Catalyzing
Research Excellence Across Diverse Academic Disciplines
ISBN Number: 978-93-95305-16-7

PERFORMANCE ANALYSIS OF VISUAL SECRET SHARING-BASED QR PROTECTION FOR PRIVACY-PRESERVING FACE AUTHENTICATION

Dr. Ujwal Ambadas Lanjewar,
Research Supervisor,
R.T.M. Nagpur university, Nagpur

ABSTRACT

The study assessed the performance of a Visual Secret Sharing (VSS) based QR protection mechanism on privacy-preserving face authentication. A research design was used that comprised the use of publicly available dataset of face images and consisted of face image processing, feature extraction, VSS shares creation, QR encoding and decoding, secret reconstruction, and face verification. Performance of the proposed scheme was analyzed on the basis of authentication accuracy, processing time, QR encoding and decoding success rates, secret reconstruction, storage, and computation cost. The results obtained indicated that the proposed scheme was able to achieve 96.40% authentication accuracy, in comparison to 94.20% by the conventional authentication technique, and 99.2% and 98.8% success rates in QR encoding and decoding, respectively. A success rate of 98.5% in secret reconstruction was also observed with an average reconstruction time of 22 ms, while share integrity verification succeeded in 99.1%. The proposed approach lowered the biometric storage from 128 KB to 96 KB but increased the processing time from 156 ms to 248 ms and increased the computation cost to 18.6%.

Keywords: *Visual Secret Sharing, QR Code, Face Authentication, Biometric Privacy, Privacy Preservation, Secret Reconstruction, Biometric Security.*

1. INTRODUCTION

The rise of new technologies related to digital identities, mobile applications, contactless payments, etc., creates a demand for privacy-preserving face authentication systems. Facial biometrics make a good candidate for such systems since there is no necessity to use physical tokens or passwords to verify users' identities. However, existing face authentication systems

ISBN Number: 978-93-95305-16-7

include storing or sending facial data which leads to problems of biometric privacy, unauthorized access, identity theft, and other issues connected to misuse of sensitive information. The fact that facial information does not change during one's lifetime makes the protection of biometric information an essential aspect of current researches. It gives an opportunity to integrate QR protection into the face authentication process to increase its security level.

Visual Secret Sharing (VSS) is a cryptographic technique which provides information security by splitting the secret visual image into several shares and allows restoring the original information only when needed shares are merged properly. Using VSS with QR codes enables one to develop a secure way of protecting visual information in such a way that the biometric data will not be visible. It can be considered a good way to represent and share authentication-related information using QR code which acts as a portable visual medium and secret sharing to avoid storing the whole biometric data in a single place. If this idea is implemented to the face authentication, it will be possible to achieve privacy by separating sensitive information into protected parts and reconstructing needed information at the point of authentication only. This scheme is especially interesting in mobile and smart-device environments where QR codes can be used conveniently for authentication purposes.

The performance analysis of the Visual Secret Sharing-based QR protection system is important to evaluate the efficiency of this technology and find out how it works in practice. There are several performance aspects to analyse, including the accuracy of face authentication, processing time, efficiency of encoding and decoding QR code, reconstruction quality, the amount of memory required, computational complexity and resistance to the unauthorized disclosure of information. These indicators will allow us to define the correlation between the security level and authentication performance and improve the design of biometric authentication systems. The present research aims to perform the performance analysis of a QR protection system based on Visual Secret Sharing in the context of face authentication.

2. REVIEW OF LITERATURE

Bhardwaj et al. (2024) conducted research on QR code security through visual cryptography technique. In their research, the areas of authentication and detection of tampering were highlighted, whereby visual cryptography technique was applied in enhancing the security of

ISBN Number: 978-93-95305-16-7

QR codes. The results indicated that visual cryptography would aid in detecting any alterations on QR code, hence making the process more secure. This research was quite important in secure QR code generation and authentication systems.

Kaur and Khanna (2020) implemented privacy-preserving multi-server biometric authentication scheme based on cancellable biometrics and secret sharing. In this research, the security issues of biometric data were investigated in the framework of remote authentication environment using the concept of cancellable biometric templates along with secret sharing. It was shown that the use of secret sharing helps to lower the risks of revealing biometric data directly.

Pan et al. (2022) developed visual cryptography protocol based on color QR codes for secret color images. This study combined visual cryptography technology with color QR code to securely encode and decode secret visual information. It proved the application potential of QR codes as a carrier of protected visual information along with the decoding ability of visual secret. This study had close connection with the application of QR technology and visual cryptography to visual information protection.

Ren and Zhang (2022) proposed a privacy-preserving system for recognizing the biometrics based on Visual Cryptography. The study examined the utilization of Visual Cryptography in privacy preserving biometric recognition. The scientists made use of secret-sharing methods in such a way that biometric data was not exposed directly but at the same time supported the recognition process. The study made the connection between Visual Cryptography and privacy preserving biometrics and gave rise to more research in Visual Secret Sharing and QR face recognition.

