International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(19s) 2026 pp. 117-127
https://doi.org/10.70917/ijcisim-2026-5004
Article

Stateless Geometric Watermarking for Replay-Resistant QR-Based Attendance Verification

Rami Khaleel Ahmed

Al-Bayan University, Baghdad, Iraq
Rami.khaleel@albayan.edu.iq

Abstract: QR codes are used in many educational institutions for attendance tracking. This is due to their low cost, rapid deployment, and compatibility with mobile devices. However, a drawback of using QR codes is their ease of resending. A student can take a picture of the code and send it to a friend, who can then use it without physically attending. This leads to problems with the accuracy of the attendance system. This study proposes a replay-resistant QR attendance framework that verifies both the decoded payload and the visual provenance of the submitted QR image. The method embeds a lightweight directional geometric watermark into perceptually stable QR modules using controlled one-pixel perturbations. A deterministic redundant mapping strategy derives embedding coordinates from the session context, enabling stateless server-side verification without storing image-specific templates or reference maps. The framework was implemented as a .NET microservice integrated with Flutter teacher and student applications and evaluated under authentic classroom capture, screenshot replay, WhatsApp forwarding, and Telegram forwarding scenarios using 100 heterogeneous smartphones and more than 1000 verification trials. Original captures achieved an average watermark matching rate of 0.94, while replay-oriented transmissions recorded lower rates due to degradation of embedded geometric signals resulting from re-compression, interpolation, scaling, and re-encoding. At an operational threshold of 0.75, the system achieved an accuracy of 96.30%, a false accept rate of 4.17%, and a false reject rate of 3.00%, with an area under the curve (AUC) of approximately 0.985. These results indicate that geometric watermarks can provide a practical and low-cost security layer for QR code-based attendance systems, without requiring specialized hardware, advanced forensic models, or reference databases for each image.
Keywords: QR code security, attendance verification, replay attack detection, geometric watermarking, stateless verification, mobile attendance systems

1. Introduction

QR codes have become common in digital services such as attendance registration, document validation, access control, and mobile authentication because they combine high data capacity, low deployment cost, and compatibility with ordinary smartphones [1,2]. In higher education, these properties make QR-based attendance attractive because instructors can display a session code and students can register attendance through a mobile scan without dedicated terminals.

Despite this convenience, QR-based attendance introduces a practical replay vulnerability. A legitimate classroom QR code can be photographed, captured as a screenshot, or forwarded to absent students through messaging applications while the encoded payload remains syntactically valid. Previous studies on QR authentication emphasize that QR-based channels can be implemented efficiently, but they remain sensitive to tampering, counterfeiting, and replay when verification is limited to the decoded content [2,3].

Current countermeasures, such as encrypted payloads, tokens, and dynamic QR code updating mechanisms, reduce the direct manipulation of the encrypted message. However, these measures do not prove that the presented image actually originated from a live classroom presentation. Therefore, QR code anti-counterfeiting research has now shifted toward visual authentication signals, copy detection patterns, and texture-based features that degrade after reprinting, recapturing, or reproducing [7,10]. However, many of these methods are designed for industrial printing and controlled acquisition rather than ordinary classroom screens and heterogeneous smartphones.

To address this gap, this study introduces a stateless geometric watermarking framework for replay-resistant QR attendance verification. Instead of relying only on payload validity, the proposed system embeds lightweight directional perturbations into perceptually stable QR modules and verifies whether these geometric cues survive the student camera capture. This places the contribution between QR attendance systems, anti-copy QR authentication, and mobile image-provenance verification.

The main contributions of this study are as follows. First, it designs a perceptual geometric watermarking method tailored to QR attendance rather than product packaging. Second, it uses deterministic redundant mapping so that the server can reconstruct candidate watermark positions without storing image-specific templates. Third, it integrates the method into a .NET microservice and Flutter-based attendance workflow. Fourth, it evaluates realistic replay scenarios, including screenshots and messaging-app forwarding, using watermark-similarity and authentication metrics.

Table 1. Comparison with representative QR security approaches.

