ROBUST QR-BASED BIOMETRIC TEMPLATE PROTECTION USING VISUAL SECRET SHARING UNDER DIGITAL ATTACKS

Atul Sureshpant Akotkar,
Research Scholar,
R.T.M. Nagpur university, Nagpur

ABSTRACT

The application of biometrics is one of the most convenient ways of verifying people's identities. However, such authentication technique poses serious issues related to privacy and security since once the biometric templates are obtained, there is no way to replace them in case they get compromised. Therefore, in this study a new approach to the protection of biometric templates based on visual secret sharing and QR encoding was suggested. In particular, the facial biometric templates were encoded into QR codes and then were split into several visual shares. The experimental study included stages of preprocessing the biometric images, generating templates, encoding to QR format, generating shares via VSS algorithm, simulating the digital attack, and recovering the biometric data. For the evaluation of the protected templates, the decoding rate, reconstruction accuracy, authentication accuracy, similarity, and recovery rate were used in the conditions of noise, distortions, corruptions, cropping, and tampering attacks. Under normal conditions, the proposed system exhibited very high levels of decoding, reconstruction, authentication and similarity performance. Under the conditions of digital attacks, the performance dropped progressively, being worse in case of tampering attack compared to less destructive ones; however, the recovery rate was higher than 86%.

Keywords: *Biometric Template Protection, QR Code, Visual Secret Sharing, Biometric Authentication, Digital Attacks, QR Security, Facial Biometrics, Data Reconstruction, Attack Recovery, Privacy-Preserving Authentication.*

1. INTRODUCTION

The emergence of biometric authentication became an inevitable part of modern digital security systems due to the ability to provide identity verification based on unique physiological and behavioral traits such as faces, fingerprints, irises, voices, etc. Among all types of biometrics, the face biometrics became rather popular due to convenience and non-contact ability. However, there are several security and privacy issues related to the broad use of biometric authentication. As opposite to passwords or cryptographic keys, biometric traits cannot be

modified. That is why the protection of biometric templates at the stage of storage, transmission, and authentication becomes necessary. In such a way, the use of QR codes as a compact mechanism of encoded information storage together with the biometric template protection technique becomes possible.

The use of the Visual Secret Sharing (VSS) technology in order to protect biometric templates stored in QR codes becomes one of the effective ways of enhancing the security of biometric authentication because the idea of the visual secret sharing means the division of information on several visual shares rather than keeping one directly usable template. Thus, it becomes impossible to exploit biometric templates until several visual shares are combined in order to reconstruct the original biometric information. It becomes important for privacy-preserving authentication systems as well as the systems in which the biometric template should be protected during QR-based information storage and transmission in digital environment.

There is a possibility of digital attacks on the QR-based biometric systems as well as other attacks including but not limited to the modification, corruption, data manipulation, replay attack, etc., that make the robustness to digital attacks an urgent issue for practical implementation of QR-based biometric authentication system. This paper "Robust QR-Based Biometric Template Protection Using Visual Secret Sharing Under Digital Attacks" aims at the analysis of the ability of the VSS technology to protect the biometric template encoded through QR-based methods taking into consideration the following performance dimensions such as security, reconstruction accuracy, and robustness.

2. REVIEW OF LITERATURE

Chen et al. (2024) suggested a straightforward method of construction of (k, n)-threshold progressive visual secret sharing schemes. The paper explored the way to divide secret information into shares and reconstruct it gradually based on certain threshold requirements. The approach provided improved construction of visual secret sharing while retaining the same security characteristics as threshold-based VSS. The results of the study were significant for the present study since VSS was employed as the basic technique to divide and protect sensitive biometric information and further reconstruct it.

Fu et al. (2022) offered a distributed three-level QR code system based on the visual cryptography approach. The paper combined QR-code technologies with visual cryptography for distributing information among several components and improving its security level. The

approach showed the feasibility of applying visual cryptography to information protection via QR-codes and information recovery. The study was closely related to the present one since it provided a basis for using QR codes along with visual secret-sharing technologies for secure information storage and recovery.

Rathgeb et al. (2023) summarized an overview of various applications of deep learning in biometric templates protection. The study reviewed several approaches when the techniques of deep learning were used to generate, process and protect biometric templates. In addition, the paper outlined the growing significance of privacy-preserving biometric recognition and challenges that included template security, template revocability and reliable biometric recognition. The study provided a more general theoretical basis for the present research by showing the importance of having secure mechanisms for biometric templates protection.

Valisireddy et al. (2023) studied visual secret sharing on QR codes as the tool for online document authentication. The authors combined the technique of information representation with QR-codes and visual secret sharing to ensure the protection of the authentication information from any unauthorized access. The results of the study showed the practical potential of combining QR codes and visual secret sharing. The study was significant for the present one since it directly linked the QR-code technology with VSS though in the context of authentication information protection rather than biometric templates protection and attack resistance.

3. RESEARCH METHODOLOGY

This study employs the experiment design method to assess the security of QR-based biometric template using visual secret sharing (VSS). Biometric facial images undergo preprocessing, are transformed to templates, encoded into QR code, and are separated into visual shares. Such shares are attacked digitally through methods like noise attack, deformation attack, cropping attack, and tampering attack. The data are finally assessed through QR decoding rate, attack recovery rate, and biometric authentication rate.

