International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

From Structure to Security: A Comprehensive Review of QR Code Technology, Vulnerabilities, and Applications

Kanishk Verma[1], Shreya Tanwar[2], Sarang Dhiman[3], Yatu Rani[4], Archana Kumar[5]

[1,2,3,4]Scholar, Department of AI-DS, ADGIPS, GGSIPU, Delhi
[5]Supervisor, Department of AI-DS, ADGIPS, GGSIPU, Delhi

Abstract
Quick Response (QR) codes are two-dimensional matrix symbols built from dark and light modules, the basic units that hold the encoded data, and any smartphone camera can read them within moments. In a few years they have moved from industrial labelling into everyday routines such as opening a restaurant menu or paying at a neighbourhood shop. Several intrinsic properties explain this uptake: Reed–Solomon error correction allows a symbol to be decoded even when part of it is damaged, dirty or hidden; omnidirectional scanning removes the need for careful alignment; and generation is inexpensive and open to anyone, which has encouraged use in marketing, education, healthcare and secure data exchange. The same openness, however, carries costs. A QR code can hold only a limited amount of data, cannot be read by a person, depends on external servers once it points to a URL, and offers no built-in way of proving who created it, which leaves it exposed to tampering, counterfeiting and quishing (QR phishing). This paper gives a structured overview of QR code technology. It describes the symbol structure and the encoding and decoding procedures, examines the main technical and security limitations, reviews protective measures based on machine learning, encryption, steganography and watermarking, and surveys applications in augmented reality, education, cashless payments and the Internet of Things.

Keywords: QR Codes, Quick Response Codes, Encoding and Decoding, Quishing, Steganography, Encryption

1. Introduction

A QR code, short for “Quick Response” code, is a two-dimensional matrix barcode intended to hold information and return it quickly to a reading device such as a smartphone. It was created in 1994 by Denso Wave, a Toyota subsidiary, to track components during automotive manufacturing, where the small capacity of conventional one-dimensional barcodes had become a bottleneck [8]; a traditional barcode, for comparison, holds only about twenty alphanumeric characters [1]. Use of the technology has since spread to commercial tracking, product labelling, advertising, entertainment, cashless payment and a broad range of mobile services, and the arrival of smartphones with built-in scanning has accelerated this trend [17]. A QR code system has two parts: an encoder, which converts input data into

a symbol, and a decoder, or scanner, which interprets the symbol and extracts the stored content. Because free online tools and mobile applications for generating and distributing custom codes are readily available, QR codes have become relevant to both personal and professional use [10][21].

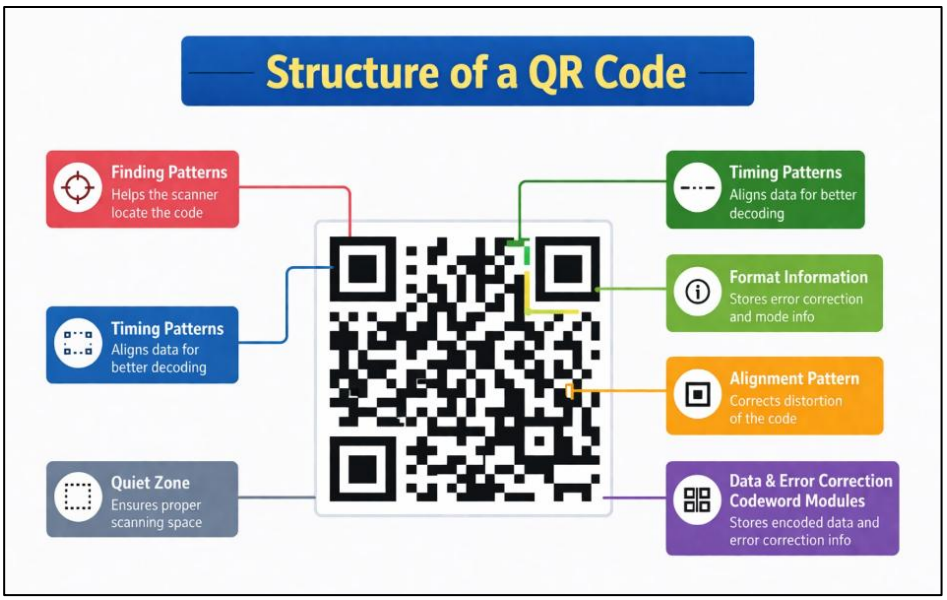


Fig. 1. Structure of a QR Code

QR codes can be grouped into several categories according to structure, capacity and purpose. The first two, QR Code Model 1 and Model 2, mark the early evolution of the standard. Model 1 holds up to 1,167 numeric characters in a symbol of at most 73 × 73 modules, whereas Model 2 adds alignment patterns that improve readability on distorted or curved surfaces and extends the capacity to 7,089 numeric characters in a grid of 177 × 177 modules. Micro QR Codes target applications where space is scarce and use a single position-detection pattern [1]. Logo QR Codes emphasise appearance and branding by blending colours, images and text into the symbol. The iQR Code is a flexible variant that supports both small and large payloads and can be produced in rectangular form or with inverted colours. The Secure QR Code (SQRC) differs from standard symbols in that it can hold public and private data together, and the Frame QR Code reserves a customisable area for visuals or text without affecting scannability [1][33]. Research variants have also been proposed, such as the nested QR code, in which two independent messages share one square image and can be read separately by slightly changing the scanning distance and angle with ordinary readers [9].