Method	Replay resistance	Stateless verification	Mobile suitability
Encrypted payload	Partial	Yes	Yes
Dynamic QR	Partial	Yes	Yes
Print watermark	Yes	No	Limited
Texture QR	Yes	Often no	Limited
Proposed framework	Yes	Yes	Yes

2. Related Work

2.1 QR-based attendance and mobile authentication

QR-based attendance systems are usually introduced to reduce manual recording time, remove paper-based lists, and enable fast classroom or meeting registration. Earlier QR authentication studies showed that the visual QR channel is attractive because it can be read by ordinary mobile cameras and can support authentication or transaction verification without specialized hardware [2,3]. In attendance settings, later systems improved usability through dynamic codes, device identifiers, or mobile application workflows [4-6]. However, these studies mainly secure the payload or the application flow. They do not deeply verify whether the scanned QR image is a live classroom capture or a copied image redistributed through another channel.

2.2 Dynamic, encrypted and token-based QR protection

Dynamic QR codes and encrypted payloads are common defenses against simple reuse. They typically include time limits, nonces, session identifiers, signatures, or encrypted data fields. Such designs are useful against expired or modified tokens, but they remain only partial defenses against short-window replay. If an absent student receives a screenshot while the session is still valid, the payload may remain correct even though the visual source is fraudulent. This limitation motivates the need for an image-level authenticity signal in addition to cryptographic content validation.

2.3 Anti-counterfeiting QR codes and copy-detection patterns

A second research direction focuses on making QR symbols difficult to copy. Optical and anti-counterfeiting methods such as mQRCode, copy-proof barcoding, information-hiding detection, and texture-hidden QR codes exploit the fact that copying, scanning, and reprinting change fine visual details [7-10]. These studies demonstrate that QR symbols can carry authentication evidence beyond their decoded payload. Nevertheless, most of them assume printed tags, controlled capture settings, spectral/spatial channel models, or dedicated quality-assessment methods. Their operating assumptions differ from classroom attendance, where the QR code is displayed on a screen, captured by heterogeneous phones, and verified with low latency.

2.4 Deep learning and forensic approaches

Recent copy-forgery work has also used learning-based approaches. For example, DMF-Net models anti-counterfeiting QR copy forgery as a forensic classification problem and extracts multi-scale features for copy identification [11]. Similarly, the use of QR codes to verify image accuracy has been explored. This approach detects image noise in machine learning datasets. These methods have the advantage of being discriminative, but one problem is that they require training data, model maintenance, and significant computational resources. In a university environment like universities, we need a simple mechanism that does not depend on the state we are working in, and can be easily implemented via a back-end API. We do not need to train a new classifier for each different environment, so we can easily apply these methods.

2.5 Research gap and positioning of this work

The reviewed literature indicates three unresolved issues. First, QR attendance systems commonly address convenience and token validity rather than image provenance. Second, anti-copy QR research provides strong evidence for visual authentication but is often optimized for printed industrial tags rather than screen-to-camera classroom capture. Third, deep forensic solutions can be accurate but may increase deployment complexity. The present work addresses these limitations by embedding a deterministic, redundant, geometric watermark into stable QR modules and verifying it statelessly from the submitted camera frame. Table 2 summarizes the positioning of the proposed work against representative categories in the literature.

Table 2. Positioning of the proposed framework within representative QR security literature.

Research stream	Representative studies	Main contribution	Limitation for classroom attendance
QR mobile authentication	Sung et al. [2]; Chow et al. [3]	Mobile QR authentication and transaction verification	Focuses on authentication flow rather than copy-origin of the image
QR attendance systems	Hashim and Jasim [4]; Mukhtar et al. [5]; Annurrahma et al. [6]	Low-cost attendance recording using mobile QR scanning	Often payload-centric; vulnerable during the valid time window
Anti-copy QR/barcodes	Pan et al. [7]; Chen et al. [8]; Xie et al. [9]; Wang et al. [10]	Visual features that degrade after copying or recapture	Mostly designed for printed tags and controlled acquisition
Learning-based copy forensics	Guo et al. [11]	Multi-scale feature learning for copy forgery identification	Requires trained forensic models and suitable data
Proposed framework	This study	Stateless geometric watermarking for screen-to-camera QR attendance	Limited to tested display and capture conditions

3. Material and Methods

3.1 System architecture and operational workflow

The proposed system consists of four main entities. We use a teacher app, a student app, a back-end verification service, and an attendance database. For example, at the beginning of a lecture, the teacher app sends a request to the back-end system to obtain the session's QR code. The generated symbol includes the attendance payload and an embedded geometric watermark. The student application allows students to scan the shown code, which sends a camera frame to the backend for payload validation and watermark extraction. Fig. 1 shows the architecture and data flow of the system.

