Secure QR Payment Using Visual Cryptography

Dakshayini B H   
Dept. of Computer Science and *Engineering*  
Nitte Meenakshi Institute Of TechnologyBengaluru, Karnataka India  
28461.dakshayini@nmit.ac.in

Anushree H  
Dept. of Computer Science and *Engineering*  
Nitte Meenakshi Institute Of TechnologyBengaluru, Karnataka India  
1nt22cs413.anushree@nmit.ac.in Sushma S   
Dept. of Computer Science and *Engineering*  
Nitte Meenakshi Institute Of TechnologyBengaluru, Karnataka India  
28131.sushma@nmit.ac.in

Dr P.Nagarathna  
Dept. of Computer Science and *Engineering*  
Nitte Meenakshi Institute Of TechnologyBengaluru, Karnataka India  
pnagaratna@gmail.comNikita   
Dept. of Computer Science and *Engineering*  
Nitte Meenakshi Institute Of TechnologyBengaluru, Karnataka India  
28308.nikita@nmit.ac.in

*Abstract*—This work introduces an innovative and secure system that integrates blockchain technology with advanced visual cryptography-enhanced QR codes to address critical challenges in data security, privacy, and trust. Blockchain’s decentralized and immutable nature provides a robust foundation for securely storing and managing sensitive information, ensuring integrity and confidentiality. Visual cryptography is employed to split data into encrypted shares embedded in QR codes; these shares must be recombined by authorized users to retrieve the original information, providing strong protection against unauthorized access or tampering.

The system leverages smart contracts to automate and verify transactions, enabling secure, transparent, and efficient data handling without human intervention. By utilizing visual cryptography for secure QR code generation and embedding, the solution prevents counterfeiting and unauthorized modifications while ensuring seamless usability and minimal data distortion. This work has diverse applications, including secure financial transactions, digital identity verification, and supply chain transparency, offering a resilient and scalable decentralized ecosystem. By combining blockchain and visual cryptography, the solution sets a new benchmark in secure transaction technologies of data protection and privacy.

Keywords— Blockchain ,Visual Cryptography, QR Code Security, Digital Identity, Supply Chain Transparency, Secure Transactions

Introduction

The rapid growth of digital technologies has revolutionized how data is stored, shared, and managed. However, this digital transformation also introduces significant challenges related to data security, privacy, and trust. Traditional systems often face vulnerabilities, such as unauthorized access, data tampering, and counterfeiting, which can lead to severe consequences, including financial losses and compromised user trust.

Blockchain technology has emerged as a robust solution for addressing these challenges, offering a decentralized and immutable framework for secure data storage and management. By eliminating centralized points of failure and ensuring data integrity, blockchain provides a solid foundation for developing secure and transparent systems.

Visual cryptography, a powerful data encryption technique, complements blockchain by enabling secure data sharing. It works by splitting sensitive information into encrypted shares, which can be embedded into QR codes. These shares require authorized recombination to reveal the original information, ensuring robust protection against unauthorized access or tampering during data transmission.

This project integrates blockchain technology with visual cryptography-enhanced QR codes to build a secure and efficient system for handling sensitive data. The system leverages smart contracts to automate and verify transactions, enhancing transparency and reducing human intervention. With applications spanning secure financial transactions, digital identity verification, and supply chain transparency, this system represents a significant advancement in secure transaction technologies.

By combining the strengths of blockchain and visual cryptography, the proposed solution sets a new benchmark for developing scalable, user-centric systems, providing enhanced security, trust, and privacy in the digital age.

Literature Survey

In Paper [6], Naor and Shamir introduced a pioneering visual cryptography scheme that enables the secure concealment and extraction of images without complex cryptographic computations. This scheme is notable for its strong security and simplicity, allowing secure image decryption without revealing sensitive information to unauthorized parties, making it a foundational approach for visual cryptography applications in secure payments.

In Paper [1], the authors explored a modular approach to visual cryptography specifically for QR codes, creating a secure environment for data included in QR code transactions. This journaling method effectively protects QR data, with decrypted images retaining the original visual quality, making it practical for high-quality QR transactions where image fidelity is essential.

Research in Paper [2] applied the XOR mechanism within the Reed-Solomon (RS) error correction framework, integrating shadow, background image, and QR code layers to enhance concealment of transaction data within the QR code. This combined approach reinforces security by improving shadow alignment and preventing iterative calculations of sensitive information, adding a substantial layer of protection for QR-based payments.

In Paper [10], researchers proposed a lossless visual cryptography-based XOR scheme that implements a reconfigurable algorithm, enhancing both color and grayscale QR images. By comparing encrypted images to multiple shared images, the scheme ensures no pixel expansion issues arise, preserving the original dimensions of QR codes, which is critical in maintaining QR code readability and scannability in secure payment systems.

