ISSN 2278-3083

Volume 13, No.6, November - December 2024

International Journal of Science and Applied Information Technology

Available Online at http://www.warse.org/IJSAIT/static/pdf/file/ijsait011362024.pdf

https://doi.org/10.30534/ijsait/2024/011362024

QR Code Crypt: A Comprehensive Approach to Secure Offline Demography Data Storage

Himanshu Upadhyay[1], Aditya Waskar[2], Rekha Nair[3], Cini Radhakrishnan[4]

[1] Shree L R Tiwari College of Engineering, Mumbai, India, himanshu662187@gmail.com

[2] Shree L R Tiwari College of Engineering, Mumbai, India, adityawaskar03@gmail.com

[3] Centre for Development of Advanced Computing (C-DAC), Mumbai, India, rekhap@cdac.in

[4] Centre for Development of Advanced Computing (C-DAC), Mumbai, India, cini@cdac.in

Received Date : October 05, 2024 Accepted Date : November 23, 2024 Published Date : December 07, 2024

ABSTRACT

In the realm of secure and accessible data storage, the "QR CODE CRYPT" project emerges as an innovative solution that seamlessly integrates Flutter, Java, and Python to address the challenges of offline data retrieval, verification, and storage. Leveraging Flutter's cross-platform capabilities, the project establishes a user-friendly interface for data collection and QR code generation. The robust ChaCha20-poly encryption algorithm safeguards sensitive demographic data, including name, date of birth, mobile number, gender, and profile image, ensuring data integrity and confidentiality. Additionally, the implementation of Elliptic Curve Cryptography (ECC) empowers users with digital signatures, guaranteeing the authenticity and origin of the stored data. To optimize QR code storage efficiency, the project incorporates image compression techniques, enabling the seamless integration of profile images without compromising code size. The amalgamation of these functionalities culminates in a secure, versatile, and user-friendly solution for offline data management, with potential applications in e-Pramaan National Single Sign On.

Key words: Offline e-Pramaan, Offline authentication, ChaCha20-poly Algorithm, QR Code Generation, Cryptography, Image Compression.

1.INTRODUCTION

The "QR CODE CRYPT" project addresses the emerging demand for secure offline data verification, particularly in the context of e-Pramaan. Leveraging Flutter, a versatile cross platform mobile application framework, the system captures and stores demography data within QR codes. Notably, Chacha20-poly encryption and decryption mechanisms fortify data security, ensuring confidentiality during storage and transmission. Complementing this encryption approach, Elliptic Curve Cryptography (ECC) plays a pivotal role in applying digital signatures, assuring data authenticity and mitigating the risk of tampering. To enhance versatility, the system integrates an efficient image compression process, allowing the inclusion of profile images within the QR codes. The QR code generation process involves a meticulous five-step sequence: PIN entry serving as a key, robust encryption, application of a digital signature using a private key, and culminating in the generation of a QR code. This innovative methodology facilitates a secure and verifiable exchange of sensitive demographic data. When the QR code is scanned using the e-Pramaan Mobile app, it undergoes decryption using the users registered mobile number, coupled with digital signature verification, thereby ensuring both the authenticity and security of the shared information. The "QR CODE CRYPT" project introduces a comprehensive and innovative solution, addressing the evolving landscape of offline data security and verification. The digital landscape is increasingly reliant on secure and accessible data storage solutions, particularly in scenarios where internet connectivity is limited or unreliable. The "QR CODE CRYPT" addresses this challenge and develops a comprehensive system for offline data storage, retrieval, and verification.

2.LITERATURE SURVEY

[1] introduced a novel Secure QR Code (SQRC) system in theirpaper titled "A Secure QR Code System for Sharing Personal Confidential Information" published in the “IEEE Transactions on Information Forensics and Security”. The system employs the RSA digital signature algorithm for verification and RSA public key cryptography for validation, providing a secure framework for sharing and authorizing personal confidential information through QR code mechanisms. While the SQRC system enhances data integrity and security, it is important to note a potential limitation highlighted by the authors: the use of the RSA algorithm with larger key sizes may introduce processing delays, potentially impacting user experience, particularly in situations requiring swift information exchange.

