JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 11 Number 2 | December 2026: 269-278
DOI: 10.15575/join.v11i2.1796

Static QR Code Indonesian Standard Protection using Visual Cryptography

Aprianti Nanda Sari[1*], Siti Dwi Setiarini[2], Eddy Bambang Soewono[3], Muhammad Reivan Naufal Mufid[4], Yazid Fauzan Prasatria[5]
[1,2,3,4,5]Computer Engineering and Informatics Department, Bandung State Polytechnic, Indonesia

Article Info

Article history:

Received August 8, 2025
Revised December 14, 2025
Accepted December 14, 2025
Published September 17, 2026

Keywords:

digital payment
QRIS
QR Code
quishing
visual cryptography

ABSTRACT

The QR Code Indonesian Standard (QRIS) is widely used in digital payments across Indonesia, offering convenience but also introducing security risks such as quishing, QR code phishing, also known as quishing, attacks that redirect payments to fraudulent accounts. This study proposes a visual cryptography-based method to enhance the security of static QRIS. The proposed method employs a (2,2)-threshold visual cryptography scheme to split a static QRIS into two shares, held separately by the merchant and the customer, such that the original QR code can only be reconstructed when both shares are combined. A mobile-based prototype was implemented, incorporating fiducial marker detection, tilt correction, and image binarization to support accurate share reconstruction under real-world conditions. Experimental evaluation was conducted through 15 reconstruction trials using various smartphones and display conditions. The results show a reconstruction success rate of 80% (12 out of 15 trials), while 20% of attempts failed due to low camera resolution and complex background patterns that interfered with marker detection and binary conversion. Compared to existing QRIS security approaches that rely on dynamic QR codes or location-based verification, the proposed method offers a novel share-based protection mechanism specifically tailored to static QRIS. These findings indicate that visual cryptography can effectively mitigate quishing attacks on static QRIS, although its practical deployment remains dependent on environmental and device-related constraints.

Corresponding Author:

Aprianti Nanda Sari,
Computer Engineering and Informatics Department, Bandung State Polytechnic, Indonesia
Jl. Gegerkalong Hilir, Ciwaruga, Kec. Parongpong, Kabupaten Bandung Barat, Jawa Barat, Indonesia 40559
Email: aprianti.nanda@polban.ac.id

1. INTRODUCTION

QR Code, an abbreviation for Quick Response Code, is a two-dimensional barcode developed by the Japanese company Denso Wave [1], [2], [3], [4]. This technology is adapted as payment mechanism called as QR Code Indonesian Standard (QRIS) in Indonesia due to its ease of use and interoperability across payment service providers [5], [6], [7]. In particular, static QRIS is widely adopted by small and medium-sized merchants because it does not require additional electronic devices or real-time system integration.

Despite the advantages offered by QRIS, a range of fraudulent techniques persistently arises, aiming to exploit unsuspecting users. One such method is QR code phishing, commonly referred to as

p-ISSN: 2528-1682
e-ISSN: 2527-9165

quishing [8], [9]. This criminal activity employs QRIS to guide victims. In instances where customers execute payments, the funds are directed to the account of the fraudster rather than being allocated to the rightful business owner [10], [11], [12].

A limited number of technologies and studies have investigated this QRIS phishing case, specifically through the implementation of dynamic QRIS and the verification of the transaction location conducted. The Dynamic QRIS refers to a QRIS that is generated in real time during a transaction within the integrated application, leading to the creation of a distinct QR code for each individual transaction. Dynamic QR codes may be presented on receipts generated by Electronic Data Capture (EDC) machines or on the displays of kiosk monitors [13]. This solution requires the seller to have another device that supports dynamic QRIS.