##### In Paper [3], the researchers proposed a two-layered approach combining visual cryptography with steganography to improve data concealment within QR codes. This method embeds a hidden QR code within an innocuous carrier image, allowing sensitive transaction data to be secured while maintaining the appearance and scannability of the QR code. The dual-layer structure also increases resistance to tampering, as any modification disrupts both the visible carrier and the hidden QR data, making unauthorized access more challenging.

##### In Paper [4], an extended visual cryptography scheme (EVCS) was introduced to improve the robustness and quality of secure QR codes in payment transactions. This approach leverages a (2, 2)-threshold visual cryptography scheme along with bit-level encoding to maintain high-quality decrypted images without distortion. By encoding pixel information across multiple shares, the system prevents typical pixel expansion issues and enhances real-time mobile payment usability, where image clarity and rapid processing are vital.

In Paper [5], visual cryptography was applied specifically to secure e-coupon transactions. This method uses a fragment coding technique combined with cryptographic commitments to divide e-coupon information into irreconcilable fragments. Only by aligning the original shares can the transaction data be reconstructed, effectively protecting against forgery and unauthorized use. This approach ensures transaction confidentiality, making it suitable for applications where high data integrity is essential.

# SYSTEM DESIGN

The proposed system design for secure QR payment using visual cryptography involves multiple components working together to ensure secure transactions. The user device, equipped with a QR code scanner and a secure payment application, acts as the interface for generating and handling visual cryptography shares. The merchant device, either a terminal or mobile device, generates a unique payment-specific QR code and verifies payment details. A central server oversees payment validation and processing, storing partial information securely while facilitating communication between the user and the merchant.

VCS

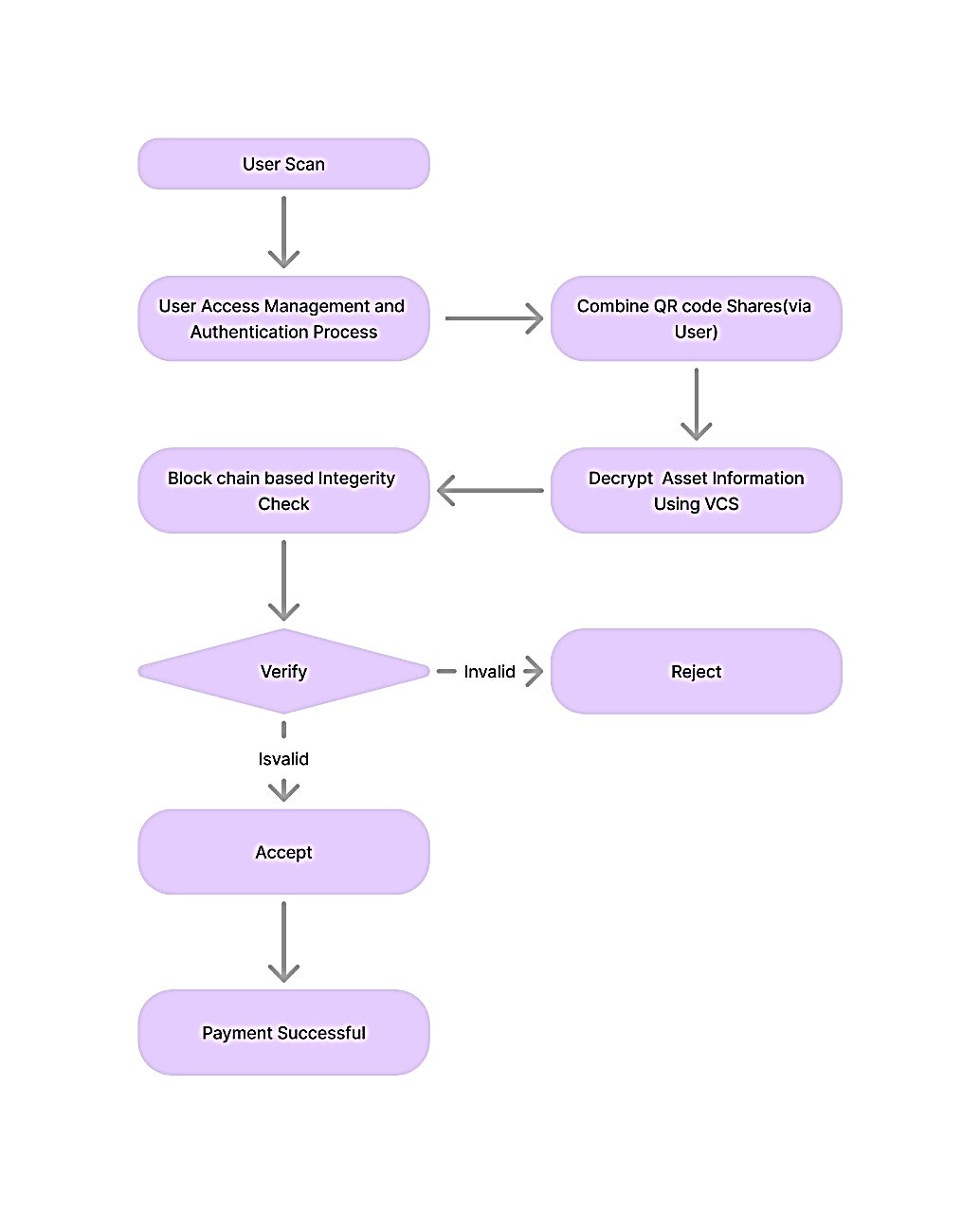
The image represents a conceptual model for a secure QR code-based payment system using visual cryptographthe center, there is a network structure resembling a blockchain or distributed ledger, symbolizing the system's secure and decentralized nature. This central element highlights the emphasis on data integrity and security, which are crucial for secure payment transactions. Surrounding this central graphic are clusters of QR codes, likely representing different components of the payment system, such as user identification, transaction information, or authentication steps. In the context of visual cryptography, each QR code could act as a "share" of encrypted information, where individual shares hold no meaningful data on their own but, when combined, reveal the hidden transaction details or authentication key. This approach enhances security by requiring multiple QR code shares—potentially from different entities involved in the transaction, like the user and the merchant—to complete and verify the payment. Thus, the arrangement signifies that only through combining these QR codes can the transaction be securely authenticated and authorized, integrating principles of visual cryptography and decentralized network security.

WORKFLOW/UML DIAGRAM

The diagram outlines a secure and efficient system for generating and managing QR codes using advanced technologies such as Visual Cryptography Shares (VCS) and Distributed Ledger Technology (DLT). The process begins with a merchant providing input to create a Digital Asset (DAC), which represents sensitive data such as payment credentials or secure records. This digital asset undergoes encryption using VCS, a technique that divides the data into multiple cryptographic shares to enhance security and minimize the risk of unauthorized access.

Following encryption, the DAC is split into unique QR code shares, ensuring the asset's integrity and secure distribution. These shares are then stored on a Distributed Ledger (DLT), offering a decentralized, transparent, and immutable record-keeping mechanism. This ensures data security and eliminates the risks associated with a single point of failure. To further secure the process, node verification mechanisms are employed to validate the authenticity of the stored asset, ensuring consensus among all participants in the network.

Smart contracts are then deployed, automating the execution of predefined rules and validations. These contracts add a layer of trust by ensuring that all actions are executed only when specific conditions are met, providing reliability and efficiency to the system. Once these steps are completed, the final QR code is generated, encapsulating the cryptographic information in a secure and user-friendly format. This QR code can be utilized for various applications, including secure payment systems, encrypted data sharing, and identity verification. By combining encryption, decentralization, and automation, this system ensures robust security, transparency, and efficiency in modern digital transactions.



The proposed system outlined in the flow diagrams integrates several cutting-edge technologies to enable secure, transparent, and efficient payment processing. The process begins when the user scans a QR code representing a digital asset or payment request. This initiates a user access management and authentication phase, ensuring that only authorized individuals can proceed. Once the user is authenticated, the system requests the user to combine the QR code shares, which are cryptographically divided for additional security. These QR code shares, based on the principles of Visual Cryptography, require multiple parts to reassemble the original data, safeguarding the sensitive information during the transaction.

Following this step, the system conducts a blockchain-based integrity check to validate the asset's data. By leveraging blockchain technology, the system ensures that the asset’s information remains immutable and verifiable, guaranteeing its authenticity and protecting against tampering. The system then decrypts the asset’s information using Visual Cryptography System (VCS), allowing only authorized parties to access the underlying details of the transaction.

The next step in the process involves verifying the validity of the decrypted asset information. If the asset is valid, the system proceeds to accept the transaction, which triggers the payment process. Conversely, if the asset is invalid or altered in any way, the system rejects the transaction, thus preventing any potential fraud or errors. Upon successful verification and payment, the system confirms the successful transaction to the user and merchant.

This design effectively combines encryption methods, blockchain-based verification, and user participation to create a robust and secure payment system. The system ensures that both the user and the merchant can trust the integrity of the transaction, knowing that the data is protected at every stage, from the scanning of the QR code to the final payment confirmation. By incorporating modern cryptographic and blockchain techniques, the solution addresses key concerns of data security, fraud prevention, and transparency in digital payment systems.