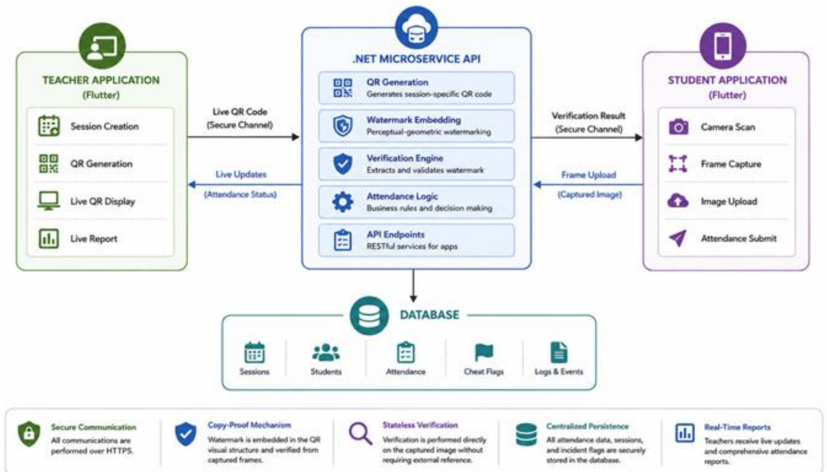

Fig. 1. Proposed attendance architecture integrating the .NET microservice API, teacher application, student application and verification database.

The entire workflow is a copy-proof verification sequence, not a payload-only sequence. First, the system prepares the attendance payload, then selects perceptually stable modules, embeds redundant geometric watermark bits and finally verifies the submitted frame by image-level analysis. The end-to-end workflow is summarized in Fig. 2.

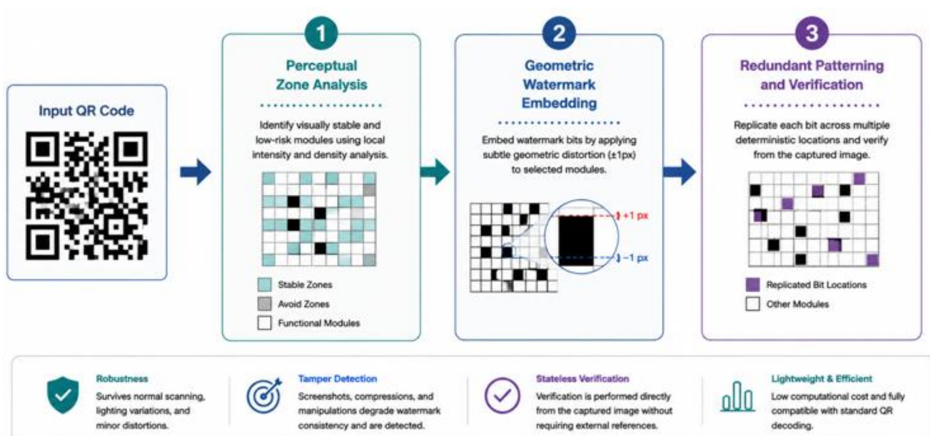

Fig. 2. Graphical abstract of the proposed copy-proof QR workflow, including perceptual-zone analysis, geometric embedding, redundant patterning and verification.

3.2 Threat model and security assumptions

The attacker is assumed to be an absent or unauthorized student with a normal smartphone and common messaging tools. Anticipated abuses include screenshot replay, forwarding via WhatsApp or Telegram, and redisplaying a captured QR image on another device. We do not assume that the attacker can compromise the backend service, the session generation process, the database, the cryptographic configuration or the watermark generator. A submission is accepted only if the decoded QR payload is valid and the recovered watermark similarity is above the operational threshold.

3.3 Perceptual-zone analysis

The embedding starts with the search for suitable stable QR domains that can be slightly modified geometrically. Let I(x,y) be the intensity of the grey level at location (x,y). The local mean and standard deviation are calculated for a local window (W) as follows:

$$\mu(x,y) = (1 / |W|)\ \Sigma_{(i,j)\in W}\ I(i,j)$$

$$\sigma(x,y) = \sqrt{[(1 / |W|)\ \Sigma_{(i,j)\in W}\ (I(i,j) - \mu(x,y))^2]}$$

We prefer regions with stable local structure, as small perturbations at the module level are less likely to destroy the QR decoding and more likely to be recovered after camera capture. This stage is based on simple local statistics rather than computationally intensive transformations, and as such, it is appropriate for real-time generation during attendance sessions.

