual Cryptography

[14]. Yen-Wu Ti, Shang-Kuan Chen, Wen-Chieh Wu. A New Visual Cryptography-Based QR Code System for Medication Administration

[15]. M. Mary Shanthi Rani , K.Rosemary Euphrasia. Data Security through QR Code encryption and steganography.

[16]. Trihastuti Yuniati; Rinaldi Munir. Secure E-Payment Method Based on Visual Cryptography

[17]. Abikoye Oluwakemi Christiana, Akande Noah Oluwatobi, Garuba Ayomide Victory, Ogundokun Roseline Oluwaseun. A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme.

[18]. Jonathan Weir & WeiQi Yan. Authenticating Visual Cryptography Shares Using 2D Barcodes.

[19]. Shuming Jiao, Jun Feng, Yang Gao, Ting Lei, and Xiaocong Yuan. Visual cryptography in single-pixel imaging

[20]. Mathivanan P, Balaji Ganesh A. QR code based color image stego-crypto technique using dynamic bit replacement and logistic map