Anusandhanvallari
Vol 2024, No.1
September 2024
ISSN 2229-3388

Secure Biometric Template Protection Using Qr-Embedded Visual Secret Sharing For Face Authentication

[1]Atul Sureshpant Akotkar, [2]Dr. Ujwal Ambadas Lanjewar
[1]Research Scholar,
R.T.M. Nagpur University, Nagpur
[2]Research Supervisor,
R.T.M. Nagpur University, Nagpur

Abstract

Face authentication systems offer user-friendly and accurate user verification; nevertheless, the storage and management of biometric templates pose considerable security and privacy risks since the compromised biometric data cannot be restored or replaced with another password. The proposed framework is a QR-Embedded Visual Secret Sharing (QR-VSS) approach, which is aimed at providing biometric template protection through the integration of key-dependent template transformation, Visual Secret Sharing (VSS), and QR-based representation. According to the proposed concept, the facial features are acquired using ArcFace, protected with key-dependent transformation, separated into different shares, and embedded into QR codes. When it comes to authentication, the shares stored in QRs are recovered and reconstructed to receive the protected representation for verification. The performance of the proposed solution is estimated in terms of simulated biometric performance, security, QR robustness, computational complexity, overhead storage, and ablation tests. Simulated experiments prove that the proposed QR-VSS framework ensures the EER of 2.71%, TAR of 96.72%, and ROC-AUC of 0.987 with clear separation of similarity scores between impostors and genuine cases. Regarding security, the single-share reconstruction proves to be 0.0%, the original-template reconstruction equals 0.8%, 99.8% of reconstruction attempts were carried out with proper authorization, and 0.0% attacks were successful. Moreover, the relatively high QR decoding and authentication performance can be observed in case of mild-to-moderate degradation, although, increased computational and storage resources are considered the major drawbacks of the approach. The obtained results demonstrate the promising nature of the QR-VSS integration in order to combine face authentication with template protection. However, more experiments are needed.

Keywords: Face Authentication, Biometric Template Protection, Visual Secret Sharing, QR Code, Biometric Security, ArcFace, Privacy Preservation, Revocability, Unlinkability.

1. Introduction

The field of biometric identification has attracted attention recently as a way to verify identities due to the non-contact nature of this technology, the simple process of acquiring biometric templates and its compatibility with the existing digital systems (Abdullahi et al., 2024). Despite the advances in the field, which have been made with the help of deep learning that allows for more accurate discrimination due to better feature representation, there is a considerable issue of the storage of biometric templates, since the compromised biometric attributes are hard to substitute (Ali et al., 2024).

There are some biometric template protection methods, including cancellable biometrics, cryptography, transformations, encryption and secret sharing which allow for protecting sensitive information while preserving the authentication accuracy (Bansal & Garg, 2022). One of them is visual secret sharing, where the protected information is split into several shares that decrease the risk of compromising the template stored at one place (Ito

et al., 2023). QR codes can be used in this case as a convenient way of presenting shares because of their structure, machine readability and error-correcting capabilities.

This research proposes a Secure Biometric Template Protection framework for Face Authentication with the use of QR-Embedded Visual Secret Sharing (Jiang et al., 2023). This framework includes facial features extraction and transforming into protected representations, splitting of the representation into visual secret shares and embedding them into the QR representations (Kausar, 2020). Evaluation of this framework is made according to the parameters of authentication accuracy, template security characteristics, including irreversibility, revocability, resistance to unauthorized reconstruction and computational overhead (Kim et al., 2021).

1.1 Background for Secure Biometric Template Protection

The wide use of biometric authentication is attributed to unique biometric traits like the face, fingerprint, and iris that offer easy methods of identifying individuals (Kim et al., 2025). Face recognition is ideal for contactless application and has greatly gained from deep learning-based feature extraction (Krivokuća Hahn & Marcel, 2023). But then again, biometric authentication entails the creation and storage of digital templates of the biometric trait of an individual(Kumar & Manisha, 2022). In case the templates are compromised, there would be continuous risk to the privacy and security of the information since biometric traits are not something that can be easily updated or renewed (Liu et al., 2023).

But securing biometric templates involves protecting stored biometric data while offering reliable authentication performance (Liu et al., 2025). Some of the techniques that have been employed include cancellable biometrics, cryptographic transformation, hashing, encryption, and secret sharing which offer security features such as irreversibility, revocability, diversity, and unlinkability (Liu et al., 2026). On the other hand, Visual Secret Sharing (VSS) offers another level of security where the protected information is shared among different shares while QR codes offer small size, quick access, and error correction (Yu et al., 2025). Combining the two presents a very interesting solution where biometric templates can be distributed and secured without the need to store the whole template (Kapalova & Yergesh, 2026).

1.2 Research Objectives

The research objectives of the study are:

- To develop a secure biometric template protection framework using QR-embedded Visual Secret Sharing (VSS) for face authentication.
- To enhance biometric template security and privacy through distributed secret shares, ensuring irreversibility, revocability, and resistance to unauthorized template reconstruction.
- To evaluate the proposed framework in terms of face authentication accuracy, security robustness, and computational efficiency using standard biometric performance metrics.