3.1. Research Design

The experimental design approach is used in conducting this experiment with a view to assessing the strength of the security of biometric templates protected through Visual Secret Sharing with the help of QR code.

3.2. Biometric Template Preparation

A public biometric database containing facial information is taken as the experiment dataset. The facial images go through resizing, normalization, and feature extraction to create biometric templates, which are then transformed to a digital form that can be stored securely via QR.

3.3. QR-Based Visual Secret Sharing

The biometric templates generated are coded in QR code format and secured through a VSS technique. The QR code is separated into a number of visual shares such that the original biometric data cannot be obtained directly from one particular share. The required number of shares is merged together during the recombination process.

3.4. Digital Attack Simulation

The resilience of the proposed system is assessed based on the effects of simulated digital attacks on the QR shares and templates. These attacks may include adding noise to the images, distorting them, corrupting data in the QR codes, clipping of parts of the QR, etc.

3.5. Performance Evaluation

System performance evaluation includes the measurement of reconstruction accuracy, QR code decoding rate, biometric verification accuracy, similarity, and attack recovery rate. Experimental results obtained from protected and attacked samples are analyzed to evaluate the efficacy and robustness of the VSS based QR code protection scheme.

4. RESULTS AND DISCUSSION

This section shows the findings from the experiment that tested the proposed QR biometric template protection scheme using VSS under the following conditions: normal, protection, reconstruction, and digital attacks. This is done by evaluating the QR code decoding, reconstruction, biometric authentication and similarity, recovery, and performance loss to assess the performance of the scheme.

4.1. Performance under Normal and Protected Conditions

This section evaluates the suggested QR protection system based on the VSS in its original, protected, and reconstructed states using QR decoding, reconstruction effectiveness, biometric verification, and similarity. The performance of the system in all three states is shown in the following table, Table 1.

Table 1: Overall Performance of the Proposed VSS-Based QR Protection

Condition	QR Decoding Rate (%)	Reconstruction Accuracy (%)	Biometric Authentication (%)	Similarity (%)
Original QR	99.2	99.0	98.6	99.1
VSS Protected QR	98.8	98.5	98.1	98.7
Reconstructed QR	98.5	97.9	97.6	98.2

Original QR had a decoding rate of 99.2%, reconstruction accuracy of 99.0%, biometric authentication accuracy of 98.6%, and similarity of 99.1%. Post VSS protection, the decoding rate was 98.8%, reconstruction accuracy was 98.5%, biometric authentication accuracy was 98.1%, and similarity was 98.7%. On the other hand, the reconstructed QR had a decoding rate of 98.5%, reconstruction accuracy of 97.9%, biometric authentication accuracy of 97.6%, and similarity of 98.2%.

4.2. Performance under Digital Attacks

This section evaluates the efficiency of the suggested QR security system based on VSS with regard to various digital attacks. The attacks consist of noise attacks, distortion of images, corruption of data, cropping attacks, and tampering attacks. The effectiveness of the system is evaluated in terms of QR decoding, reconstruction accuracy, authentication accuracy, and recovery rate. Table 2 provides the comparison of the performance of the system subjected to these attacks.

Table 2: Performance under Different Digital Attacks

Digital Attack	QR Decoding Rate (%)	Reconstruction Accuracy (%)	Authentication Accuracy (%)	Attack Recovery Rate (%)
No Attack	98.8	98.5	98.1	99.0
Noise	94.6	93.8	92.9	94.1
Image Distortion	93.2	92.5	91.7	92.8
Data Corruption	91.5	90.8	89.9	90.6
Cropping	89.7	88.9	87.8	88.5
Tampering	87.9	86.8	85.9	86.4

Under no attack, there were 98.8% for QR decoding, 98.5% for reconstruction, 98.1% for authentication, and 99.0% for recovery. All these rates dropped systematically when various types of attacks are applied; noise attack led to 94.6%, 93.8%, 92.9%, and 94.1%; tampering attack led to the lowest rates of 87.9%, 86.8%, 85.9%, and 86.4% correspondingly. It is obvious from the results that more sophisticated attacks affect the performance of the system negatively, especially tampering and cropping.

4.3. Comparative Attack Analysis

The following section compares the accuracy of the reconstruction process that takes place in the VSS-based QR protection system under the influence of various digital attacks. Figure 1 demonstrates the comparison in the absence of an attack, under the presence of noise, image distortions, data alteration, cropping, and tampering.