3.4 Geometric watermark embedding and redundant mapping

Then, after region selection, the watermark message is transformed into a stream of bits. Each bit is encoded as a directional one-pixel perturbation of a selected QR module. A width extension encodes one binary state and a height extension encodes the other. This geometric principle is shown in Fig. 3.

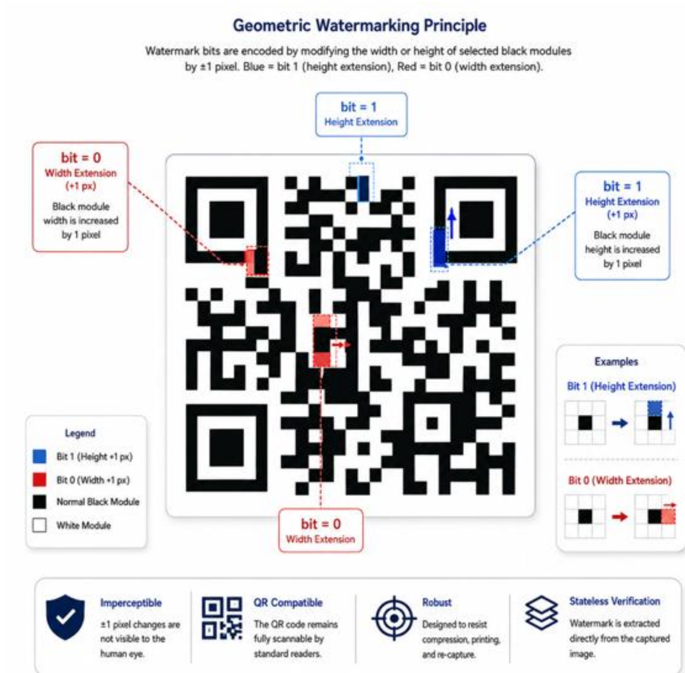

Fig. 3. Principle of geometric watermarking. Binary watermark states are represented by directional module perturbation.

$$M'_k = (w + 1, h), \text{ if } b_k = 0$$

$$M'_k = (w, h + 1), \text{ if } b_k = 1$$

The blurring is designed to be harmless to the image so as not to cause any problems. Because the data itself remains unchanged, the QR code still works perfectly with scanners. This visual cue is useful because the image can be decoded even if the embedded watermark quality is reduced after recapturing, re-swiping, re-compressing, or displaying it on a screen again.

To improve robustness, the watermark bits are repeated at deterministic positions based on the session context. In the implementation, we use redundancy $r = 3$. This design allows the verification to re-create the same candidate locations without the need to keep an embedding template for each image. The embedding sequence is described algorithmically in Algorithm 1 to reduce figure redundancy and emphasize the scientific procedure.

$$B_{rep} = \mathrm{Repeat}(B, r)$$

3.5 Stateless extraction and decision logic

During verification, the backend receives the submitted camera frame, performs preprocessing and geometric alignment, regenerates the candidate coordinates and samples each selected module. Directional pixel comparison is used to infer whether the observed deformation is closer to width or height extension. Replicated estimates are then combined by majority voting. The extraction and verification sequence is also formalized in Algorithm 1.

$$\hat{b}_i = \mathrm{Majority}(x_{i,1}, x_{i,2}, \ldots, x_{i,r})$$

The recovered watermark is compared with the original watermark using the Match Ratio (MR):

$$MR = (1 / N) \Sigma_{(i=1)}^{N} 1(\hat{b}_i = b_i)$$

Where N represents the number of watermark bits, b_i is the bit to be included, and $\hat{b}_i$ is the bit to be recovered. The 1(.) pointer function is used. If the watermark error ratio (MR) is greater than or equal to the threshold T, the request is accepted. Otherwise, it is considered suspicious and sent to the teacher for review.