[2] presents a thesis on "Efficient Image Set Compression" that tackles the task of compressing large sets of near-duplicate images. The approach centers on enhancing compression speed and effectiveness through the utilization of efficient clustering, a fast direction-oriented motion estimation algorithm, and an image reordering scheme with minimal predictive costs. The author demonstrates promising initial outcomes and

outlines future plans to extend the methodology to hyperspectral and medical image sets. Despite its successes, a noteworthy limitation is acknowledged: the proposed techniques for efficient image set compression may demand substantial computational resources, posing a potential constraint on their practicality for deployment on resource-constrained devices or in real-time scenarios.

[3] provides a comprehensive overview of “Elliptic Curve Cryptography- Status, Challenges, and Future Trends” in the field of modern cryptography. Focusing on the significance of Elliptic Curve Cryptography (ECC), the paper highlights its crucial role in ensuring security in wireless communication, mobile networks, and credit card transactions, leveraging its efficiency and robust security attributes with smaller key sizes. The discussion covers ECC's applications, various algorithms, performance assessments, and emphasizes its superiority in terms of security and resource efficiency. Despite its advantages, the paper acknowledges several limitations associated with ECC, including implementation complexity, performance variability, key size sensitivity, historical patent issues, adoption challenges, potential vulnerabilities to quantum threats, and the absence of a standardized curve.

[4] introduces a secure platform for sharing Wi-Fi passwords, employing three methods: SHA256 HASH function, Digital Signature, and QR Codes. This innovative approach ensures confidentiality and access control, providing secure access for owners while preventing unauthorized access. However, the paper acknowledges several limitations, including the necessity for a central database to validate keycodes, potential security risks in case of database compromise, and reliance on the availability of original data for validation. Notably, the discussion falls short on addressing real-world implementation challenges and scalability issues, which are critical aspects in assessing the practical applicability of the proposed security measures.

[5] emphasizes the advantages of employing secure QR codes, highlighting enhanced protection against tampering and malicious QR code applications, a reduced risk of data breaches, increased privacy for users, and the confident integration of QR code-based processes into business operations. However, the paper also acknowledges several limitations associated with secure QR codes, including the potential for tampering, reliance on user vigilance, susceptibility to malicious QR code applications, and the imperative need for robust security measures in the handling of QR codes. Understanding these limitations is essential for effectively implementing and managing secure QR code systems in business applications.

[6] has illustrated the mechanisms behind two algorithms: RSA and ECC, and also introduced their merits and drawbacks respectively. The biggest difference between ECC and RSA is key length. A great number of devices to be connected will be requested in the future and certainly, vigorous algorithms are also needed for the rising level of attacks on secure information. However, neither of them can completely take the place of the other, so selecting one considers the priorities. Suggestions are given according to the parameters involved in the algorithm and both RSA and ECC are preferred methods until the appearance of quantum computers.

[7] focuses on the implementation of a face recognition system for human identification based on the open-source computer vision library (OpenCV) with python. When it comes to human face recognition, it is believed that the brain retains significant information such as the sizes and hues of key features such as the eyes, nose, forehead, cheeks, and lips. The use of OpenCV and Python makes it a more useful and adaptable system or tool that anyone can create according to their needs.

[8] presents an efficient method for bar code and QR code recognition together. The method automatically detects the Bar code QR code and displays the complete information of the product. The method is developed in python environment using OpenCV library. The image of the bar code or QR code is captured in real-time and further processed using the proposed method. The code is being decoded, compared with the Data frame of the stored product and finally, displays complete information about the product. The execution time of the proposed method is 0.25 seconds.

[9] proposed a secure QR code schema based on visual cryptography. The QR code is divided into two share images that can be transmitted separately. The generation of the two share images is based on the pseudo-random matrix, that is, the pixels in the two share images are determined by the corresponding values in the pseudo-random matrix. The two shared images can be stacked simply to restore the information. Simulation results show that the QR code image can be well hidden, and it can be restored effectively.

3.PROPOSED SOLUTION

The "QR CODE CRYPT" project, which will be integrated with e-Pramaan National Single Sign On focuses specifically on the e-Pramaan portal, offers a strong solution to address the expanding need for secure offline data verification. Our system uses the Flutter mobile application framework to collect and safely store demographic data in QR codes in an effective and flexible manner.