2. How a QR Code Works

A. Structure of a QR Code Symbol

A QR code symbol is a square grid of small modules (Fig. 1). The grid is divided into function patterns and an encoding region, and it is surrounded on all four sides by a blank border called the quiet zone, which allows the symbol to be separated from its background during scanning. The function patterns let a scanner find the symbol, orient it and interpret its layout: finder patterns detect position, separators set the finder patterns apart from the data, timing patterns provide the coordinate reference and alignment patterns compensate for distortion. The remainder of the symbol, the encoding region, holds the format and version information, the data codewords and the error correction codewords (Fig. 2), so that the

content can be recovered even if the symbol is partly damaged or deformed [1][9]. The six components are described below.

1. **Finder Pattern:** Finder patterns are position-detection markers located at three corners of the symbol: top-left, top-right and bottom-left. Each consists of nested squares, a 7×7 dark outer ring, a 5×5 light ring and a 3×3 dark centre, which yields a 1:1:3:1:1 ratio of dark and light modules along any line through its centre. This ratio is rare in ordinary imagery, so a scanner can locate the symbol quickly and determine its orientation before decoding begins.
2. **Encoding Region:** The encoding region carries the payload of the symbol: the data itself, the error correction codewords and the metadata that describes them. Reserved areas hold this metadata. Format information is stored in narrow strips one module wide next to the finder patterns, while version information (present in symbols of version 7 and above) occupies two blocks, a 6×3 block above the bottom-left finder pattern and a 3×6 block beside the top-right one. Fixing these positions allows a scanner to read the decoding parameters before it attempts to read the data.
3. **Separators:** Separators are strips of light modules, one module wide, that run along the inner sides of each finder pattern and mark a clear boundary between the finder patterns and the rest of the symbol. This isolation prevents data modules from being mistaken for part of a position marker and improves decoding accuracy.
4. **Timing Patterns:** Two timing patterns, one horizontal and one vertical, consist of alternating dark and light modules. They run along the sixth row and the sixth column respectively, between the separators. Together they form a reference grid from which the scanner derives module spacing and alignment, and they also help it establish the size and version of the symbol.
5. **Alignment Pattern:** Alignment patterns are small reference markers made of concentric squares: a dark 5×5 outer ring, a light 3×3 ring and a single dark module at the centre. Their function is to correct geometric distortion, which arises mainly when a code is photographed at an angle or printed on an uneven surface. They are present from version 2 onward, and their number grows with the version so that larger symbols remain decodable.

S No.	Error-Correction Level	Approximate Amount of Correction
1.	L	7%
2.	M	15%
3.	Q	25%
4.	H	30%

Fig. 2. Error Correction Levels

6. **Quiet Zone:** The quiet zone is an empty margin around the symbol, normally four modules wide, that contains no data. It acts as a buffer so that surrounding text, images or markings are not confused with the code. Without it a scanner may be unable to tell where the symbol starts and ends, which leads to misreads or failed scans.

B. Encoding Procedure

Generating a QR code is a sequence of well-defined steps that balance storage efficiency against reliable decoding. The process starts with data analysis: the input, for instance text or a URL, is examined to select the most suitable encoding mode (numeric, alphanumeric, byte or Kanji), so that the data is

represented in as few bits as possible. The data is then converted to a bit stream and divided into 8-bit codewords, preceded by a mode indicator and a character count indicator whose length depends on the version. Next, Reed–Solomon error correction is applied, producing extra codewords that make it possible to detect and repair errors caused by damage, dirt or partial occlusion. Four error correction levels are available (L, M, Q and H), restoring roughly 7%, 15%, 25% and 30% of the codewords respectively (Fig. 2); a higher level improves resilience but leaves less room for data [14]. The data and error correction codewords are combined into a final message, with padding added where needed to fill the capacity of the chosen version. The message is then placed in the module matrix in a predefined zig-zag order. A mask pattern, chosen from several predefined options, is applied to avoid visually ambiguous arrangements and so improve scanner readability. Finally, the format and version information, which records the error correction level and the mask used, is written into its reserved regions. The outcome is a complete symbol that can be printed or displayed and scanned reliably under varied real-world conditions [1].

C. Decoding Procedure

Decoding reverses the generation steps in a systematic order. The scanner first captures an image of the symbol and classifies each region as a dark or a light module, which gives a binary representation. The finder and alignment patterns are used to locate the symbol and correct its orientation and perspective. The format information is then read to obtain the error correction level and the mask pattern, and the version information is read to determine the size and data capacity of the symbol, so that its layout can be interpreted correctly. Once the mask has been identified it is removed, normally through an XOR operation, which restores the original bit stream. This stream is split into data codewords and error correction codewords, which are reassembled in their original order, and Reed–Solomon decoding detects and corrects errors so that the message survives distortion or partial damage. Finally, the corrected data is converted back to its original form, such as text or a URL, according to the mode indicator and the character count, and is presented to the user.

3. Challenges and Limitations of QR Codes

Despite its many benefits, QR code technology faces challenges that limit its effectiveness in practice, and these are technical as well as related to security and user behaviour. Codes can easily be copied, altered or replaced, which makes them open to tampering and counterfeiting. Reading performance depends on scanning conditions, so poor lighting, physical damage or low-quality printing can make a symbol unreadable. Users also differ in their familiarity with the technology, which can lead to confusion or careless use. As QR codes spread into IoT systems, supply chains and digital payments, secure data handling and smooth integration across platforms and devices become more important and harder to achieve. A further concern is that the ability of a code to store and redirect information can be abused: attackers may embed links to phishing sites, malware downloads or other unsafe content, frequently without the user noticing. A systematic review of QR phishing detection, covering 44 studies from 2015 to 2025, reports that the field is still held back by the lack of large standardised datasets, limited computing resources, adversarial manipulation, and weak model interpretability and user trust [13]. Overcoming these challenges calls for better security measures, greater user awareness and more dependable system design, which together would make QR code technology safer and more trustworthy across its many applications.

A. Limited Data Capacity

A QR code can hold only a limited amount of data, in the order of a few kilobytes. At the largest size, version 40, with the lowest error correction level, the standard allows 7,089 numeric characters, 4,296 alphanumeric characters, 2,953 bytes of binary data or 1,817 Kanji characters [14]. These figures may be inadequate for complex or data-intensive uses, and they shrink further as the error correction level is raised, because more of the symbol is reserved for redundancy. In practice, most deployed codes therefore store a URL that points to content on an external server instead of the content itself. This extends what a code can deliver but introduces a dependence on network connectivity and remote infrastructure: if the network is unavailable or slow, or if the linked content is changed or removed, the code may fail to deliver the intended information [4]. The reliance on external links also raises questions of security, data integrity and long-term reliability, since the user has no control over the hosted resource. Limited capacity therefore remains a significant constraint wherever secure, offline access or the direct storage of larger volumes of information is required [10].

B. Security Vulnerabilities

QR codes are inherently exposed to security threats because they have no built-in mechanism for authentication or verification. An attacker can therefore replace a genuine code, or place a fake one over it, in public locations such as posters, payment stands and advertisements [20]. Anyone who scans the altered code may be redirected to a malicious website, exposed to malware, or induced to authorise a fraudulent payment. Since a QR code cannot be read by a person, its content cannot be checked before the scan [2][37]. The weakness is not limited to the codes themselves: an analysis of 100 barcode scanner applications found that some check URLs or use cryptography, while others offer weaker protection than they claim [10]. A widespread attack is quishing (QR phishing), in which fake codes are used to deceive users [7][13]. Such codes lead to fraudulent websites that closely imitate genuine ones, and the victim may be asked for passwords, personal details or banking credentials, which are then stolen and misused. Scanning a malicious code may also start an automatic download of harmful software [18]. Empirical evidence shows that the threat is real: in a real-world phishing campaign at a research campus, a professionally designed QR poster that offered a voucher led 25 of the 30 participants who entered an e-mail address to do so, against five for a plain version, even though fewer than one per cent of potential participants responded overall [18]. Attackers are also adopting generative AI: a recent proof of concept combines quishing with a browser-in-the-browser attack in which a large language model produces the deceptive pop-up content in real time [2]. As QR codes enter critical applications such as digital payments, authentication, ticketing and IoT, the consequences of these threats grow more serious. Stronger measures, including encryption, secure code generation and verification mechanisms, are therefore needed, together with user awareness and cautious scanning habits.

C. QR Code Tampering

Unlike a written link, a QR code cannot be read directly by a person, and its content cannot be verified without scanning it. Users are thus forced to rely on trust and may scan a code without knowing its true purpose. Tampering, in which a genuine code is modified or substituted by a malicious one, is a major concern, and in retail settings it appears as barcode substitution fraud [8]. Counterfeiting is related but distinct: it involves producing fake codes that closely resemble authentic ones so that users cannot tell them apart [12][32]. Counterfeit goods are reported to account for about 3.3% of world trade [12], and printable graphical codes have been shown to be clonable [32]. The ease with which codes can be

generated with free online tools makes convincing replicas cheap to produce, and attackers often make them look as if they belong to trusted organisations such as banks, payment providers or well-known brands. A common real-world tactic is physical replacement, where counterfeit QR stickers are fixed over the original codes on payment boards, posters, packaging or restaurant menus, so that victims are sent to malicious destinations without noticing [10]. Because a code often triggers a redirect or an action automatically, a single scan can result in phishing, financial fraud or data theft, and the absence of visible indicators makes early detection difficult. Encrypted or dynamic QR codes [2], together with checks on the source before scanning, are therefore recommended to lower the risks of tampering and counterfeiting [5][16].

4. Securing QR Codes

Since QR codes are widely used to carry important information, protecting that information has become essential. A standard QR code has no protection of its own, so anyone with a scanner can read its content. Encryption addresses this by transforming the data into an unreadable form with a chosen algorithm before the code is generated; after scanning, the original content is recovered with the correct key or procedure [6]. Secure systems can also combine encryption with digital watermarking to guard sensitive data against unauthorised access while preserving reliable retrieval and usability, as in a medical-privacy application that pairs GAN-based robust watermarking with AES encryption [11]. Together these measures protect sensitive information and prevent its misuse. Several families of solutions to QR code security problems are outlined below.

A. Machine Learning-Based Detection

Current research places strong emphasis on detection systems based on machine learning, which can recognise malicious QR codes from patterns in their structure or content. Such models adapt better than rule-based or blacklist methods to new threats, including quishing and attacks assisted by AI [15][22]. Two broad approaches can be distinguished. Content-based methods extract the embedded URL and classify it: QR Shield combines Random Forest and XGBoost classifiers and reaches an accuracy of 96.8% in detecting malicious URLs [19], and earlier work applied Naive Bayes and logistic regression to the words of the URL [7]. Their drawback is that the payload has to be decoded first, which can expose the user to the malicious content. Image-based methods analyse the symbol itself. Trad and Chehab classify QR codes from their structure and pixel patterns without reading the payload, obtaining an AUC of about 0.91 with XGBoost [15]; QRiS derives 24 transparent structural features from the layout, uses 400,000 generated samples, and reaches an accuracy of up to 83.18% [5]; and a lightweight deep learning model separates normal, phishing and malware codes with about 99% overall accuracy, although its recall for malware is lower [16]. Together these results indicate that combining structural analysis with ML models improves detection accuracy and real-world usability [15][22]. Open problems remain, notably the shortage of large standardised datasets and the limited interpretability of black-box models [13].

B. Encryption for Data Protection

Encryption methods such as the Advanced Encryption Standard (AES) protect the data stored in a QR code by converting readable information into ciphertext [3]. The ciphertext appears as a random sequence of characters and cannot be interpreted without the correct key, so a person who scans the code without authorisation obtains only meaningless data. Encryption thus works as a digital lock that only holders of the key can open, which is valuable in online payments, login systems and the exchange of

private data. Security can be strengthened further through multi-layer encryption, in which data is encrypted more than once with different methods or keys, much like locking a box inside another locked box: an attacker who defeats one layer still faces the others. A recent dual-layer scheme illustrates the idea. It encrypts an image with a chaotic variant of AES, protects the session key with a static key, and distributes both keys through a steganographically modified QR code, reaching near-ideal entropy (about 7.997) and an NPCR above 99.6%, which indicates strong resistance to differential attacks [3]. A related approach combines a QR code with GAN-based watermarking and AES to keep patient data private in a medical device [11]. As a result of such developments, QR codes are becoming more dependable carriers of sensitive information, and the risk of data theft or misuse is reduced.

C. Steganography for Concealed Protection

Steganography, literally "concealed writing", hides a message inside another medium, such as an image, an audio or video file or a text, so that the existence of the message itself goes unnoticed [3]. Its main objective is visual imperceptibility: changes made to the cover medium must not be detectable by the human eye. In image-based methods, a QR code, which consists of black and white patterns, is first quantised into binary values to reduce the amount of data to be hidden. This compact representation can be embedded in a colour image with minimal change in luminance, so that image quality is preserved and the hidden content remains undetected [31]. QR codes are attractive carriers for a second reason: because their error correction capacity can absorb small deliberate changes, secret bits can be placed in a cover QR code without making it unreadable. Huang et al. exploit this by embedding the secret with an (8,4) Hamming code, which gives a higher payload and better embedding efficiency than earlier schemes while keeping the marked symbol valid and therefore unremarkable to onlookers [17].

Encoding Process: Encoding begins with the choice of the secret message to be transmitted. The message is converted into a QR code with a QR code generator, which turns the data into a compact binary form (Fig. 3). The generated code is then quantised, and its bits are embedded in a colour image by altering the least significant bits (LSB) of the image pixels, a change that remains visually imperceptible. The modified image, called the stego image, is saved and can be circulated without any sign that hidden information is present [14].

Decoding Process: Decoding recovers the hidden QR code from the stego image and then the original message (Fig. 4). The stego image is selected and the embedded bits are extracted by reversing the LSB substitution. These bits are dequantised to reconstruct the QR code, which is finally read with a QR code scanner to obtain the hidden message, identical to the one originally embedded. The integrity of the information is thus maintained during transmission, and the process remains reliable even when the image contains minor distortions [14].



Fig. 4. Decoding Process of Steganography

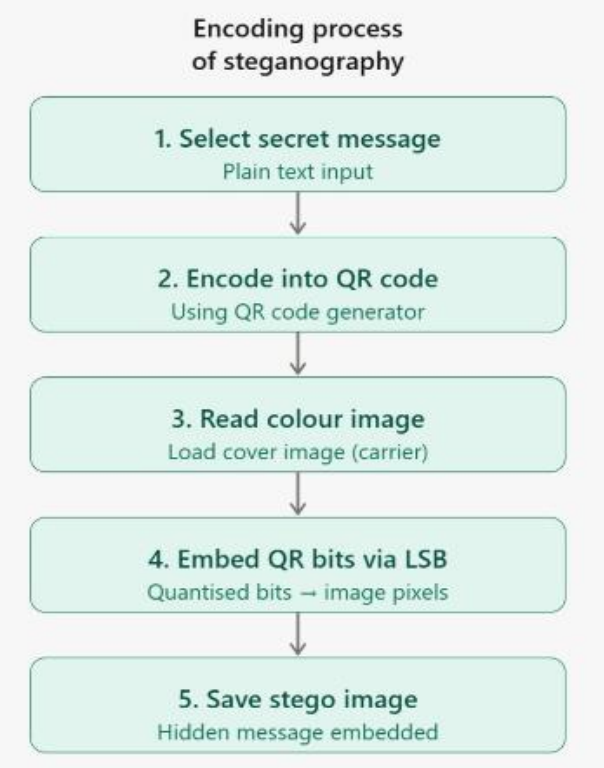


Fig. 3. Encoding Process of Steganography

D. Watermarking and Visual Features for Authentication

Whereas encryption and steganography protect confidentiality, watermarking and visual features address authenticity, that is, whether a code is the genuine one. Alsuhibany embeds a market-specific watermark in the QR image through lightweight least-significant-bit modification and uses a neural network to decide whether a scanned code is genuine or forged; on a dataset of 5,000 QR samples the system separated genuine from fraudulent codes with high accuracy, and it is aimed at barcode substitution fraud [8]. In a physical approach, Yan et al. combine QR codes with visual features, namely the natural texture of fibre paper, which acts as a physical unclonable function, and printed micro features, and report verification accuracies of 99.6% and 99.9% respectively; the system is described as compatible with existing QR-based logistics without extra manufacturing cost [12]. Both approaches show that authenticity can be checked with ordinary mobile devices, although the first requires each market to maintain its own watermark and the texture feature of the second requires special paper.

5. Applications of QR Code Technology

QR codes are used in a wide range of fields because of their simplicity, speed and versatility in storing and retrieving information. Their ease of scanning with a smartphone makes them an effective link between the physical and the digital world. Some common applications are described below.

A. Augmented Reality

Augmented reality (AR) lets users interact with physical and virtual content at the same time by overlaying digital elements on the real-world environment in real time. Most AR systems are marker-based: markers are recognised to determine where virtual models should be placed on the screen [23]. Such systems have notable limitations because they depend on pre-registered markers and on virtual content hosted on online platforms. Users often have to download the linked virtual objects well in

advance, and the inability to update markers or content dynamically reduces flexibility and real-time effectiveness. Recent work in AR therefore stresses dynamic content generated in real time, and combining QR codes with AR is a promising way to achieve it [24]. In this approach the QR code serves as a marker whose position and orientation are easily detected and tracked, and the data it holds, usually a URL, is used to fetch the corresponding 3D virtual object at run time. Once the code is scanned, the system estimates the marker's location and overlays the virtual content accordingly, which removes the need for prior registration or pre-downloaded assets and improves flexibility, scalability and user experience. Augmented Reality QR Codes (AQR) go a step further. Whereas conventional codes redirect users to static content such as text or a website, an AQR code triggers real-time AR content when scanned and acts both as a data carrier and as a spatial marker, so the system can decode the information and also position and render virtual objects in the real environment [25]. AQR is increasingly used in education, marketing, gaming and industrial training [34][35].

B. QR Codes in Education

QR codes are playing a growing role in modern education by making learning more interactive, efficient and, above all, accessible. Students are already familiar with them and find them useful because they are simple to use and give quick access to information through a clean, clear design. Many students prefer material that offers both short summaries for quick understanding and detailed explanations for deeper study; this combination lets them learn at their own pace and improves the overall experience. QR codes also support the idea of portable learning, which according to [27] is characterised by "area freedom", "time autonomy" and "significant substance". Motivation is crucial to learning, particularly in a world full of distractions, and keeping students interested is difficult. QR-supported learning environments can help by providing immediate access to engaging material such as videos, quizzes and additional resources, which keeps students motivated and actively involved. The work in [26] likewise recognises the part played by QR codes in education and highlights "mobile learning", a paradigm that uses portable devices to improve traditional teaching. Because QR codes can also activate AR content, as noted earlier, they can be used to build games based on learning material. The technology can further help to prevent unfair means in examinations. The authors of [28] proposed a method for detecting tampering with OMR sheets after an examination: details of the examinee, the number of responses marked and similar information are stored in an encrypted QR code, which is decrypted at the evaluation centre and checked for any alteration.

C. Cashless Payments

QR codes have become a popular payment method because they are simple, fast and easy to use. A user completes a transaction by scanning a code with a smartphone, with no need for cash or physical cards, which makes payment contactless and convenient in busy places and for everyday purchases. When linked to mobile wallets or banking applications, a scan results in an instant payment [36]. For merchants the method is inexpensive: no costly terminal or complicated installation is required, and a printed or displayed code is sufficient to begin accepting payments. Small shops, street vendors and local businesses can consequently adopt digital payment with little investment. QR payments also promote financial inclusion by bringing more people into the digital payment system, including those in remote or less developed regions [29][30]. Dynamic QR codes, which change for every transaction, add a further layer of security by lowering the risk of fraud or misuse [2]. The digital records generated by QR payments also help users and businesses to monitor spending and manage their finances. Payment is, however, one of the settings in which the tampering attacks described above are most damaging, since a

counterfeit code placed on a payment board can divert funds [10]. Overall, QR codes have made payments more convenient, affordable and widely accessible, provided that appropriate safeguards accompany them.

D. Internet of Things

QR codes make it easy to identify physical objects and link them to digital information that users can reach instantly with a smartphone. Building on this idea, the authors of [4] introduced executable QR codes (eQR codes), which embed a small program in the code itself. Conventional codes rely on an internet connection to fetch data, whereas an eQR code can perform actions and interact with the user even offline, since the required logic is already stored in the symbol. This makes it more independent and dependable where connectivity is poor, and it turns even simple, "non-smart" objects into interactive ones. The authors focus on a compact language, QRtree, designed for decision trees; in their example the QRtree version of a program takes 234 bytes, less than half of the equivalent Python bytecode (634 bytes) [4]. A code printed on a machine, product or device can provide step-by-step instructions, safety guidelines or troubleshooting help without network access, and can guide the user through a procedure so that complex tasks are easier to follow. Such guidance is especially useful in industrial settings, educational environments and remote locations, for example for instructions on rescue devices in mountains or caves where there is no coverage [4]. Although eQR codes do not provide full IoT functionality, they embed a degree of intelligence in physical objects and thus contribute to the broader IoT vision by letting objects guide, assist and interact with users independently [4]. In a different IoT role, QR codes serve as product identifiers in supply-chain tracking and anti-counterfeiting systems, where visual features verify authenticity while the code provides traceability [12]. The approach is inexpensive, simple to implement and reduces dependence on network infrastructure, opening possibilities for smarter interaction in manufacturing, maintenance, education and consumer products.

6. Conclusion

QR code technology has grown into a powerful and versatile tool that supports efficient data sharing, smooth user interaction and applications in education, digital payments, security systems and augmented reality. Its simplicity, low cost and compatibility with smartphones have driven its rapid adoption. Encrypted QR codes, steganography-based techniques and AR-integrated systems have broadened what the technology can do, making secure, interactive and intelligent uses possible, and they have opened new roles in the IoT, where a QR code can bridge physical objects and digital systems. Even so, significant challenges persist. Restricted data capacity, reliance on external links and the lack of built-in authentication leave QR codes open to misuse, and tampering, counterfeiting and quishing show the danger of trusting QR-based systems blindly. Issues related to scanning conditions, user awareness and interoperability further limit effectiveness in real-world settings. The studies reviewed here indicate that no single defence is sufficient: machine learning can flag suspicious codes before they are opened, encryption and steganography protect the payload, and watermarking and visual features help to verify that a code is genuine. Each of these has limits, including the scarcity of large standardised datasets, the cost of cryptographic operations and the need for special scanners or print materials, and evidence from phishing experiments shows that user behaviour remains decisive. Future work should therefore concentrate on stronger encryption, dynamic QR systems, interpretable detection models trained on shared benchmark datasets and secure data handling, together with user education and safe scanning

habits. By combining technical progress with better security practice and informed use, QR codes can remain a dependable and efficient tool in an increasingly digital world.

List of References

1. S. Tiwari, "An introduction to QR code technology," in Proceedings of the 2016 IEEE International Conference on Information Technology (ICIT), 2016, pp. 39–43, doi: 10.1109/ICIT.2016.38.
2. M. W. Akram, K. Sood, M. Ul Hassan and B. Subba, "Exemplifying Emerging Phishing: QR-Based Browser-in-the-Browser (BiTB) Attack," in IEEE Networking Letters, vol. 7, no. 4, pp. 274-278, Dec. 2025, doi: 10.1109/LNET.2025.3605640.
3. Md Rishadul Bayesh, D. Das, and Md Ahadullah, "A dual-layer image encryption framework using chaotic AES with dynamic S-boxes and steganographic QR codes," Journal of Information Security and Applications, vol. 96, p. 104322, Jan. 2026, doi: 10.1016/j.jisa.2025.104322.
4. S. Scanzio, M. Rosani, M. Scamuzzi, and G. Cena, "QR codes: From a survey of the state of the art to executable eQR codes for the Internet of Things," IEEE Internet of Things Journal, vol. 11, no. 13, pp. 23699–23710, Jul. 2024, doi: 10.1109/JIOT.2024.3385542.
5. M. W. Akram, K. Sood, and M. U. Hassan, "QRiS: A preemptive novel method for quishing detection through structural features of QR," arXiv preprint arXiv:2510.17175, Oct. 2025, doi: 10.48550/arXiv.2510.17175.
6. N. Nigam and R. Bhandari, "Performance analysis of QR phishing detection approaches," Journal of Information Systems Engineering and Management, vol. 10, pp. 221–225, 2025, doi: 10.52783/jisem.v10i33s.5472.
7. G. Awuah Amoah and J. B. Hayfron-Acquah, "QR code security: Mitigating the issue of quishing (QR code phishing)," International Journal of Computer Applications, vol. 184, pp. 34–39, 2022, doi: 10.5120/ijca2022922425.
8. S. A. Alsuhibany, "Innovative QR code system for tamper-proof generation and fraud-resistant verification," Sensors, vol. 25, p. 3855, 2025, doi: 10.3390/s25133855.
9. K.-C. Chou and R.-Z. Wang, "The Nested QR Code," in IEEE Signal Processing Letters, vol. 27, pp. 1230-1234, 2020, doi: 10.1109/LSP.2020.3006375.
10. H. Wahsheh and F. Luccio, "Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions," Information, vol. 11, p. 217, 2020, doi: 10.3390/info11040217.
11. J. Liu, J. Han, K. Fu, J. Jia, D. Zhu and G. Zhai, "Application of QR Code Watermarking and Encryption in the Protection of Data Privacy of Intelligent Mouth-Opening Trainer," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10510-10518, June 2023, doi: 10.1109/JIOT.2023.3242319.
12. Y. Yan, Z. Zou, H. Xie, Y. Gao and L. Zheng, "An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6789-6799, April 2021, doi: 10.1109/JIOT.2020.3035697.
13. S. A. Galadima, M. Shrivastava, and K. Srivastava, "A systematic literature review of QR code phishing detection techniques," Journal of Applied Bioanalysis, vol. 11, no. S10, pp. 273–287, 2025, doi: 10.53555/jab.v11si10.1400.
14. M. M. S. Rani and K. R. Euphrasia, "Data security through QR code encryption and steganography," Advanced Computing: An International Journal (ACIJ), vol. 7, pp. 1–7, 2016, doi: 10.5121/acij.2016.7201.

15. F. Trad and A. Chehab, "Detecting quishing attacks with machine learning techniques through QR code analysis," arXiv preprint arXiv:2505.03451, May 2025, doi: 10.48550/arXiv.2505.03451.
16. M. Sarkhi and S. Mishra, "Detection of QR code-based cyberattacks using a lightweight deep learning model," Engineering, Technology & Applied Science Research, vol. 14, pp. 15209–15216, 2024, doi: 10.48084/etasr.7777.
17. P.-C. Huang, C.-C. Chang, Y.-H. Li and Y. Liu, "Efficient QR Code Secret Embedding Mechanism Based on Hamming Code," in IEEE Access, vol. 8, pp. 86706-86714, 2020, doi: 10.1109/ACCESS.2020.2992694.
18. M. Geisler, D. Pöhn, and W. Hommel, "Hooked: A real-world study on QR code phishing," arXiv preprint arXiv:2407.16230, 2024, doi: 10.48550/arXiv.2407.16230.
19. H. Almousa, A. Almarzoqi, A. Alassaf, G. Alrasheed, and S. Alsuhibany, "QR Shield: A dual machine learning approach towards securing QR codes," International Journal of Computing and Digital Systems, vol. 16, no. 1, pp. 887–898, 2024, doi: 10.12785/ijcds/160164.
20. S. Vaithilingam and S. A. Mohan Shankar, "Enhancing security in QR code technology using AI: Exploration and mitigation strategies," International Journal of Intelligence Science, vol. 14, 2024, doi: 10.4236/ijis.2024.142003.
21. P. Kieseberg et al., "QR code security," in Proc. 8th Int. Conf. Advances in Mobile Computing and Multimedia (MoMM), New York, NY, USA: ACM, 2010, pp. 430–435, doi: 10.1145/1971519.1971593.
22. M. Weinz, N. Zannone, L. Allodi, and G. Apruzzese, "The impact of emerging phishing threats: Assessing quishing and LLM-generated phishing emails against organizations," in Proc. 20th ACM Asia Conf. Computer and Communications Security (ASIA CCS), ACM, 2025, pp. 1550–1566, doi: 10.1145/3708821.3736195.
23. L. F. de Souza Cardoso, F. C. M. Q. Mariano, and E. R. Zorzal, "A survey of industrial augmented reality," Computers & Industrial Engineering, vol. 139, p. 106159, Jan. 2020, doi: 10.1016/j.cie.2019.106159.
24. P.-Y. Lin, W.-C. Wu, and J.-H. Yang, "A QR code-based approach to differentiating the display of augmented reality content," Applied Sciences, vol. 11, p. 11801, 2021, doi: 10.3390/app112411801.
25. T.-W. Kan, C.-H. Teng, and W.-S. Chou, "Applying QR code in augmented reality applications," in Proc. 8th Int. Conf. Virtual Reality Continuum and Its Applications in Industry (VRCAI), ACM, 2009, pp. 253–257, doi: 10.1145/1670252.1670305.
26. R. Dorado, E. Torres-Jiménez, C. Rus-Casas, and M. Jiménez-Torres, "Mobile learning: Using QR codes to develop teaching material," in Proc. 2016 Technologies Applied to Electronics Teaching (TAEE), Seville, Spain, 2016, pp. 1–6, doi: 10.1109/TAEE.2016.7528363.
27. A. Sondhi and R. Kumar, "QR codes in education: A review," International Journal of Scientific Research in Science and Technology, vol. 9, no. 1, pp. 193–205, Jan.–Feb. 2022, doi: 10.32628/IJSRST229118.
28. S. Tiwari and S. Sahu, "A novel approach for the detection of OMR sheet tampering using encrypted QR code," in Proc. 2014 IEEE Int. Conf. Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2014, pp. 1–5, doi: 10.1109/ICCIC.2014.7238430.
29. P. Nandru, S. A. Senthil, and C. Madhavaiah, "Adoption intention of mobile QR code payment system among marginalized street vendors: An empirical investigation from an emerging economy,"

Journal of Science and Technology Policy Management, vol. 15, 2023, doi: 10.1108/JSTPM-03-2023-0035.
30. A. Mishra, G. K. Jha, and N. Gupta, "Unlocking digital payments: The role of QR codes in India's digital payment revolution," International Journal of Research Publication and Reviews, vol. 5, no. 4, pp. 9365–9375, Apr. 2024, doi: 10.55248/gengpi.5.0424.1124.
31. M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Farag Allah, "Steganography of encrypted messages inside valid QR codes," IEEE Access, vol. 8, pp. 27861–27873, 2020, doi: 10.1109/ACCESS.2020.2971984.
32. O. Taran, S. Bonev and S. Voloshynovskiy, "Clonability of Anti-counterfeiting Printable Graphical Codes: A Machine Learning Approach," ICASSP 2019, Brighton, UK, 2019, pp. 2482-2486, doi: 10.1109/ICASSP.2019.8682967.
33. DENSO WAVE Incorporated, "QR Code.com," Available: https://www.qrcode.com/en/
34. Uniqode, "Augmented reality QR codes: Basics and applications," Available: https://www.uniqode.com/blog/qr-code-basics/augmented-reality-qr-codes
35. AR Code, "AR Code: Augmented reality QR codes platform," Available: https://ar-code.com/
36. FasterCapital, "QR Code payments: The rise of QR code payments in India," Available: https://fastercapital.com/content/QR-Code-Payments--Scanning-Success--The-Rise-of-QR-Code-Payments-in-India.html
37. rustLab, "Malicious QR codes: The new gateway to online fraud," Available: https://trustlab.upct.es/en/2025/09/23/malicious-qr-codes-the-new-gateway-to-online-fraud/