3.6 Algorithm 1. Pseudocode of stateless geometric watermark embedding and verification.

```
Input: attendance payload P, session identifier S, secret key K, QR module matrix Q, redundancy factor r,
threshold T
Output: watermarked QR image Qw and verification decision D

Embedding phase (teacher/backend)
1: Generate QR module matrix Q from payload P.
2: Compute local statistics for candidate QR regions using a window W.
3: Select perceptually stable modules C that do not affect finder, timing, alignment, or format areas.
4: Derive a deterministic pseudo-random seed H = Hash(S || K).
5: Generate candidate embedding coordinates E from C using H.
6: Convert the watermark message into bitstream B and create B_rep = Repeat(B, r).
7: for each bit b_k in B_rep do
8:     Select coordinate e_k from E.
9:     if b_k = 0 then apply a one-pixel width perturbation to the selected module.
10:    else apply a one-pixel height perturbation to the selected module.
11: end for
12: Output the final watermarked QR image Qw.

Verification phase (student/backend)
13: Receive submitted camera frame F from the student application.
14: Decode and validate payload P, session S, timestamp, and student eligibility.
15: Preprocess F and align the detected QR region to the module grid.
16: Recompute C, H, and E using the same stateless deterministic rules.
17: for each replicated watermark position e_k do
18:     Sample local geometry and infer recovered bit x_k by directional comparison.
19: end for
20: Recover each watermark bit using majority voting: b_hat_i = Majority(x_i,1, ..., x_i,r).
```

21: Compute Match Ratio MR = (1/N) * sum Indicator(b_hat_i = b_i).
22: if MR >= T and payload validation is successful then D = Accepted.
23: else D = Suspicious and the submission is flagged for instructor review.
24: return D and MR.

3.7 Experimental setup and evaluation metrics

The framework was implemented as a .NET 7 microservice API integrated with Flutter teacher and student applications. The evaluation used 100 heterogeneous smartphones across Android and iOS platforms. More than 300 QR image samples were collected and expanded into more than 1000 verification trials. The tested scenarios were authentic live classroom capture, screenshot replay, WhatsApp forwarding and Telegram forwarding. Table 3 summarizes the implementation and evaluation configuration.

Table 3. Settings of implementation and evaluation.

Component	Configuration
Back-end architecture	.NET 7 microservice API
Mobile framework	Flutter teacher and student applications
QR generation library	QRCoder
Watermark strategy	Geometric directional perturbation with redundancy r = 3
Verification model	Stateless watermark extraction
Number of devices	100 smartphones
Experimental trials	More than 1000
QR image samples	More than 300
Supported platforms	Android and iOS

It was evaluated by using watermark-similarity and authentication metrics. Visual watermark recovery was measured in terms of MR. Operational verification behavior was measured by accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), precision, recall and F1-score.

4. Results and Discussion

The experimental results show a clear discrimination between genuine live captures and replay attacks. In authentic scans the geometric watermark was preserved with mean MR 0.94 and standard deviation 0.03. For screenshot replay, WhatsApp forwarding and Telegram forwarding, these mean MR values were 0.57, 0.53 and 0.56 respectively. Numerical Match Ratio results are reported in Table 4.

Table 4. Verification scenarios match ratio results.

Scenario	Mean MR	SD	Decision
Authentic live capture	0.94	0.03	Accepted
Screenshot replay	0.57	0.05	Suspicious
WhatsApp forwarding	0.53	0.06	Suspicious
Telegram forwarding	0.56	0.05	Suspicious

The same separation can also be observed at the distributional level. As shown in Fig. 4, real captures are clustered above the selected operational threshold whereas replay-oriented samples are located well below.

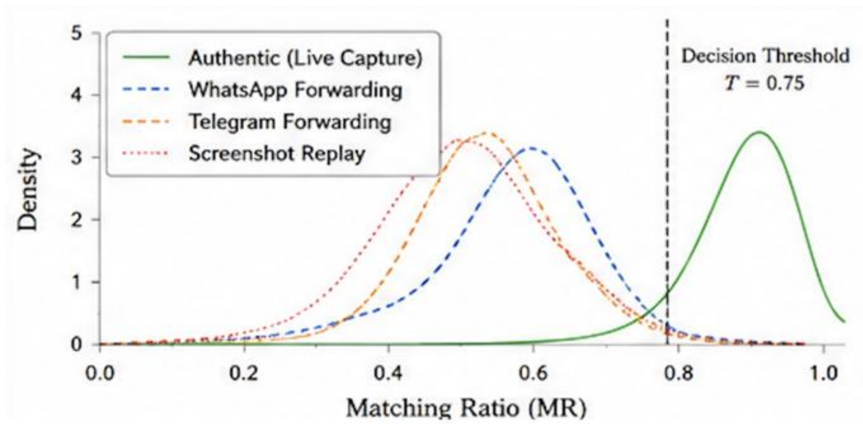

Fig. 4. Distribution of Match Ratio for real and replay-based verification scenarios. Dashed vertical line indicates the selected operational threshold T = 0.75.

The separation confirms the central premise of the framework. Messaging applications and screenshot workflows can preserve QR readability, but they alter fine geometric cues encoded in selected modules. Compression, scaling, interpolation, and re-rendering reduce the consistency of recovered watermark bits; therefore, replay-oriented submissions fall below the selected acceptance threshold.

For T = 0.75, the system achieved an overall accuracy of 96.30%. The FAR was 4.17%, which means that only a small fraction of the submissions aimed at replay was wrongly accepted. The FRR was 3.00%, indicating that authentic classroom scans would rarely be rejected given the conditions tested. As summarized in Table 5, the precision, recall and F1-score were 93.95%, 97.00% and 95.45% respectively.

Table 5. Authentication results at T = 0.75.

Metric	**Result**
Accuracy	96.30%
FAR	4.17%
FRR	3.00%
Precision	93.95%
Recall	97.00%
F1-score	95.45%

The receiver operating characteristic analysis supports the same conclusion. As shown in Fig. 5, the area under the curve of the framework was about 0.985, indicating high discrimination between genuine and replay-oriented submissions. The confusion matrix in Fig. 6 also shows that at the selected threshold most of the authentic captures and attack samples were correctly classified.

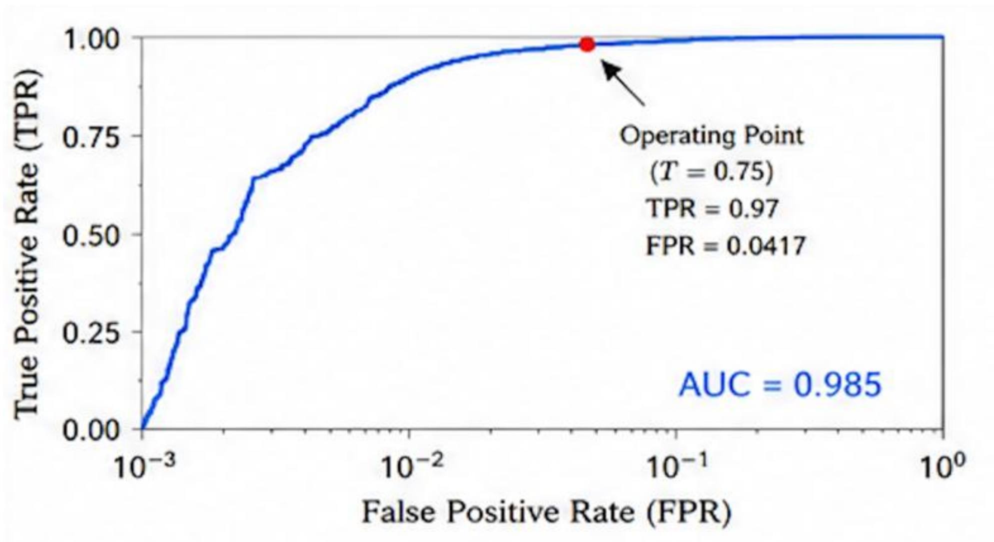

Fig. 5. Receiver operating characteristic curve of the proposed replay resistant QR verification framework at the selected operating threshold T=0.75.

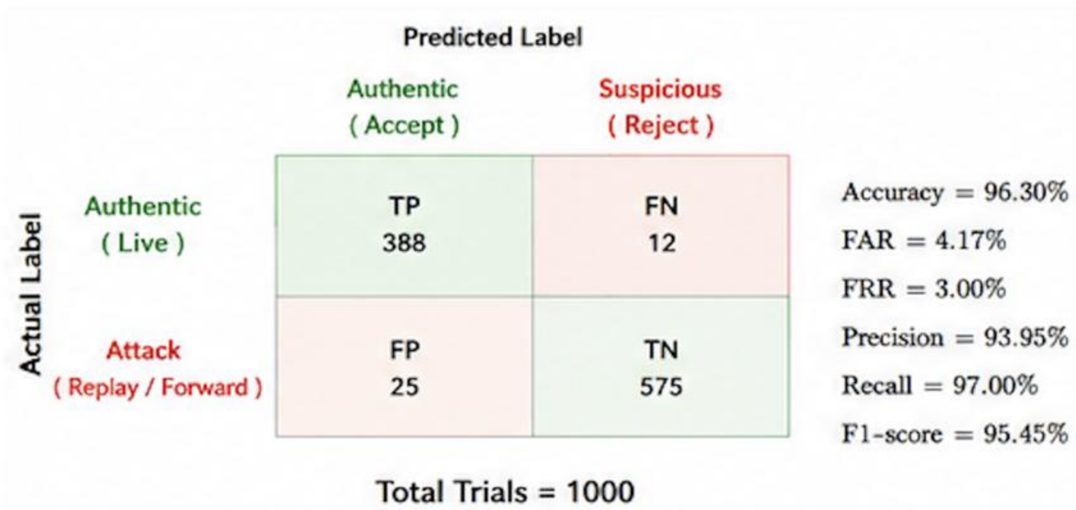

Fig. 6. Confusion matrix of the true positive, false negative, false positive and true negative classification outcome across verification trials.

The proposed approach provides an additional visual evidence layer compared to payload-only QR attendance systems. Replay attacks are possible during the validity of a traditional encrypted or time-limited QR token. On the other hand, the proposed framework tests whether the submitted frame contains the expected geometric watermark with sufficient strength. It is not a replacement for payload security but a complement to it, confirming the provenance of the image. Fig. 12 summarizes the workflow of classroom deployment, starting from QR generation to reporting of suspicious events.

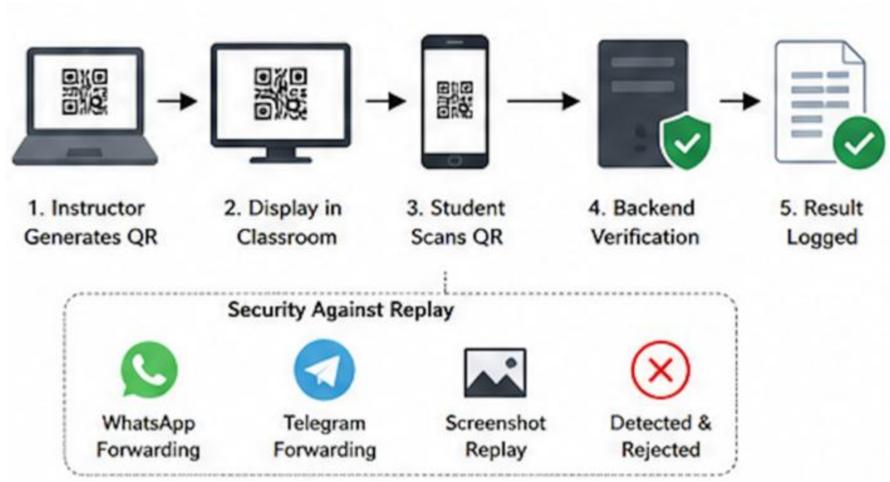

Fig. 7. Operational workflow in classroom attendance environment — QR generation, classroom display, student scanning, backend verification and replay-detection reporting.

This method is more useful for classroom use than many of the industrial anti-counterfeit methods. It does not need high resolution printing, external image templates, frequency domain transforms or deep forensic models. The local geometric analysis and deterministic mapping extraction stage is ready to be integrated in a real-time attendance service.

5. Limitations and Future Work

Although the proposed framework achieved strong discrimination under the tested scenarios, several limitations remain. The current implementation assumes moderate geometric alignment and may require stronger perspective correction for extremely oblique captures, low-light classrooms, or heavily blurred frames. In addition, the evaluation focused on smartphone-based replay through screenshots and messaging applications; future work should examine adversarial image restoration, screen-to-screen recapture at different refresh rates, and larger multi-institution deployments.

6. Conclusion

In this paper, we propose a QR attendance framework that is resistant to fraud based on perceptual geometric watermarking and stateless verification. The method embeds a lightweight directional watermark into visually stable QR modules, redundantly maps watermark bits via session-derived coordinates and reconstructs the watermark from the submitted camera frame at verification.

Results show that real classroom captures have high watermark consistency while replay-based submissions via screenshot forwarding and messaging platform redistribution lead to measurable degradation. The framework offers a workable compromise between fraud detection and usability with an accuracy of 96.30%, FAR of 4.17% and FRR of 3.00%.

This design is particularly relevant in education environments, as it enhances QR attendance integrity without the need for specialized hardware or computationally intensive image forensics. Future work should extend evaluation to larger institutions, more varied display conditions, print-and-rescan attacks, strong perspective distortion, and adaptive threshold calibration.

REFERENCES

1. International Organization for Standardization. ISO/IEC 18004:2015: Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification. Geneva: ISO; 2015.

2. Sung S, Lee J, Kim J, Mun J, Won D. Security analysis of mobile authentication using QR-codes. In: Computer Science & Information Technology - Computer Science Conference Proceedings. 2015;5:151-160. doi:10.5121/csit.2015.51612.
3. Chow YW, Susilo W, Yang G, Phillips JG, Pranata I, Barmawi AM. Authentication and transaction verification using QR codes. In: Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. 2010. p. 1-6.
4. Hashim MH, Jasim HA. An efficient student attendance scheme based on QR code and device identifier. 2023.
5. Mukhtar MAO, Sayed MH, Abdrahman OAO, Idres MIM, Baballa MYH. A proposed mobile-based and secured attendance recording system using Quick Response Codes. Journal of Applied Sciences Technology and Computing. 2024;1(2):1-12.
6. Annurrahma KD. Design of a meeting attendance system based on dynamic QR codes. Journal of Research and Innovation. 2025.
7. Pan H, Yang L, Chen YC, Xue G, You CW, Ji X. mQRCode: secure QR code using nonlinearity of spatial frequency in light. In: Proceedings of the 25th Annual International Conference on Mobile Computing and Networking (MobiCom). 2019. doi:10.1145/3300061.3345428.
8. Chen C, Li M, Ferreira A, Huang J, Cai R. A copy-proof scheme based on the spectral and spatial barcoding channel models. IEEE Transactions on Information Forensics and Security. 2020;15:1056-1071. doi:10.1109/TIFS.2019.2934861.
9. Xie N, Hu J, Chen J, Zhang Q, Chen C. Detection of information hiding at anti-copying 2D barcodes. IEEE Transactions on Circuits and Systems for Video Technology. 2022;32(1):437-450. doi:10.1109/TCSVT.2021.3059092.
10. Wang T, Zheng H, You C, Ju J. A texture-hidden anti-counterfeiting QR code and authentication method. Sensors. 2023;23(2):795. doi:10.3390/s23020795.
11. Guo Z, Zheng H, You C, Wang T, Liu C. DMF-Net: Dual-Branch Multi-Scale Feature Fusion Network for copy forgery identification of anti-counterfeiting QR code. arXiv. 2022. doi:10.48550/arXiv.2201.07583.
12. Chow YW, Susilo W, Wang J, Buckland R, Baek J, Kim J, Li N. Utilizing QR codes to verify the visual fidelity of image datasets for machine learning. Journal of Network and Computer Applications. 2021;173:102834. doi:10.1016/j.jnca.2020.102834.
13. Wang R, Li X, Zhang Y, et al. Enhancing QR code system security by verifying human scanners' identities. In: ACM Conference Proceedings. 2024. doi:10.1145/3643833.3656128.
14. Picard J, Landry P, Bolay M. Counterfeit detection with QR codes. In: Proceedings of the 21st ACM Symposium on Document Engineering (DocEng). 2021. doi:10.1145/3469096.3474924.
15. Nguyen HP, Retraint F, Morain-Nicolier F, Delahaies A. A watermarking technique to secure printed matrix barcode: application for anti-counterfeit packaging. IEEE Access. 2019;7:131839-131850. doi:10.1109/ACCESS.2019.2941484.
16. Xie R, Hong C, Zhu S, Tao D. Anti-counterfeiting digital watermarking algorithm for printed QR barcode. Neurocomputing. 2015;167:625-635. doi:10.1016/j.neucom.2015.04.026.