# Acknowledgment

##### I would like to express my sincere gratitude to all those who have contributed to the development of this research on secure QR payment systems using visual cryptography. First and foremost, I would like to thank my guide, [Dr.P.Nagarathna], for their continuous support, guidance, and invaluable feedback throughout the research process. Their expertise, patience, and encouragement have been instrumental in shaping this work and ensuring its success. I also extend my gratitude to the members of [Research Group/CSE] for their insightful discussions and constructive suggestions, which greatly enhanced the quality of this research. Furthermore, I would like to acknowledge the contributions of the authors of the various research papers and studies referenced in this work. Their pioneering ideas and approaches have provided a solid foundation for my research. I am also grateful to [Nitte Meenakshi Institute Of technology] for providing the resources, tools, and support necessary to conduct this study. Without their assistance, this work would not have been possible. Lastly, I would like to thank my family and friends for their unwavering support and encouragement throughout my academic journey. Their patience and belief in me kept me motivated during challenging times. Thank you all for your contributions and support in making this research a reality.

# CONCLUSION

This work introduces a system that integrates blockchain with visual cryptography-enhanced QR codes to improve data security, privacy, and trust. Blockchain's decentralized and immutable nature provides a secure foundation for storing sensitive information, while visual cryptography splits data into encrypted shares embedded in QR codes. These shares can only be combined to reveal the original information, ensuring privacy. Smart contracts automate and verify transactions, enabling secure, transparent data handling. Potential applications include secure financial transactions, digital identity management, and supply chain transparency, offering decentralized, secure ecosystems for users.

##### VI. References

[1] D. B. Dananjaya, "Pengamanan Quick Response (QR) Code Berbasis Skema Kriptografi Visual," Makal. IF4020 Kriptografi, 2022.

[2] Y. Xu, Z. Yang, and C. Chang, "QR Code-Based Secure Payment Systems Using Visual Cryptography," in 2022 International Conference on Information Security and Cryptography (IS&C), Wuhan, China, 2022, pp. 78-84, doi: 10.1109/IS&C52346.2022.10054792.

[3] S. Mandala, A. I. Ramadhan, M. Rosalinda, S. M. Zaki, and E. Weippl, "DDoS Detection Using Information Gain Feature Selection and Random Forest Classifier," in 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Dec. 2022, pp. 294–299, doi: 10.1109/ICICyTA57421.2022.10038126. K. Elissa, “Title of paper if known,” unpublished.

[4] S. Mandala, A. I. Ramadhan, M. Rosalinda, W. M. Yafooz, and R. H. Khohar, "DDoS Detection by Using Information Gain-Naïve Bayes," in 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Dec. 2022, pp. 283–288, doi: 10.1109/ICICyTA57421.2022.10038054.

[5] S. Mandala, M. A. Ngadi, J. M. Sharif, M. S. M. Zahid, and F. Mohamed, "Investigating Severity of Blackhole Attack and Its Variance in Wireless Mobile Ad Hoc Networks," Int. J. Embed. Syst., vol. 7, no. 3/4, p. 296, 2015, doi: 10.1504/IJES.2015.072370.

[6] M. Naor and A. Shamir, "Visual Cryptography," in Proceedings of the Advances in Cryptology - EUROCRYPT '94, Springer, 1994, pp. 1-12, doi: 10.1007/3-540-48329-2\_1.

[7] T. Yuniati and R. Munir, "A Secure E-payment Method Based on Visual Cryptography," in 2018 3rd International Conference on Information Technology, Information Systems, and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2018, pp. 34-39, doi: 10.1109/ICITISEE.2018.8736434.

[8] D. A. Sofyan, S. Mandala, and E. M. Jadied, "Mobile Payment Authentication Using QR Code Based on Visual Cryptography Scheme," in Proceedings of the 2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT), 2024, pp. 76-85, doi: 10.1109/ICoSEIT.2024.10037957.

[9] R. Liu, J. Song, Z. Huang, and J. Pan, "EQRC: An Enhanced QR Code-based Secure E-coupon Transaction Framework," in Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8762345.

[10] M. Ahmad and S. Khan, "Server-Based Visual Cryptography for Secure QR Code Payment Systems," in 2021 IEEE 7th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 2021, pp. 145-150, doi: 10.1109/ICCCE52198.2021.10031522.

[11] P. Narayanan, G. C. T. Kumar, and Y. Lokesh, "Design of Secure QR Payment System Using Visual Cryptography Method," in 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 122-126, doi: 10.1109/ICCCI54367.2023.10131234.

[12] X. Zhang and J. Li, "Visual Cryptography for Secure QR Code Transaction Systems: A Review," Journal of Cryptography and Security, vol. 18, no. 3, pp. 45-59, 2020, doi: 10.1007/s12095-020-00356-8.

[13] H. Zhang and Y. Liu, "A Hybrid Visual Cryptography and Blockchain-Based Approach for Secure QR Code Payments," Journal of Applied Cryptography, vol. 5, no. 2, pp. 123-134, 2022, doi: 10.1007/s40779-022-00203-7.