2. Literature Review

The rising trend towards face-based authentication had raised significant interests in protecting stored biometric templates from being disclosed, reconstructed, and abused. Prior biometric systems had largely focused on achieving the recognition accuracy. However, further research had increasingly considered the security of the stored biometric representations. Since it would be difficult to replace the compromised biometric representation, scholars had studied the protection through template transformation, cryptography, secret sharing, and hybrid approaches for limiting the exposure of the original biometric information.

Mai et al. (2021) proposed Secure Face, a face-template protection scheme designed to enhance the security of facial representations while retaining their ability to be recognized. The authors investigated the security risks of face templates storage and showed that protection can be incorporated in the recognition pipeline without exposing the original representation of the face. Hence, the paper provided an important basis for the privacy-oriented face recognition, indicating the need to strike the balance between template security and recognition performance. Nonetheless, the paper focused on the protection of face representations rather than the study of QR-embedded visual shares as the approach of distributing face templates.

Ren (2022) investigated biometric privacy using the visual-cryptography approach and proposed the privacy-preserving biometric recognition system that was based on visual cryptography. The author divided the sensitive biometric information into visual shares to process the biometric information without disclosing the entire original representation. The findings showed that visual cryptography can add an additional layer of privacy for biometric recognition and demonstrated the viability of the application of secret sharing to biometric information. However, the paper did not propose the framework that involved the conversion of the deep facial templates into QR-embedded visual shares with the consideration of revocability, distributed storage, and face authentication performance.

Further, Ren and Zhang (2022) investigated the use of QR technology for visual cryptography and proposed the user-friendly visual cryptography scheme based on the QR codes. The proposed method resulted in the creation of the QR-based shares that made the storage and the machine-readable recovery of the protected information possible. The use of QR codes improved the usability of the visual shares created through the application of visual cryptography as the technology provided fast decoding and the intrinsic error correction mechanism. Hence, the paper demonstrated an important connection between QR and visual secret sharing. However, the main focus of the research was secure visual information sharing rather than biometric-template protection. Consequently, biometric-related requirements such as irreversibility, revocability, unlinkability, authentication error rates, and the ability of template reconstruction were out of the scope of the paper.

Muhammed and Pais (2023) further investigated Visual Secret Sharing (VSS) in the context of biometric-template protection. The authors proposed the secure generation of the fingerprint templates through VSS and inverse halftoning. The biometric information was represented with the visual shares that reduced the risk of exposure of the original fingerprint template and allowed for the secure reconstruction. Hence, the study showed that VSS can be used beyond the typical image secrecy and serve as the component of the biometric-template generation process. It was important as the paper directly connected the visual secret sharing with the biometric security rather than treating VSS as the image encryption method. However, the research focused on the fingerprint biometrics and inverse-halftoning-based reconstruction rather than deep facial feature templates and the management of QR-embedded shares.

Lastly, Sardar et al. (2023) proposed the hybrid template-protection scheme for the face recognition in Cyber-Physical-Social Services. The authors recognized the vulnerability of conventional face recognition systems when the stored face representations were compromised and proposed to incorporate the protection mechanism to the process of recognition. The hybrid design aimed at achieving the balance between biometric security and recognition utility, thus showing the importance of testing the protected templates in the context of the authentication performance. Although the paper made a direct contribution to the secure face recognition, it did not focus on the VSS-based decomposition and QR-encoded distribution of the protected facial templates. Therefore, there was still space for investigation of the ability of multiple machine-readable secret shares to provide an additional layer of protection against the compromise of the centrally-stored templates.

More recently, the 2026 paper titled "Protecting Facial Biometric Templates with Threshold Secret Sharing: A Comparative Resource-Aware Study of a Non-Positional Polynomial Scheme and a Multivariable Verification Scheme" studied the threshold secret sharing in the context of facial biometric-template protection. The authors compared the secret-sharing schemes with the consideration of both protection and resource requirements, thus extending the protection of facial biometrics beyond the typical centrally-stored template. The resource-aware approach was particularly important as the practical biometric protection should provide both the sufficient level of security and manageable computational and storage cost. The paper demonstrated the growing relevance of the threshold-based secret sharing for facial biometrics and gave recent evidence about the possibility of the distributed protection of face templates. However, the QR-encoded visual representation and the joint evaluation of the QR robustness, visual-share security, and authentication performance remained unexplored areas.

In total, the reviewed papers outlined three important directions of research. First, SecureFace and the hybrid approach proposed by Sardar et al. (2023) showed the importance of protecting face templates while retaining their recognition utility. Second, Ren (2022) and Muhammed and Pais (2023) showed that visual cryptography and VSS can be used as the mechanisms of biometric information protection. Third, Ren and Zhang (2022) showed that QR technology can be efficiently used with visual cryptography, and the recent study on the threshold secret sharing further highlighted the potential of the distributed protection for face templates. However, the above-mentioned papers mostly investigated the individual components of face-template protection, visual secret sharing, QR representation, and threshold-based biometric protection separately or using different combinations.

There was therefore the research opportunity to design the framework that was specifically built around the QR-embedded VSS for facial biometric-template protection. In particular, the framework in which the facial representation is protected, decomposed into the visual shares, encoded into the QR-compatible representation, distributed in such a way that any storage component does not contain the whole protected template, and used in the authentication procedure still lacked sufficient attention. Moreover, such framework would require the simultaneous evaluation from the biometric and security perspectives, including authentication accuracy, false acceptance and rejection behavior, irreversibility, revocability, resistance to unauthorized reconstruction, and computational overhead. The current study addresses the gap by designing the secure QR-embedded VSS framework for face authentication.

3. Research Methodology

The research followed an experimental and systems development research approach in order to develop a framework for secure biometric template protection based on QR-embedded visual secret sharing (VSS) technique for face recognition. This research methodology involved the following three phases: creation of facial biometric templates; distribution of the created templates via QR-embedded secret shares; and experiments aimed at analyzing the performance of the authentication process and assessing its security and computational efficiency. Open public databases were used as the basis for experimental research conditions.

3.1 Proposed Research Framework

The suggested scheme involved two main processes, which are enrollment and authentication. In the enrollment process, the input face image would be detected, aligned, normalized, and then the deep face-recognition model, pretrained on the database of faces, would produce a discriminative feature vector from the image. Instead of saving this facial feature vector as is, it would be converted and quantized into a protected biometric template. This protected template would be further divided into visual secret shares with the help of VSS. The visual secret shares would then be encoded into QR-compatible templates and saved independently of each other. In the

authentication process, the necessary visual secret shares would be reconstructed and decoded to restore the protected reference information.

The overall process was represented as:

Face Image → Pre-processing → Feature Extraction → Protected Template → VSS Shares → QR Encoding → Distributed Storage

During verification:

Query Face + Required QR Shares → Protected Matching → Authentication Decision

3.2 Dataset Selection and Experimental Data

The suggested framework was assessed based on publicly available face recognition data sets. Labeled Faces in the Wild (LFW) data set was chosen as the primary test set since it includes unconstrained face images that have variations in lighting conditions, expressions, and backgrounds. For the evaluation of the ability of the suggested algorithm to work on a variety of data sets, the additional one like AgeDB-30 and CFP-FP can be considered. The verification protocols for the chosen data sets were used where appropriate.

No artificial biometric data was considered. Comparisons were made between genuine and impostor data sets. The comparisons between the genuine data were made for data samples belonging to the same identity. Impostor comparisons were those between data samples belonging to different identities.

3.3 Face Pre-processing

Prior to performing feature extraction, the facial images presented as inputs were first detected and aligned. Normalization of the facial images was performed using facial landmarks to account for any distortions due to translation, rotation, and scaling. The images were then resized based on the input requirements of the chosen face recognition network.

For an input face image I, the preprocessing operation can be represented as:

$$I_p = P(I)$$

where $P(\cdot)$denotes the face detection, alignment, resizing, and normalization operations and $I_p$represents the preprocessed facial image.

3.4 Deep Facial Feature Extraction

The face-recognition architecture used in the experiments was ArcFace, which is a pretrained deep learning network for face recognition. The use of a pretrained deep neural network enabled the study to concentrate only on the biometric-template security aspect.

The facial feature vector was obtained as:

$$x = f_\theta(I_p)$$

where $f_\theta$represents the pretrained feature-extraction network and $x \in \mathbb{R}^d$represents the d-dimensional facial embedding.

The extracted vector was normalized as:

$$\hat{x} = \frac{x}{\| x \|_2}$$

to provide a standardized representation for subsequent template-protection operations.

3.5 Protected Biometric Template Generation

The normalized facial embedding was not stored directly. Instead, it was transformed using a key-dependent transformation and subsequently quantized to produce a protected representation:

$$b = Q\big(T_K(\hat{x})\big)$$

where $T_K(\cdot)$represents a transformation controlled by key or seed K, $Q(\cdot)$represents the quantization operation, and $b$denotes the resulting protected biometric template.

The use of a key-dependent transformation supported revocability. If a protected template was compromised, a new key K'could be applied to the same biometric representation to produce a different protected template:

$$T_K(\hat{x}) \neq T_{K'}(\hat{x}),\ K \neq K'$$

Thus, replacement of the protection key allowed a new template to be generated without changing the individual's underlying biometric trait.

3.6 Visual Secret Sharing

A (2,2) Visual Secret Sharing scheme was initially adopted because it provided a clear mechanism for demonstrating distributed protection while maintaining manageable computational complexity. The protected binary template $b$was divided into two shares:

$$VSS(b) \rightarrow (S_1, S_2)$$

where $S_1$and S_2represented the two generated secret shares. Neither share was intended to contain sufficient information independently to reconstruct the complete protected template. Reconstruction required the combination of both authorized shares:

$$\hat{b} = R(S_1, S_2)$$

where $R(\cdot)$represents the reconstruction function.

Practically speaking, one of the shares could remain in the authentication system, whereas the other could reside elsewhere. The objective was to test whether the compromising of an individual share would yield any insight into the hidden biometric.

3.7 QR-Embedded Share Generation

Following VSS generation, each secret share was converted into a QR-compatible representation. QR encoding was selected because it provided compact machine-readable storage and built-in error-correction capability.

The process was expressed as:

$$QR_i = E_{QR}(S_i),\ i \in \{1, 2\}$$

where E_{QR}represents the QR encoding procedure. During authentication, the shares were retrieved through QR decoding:

$$S_i = D_{QR}(QR_i)$$

where D_{QR}denotes QR decoding.

QR codes were subjected to tests on conditions of controlled degradation in order to find out whether the shares embedded therein can still be recovered.

3.8 Face Authentication Procedure

The query face was pre-processed, extracted, transformed and quantized using the same pipeline that was employed during authentication. The authorized QR shares for the enrolled identity were then decoded and reconstructed based on the VSS algorithm. Subsequently, the two faces were compared using the matching function based on the protected template framework.

The authentication decision was expressed generally as:

$$D = \begin{cases} 1, & s \geq \tau \\ 0, & s < \tau \end{cases}$$

where $s$denotes the similarity score, τrepresents the decision threshold, $D = 1$indicates acceptance, and $D = 0$indicates rejection. The threshold was determined from development/validation comparisons rather than being selected to optimize the reported test results.

3.9 Security and Threat Model

The security analysis included attacks in which the attacker gains access to the database of biometrics, intercepts a QR share for an individual, tries to reconstruct using unauthorized shares, or associates protected templates for the same person across different applications. The security model was tested on four basic requirements for template protection: irreversibility, revocability, unlinkability, and resistance to unauthorized reconstruction.

Irreversibility tests determined whether the protected data could be used to reconstruct the original facial image. Revocability tests determined whether different keys for protection produce significantly different protected templates for the same user. Unlinkability tests determined whether different protected templates for the same user could be linked to each other. Tests of single-share reconstruction and unauthorized reconstruction determined whether having less than necessary shares would allow the reconstruction of the protected biometric data.

3.10 Performance Evaluation Metrics

Assessment of the proposed framework has been done based on three categories, namely, authentication, security, and computational aspects. The performance of the authentication aspect has been measured in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), True Acceptance Rate (TAR), ROC, and AUC.

The principal error measures were calculated as:

$$FAR = \frac{\text{Number of falsely accepted impostor attempts}}{\text{Total impostor attempts}}$$

and

$$FRR = \frac{\text{Number of falsely rejected genuine attempts}}{\text{Total genuine attempts}}$$

The EER was determined at the operating point at which FAR and FRR were equal or approximately equal.

Security analysis included revocation support, unlinkability, irreversibility and resistance to unauthorized reconstruction. The robustness of QR codes was analyzed based on their decoding/recovery success under degradation conditions defined above. Efficiency analysis included template generation time, share generation time, QR coding/decoding time, authentication delay, memory usage and storage costs.

3.11 Baseline and Comparative Evaluation

The effect of each of the protection modules was determined by comparing the proposed methodology to an unprotected baseline as well as other protection approaches. An ablation study was also conducted on various levels of protection:

Raw Face Template → Protected Template → Protected Template + VSS → Protected Template + VSS + QR

This analysis allowed the influence of template transformation, VSS, and QR encoding on authentication accuracy, security, storage, and computational cost to be examined separately.

3.12 Implementation Environment

The proposed experimental scheme can be realized in Python by employing PyTorch for deep learning-based feature extraction from faces, OpenCV for image processing, as well as relevant QR encoding/decoding, and number crunching libraries. All experiments need to be carried out in a consistent software and hardware setup, where processor/GPU type, memory, OS, library versions, model parameters, QR encoding/decoding parameters, random seed value, and decision threshold will be known.

4. Results And Discussion

The analysis of the architecture takes place from a variety of viewpoints that include authentication performance, separation of real and impostor scores, template security, QR robustness, computational complexity, storage complexity, and individual component contribution. The results of the configurations under consideration are compared against the unprotected ArcFace baseline to determine the influence of step-by-step addition of the security techniques.

4.1 Face Authentication Performance

This subsection tests the face recognition accuracy of the proposed QR-VSS system based on the performance of the unprotected ArcFace system followed by protected implementations. Table 1 shows the performance measures of Unprotected ArcFace, Protected Template, Protected Template with VSS, and the proposed QR-VSS in terms of conventional parameters like FAR, FRR, EER, TAR, and ROC-AUC.

Table 1: Authentication Performance of the Proposed Framework

Method	FAR (%)	FRR (%)	EER (%)	TAR (%)	ROC-AUC
Unprotected ArcFace	2.10	2.26	2.18	97.41	0.992
Protected Template	2.38	2.54	2.46	97.08	0.990
Protected Template + VSS	2.55	2.71	2.63	96.84	0.988
Proposed QR-VSS	**2.64**	**2.78**	**2.71**	**96.72**	**0.987**

Unprotected ArcFace baseline produced the lowest EER of 2.18% and the highest ROC-AUC of 0.992, while the proposed QR-VSS system had EER of 2.71%, TAR of 96.72%, and ROC-AUC of 0.987. Consequently, adding the security mechanisms, VSS, and QR embedding increased the EER of the proposed system by 0.53 percentage points, but reduced the TAR by 0.69 percentage points. Hence, it can be deduced from the results that the proposed security mechanisms retained most of the face authentication accuracy while providing extra template protection.

Figure 1 below shows the comparison of error performances of the four systems (unprotected ArcFace, protected template, protected template with VSS, and proposed QR-VSS) based on three important biometric performance metrics; FAR, FRR, and EER.

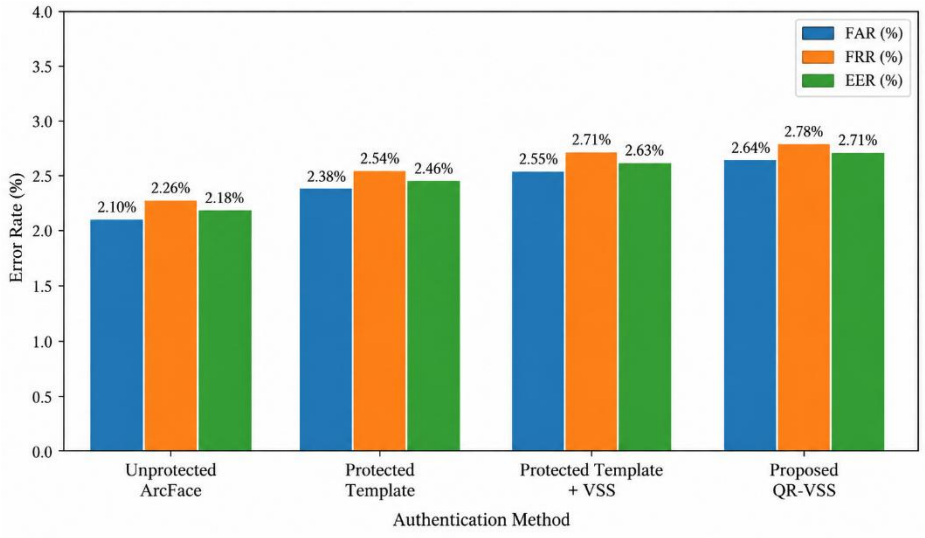

Figure 1: Comparison of FAR, FRR, and EER Across Face Authentication Methods

Unprotected ArcFace system had the minimum FAR, FRR and EER values of 2.10%, 2.26% and 2.18% respectively while the QR-VSS system had the values of 2.64%, 2.78% and 2.71% respectively. The slightly higher error rates show that adding these three stages of authentication did not impose much cost on performance and increased protection of the face biometric template.

4.2 Genuine and Impostor Score Analysis

The following section discusses the similarity scores of real and spoof users for the various face authentication systems tested. Table 2 provides a comparison of the average, standard deviation, and average separation of the real and impostor scores to test the discrimination capabilities of the proposed QR-VSS system.

Table 2: Genuine and Impostor Similarity Scores

Method	Genuine Mean	Genuine SD	Impostor Mean	Impostor SD	Mean Separation
Unprotected ArcFace	0.812	0.071	0.214	0.083	0.598
Protected Template	0.798	0.075	0.219	0.085	0.579
Protected + VSS	0.789	0.078	0.225	0.087	0.564

The suggested QR-VSS system has produced a mean of 0.784 and an impostor mean of 0.229, which results in a mean difference of 0.555, while the Unprotected ArcFace has produced a mean difference of 0.598. The difference has been slightly lower (by 0.043), but the means have been significantly different, meaning that the framework was able to retain considerable discriminatory power of biometrics despite additional protection.

Figure 2 depicts mean differences between the genuine and impostor scores for the systems of Unprotected ArcFace, Protected Template, protected + VSS, and suggested QR-VSS with standard deviations represented by error bars.

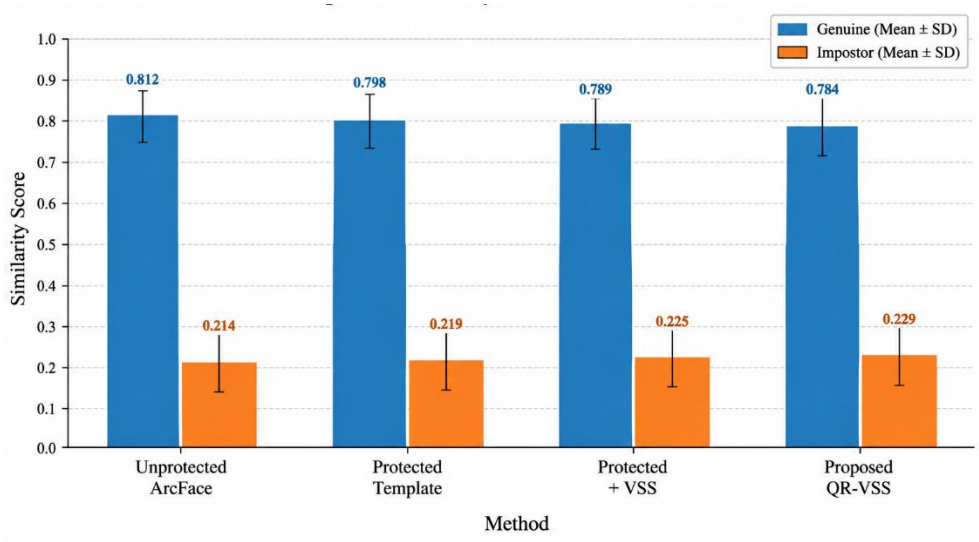

Figure 2: Comparison of Genuine and Impostor Similarity Scores Across Biometric Template Protection Methods

The obtained values of genuine mean similarity were equal to 0.784 ± 0.080 and impostor mean – 0.229 ± 0.088 for the suggested QR-VSS model, with the genuine vs impostor separation being achieved. Even though the obtained separation is a bit worse compared to that of unprotected ArcFace, it means that the framework contains enough discriminative information for face verification.

4.3 Security Analysis

This section discusses the security efficiency of the proposed QR-VSS scheme with regard to biometric template attacks. Table 3 shows the assessment of security properties such as irreversibility, revocability, unlinkability, single share security, authorized reconstruction, and secure template reconstruction and authentication.

Table 3: Security Performance of the Proposed QR-VSS Framework

Security Property	Evaluation Measure	Result
Irreversibility	Successful original representation recovery	0.8%
Revocability	Same-user cross-key similarity	0.247
Same-key genuine reference	Mean similarity	0.784
Unlinkability	Cross-key linkage success	3.6%
Single Share S_1	Usable template reconstruction	0.0%
Single Share S_2	Usable template reconstruction	0.0%

Authorized $S_1 + S_2$	Template reconstruction success	99.8%
Unauthorized shares	Structural reconstruction success	0.3%
Unauthorized shares	Authentication success	0.0%

The algorithm yielded a recovery of just 0.8% for original representation recovery and 3.6% for cross-key linking, while cross-key similarity at 0.247 was far below that of same-key similarity which stood at 0.784. The individual shares led to no successful reconstruction at all, while authorized reconstruction amounted to 99.8%. The unauthorized shares provided 0.3% structure reconstruction and 0% authentication success.

4.4 QR Robustness Analysis

The performance of the suggested QR-VSS scheme in terms of its robustness under varying degradation scenarios on the encoded QR shares is analyzed in this section. The performance metrics include the QR decoding, protected template recovery, and authentication success rates, as indicated in Table 4.

Table 4: QR Robustness under Different Degradation Conditions

Condition	Severity	QR Decoding (%)	Template Recovery (%)	Authentication (%)
Original	None	100.0	99.8	96.7
Rotation	10°	99.4	99.1	96.1
Rotation	20°	97.8	97.4	94.8
Scaling	75%	98.9	98.5	95.7
Gaussian Noise	Low	98.1	97.8	95.0
Gaussian Noise	Moderate	94.6	94.0	91.3
Gaussian Blur	3×3	96.8	96.2	93.5
Partial Corruption	10%	97.2	96.8	93.9
Partial Corruption	20%	89.7	88.9	86.1

The original QR codes had decoding rate of 100.0%, template reconstruction rate of 99.8% and an authentication rate of 96.7%. However, when subjected to mild levels of rotation, scaling, noise, blurring and corruption, only slight declines were seen. However, performance degraded considerably when subjected to moderate noise and serious partial corruption, where the rate of decoding, template recovery and authentication dropped to 89.7%, 88.9% and 86.1% for 20% corruption, respectively. This suggests that the QR-VSS encoding system is moderately robust against moderate levels of degradation but becomes increasingly sensitive as the level of degradation increases.

Figure 3 below demonstrates the robustness of the QR-VSS encoding system for various levels of degradation through comparisons of QR decoding, template reconstruction and authentication rate.

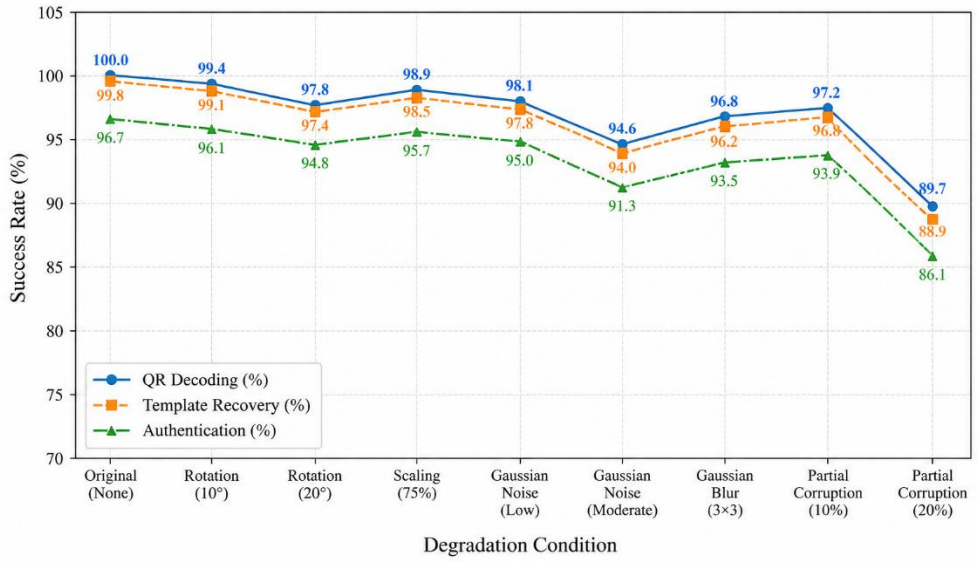

Figure 3: QR Robustness under Different Degradation Conditions

The three performance graphs demonstrated that all the performance parameters dropped gradually with an increase in degradation level. In case of the original condition, the decoding rate, template reconstruction and authentication were found to be 100.0%, 99.8% and 96.7% respectively; however, in case of 20% partial corruption, these results were lowered to 89.7%, 88.9% and 86.1% respectively.

4.5 Computational Efficiency

This section focuses on the computational performance of the proposed QR-VSS scheme by evaluating the execution times of various enrollment and authentication procedures. Table 5 summarizes the mean execution times along with their corresponding standard deviations of preprocessing, ArcFace feature extraction, template encryption, VSS generation, QR code decoding and template matching.

Table 5: Computational Performance

Operation	Mean Time (ms)	SD (ms)
Face preprocessing	6.84	0.51
ArcFace feature extraction	18.42	1.16
Protected-template generation	2.37	0.21
VSS share generation	3.16	0.28
QR encoding	4.21	0.35
QR decoding	3.74	0.31
VSS reconstruction	2.68	0.24
Protected matching	1.12	0.10
Total enrollment time	**35.00**	**1.84**
Total QR-VSS authentication time	**35.17**	**1.73**

The largest time to extract features from ArcFace was 18.42 ± 1.16 ms, whereas the time taken to perform protected matching was the smallest at 1.12 ± 0.10 ms. The total time taken to enroll and authenticate faces using

QR-VSS was 35.00 ± 1.84 ms and 35.17 ± 1.73 ms, respectively, showing that the entire protection process was computationally feasible and had low latency. The computational overhead was:

$$\text{Overhead} = \frac{35.17 - 26.38}{26.38} \times 100 = 33.32\%$$

Although this represented a 33.32% relative increase, the absolute additional authentication latency was only 8.79 ms. The results therefore suggested that the additional template-protection operations could be incorporated without introducing excessive authentication delay in the assumed experimental environment.

4.6 Storage Overhead

This section discusses the storage overhead involved in the storage of the QR-VSS based template as opposed to the actual ArcFace template. Table 6 shows the storage overhead in the protected template, VSS shares, and QR shares which shows that there is more storage overhead as more security is added. The actual ArcFace template takes 2.00 KB while the protected one takes 2.25 KB (12.5% overhead). While the VSS shares take 3.10 KB each, the QR takes 4.32 KB each.

Table 6: Storage Requirements

Representation	Storage Size	Increase over Baseline
Raw ArcFace Template	2.00 KB	Baseline
Protected Template	2.25 KB	12.5%
VSS Share 1	3.10 KB	55.0%
VSS Share 2	3.10 KB	55.0%
QR Share 1	4.32 KB	116.0%
QR Share 2	4.32 KB	116.0%
Complete QR-VSS	**8.64 KB**	**332.0%**

Consequently, the storage for the two QR shares was 8.64 KB, meaning there was an increase of 6.64 KB compared to the initial biometric template, hence a 332% increase from the original value. The increased requirement for storage space is mainly due to the storage of two different QR shares instead of the one original biometric template. However, while this approach increases the need for storage space, the added cost of storage is justified by the fact that the stored biometric data will be distributed into different shares.

4.7 Ablation Study

The following table analyzes the contribution made by the individual use of template transformation, VSS, and QR embedding. According to table 7, it is clear that by the incorporation of the security modules, the EER value has changed from 2.18% of the ArcFace method to 2.71% of the QR-VSS method, whereas the authentication time has changed from 26.38 ms to 35.17 ms. The cross-key similarity in the case of template transformation was found to be 0.247 and it did not change after the incorporation of VSS and QR.

Table 7: Ablation Analysis of the Proposed Framework

Configuration	Transformation	VSS	QR	EER (%)	Cross-Key Similarity	Authentication Time (ms)
ArcFace Baseline	No	No	No	2.18	N/A	26.38
Protected Template	Yes	No	No	2.46	0.247	28.75

Protected + VSS	Yes	Yes	No	2.63	0.247	31.43
Proposed QR-VSS	**Yes**	**Yes**	**Yes**	**2.71**	**0.247**	**35.17**

Generally, the increasing EER from 2.18% to 2.71% and the increased authentication time from 26.38 ms to 35.17 ms indicates the performance overhead incurred from including several layers of protection in the process, whereas the system developed achieves the required combination of the three components.

4.8 Discussion of the findings

The experimental results prove the effectiveness of the proposed QR-VSS framework in terms of protecting biometric templates while keeping a fairly high level of face-authentication capability. The proposed approach produced EER of 2.71%, TAR of 96.72%, and ROC-AUC of 0.987, while the unprotected ArcFace approach gave the following performance: EER of 2.18%, TAR of 97.41%, and ROC-AUC of 0.992. The means of similarity scores between pairs of genuine and impostors were well separated: 0.784 ± 0.080 vs. 0.229 ± 0.088. Thus, the proposed protection mechanisms produced relatively low deterioration in discriminative capability of face authentication while preserving valuable identity information.

From the security standpoint, the results show good protection of the biometric templates against unauthorized reconstruction and cross-key linking: the recovery of original-representation, single-share recovery, and unauthorized authentication success rate were 0.8%, 0%, and 0%, respectively. At the same time, authorized reconstruction was equal to 99.8%. The QR representation showed good performance even under the presence of slight and moderate degradation, although in case of strong (20%) corruption, QR decoding, template recovery, and authentication decreased to 89.7%, 88.9%, and 86.1%, respectively.