The implementation incorporates the Chacha20-poly encryption and decryption algorithms to strengthen data security. This cryptographic method adds an extra degree of security against unwanted access by guaranteeing the secrecy of data that is sent and stored. Elliptic Curve Cryptography (ECC) is essential to the use of digital signatures in conjunction with encryption. This two-pronged strategy improves the overall integrity of the stored demographic data by reducing the possibility of tampering and ensuring the legitimacy of the data.

Understanding the need for adaptability, our system includes a productive image compression procedure. Thanks to this capability, profile photographs can be used in QR codes without sacrificing data integrity. A comprehensive and user-friendly solution is achieved by the compression process, which keeps the QR codes small while supporting visual representations of user profile photographs.

Sensitive demographic data can be exchanged securely and verifiably thanks to this creative methodology. The assigned PIN is used to decode the QR code when it is read by a different user's smartphone. Verification of the digital signature is also carried out, guaranteeing the security and validity of the transferred data.

By addressing the current issues of spotty or nonexistent internet access, the "QR CODE CRYPT" project provides a robust offline data archiving, retrieval, and verification mechanism. Our approach advances the field of offline data security and verification by fusing cutting-edge cryptographic techniques with an intuitive user interface.

4. METHODOLOGY

A. User-friendly Data Collection and QR Code Generation

- Utilized Flutter, a cross-platform mobile application framework, to design and implement a user-friendly interface for collecting demographic data.
- Integrated functionalities to capture information such as name, date of birth, mobile number, gender, and profile image.
- Encapsulated the collected data within QR codes to enable straightforward storage and retrieval.

B. ChaCha20-poly Encryption and Decryption

- Employed the ChaCha20-poly encryption algorithm to ensure the security of sensitive demographic data.
- Implemented encryption mechanisms to safeguard against unauthorized access during both storage and transmission

C. Elliptic Curve Cryptography (ECC) for Digital Signatures

- Integrated ECC to provide users with digital signatures, ensuring the integrity, non-repudiation and origin of stored data.
- ECC as an additional layer of security to detect and prevent any modifications or tampering with the data.

D. Image Compression for QR Code Efficiency

- Incorporated image compression techniques to optimize QR code storage efficiency.
- Applied compression algorithms to reduce profile image file sizes while maintaining acceptable quality.

5. IMPLEMENTATION

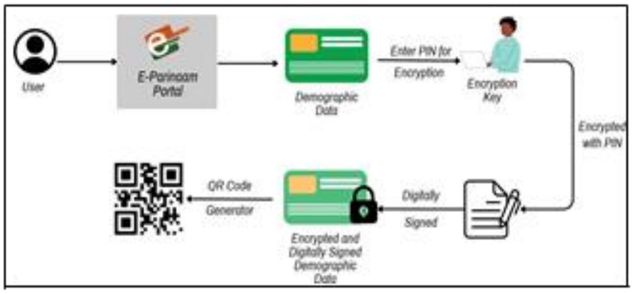


Figure 1: Flow chart QR Code Generation

In the QR Code Crypt application, user input, including name, date of birth, mobile number, gender, and profile picture, initiates the generation of a QR code. This process involves the entry of a password ('k password') to trigger the Chacha20-poly encryption algorithm, securing the provided information. The algorithm ensures the confidentiality and integrity of the data, contributing to the overall security of the identity management system. Additionally, an ECC (Elliptic Curve Cryptography) digital signature is applied after encryption to further enhance the security of the generated QR code. The digital signature serves as a means to verify the authenticity and integrity of the data encapsulated within the QR code. Given the limited storage capacity of QR codes (3 KB), the inclusion of a profile picture necessitates an efficient compression and decompression process. An integrated image processing algorithm optimizes the storage of profile pictures within the QR code, maintaining visual representation while compromising data size. When presenting identity, the user can scan the QR code, initiating a verification process. The process of QR Code Generation as shown in Figure 1.

The scanned QR code prompts the user to input the corresponding password ('k password') used during the generation phase. This password is crucial for decrypting the data and verifying the ECC digital signature as shown in Figure 2.