In a study conducted by Ajhari, the Haversine formula was employed to determine the distance between the transaction location and the location registered by the merchant [14]. Should the distance of a transaction taking place at a specific location surpass a predetermined threshold, the buyer will receive a notification regarding the potential risk of quishing. Moreover, this study has not yet thoroughly examined the potential for detection errors manifested as false positives and false negatives, which may affect the reliability of the proposed quishing detection system. False positives may arise when legitimate transactions are misidentified as quishing. This can occur, for instance, if a merchant relocates or conducts business outside of its registered area, leading to a valid transaction being either blocked or marked as suspicious. In contrast, false negatives may arise when a quishing attack takes place in proximity to a legitimate merchant, leading to the system's failure to identify it as an anomaly and consequently processing the fraudulent transaction. The absence of comprehensive evaluation or analysis concerning these two risks indicates that the efficacy of the proposed location-verification-based detection method cannot be thoroughly appraised, thereby introducing the potential for detection failure in practical applications.

To the best of our knowledge, there is a lack of studies that specifically address the protection of static QRIS against quishing attacks using a share-based visual cryptography approach that does not depend on dynamic QR generation or location-based verification.

In relation to the previously mentioned investigation gap, the contributions of this study are listed as follows. This study presents a novel security mechanism based on visual cryptography to safeguard static QRIS. The approach involves dividing the QR code into two complementary shares, which are held separately by the merchant and the customer. This ensures that the original QR code can only be reconstructed when both shares are combined [15], [16]. A prototype based on mobile technology has been developed to implement this mechanism, utilizing fiducial marker detection and image preprocessing techniques to facilitate precise share alignment and reconstruction in real-world scanning conditions. In addition, an experimental evaluation is performed to illustrate the efficacy of the proposed approach, while also identifying significant practical limitations associated with camera resolution and the complexity of the environmental background.

2. METHOD

The proposed method consists of two main processes—share generation and secret reconstruction—both implemented using a (2,2)-threshold visual cryptography scheme. The subsequent sub-chapters provide a comprehensive overview of the processes involved in the two stages of the proposed method.

2.1 Share Generations

In the share generation stage, the static QRIS provided by the merchant is processed through text extraction, QR re-encoding, image binarization, and 2×2 subblock encoding to produce two complementary shares: a merchant share and a customer share. The merchant share is displayed either on a printed medium or on a screen, while the customer share is securely stored on the server. To support reliable reconstruction in real-world conditions, the merchant share is augmented with an ArUco fiducial marker to facilitate automated detection, orientation correction, and homography-based alignment[17], [18], [19]. This process is shown in Figure 1.

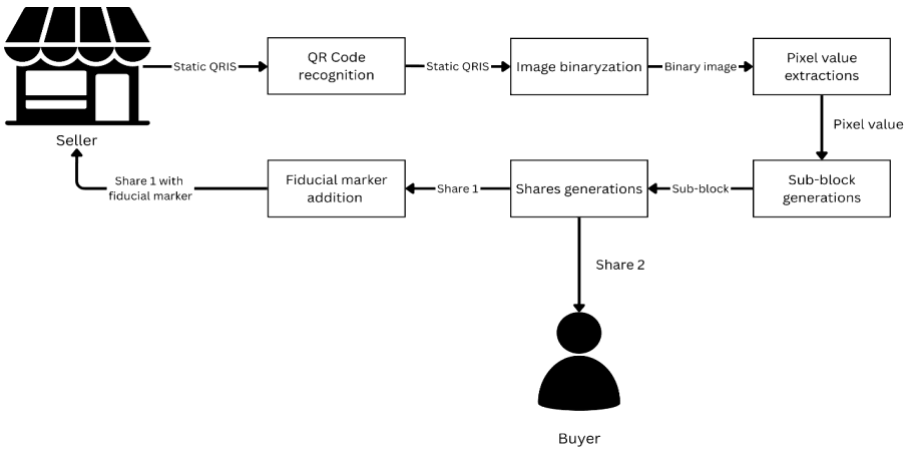


Figure 1. Share Generations Process

Here are the comprehensive steps and mathematical notations employed in the process of share creation. The notations employed in this procedure are presented in Table 1.

Table 1. Notations used

Notation	Definition
$D_{QR}(a)$	Function to extract information on QRIS a.
$E_{QR}(a)$	Function to convert string a to QR Code
$pix(x, y)$	Function to read pixel values at coordinates (x,y)
$random(x, y)$	Function to retrieve an element selected at random integer from the range x to y.

1. Instantiate six 2×2 matrices pat_i where $1 \leq i \leq 6$ as detailed below.

$$pat_1 = [1\ 0\ 0\ 1\ ], pat_2 = [0\ 1\ 1\ 0\ ], pat_3 = [1\ 0\ 1\ 0\ ],$$
$$pat_4 = [0\ 1\ 0\ 1\ ], pat_5 = [1\ 1\ 0\ 0\ ], pat_6 = [0\ 0\ 1\ 1\ ]$$

2. Verified seller have the privilege to submit static QRIS images a.
3. The system will detect what was provided QRIS and extract the informational text t according to the equation (1).

$$t = D_{QR}(a) \quad (1)$$

4. Transform t into a QR Code q according to the equation (2).

$$q = E_{QR}(t) \quad (2)$$

5. Instantiate a matrix S of dimensions $n \times n$, where n is the common size of a QR Code.
6. For each pixel in q, retrieve the pixel value. If the pixel value is 0 (black), assign 0 to the corresponding element in S. If the pixel value is 255 (white), assign a value of 1 to the element in S as per the equation (3).

$$S[i, j] = \{0\ pix(i, j) = 0\ \ 1\ pix(i, j) = 255 \quad (3)$$

7. Construct two matrices S_1 and S_2 of dimension $2n \times 2n$ that represent two shares.
8. For each $S[i, j]$, where $1 \leq i, j \leq \frac{n}{2}$, do:
    a. Select randomly integer k where $1 \leq k \leq 6$. The 2×2 subblock reffered as b_k is filled from the matrix patters pat_k initiated from the step number 1
    b. If $S[i][j] = 0$, or the pixel color is black, find its complement by using equation (4).

$$b'_k = \{pat_{k+1}\ if\ k\ mod\ 2 = 1\ \ pat_{k-1}\ if\ k\ mod\ 2 = 0 \tag{4}$$

c. If $S[i][j] = 1$, or the pixel color is white, find its complement by using equation (5).

$$b'_k = b_k = \ pat_k \tag{5}$$

d. Project the subblock into shares S_1 and S_2. For each element in a subblock dx, dy where $1 \leq dx, dy \leq 2$ the coordinates on the share are calculated based on equation (6)(7)(8)(9).

$$y = 2i + dy \tag{6}$$
$$x = 2j + dx \tag{7}$$
$$S_1[y][x] = \ b_k[dy][dx] \tag{8}$$
$$S_2[y][x] = \ b'_k[dy][dx] \tag{9}$$

9. Convert the two matrices, S_1 and S_2 into share images where the white pixel becomes transparent. Finally, distribute $S_1$to seller and S_2 to the costumer.

2.2 Secret reconstructions

The secret reconstruction process begins when the customer captures the merchant share using a mobile device. The system detects the ArUco marker (OpenCV dictionary DICT_4X4_50), corrects perspective distortion [17], [20], [21], extracts the share region, performs adaptive binarization, and overlays the captured share with the stored customer share to reconstruct the static QRIS. The resulting QR code is subsequently decoded to verify payment authenticity. This process is shown in Figure 2. This pipeline ensures that reconstruction is resilient against variations in angle, lighting, and display media.

Later to the generation of the two shares, denoted as S_1 and S_2, through the visual cryptography process, the subsequent phase involves the reconstruction procedure aimed at recovering the secret image that encompasses the static QRIS.

1. Both shares S_1 and S_2 are binary matrices of dimensions $2n \times 2n$, where n is the size of the secret. These matrices are partitioned into multiple sub-blocks, each measuring 2×2.
2. For each subblock, Determine the frequency of entries that have a value of 0 (black), denoted by f. Project onto $S[i][j]$, where $1 \leq i, j \leq n$ as per equation (10).

$$S[i][j] = \{0\ f = 4\ 1\ otherwise \tag{10}$$

3. Transform the S matrix into a QRIS image, subsequently extracting the information it contains.

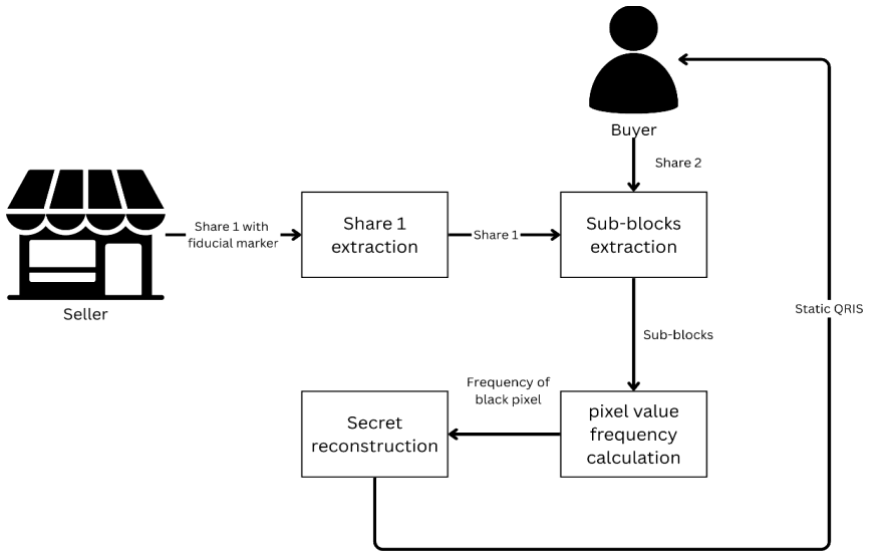


Figure 2. Secret reconstructions process

2.3 Experimental Setup

A mobile-based prototype has been designed and constructed to comply with the proposed method. In order to assess the functionality of the prototype, a total of 15 experiments were conducted. This study establishes a systematic experimental configuration that includes device specifications, shared dimensions, display media, and the technical parameters employed throughout the demonstration. Table 2 explains a transparent and quantifiable analysis of the experimental outcomes.

Table 2. Experimental configuration

Category	Configurations	Detail
smartphone	Operating system	Android
	Camera resolution	64 Megapixel
Seller's share	Display device	Laptop screen
	Physical display size	16.1 cm × 16.1 cm
	resolution	122 × 122 pixels
QRIS	QR code size	61 × 61 modules
ArUco marker parameters	Dictionary	OpenCV DICT_4X4_50
	Marker size	24 × 24 pixels
Enviromental conditions	Lighting	Indoor demonstration environment
	Background	Laptop screen with uniform color
	Capture angle	Various angle

3. RESULT AND DISCUSSION

Following the establishment of the static QRIS security method in the preceding chapter, the subsequent phase involves the development of a mobile-based prototype. To gain access to the system, both sellers and customers are required to authenticate their identities by entering a designated username and password.

In the course of the share generation phase, it is required upon the seller to upload a static QRIS image. Nevertheless, the procedure outlined in subsection 2.2. cannot be executed straightforwardly; therefore, an additional procedure is undertaken, specifically the incorporation of a fiducial marker. This pattern consists of a black-and-white square featuring a distinctive design that can be automatically identified and recognized by a computer through the application of computer vision techniques. The objective is to furnish information regarding the position and orientation of objects in the real world, in relation to the camera. In this study, the type of fiducial marker used was the ArUco marker. An illustration of the creation of two shares is presented as per Figure 3 and Figure 4.

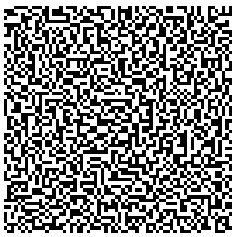


Figure 3. Costumer's Share

Figure 4. Seller's Share with Fiducial Marker

p-ISSN: 2528-1682
e-ISSN: 2527-9165

In a similar manner, the share reconstruction process requires the implementation of various digital image processing techniques to accurately extract the seller's shares. Figure *5* illustrates the techniques employed and describes as follows.

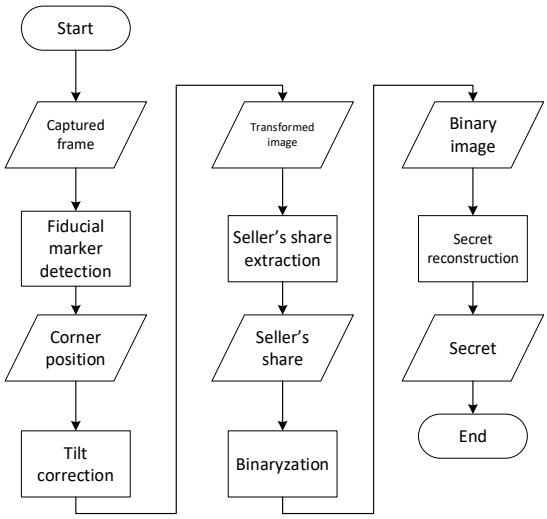


Figure 5. share reconstruction steps with various digital image processing

1. Utilizing a mobile phone camera, customers can capture images of the shares offered by sellers. Nonetheless, this process presents several challenges, including the acquisition of images at varying angles and distances, along with the geometric and flat distortions introduced by the image capture device as shown in Figure 6.

Figure 6. Original frame

2. The system will detect fiducial markers and perform tilt corrections. The result of this procedure is shown in Figure 7.

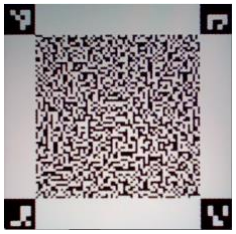


Figure 7. Tilt correction

3. Once the transformed image is oriented perpendicularly, proceed to extract the segment of the image that covers the seller's share as illustrated in Figure 8.

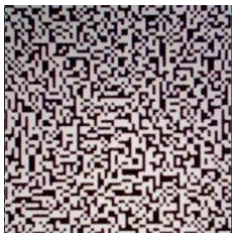


Figure 8. Share extraction

4. The images from the preceding stage are transformed into a binary format (as shown in Figure 9) to facilitate the execution of the secret reconstruction operation, as elaborated in sub-chapter 2.2. The initial QRIS, following the execution of the secret reconstruction method, is depicted in Figure 10.

Figure 9. Binaryzation

Figure 10. Secret reconstruction

4.1 Security Analysis

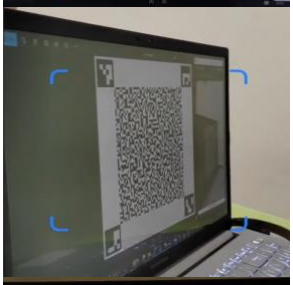
From a security perspective, the proposed visual cryptography–based scheme significantly enhances the protection of static QRIS against quishing attacks by eliminating reliance on a single visible QR code. Since the static QRIS is divided into two independent shares, neither the merchant share nor the customer share reveals any meaningful information when observed individually, preventing attackers from reconstructing or replacing the QR code without access to both components. This mechanism effectively mitigates common QR replacement attacks, as an adversary cannot generate a valid QRIS even if the merchant share is copied or photographed. Furthermore, the use of fiducial markers ensures that any unauthorized modification or substitution of the displayed share disrupts the reconstruction process, resulting in detection failure rather than fraudulent payment redirection. However, the security of the system remains dependent on the secure storage of the customer share and assumes that attackers cannot simultaneously compromise both shares. While the scheme does not address social engineering attacks that trick users into bypassing the verification process, it provides a strong cryptographic and visual barrier against QR code manipulation, offering a practical security improvement for static QRIS deployments.

4.2 Non-Technical Analysis

The experimental results indicate that the proposed visual cryptography approach successfully protects static QRIS from quishing attacks by requiring the combination of both the merchant's and the customer's shares to accurately reconstruct the authentic QR code. Nevertheless, the experiments also uncovered specific limitations that may influence the method's reliability in practical applications. In particular, three out of fifteen trials were unsuccessful as a result of the intricate background patterns present behind the seller’s share as shown in Table 3.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Table 3. Documentation of an unsuccessful trial

Cause	Documentation
Some areas on the share are covered/damaged	
Extreme capturing angles	
Low light environment	

Several reconstruction failures observed during the experiments were caused by unfavorable capture conditions, including partial occlusion of the QR share, excessively steep capturing angles, and low-light environments. Partial occlusion resulted in incomplete visibility of the QR share and ArUco markers, preventing accurate corner detection and leading to unreliable homography estimation. Extreme capturing angles introduced significant perspective distortion, compressing and skewing the QR modules and marker geometry, which destabilized the tilt-correction process and caused misalignment during share overlay. Low-light conditions further degraded performance by reducing image contrast and introducing sensor noise, making it difficult to distinguish true QR modules from shadow-induced dark pixels and weakening marker detection. The combined effects of occlusion, geometric distortion, and insufficient illumination caused early-stage failures in marker detection and alignment, ultimately preventing the successful reconstruction of the original QRIS.

4. CONCLUSION

This study has presented a visual cryptography–based approach to securing static QRIS against quishing attacks by splitting the QR code into two complementary shares held by the merchant and the customer. Experimental results demonstrate that the proposed system is capable of reconstructing and validating the original QRIS in 12 out of 15 trials, corresponding to a success rate of 80%, confirming its effectiveness in preventing QR replacement attacks when both shares are correctly captured. From a security standpoint, the share-based mechanism ensures that neither share reveals meaningful information on its own, thereby significantly reducing the risk of unauthorized QR manipulation.

Nevertheless, the evaluation also revealed several technical limitations that affect reconstruction reliability in real-world scenarios. Failures occurred primarily under adverse capture conditions, including partial occlusion of the displayed share, excessively steep camera angles, and low-light environments, which degraded fiducial marker detection, binarization, and homography estimation. These findings indicate that while the proposed method strengthens the security of static QRIS, its practical deployment requires controlled display conditions, adequate illumination, and near-perpendicular camera positioning.

Future work will focus on improving robustness by incorporating adaptive image preprocessing, more resilient marker detection techniques, and usability-oriented guidance to assist users during scanning. With these enhancements, visual cryptography has strong potential to serve as a practical and lightweight security layer for static QRIS without requiring additional merchant infrastructure.

ACKNOWLEDGEMENTS

This research was funded by Bandung State Polytechnic under contract number 109.16/R7/PE.01.03/2025.

REFERENCES

[1] I. Benito-Altamirano, D. Martínez-Carpena, H. Lizarzaburu-Aguilar, C. Fàbrega, and J. D. Prades, "Reading QR Codes on challenging surfaces using thin-plate splines," *Pattern Recognit Lett*, vol. 184, pp. 37–43, Aug. 2024, doi: 10.1016/j.patrec.2024.06.004.

[2] A. Kumari and K. K. Gaikwad, "Data carriers for real-time tracking and monitoring in smart, intelligent packaging applications: A technological review," *Next Materials*, vol. 8, p. 100591, Jul. 2025, doi: 10.1016/j.nxmate.2025.100591.

[3] A. N. Sari and T. G. Abdillah, "Metode Absensi Mahasiswa berbasis QR Code dan Time-Based One-Time Password," *Jurnal Informatika Polinema*, vol. 7, no. 2, pp. 29–34, 2021, doi: 10.33795/jip.v7i2.492.

[4] I. Das, D. Das, and C. QR, "QR Code and its effectiveness in Library services," *Library Philosophy and Practice (e-journal). Accessed on*, vol. 9, no. 10, p. 2022, 2021.

[5] K. Natsir, N. Bangun, M. B. Attan, and J. S. Landias, "PENGGUNAAN QRIS SEBAGAI ALAT PEMBAYARAN DIGITAL UNTUK MENINGKATKAN PRODUKTIVITAS UMKM," *Jurnal Serina Abdimas*, vol. 1, no. 3, pp. 1154–1163, Aug. 2023, doi: 10.24912/jsa.v1i3.26208.

[6] D. Prawitasari, F. D. Badiani, S. D. Rachmawati, F. P. Ningrum, and N. L. Mufidah, "QRIS in indonesia: a comprehensive literature review on adoption, challenges, and opportunities," *Revenue: Jurnal Manajemen Bisnis Islam*, vol. 5, no. 1, pp. 91–102, 2024.

[7] D. I. Saibil, F. Sodik, and A. A. Mardiah, "FAKTOR MEMPENGARUHI NIAT MENGGUNAKAN QRIS PADA SHARIA MOBILE BANKING SAAT PANDEMI COVID-19 (MODIFIKASI MODEL UTAUT 2)," *NISBAH: Jurnal Perbanka Syariah*, vol. 8, no. 2, pp. 75–92, Dec. 2022, doi: 10.30997/jn.v8i2.6353.

[8] G. A. Amoah and J. B. Hayfron-Acquah, "QR Code security: mitigating the issue of quishing (QR Code Phishing)," *Int J Comput Appl*, vol. 184, no. 33, pp. 34–39, 2022.

[9] L. J. L. Bekavac, S. Mayer, and J. Strecker, "QR-code integrity by design," in *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–9.

[10] G. Awuah Amoah, "QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)," 2022.

[11] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Phishing with Malicious QR Codes," in *Proceedings of the 2022 European Symposium on Usable Security*, New York, NY, USA: ACM, Sep. 2022, pp. 160–171. doi: 10.1145/3549015.3554172.

[12] G. A. Amoah and J. B. Hayfron-Acquah, "QR Code security: mitigating the issue of quishing (QR Code Phishing)," *Int J Comput Appl*, vol. 184, no. 33, pp. 34–39, 2022.

[13] InterActive QRIS, "QRIS Statis & Dinamis." Accessed: Jul. 16, 2025. [Online]. Available: https://qris.interactive.co.id/homepage/qris-why-choose-us-qris-statis-dan-dinamis.php?lang=id

[14] A. A. Ajhari, "Analisis Keamanan Sistem Pembayaran Digital Quick Response Code Indonesian Standard (QRIS)."

[15] C. Bhardwaj, H. Garg, and S. Shekhar, "An approach for securing QR code using cryptography and visual cryptography," in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, IEEE, 2022, pp. 284–288.

[16] S. Mittal, P. Kaur, and K. R. Ramkumar, "Achieving Privacy and Security Using QR-Code through Homomorphic Encryption and Steganography," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, Sep. 2021, pp. 1–6. doi: 10.1109/ICRITO51393.2021.9596265.

[17] A. van Putten, M. F. Giersberg, and T. B. Rodenburg, "Tracking laying hens with ArUco marker backpacks," *Smart Agricultural Technology*, vol. 10, p. 100703, Mar. 2025, doi: 10.1016/j.atech.2024.100703.

[18] M. Kalaitzakis, B. Cain, S. Carroll, A. Ambrosi, C. Whitehead, and N. Vitzilaios, "Fiducial markers for pose estimation: Overview, applications and experimental comparison of the artag, apriltag, aruco and stag markers," *J Intell Robot Syst*, vol. 101, no. 4, p. 71, 2021.

[19] T. Yuan, Y. Song, G. A. Kraan, and R. H. M. Goossens, "Identify finger rotation angles with ArUco markers and action cameras," *J Comput Inf Sci Eng*, vol. 22, no. 3, p. 031011, 2022.

[20] R. Berral-Soler, R. Muñoz-Salinas, R. Medina-Carnicer, and M. J. Marín-Jiménez, "DeepArUco++: Improved detection of square fiducial markers in challenging lighting conditions," *Image Vis Comput*, vol. 152, p. 105313, Dec. 2024, doi: 10.1016/j.imavis.2024.105313.
[21] T.-Y. Yang *et al.*, "Positioning of autonomous mobile robot using multi-lateration with pattern recognition and differential evolution," *Rob Auton Syst*, vol. 193, p. 105113, Nov. 2025, doi: 10.1016/j.robot.2025.105113.