3. RESEARCH METHODOLOGY

This study employs the experimental research methodology for assessing the effectiveness of the VSS-enabled QR protection scheme for privacy-preserved face recognition system. Face dataset is used for processing together with Visual Secret Sharing, QR code generation/decoding and face authentication process. The performance of the proposed technique is analyzed based on accuracy, processing time, efficiency, storage requirement and computation. The findings are compared with traditional face authentication schemes through tabulation and graphics.

ISBN Number: 978-93-95305-16-7

3.1. Research Design

This study makes use of experimental and performance evaluation methodology to analyze the QR code protection scheme using Visual Secret Sharing (VSS) for secure face authentication. The proposed scheme is implemented and evaluated in controlled environment for the security, authentication accuracy, and performance aspect

3.2. System Development

Face recognition scheme has been developed by combining facial image processing, Visual Secret Sharing, QR code encoding, and authentication checking. Facial details are transformed to a protected form and segmented to produce visual shares utilizing the VSS scheme. This protected data is then encoded in QR format for further processing.

3.3. Dataset

The face images dataset which is publicly available and appropriate for the experimentation is taken. This dataset consists of images of different faces. These images undergo various pre-processing steps like resizing and normalization before conducting authentication experiments.

3.4. Proposed Authentication Process

The procedure of authentication is made up of capturing an image of the face, pre-processing, extracting features, generating protected information, generating VSS shares, QR encoding, QR decoding, reconstructing secrets and verifying the face. In the process of authentication, the necessary protected shares are reconstructed and compared against the registered facial image.

3.5. Performance Evaluation

Parameters for evaluating the effectiveness of the system include authentication accuracy, processing time, time taken in encoding/decoding QR, reconstruction efficiency, storage needed, and computational complexity. Additionally, security performance in terms of protection of the facial information from unauthorized access will also be evaluated.

ISBN Number: 978-93-95305-16-7

3.6. Comparative Analysis

The performance of the proposed VSS-based QR protection technique is evaluated against a conventional or unprotected face authentication technique. The evaluation is done by analyzing the privacy protection and authentication performance trade-offs among other issues.

3.7. Data Analysis

Results from experiments are presented in tables and graphs. Descriptive statistics techniques are employed to describe the results achieved, whereas comparative analysis helps identify the strengths and weaknesses of the methods being evaluated.

4. RESULTS AND DISCUSSION

The study provide information on the effectiveness of the new VSS based QR protection method in privacy preserving face authentication in terms of authentication accuracy, processing efficiency, QR protection, reconstruction of the secrets and computation cost. From tables 1-5 we see that there are some discrepancies between conventional and new methods with respect to performance related to authentication and privacy in addition to the new computation costs.

4.1. Authentication Performance

This section examines the validity and effectiveness of face recognition through comparison of traditional authentication process with the new suggested method of protecting QR using VSS technique. Table 1 illustrates comparison between accuracy of authentication, false accept rate, and false reject rate for assessing the validity of biometric verification.

Table 1: Comparison of Authentication Performance

Method	Authentication Accuracy (%)	False Acceptance Rate (%)	False Rejection Rate (%)
Conventional Face Authentication	94.20	2.80	3.00
Proposed VSS-Based QR Protection	96.40	1.90	1.70

The outcomes show that there is a success rate of 99.2% in QR code encoding and 98.8% in QR code decoding. As far as the secret reconstruction, it is successful at 98.5% with the average time taken to reconstruct the secret at 22 ms while verifying the share integrity is at 99.1%.

ISBN Number: 978-93-95305-16-7

4.2. Processing Performance

The above discussion analyzes the computational complexity and efficiency of both the existing and proposed systems for face authentication purposes. The below Table 2 gives the comparison of processing time from face pre-processing to face verification stage in milliseconds (ms).

Table 2: Processing Time Analysis

Processing Stage	Conventional Method (ms)	Proposed Method (ms)
Face Preprocessing	38	39
Feature Extraction	72	74
VSS Share Generation	0	31
QR Encoding	0	18
QR Decoding	0	16
Secret Reconstruction	0	22
Face Verification	46	48
Total Processing Time	156	248

Preprocessing took 38 ms, feature extraction took 72 ms, and verification took 46 ms in total in the traditional approach. The new technique involved taking 39 ms, 74 ms, 31 ms, 18 ms, 16 ms, 22 ms, and 48 ms for each stage. Therefore, the new technique took 92 ms extra time because of VSS, QR coding and decoding, and secret reconstruction steps.

4.3. QR and Secret Reconstruction Performance

This section provides an analysis of the effectiveness and efficiency of QR code security and secret reconstruction through VSS in the proposed face recognition system. The following table provides the results for QR coding and decoding, secret reconstruction, time taken for reconstruction, and share integrity.

Table 3: QR Protection and Reconstruction Results

Parameter	Result
QR Encoding Success Rate	99.2%
QR Decoding Success Rate	98.8%

ISBN Number: 978-93-95305-16-7

Secret Reconstruction Success Rate	98.5%
Average Reconstruction Time	22 ms
Share Integrity Verification	99.1%

The results show that the QR encoding is successful 99.2% of the time and that the QR decoding is successful 98.8% of the time. The results for the reconstruction of the secret have been successful 98.5%, taking an average of 22ms, while the share integrity verification has been successful 99.1%.