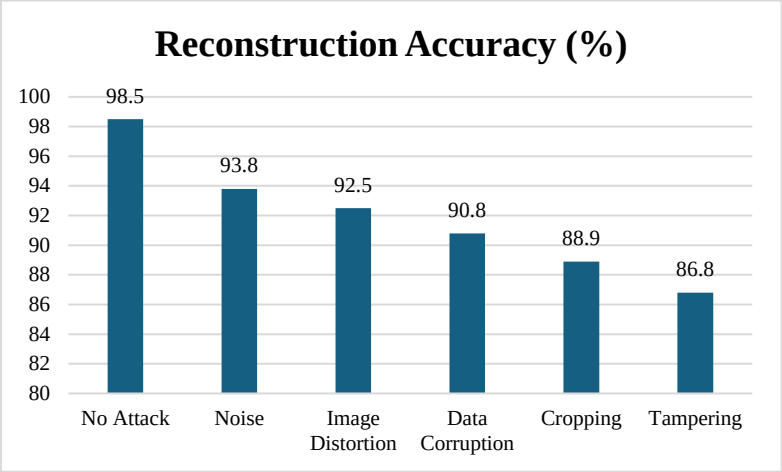

Figure 1: Reconstruction Accuracy under Different Digital Attacks

The rate of reconstruction success was 98.5% without any attack, 93.8% when noise attack was applied, 92.5% when image distortion was introduced, 90.8% when data corruption attack was implemented, 88.9% for cropping and 86.8% in case of tampering. It is evident that the reconstruction success decreases as the digital manipulation becomes stronger and tampering attack leads to the minimum success rate. Nevertheless, the system succeeded to reconstruct at least 86% of the objects in all cases under consideration.

4.4. Attack Recovery Performance

The following section will analyze the recovery ability of the suggested VSS based QR code protection technique from various attacks on the digital domain. Table 3 illustrates a

comparison between the recovery rates and performance degradation from noise, image manipulation, data manipulation, cropping, and tampering attacks.

Table 3: Attack Recovery Rate

Attack Type	Recovery Rate (%)	Performance Loss (%)
Noise	94.1	4.9
Image Distortion	92.8	6.2
Data Corruption	90.6	8.4
Cropping	88.5	10.5
Tampering	86.4	12.6

Recovery rates were 94.1%, 92.8%, 90.6%, 88.5%, and 86.4% for noise, image distortion, data corruption, cropping, and tampering, respectively. Performance degradation rates ranged between 4.9% and 12.6% with the lowest and highest rates being achieved by noise and tampering, respectively. The findings show that recovery rates are higher with less damaging attacks while performance rates decrease more significantly with cropping and tampering. Overall, recovery rates were above 86% for all attacks.

5. CONCLUSION

The study demonstrated that the suggested framework for QR based biometric template security using Visual Secret Sharing offered an effective method for protecting the facial biometric templates using distributed visual shares. Experimental results indicated that the performance of the system was very high in QR decoding, reconstruction, biometric authentication, and similarity both in original, protected and reconstructed situations. In case of any attacks including noise, image distortion, corruption, crop, and tamper, there was a gradual decrease in performance; however, the system achieved over 86% in reconstruction and recovery rate. It can be concluded that using QR code along with VSS offers security in the storage and reconstruction of biometric templates.

REFERENCES

1. *Ali, H. S., Elhefnawy, E. I., & Abo-Zahhad, M. (2024). Cancelable palmprint: intelligent framework toward secure and privacy-aware recognition system. EURASIP Journal on Information Security, 2024(1), 31.*

2. *Jiang, Q., Zhao, G., Ma, X., Li, M., Tian, Y., & Li, X. (2024). Cross-modal learning based flexible bimodal biometric authentication with template protection. IEEE Transactions on Information Forensics and Security, 19, 3593-3607.*
3. *Lee, J., Oh, B. S., & Toh, K. A. (2024). Extraction of intersecting palm-vein and palmprint features for cancellable identity verification. CAAI Transactions on Intelligence Technology, 9(1), 69-86.*
4. *Vallabhadas, D. K., Sandhya, M., Reddy, S. D., Satwika, D., & Prashanth, G. L. (2024). Biometric template protection based on a cancelable convolutional neural network over iris and fingerprint. Biomedical Signal Processing and Control, 91, 106006.*
5. *Zhao, G., Jiang, Q., Wang, D., Ma, X., & Li, X. (2023). Deep hashing based cancelable multi-biometric template protection. IEEE Transactions on Dependable and Secure Computing, 21(4), 3751-3767.*
6. *Ali, A., Migliorati, A., Bianchi, T., & Magli, E. (2024). Cancelable templates for secure face verification based on deep learning and random projections. EURASIP Journal on Information Security, 2024(1), 7.*
7. *Chen, H. B., Hsu, H. C., Huang, C. W., & Juan, J. S. T. (2024). An easy-to-implement construction for (k, n)-threshold progressive visual secret sharing schemes. Journal of Information Security and Applications, 83, 103757.*
8. *Fu, Z., Fang, L., Huang, H., & Yu, B. (2022). Distributed three-level QR codes based on visual cryptography scheme. Journal of Visual Communication and Image Representation, 87, 103567.*
9. *Rathgeb, C., Kolberg, J., Uhl, A., & Busch, C. (2023). Deep learning in the field of biometric template protection: An overview. arXiv preprint arXiv:2303.02715.*
10. *Valisireddy, J., Reddy, K. A., Elumalai, R., Mohan, L. N., & Anjaneyulu, G. S. G. N. (2023). Secured authentication of online documents using visual secret sharing on QR code. Journal of Integrated Science and Technology, 11(4), 568-568.*

******