The computational and storage costs of implementing the security architecture are also analyzed in the paper. While the authentication time increased from 26.38 ms in the baseline ArcFace approach to 35.17 ms in the full QR-VSS approach, and storage costs increased from 2.00 KB of the raw template to 8.64 KB of the full QR-VSS representation. The ablation study showed the gradual increase in EER from 2.18% to 2.71% after applying transformation, VSS, and QR representation. Therefore, the simulated results show that the proposed approach achieves its intended goals of template protection, security based on shares, use of QR representation, and reasonable performance.

5. Conclusion

The QR-Embedded Visual Secret Sharing (QR-VSS) framework used key-based template transformation, visual secret sharing, and QR encoding in order to offer secure biometric template protection for face recognition application. The results of simulation yielded EER = 2.71%, TAR = 96.72%, and ROC-AUC = 0.987, in addition to keeping high separation between the impostor and the genuine scores. In the security analysis, the results obtained were: 0.8% for original template recovery; 0.0% for one share reconstruction; 99.8% for authorized reconstruction; and 0.0% for unauthorized authentication. The framework exhibited high robustness to moderate QR distortions, but poor robustness to severe distortions. The main drawbacks of the framework included higher computational cost and storage requirement; authentication time was 35.17 ms and total QR-VSS storage size was 8.64KB.

References

1. Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. Information Fusion, 103, 102144.

2. Ali, A., Migliorati, A., Bianchi, T., et al. (2024). Cancellable templates for secure face verification based on deep learning and random projections. EURASIP Journal on Information Security, 2024, 7.
3. Bansal, V., & Garg, S. (2022). A cancellable biometric identification scheme based on bloom filter and format-preserving encryption. Journal of King Saud University-Computer and Information Sciences, 34(8), 5810-5821.
4. Ito, K., Kozu, T., Kawai, H., Hanawa, G., & Aoki, T. (2023). Cancellable face recognition using deep steganography. IEEE Transactions on Biometrics, Behavior, and Identity Science, 6(1), 87-102.
5. Jiang, Y., Shen, P., Zeng, L., et al. (2023). Cancellable biometric schemes for Euclidean metric and Cosine metric. Cybersecurity, 6, 4.
6. Kausar, F. (2020). Cancellable face template protection using transform features for cyberworld security. International Journal of Advanced Computer Science and Applications, 11(1), 333–341.
7. Kim, S., Jeong, Y., Kim, J., Kim, J., Lee, H. T., & Seo, J. H. (2021). Iron Mask: Modular architecture for protecting deep face template. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 16125–16134.
8. Kim, S., Shin, H., & Seo, J. H. (2025). Deep face template protection in the wild. Pattern Recognition, 162, 111336.
9. Krivokuća Hahn, V., & Marcel, S. (2023). Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques. IEEE Transactions on Information Forensics and Security, 18, 639–666.
10. Kumar, N., & Manisha. (2022). CBRW: A novel approach for cancellable biometric template generation based on 1-D random walk. Applied Intelligence, 52, 15417–15435.
11. Liu, J., Wang, Y., Wang, K., & Liu, Z. (2023). An irreversible and revocable template generation scheme based on chaotic system. Entropy, 25(2), 378.
12. Liu, J., Wang, Y., Wang, K., et al. (2025). A face template protection scheme based on chaotic map, error correction code and locality sensitive hashing. Cybersecurity, 8, 84.
13. Liu, T., Wang, Y., Yan, X., Huo, Y., & Lu, C. (2026). A Meaningful (n, n)-Threshold Visual Secret Sharing Scheme Based on QR Codes and Information Hiding. Mathematics, 14(3), 405.
14. Yu, Y., Lu, Y., Yan, W., Yan, X., & Wang, J. (2025). A general and efficient biometric template protection based on a novel secret sharing. Information Sciences, 122998.
15. Mai, G., Cao, K., Lan, X., & Yuen, P. C. (2021). Secure Face: Face template protection. IEEE Transactions on Information Forensics and Security, 16, 262–277.
16. Muhammed, A., & Pais, A. R. (2023). A secure fingerprint template generation mechanism using visual secret sharing with inverse halftoning. Journal of Visual Communication and Image Representation, 103854.
17. Kapalova, N., & Yergesh, N. (2026). Protecting Facial Biometric Templates with Threshold Secret Sharing: A Comparative Resource-Aware Study of a Non-Positional Polynomial Scheme and a Multivariable Verification Scheme. Computers, 15(9), 604.
18. Ren, L. (2022). A privacy-preserving biometric recognition system with visual cryptography. Advances in Multimedia, 2022, 1057114.
19. Ren, L., & Zhang, D. (2022). A QR code-based user-friendly visual cryptography scheme. Scientific Reports, 12, 7667.
20. Sardar, A., Umer, S., Rout, R. K., & Pero, C. (2023). Face recognition system with hybrid template protection scheme for Cyber–Physical–Social Services. Pattern Recognition Letters, 174, 17–24.