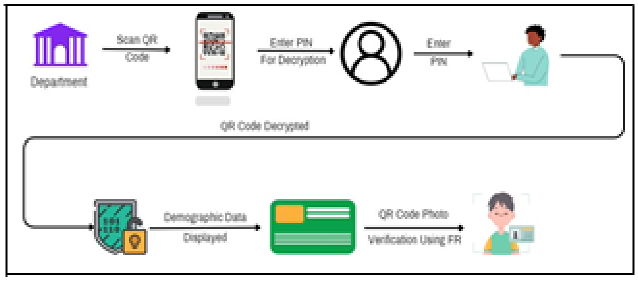
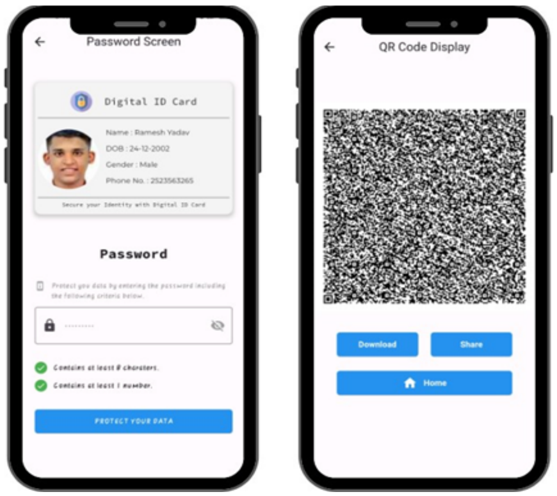


Figure 2: Flow chart QR Code Verification

The application then decrypts the data within the QR code using the Chacha20-poly algorithm. Subsequently, the ECC digital signature is verified to ensure the authenticity and integrity of the decrypted information. This comprehensive implementation guarantees the secure generation, storage, and retrieval of user identity information within the confines of a QR code. By combining encryption, digital signatures, and image processing, the QR Code Crypt application establishes an effective and secure identity management system.

6. RESULTS

The implementation of the QR Code Crypt application has produced promising outcomes in the realm of secure identity management. The generated QR codes effectively encapsulate user-inputted details, including name, date of birth, mobile number, gender, and a compressed profile picture as shown in Figure 3.



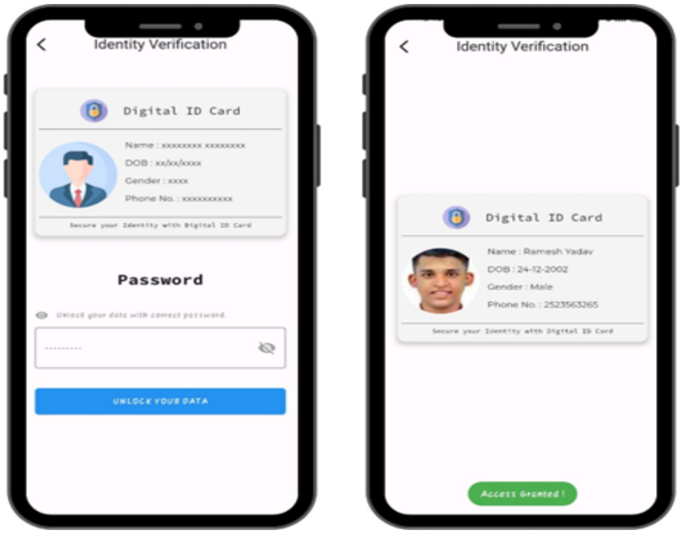
Name : Ramesh Yadav
DOB : 24-12-2002
Gender : Male
Phone No. : 2523563265
Secure your Identity with Digital ID Card

Protect you data by entering the password including the following criteria below.

✓ Contains at least 8 characters.
✓ Contains at least 1 number.