4.4. Storage and Computational Overhead

This section evaluates the storage and computation requirements of the traditional and the proposed VSS-based QR authentication system. Table 4 shows comparison between biometric storage, secured shares, QR code dimensions, memory requirement, and computation cost.

Table 4: Storage and Computational Comparison

Parameter	Conventional Method	Proposed VSS-Based QR
Average Biometric Storage (KB)	128	96
Number of Protected Shares	1	3
Average QR Size (KB)	0	18
Memory Usage (MB)	142	158
Computational Overhead (%)	0	18.6

The proposed approach resulted in an average biometric data reduction of 32 KB (from 128 KB to 96 KB) with a rise in protected shares from 1 to 3. An average QR file size was 18 KB against 0 KB in case of the standard approach. There was an increase in memory consumption from 142 MB to 158 MB and the computational overhead rose from 0% to 18.6%.

4.5. Overall Performance Comparison

This section gives an overall comparison of the traditional face authentication method and the proposed VSS QR protection scheme in terms of authentication, processing, decoding of the QR, reconstruction, storage, computational complexity, and privacy preservation. The various performance metrics for the two schemes are summarized in Table 5 below.

ISBN Number: 978-93-95305-16-7

Table 5: Overall Performance of the Evaluated Systems

Performance Parameter	Conventional Authentication	Proposed VSS-Based QR
Authentication Accuracy (%)	94.20	96.40
Processing Time (ms)	156	248
QR Decoding Success (%)	0.00	98.80
Reconstruction Success (%)	0.00	98.50
Storage Requirement (KB)	128	96
Computational Overhead (%)	0	18.60
Privacy Protection	Limited	Enhanced

The result indicates that the suggested VSS-based QR authentication method provided 96.40% accuracy, whereas the traditional method obtained only 94.20%. However, the processing time was higher at 248 ms compared to 156 ms. QR decoding and reconstruction were 98.80% and 98.50%, respectively. The storage was reduced from 128 KB to 96 KB but computational overhead increased to 18.60%. The privacy level also changed from Limited to Enhanced.

5. CONCLUSION

The study revealed that the VSS-based QR protection technique offered an effective privacy-enhancing mechanism for face authentication through encryption of the biometric information using share generation, QR coding, decoding, and secret reconstruction techniques. The proposed method attained an authentication accuracy of 96.40% as opposed to 94.20% obtained in the traditional face authentication system. Moreover, the QR encoding and decoding attained an accuracy of 99.2% and 98.8% respectively, while secret reconstruction attained an accuracy of 98.5% with an average reconstruction time of 22 milliseconds. The share integrity verification achieved an accuracy of 99.1%. On the other hand, the proposed technique managed to reduce the size of biometric data storage requirement from 128 KB to 96 KB but at the expense of increasing the processing time from 156 ms to 248 ms and computation overhead to 18.6% due to the use of the extra processes such as VSS, QR and secret reconstruction.

ISBN Number: 978-93-95305-16-7

REFERENCES

1. *Ali, A., Migliorati, A., Bianchi, T., & Magli, E. (2024). Cancellable templates for secure face verification based on deep learning and random projections. EURASIP Journal on Information Security, 2024(1), 7.*
2. *Ito, K., Kozu, T., Kawai, H., Hanawa, G., & Aoki, T. (2023). Cancelable face recognition using deep steganography. IEEE Transactions on Biometrics, Behavior, and Identity Science, 6(1), 87-102.*
3. *Kim, S., Shin, H., & Seo, J. H. (2025). Deep face template protection in the wild. Pattern Recognition, 162, 111336.*
4. *Liu, H., Gao, Y., Liu, C., Sun, J., Guo, X., Zhang, H., & Wan, W. (2023). CanBiPT: Cancelable biometrics with physical template. Pattern Recognition Letters, 172, 213-220.*
5. *Ren, L., & Zhang, D. (2022). Toward privacy protection of sensed biometric features with extended visual cryptography. Microprocessors and Microsystems, 91, 104540.*
6. *Arora, A., Garg, H., & Shivani, S. (2023). Privacy Protection of Digital Images Using Watermarking and QR Code-based Visual Cryptography. Advances in Multimedia, 2023(1), 6945340.*
7. *Bhardwaj, P., Agrawal, S., Srivatsava, A., & Mukesh, R. (2024, July). Enhancing QR code security: authentication and tamper detection using visual cryptography. In 2024 2nd world conference on communication & computing (WCONF) (pp. 1-7). IEEE.*
8. *Kaur, H., & Khanna, P. (2020). Privacy preserving remote multi-server biometric authentication using cancellable biometrics and secret sharing. Future Generation Computer Systems, 102, 30-41.*
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 Communication and Image Representation, 82, 103405.*
10. *Ren, L., & Zhang, D. (2022). A Privacy-Preserving Biometric Recognition System with Visual Cryptography. Advances in Multimedia, 2022(1), 1057114.*