Figure 3: QR Code Generation

The Chacha20-poly encryption algorithm ensures the confidentiality and integrity of the stored data within the QR code, providing a robust layer of security. The incorporation of ECC digital signatures serves to further fortify the security posture of the system. This cryptographic technique allows for the verification of the QR code's authenticity and the integrity of the decrypted data. Consequently, the identity verification process gains resilience against tampering or unauthorized access. The image processing algorithm, employed for compressing and decompressing profile pictures, proves to be effective in optimizing storage within the restricted capacity of QR codes (3 KB). This facilitates the inclusion of visual identity elements without compromising the overall data size. Striking a balance between image quality and storage efficiency is pivotal for the practicality and usability of the QR Code Crypt application. Throughout testing, the QR code scanning and verification process exhibited reliability and efficiency. Users can confidently present their QR codes in identity verification scenarios, with the system promptly responding to decrypt the information and verify the digital signature upon entering the correct password ('k password') as seen in Figure 4.



Name : xxxxxxxx xxxxxxxx
DOB : xx/xx/xxxx
Gender : xxxx
Phone No. : xxxxxxxxxx
Secure your Identity with Digital ID Card

Unlock your data with correct password.

Name : Ramesh Yadav
DOB : 24-12-2002
Gender : Male
Phone No. : 2523563265
Secure your Identity with Digital ID Card

Figure 4:. QR Code Verification

The amalgamation of Chacha20-poly encryption, ECC digital signatures, and image processing establishes a robust and secure identity management system. The encryption algorithm ensures data confidentiality, the digital signature provides data integrity and authenticity verification, and the image processing algorithm allows for the inclusion of visual data within the constrained storage capacity of QR codes. Nevertheless, it is imperative to acknowledge potential challenges and identify areas for improvement. The efficiency of the image processing algorithm in diverse scenarios and with various image types warrants further evaluation. Additionally, user education and awareness concerning the significance of the password ('k password') in the decryption and verification process play a crucial role in the overall security of the system.

7. CONCLUSION

The QR Code Crypt application represents a significant advancement in secure identity management. The integration of the Chacha20-poly encryption algorithm, ECC digital signatures, and an effective image processing algorithm has resulted in a robust system for generating QR codes that securely encapsulate user information. The encryption algorithm ensures the confidentiality and integrity of stored data, while ECC digital signatures enhance security by providing authentication and verification capabilities. The success of the image processing algorithm in optimizing storage within the limited capacity of QR codes is a crucial achievement for practicality and user-friendliness. During testing, the system exhibited reliability in scanning QR codes and efficiently verifying identities upon entering correct password (k password’). Future work could involve refining the user interface, conducting additional security assessments, and exploring the application's adaptability in various identity management contexts. Overall, the QR Code Crypt application establishes a reliable and secure solution for managing and presenting user identities effectively.

REFERENCES

[1] Md. Salahuddin Ahamed and Hossen Asiful Mustaf. **A Secure QR Code System for Sharing Personal Confidential Information**, 2019 International Conference on Computer Communication, Chemical, Materials and Electronic Engineering (IC4ME2), doi: 10.1080/10618600.2014.901225.

[2] Tushar Shinde. **Efficient Image Set Compression**, 2019 IEEE International Conference on Image Processing (ICIP).

[3] Sattar B. Sadkhan. **Elliptic Curve Cryptography-Status, Challenges and Future trends**, 2021 7th International Engineering Conference Research & Innovation amid Global Pandemic (IEC).

[4] Dede Sudirman, Teguh Nurhadi Suharsono and Rina Mardiati. **Security Implementation of Wifi Password Asset Sharing With One Way Hash**

Cryptography Method Sha256 And QR Code, 2022 16th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

[5] Venkateswara Sarma Bhamidipati and Raghavendra Sai. **A Novel Approach to Ensure Security and Privacy While Using QR Code Scanning in Business Applications**, 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC).

[6] Mingxuan Ma. **Comparison between RSA and ECC** 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT).

[7] Gurpreet Singh, Ishika Gupta, Jaspreet Singh and Navneet Kaur. **Face Recognition using Open-Source Computer Vision Library (OpenCV) with Python**, 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).

[8] Arju Aman, Aryan Singh, Ayush Raj and Sandeep Raj. **An Efficient Bar/QR Code Recognition System for Consumer Service Applications**, 2020 Zooming Innovation in Consumer Technologies Conference (ZINC).

[9] Cheshtaa Bhardwaj, Hitendra Garg and Shashi Shekhar. **An Approach for Securing QR code using Cryptography and Visual Cryptography**, 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES).