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

QR Codes in the Digital Era: A Comprehensive Study

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

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

Abstract
Quick Response (QR) codes are simple scannable squares formed using black and white modules (fundamental units which store the data) that allow people to access information instantly using a smartphone camera, and over the past few years, they have quietly become a common part of daily life — from scanning a menu at a restaurant to making quick and easy payments at a local store. QR codes offer several inherent advantages that make them highly effective for modern data encoding and communication systems. One of the most significant benefits is their robust error correction capability, which allows accurate decoding even when a portion of the code is damaged, distorted, or partially obscured. Their fast and omnidirectional scanning capability further enhances usability, as they can be read quickly from any angle without precise alignment. Moreover, QR codes are easy to generate and widely accessible, allowing individuals and organizations to create and deploy them across diverse applications such as marketing, education, healthcare, and secure data sharing. Despite their advantages, QR codes also present several challenges and limitations as they are limited by their finite storage capacity, lack of human readability, dependence on external systems, and susceptibility to misuse or malicious exploitation. The aim of this paper is to provide a thorough understanding of the QR Code technology.

Keywords: QR Codes, Quick Response Codes, Encoding and Decoding

1. Introduction

A QR code, short for "Quick Response" code, is a type of two dimensional matrix barcode designed to store and rapidly retrieve information using devices such as smartphones. Originally this technology was developed in 1994 by the Toyota subsidiary Denso Wave, and were first utilized for tracking components in automotive manufacturing, to address and solve the issue of limited data storage capacity of traditional barcodes [8]. Over time, their application has expanded significantly across various domains, including commercial tracking, product labelling, marketing, entertainment, cashless payments, and mobile-based services. The widespread adoption of smartphones equipped with built in scanning capabilities has further accelerated their use in everyday activities [17]. Technically, the QR code system operates through two primary components: an encoder, which converts data into a QR code, and a decoder (or scanner), which interprets and extracts the embedded information. Additionally, the

availability of online tools and applications has made it easy for users to generate and distribute custom QR codes, contributing to their growing relevance in both personal and professional contexts. [10][21]
QR codes can be broadly grouped into several categories based on their structure, capacity, and application. The earliest versions, QR Code Model 1 and Model 2, highlight the evolution of the technology. Model 1 supports up to 1,167 numeric characters with a maximum size of 73 × 73 modules, while Model 2 improves upon this by enhancing readability under distortion or curved surfaces through the use of alignment patterns, and can store up to 7,089 numerals with a size of 177 × 177 modules. Micro QR Codes are used to address the problems related to area. They have just a single orientation detection pattern. [1] Logo QR Codes focus on aesthetics and branding by integrating colours, images, and text into the code design. The iQR Code is a flexible type of QR code that can store both small and large amounts of data. It can also appear in different formats like rectangular shapes or inverted colors, making it useful in many applications. Secure QR Code (SQRC) is a type of QR Code which can store both public and private data, differentiating it from the traditional QR Codes. A Frame QR Code is a type of QR code that includes a customizable area for adding visuals or text while still maintaining its scannable functionality.[1][33]

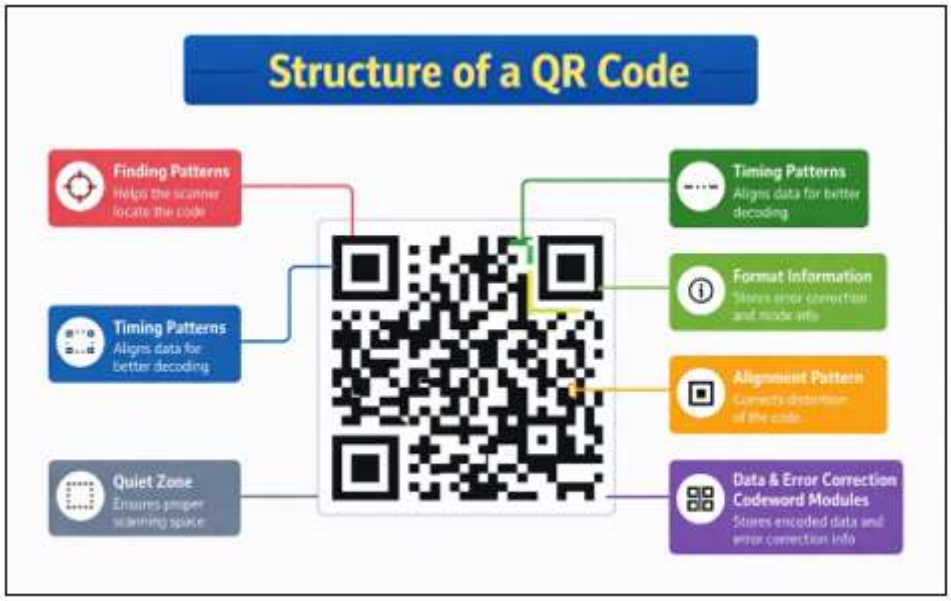


Fig. 1. Structure of a QR Code

2. Working of a QR Code

A. Structure of QR Codes

A QR code symbol is composed of small square modules arranged in a structured two-dimensional grid, forming a larger square pattern (Fig. 1.). This structure is divided into function patterns and an encoding region, and it is enclosed on all four sides by a margin known as the quiet zone, which ensures accurate detection during scanning. The function patterns play a critical role in enabling scanners to correctly locate, align, and interpret the QR code. These patterns include the finder patterns for position detection, separators to isolate key elements, timing patterns for coordinate mapping, and alignment patterns to correct distortion. The remaining portion, referred to as the encoding region, stores the actual information, including format and version details, along with the encoded data and associated error

correction codewords (Fig. 2.), ensuring reliable data retrieval even in the presence of partial damage or distortion.[1][9]

1. **Finder Pattern:** Finder patterns are distinctive position-detection markers placed at three corners of a QR code—top-left, top-right, and bottom-left. Each pattern is formed by a series of nested squares: a 7×7 dark outer square, a 5×5 light square inside it, and a 3×3 dark square at the center, following a consistent 1:1:3:1:1 ratio of light and dark modules. This unique structure is intentionally designed to stand out from the rest of the code, allowing scanners to quickly locate the QR code and determine its correct orientation for accurate decoding.
2. **Encoding Region:** The encoding region is the part of the QR code that holds all essential information, including the actual data, along with format and version details and error correction codewords. Specific areas within this region are reserved to store this metadata: format information is placed in small one-module-wide sections near the finder patterns, while version information is allocated in defined blocks—typically a 6×3 area above the bottom-left finder pattern and a 3×6 area beside the top-right finder pattern. This structured arrangement ensures that scanners can efficiently interpret both the data and its associated parameters during decoding.
3. **Separators:** Separators are narrow, one-module wide strips of white space that surround the finder patterns, creating a clear boundary between these patterns and the encoding region. This separation helps scanners distinguish position-detection elements from the actual data, improving decoding accuracy.
4. **Timing Patterns:** Timing patterns in a QR code consist of two lines—one horizontal and one vertical—made up of alternating dark and light modules. The horizontal pattern runs along the sixth row, while the vertical pattern is placed in the sixth column, both positioned between the separators. These patterns act as a reference grid, helping the scanner determine the spacing and alignment of modules, as well as assisting in identifying the overall structure and version of the QR code for accurate decoding.
5. **Alignment Pattern:** Alignment patterns are smaller reference markers within a QR code, designed as concentric squares with a dark outer layer (5×5), a light inner layer (3×3), and a single dark module at the center. These patterns help correct distortion, especially when the code is scanned at an angle or on uneven surfaces. They are included in QR codes of version 2 and above, with their number increasing as the code size (version) grows to maintain decoding accuracy.

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 a clear margin surrounding the QR code, typically four modules wide, that contains no data. This empty space acts as a buffer, ensuring that nearby text, images, or markings do not interfere with the scanner's ability to correctly detect and read the code. Without this

dedicated boundary, scanners may struggle to distinguish where the code begins and ends, leading to misreads or complete scan failures.

B. Encoding of QR Code

The process of generating a QR code involves several structured steps to ensure efficient data storage and reliable decoding. It begins with data analysis, where the input (such as text or a URL) is examined to determine the most suitable encoding mode—numeric, alphanumeric, byte/binary, or Kanji—so that the data can be represented using the fewest possible bits. In the next stage, the selected data is converted into a binary format and divided into 8-bit codewords, along with the addition of a mode indicator and a character count indicator, which varies depending on the QR code version. To enhance reliability, error correction coding is applied using Reed–Solomon techniques, generating additional codewords that enable the detection and recovery of errors caused by damage, dirt, or partial obstruction. The data and error correction codewords are then combined and organized into a final message structure, with padding added where necessary to meet size requirements. This message is subsequently mapped onto the QR code matrix, where the bits are placed in a predefined zig-zag pattern within the grid of black and white modules. To further improve scanning accuracy, a masking process is applied using one of several predefined patterns, which helps eliminate visually ambiguous arrangements and ensures better readability by scanners. Finally, format and version information—such as the error correction level and mask pattern used—are embedded in specific regions of the code. The result is a fully constructed QR code that can be printed, displayed, and reliably scanned across a variety of real-world conditions.[1]

C. Decoding Process of QR Code

The decoding of a QR code follows a systematic process to accurately retrieve the embedded information. Initially, the scanner captures the QR code image and identifies the arrangement of black and white modules, interpreting them as binary data. Structural elements such as finder and alignment patterns are used to correctly locate and orient the code. The system then extracts format information, including the error correction level and mask pattern, which is subsequently used to remove the applied masking. Next, the version information is determined to understand the size and data capacity of the QR code, enabling proper interpretation of its layout. The masking is then reversed, typically using an XOR operation, to recover the original encoded bit stream. The decoded stream is separated into data codewords and error correction codewords, which are reorganized to reconstruct the original message. Error detection and correction are performed using Reed–Solomon algorithms, ensuring reliable recovery even in the presence of distortions or partial damage. Finally, the corrected data is decoded into its original form—such as text or a URL—based on the encoding mode and character count, and is then presented to the user.

3. Challenges and Limitations of QR Code

Even though the QR code technology offer many benefits, it also comes with several challenges that can affect how effectively it is used in real-world situations. These challenges are not only technical but also related to security and user behavior. For example, QR codes can be easily copied, altered, or replaced, making them vulnerable to tampering and counterfeiting. Their performance also depends on proper scanning conditions—poor lighting, damage, or low-quality printing can make them difficult to read. In addition, not all users are equally familiar with QR technology, which can sometimes lead to confusion

or misuse. As QR codes are increasingly used in important areas like IoT systems, supply chains, and digital payments, the need for secure data handling and smooth system integration becomes more critical. Ensuring that QR codes work safely across different platforms and devices adds another layer of complexity. Moreover, while QR codes are mainly used for legitimate purposes, their ability to store and redirect information can also be misused. Attackers can embed harmful links that lead to phishing websites, malware downloads, or other unsafe content, often without the user realizing it. Because of these risks, it is important to develop better security measures, improve user awareness, and design more reliable systems. Addressing these challenges will help in making QR code technology safer, more trustworthy, and more effective across a wide range of applications.

A. Limited Data Capacity

QR codes have a limited data storage capacity, typically allowing only a few kilobytes of information to be encoded directly. In practical terms, they can store around 7,000 numeric characters or approximately 4,000 alphanumeric characters, which may not be sufficient for more complex or data-intensive applications. This limitation becomes more significant when error correction levels are increased, as higher error correction reduces the amount of space available for actual data.[14] As a result, most real-world applications rely on embedding URLs that redirect users to externally hosted content, rather than storing all the information within the QR code itself. While this approach extends the functionality of QR codes, it also introduces a dependency on internet connectivity and external servers. If the network is unavailable, slow, or the linked content is modified or removed, the QR code may fail to deliver the intended information.[4] Additionally, this reliance on external links can raise concerns related to security, data integrity, and long-term reliability, as users have no direct control over the hosted content. Therefore, the limited data capacity of QR codes remains a key constraint, especially in applications that require secure, offline access or the storage of large amounts of information directly within the code.[10]

B. Security Vulnerabilities

QR codes are inherently vulnerable to security threats because they lack built-in authentication or verification mechanisms. This makes it easy for attackers to replace or overlay legitimate QR codes with fake ones, especially in public places such as posters, payment stands, or advertisements.[20] When users scan these altered codes, they may be unknowingly redirected to malicious websites, exposed to malware, or even tricked into making unauthorized financial transactions. The problem is further worsened by the fact that QR codes are not human-readable, so users cannot verify the content before scanning. [2][37] One common form of attack is Quishing (QR phishing), where attackers use fake QR codes to mislead users.[7][13] These codes often redirect users to fraudulent websites that closely resemble genuine ones, making it difficult to identify the threat. Once on these sites, users may be asked to enter sensitive information such as passwords, personal details, or banking credentials, which can then be stolen and misused. In some cases, scanning a malicious QR code may also trigger automatic downloads of harmful software onto the user's device.[18] As QR codes become more widely used in critical applications like digital payments, authentication systems, ticketing, and IoT environments, the impact of such security risks becomes more serious. Therefore, it is essential to implement stronger security measures such as encryption, secure QR code generation, and verification mechanisms. At the same time, increasing user awareness and encouraging cautious scanning practices can play a key role in reducing the chances of such attacks and ensuring safer use of QR code technology.

C. QR Code Tampering

Unlike traditional barcodes or written links, QR codes are not human-readable, meaning users cannot

directly understand or verify the information they contain without scanning them. This creates a strong dependence on trust and increases the chances of misuse, as users may scan codes without knowing their actual intent. One major concern is QR code tampering, where a legitimate QR code is modified or replaced with a malicious one. Similarly, QR code counterfeiting involves creating fake QR codes that closely resemble genuine ones, making it difficult for users to distinguish between authentic and fraudulent codes.[12][32] These risks are further increased by how easy it is to generate QR codes using free online tools, allowing attackers to create highly convincing replicas with little effort. In many cases, attackers design QR codes that appear to belong to trusted organizations such as banks, payment services, or popular brands, thereby increasing the likelihood of user trust. A common real-world tactic is physical code replacement, where fake QR code stickers are placed over original ones on payment boards, posters, product packaging, or restaurant menus, redirecting users to malicious destinations without their knowledge.[10] Additionally, since QR codes often redirect users to external websites or trigger actions automatically, even a single scan can lead to serious consequences such as phishing attacks, financial fraud, or data theft. The lack of visible indicators makes it difficult for users to detect such threats in advance. Therefore, it is essential to implement stronger security practices, such as using encrypted or dynamic QR codes[2], and to promote user awareness by encouraging individuals to verify sources before scanning. These measures can help reduce the risks associated with QR code tampering and counterfeiting and ensure safer usage in everyday applications.[5][16]

4. QR Code Security

As QR codes are widely used to share important information, keeping that data secure has become very important. Regular QR codes do not have built-in protection, so anyone can scan and access the data easily. To overcome this, encryption is used to convert the data into a coded and unreadable form using specific algorithms before generating the QR code. When the code is scanned, decryption is applied using the correct key or method to convert the data back into its original readable form [6]. Furthermore, a secure QR code system combines encryption and digital watermarking to protect sensitive data from unauthorized access, while maintaining reliable data retrieval and usability [11]. This approach helps protect sensitive information and prevents unauthorized access or misuse. Some of the solutions to the QR Code security related issues are mentioned below:-

A. Intelligent Detection using Machine Learning

Modern research strongly focuses on machine learning-based detection systems, which can identify malicious QR codes by analyzing patterns in structure and behaviour. These models are more effective than traditional methods because they can adapt to new threats like quishing and Ai-based attacks. Recent studies also show that combining QR structure analysis with ML models improves detection accuracy and real-world usability. [15][22]

B. Strong Encryption for Data Protection

Encryption methods like the Advanced Encryption Standard (AES) are used to keep the data inside QR codes safe. They work by converting normal, readable information into a secret code (called encrypted data).[3] This code looks like random characters and cannot be understood by anyone who does not have the correct key to decode it. So, even if an unauthorized person scans the QR code, they will only see meaningless data instead of the actual information. In simple terms, encryption acts like a digital lock. Only people who have the right “key” can unlock and read the information. This is very useful in situations like online payments, login systems, or sharing private data, where security is important. To

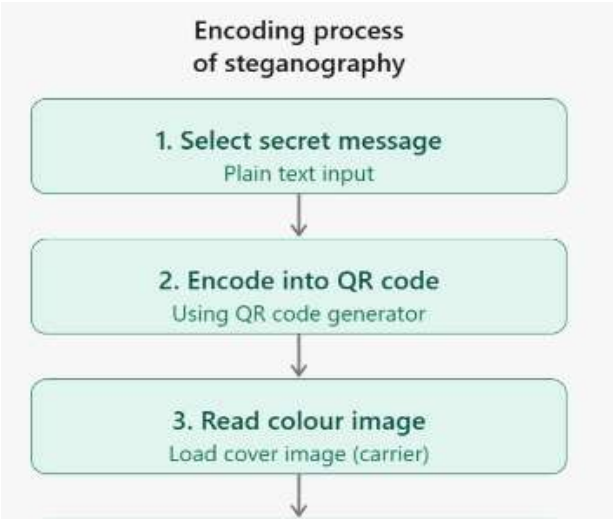
make things even safer, modern systems use multi-layer encryption. This means the data is encrypted more than once using different methods or keys. It's like putting a box inside another box and locking each one separately. Even if a hacker manages to break one layer, they still have to get through other layers, which is very difficult and time-consuming.[19] Because of these improvements, QR codes are becoming more secure and trustworthy for storing and sharing sensitive information, reducing the chances of data theft or misuse.

C. Steganography for Hidden Security

Steganography, which literally means "concealed writing," is a technique used to hide a message within another medium such as an image, audio file, video, or text, so that the very existence of the message remains unnoticed.[3] The primary goal of this approach is to ensure visual imperceptibility, meaning that any modifications made to the cover medium should not be detectable to the human eye. To achieve this in image-based methods, a QR code—composed of black and white patterns—is first quantized and represented as binary values (0s and 1s), reducing the amount of data to be embedded. This optimized representation allows the QR code to be seamlessly embedded into a color image with minimal changes in luminance, ensuring that the overall visual quality remains intact and the hidden information stays undetectable.[31]

Encoding Process: The encoding process in steganography begins with selecting the secret message that needs to be securely transmitted. This message is first converted into a QR code using a suitable QR code generator, effectively transforming the data into a compact binary form (Fig. 3.). The generated QR code is then quantized, and its bits are embedded into a color image by modifying the least significant bits (LSB) of the image pixels. This method ensures that the changes remain visually unnoticeable. Finally, the modified image, known as the stego image, is saved and can be shared without revealing the presence of the hidden information.[14]

Decoding Process: The decoding process in steganography focuses on retrieving the hidden QR code from the stego image and extracting the original secret message (Fig. 4.). It begins by selecting the stego image, from which the embedded QR code bits are extracted using the reverse of the LSB substitution method. These bits are then dequantized to reconstruct the original QR code. Finally, the recovered QR code is scanned using a QR code reader to obtain the hidden message, which is identical to the original data embedded during the encoding process. This ensures that the integrity of the information is preserved throughout the transmission. The process remains reliable even when minor distortions are present in the image.[14]



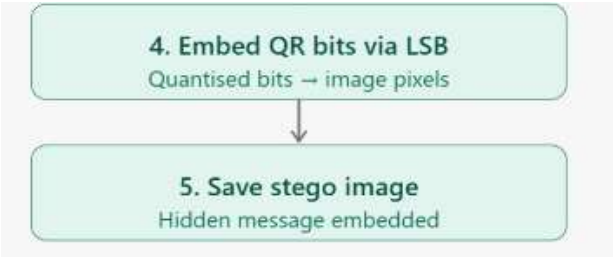


Fig. 3. Encoding Process of Steganography

Fig. 4. Decoding Process of Steganography

5. Applications of QR Code Technology

QR codes have found widespread use across a variety of domains due to their simplicity, speed, and versatility in storing and accessing information. Their ability to be easily scanned using smartphones has made them an effective tool for bridging physical and digital interactions. Some common applications of QR Codes are:-

A. Augmented Reality

Augmented Reality is a technology which allows the users to interact with physical and virtual content simultaneously. It enhances the Real-world environment by overlaying digital elements onto it in real time. Most of the AR technologies are marker-based i.e. Recognition through markers is used to locate and identify the relative placement or position of the virtual models on the screen.[23] Marker-based AR systems face several limitations, primarily due to their dependence on pre-registered markers and associated virtual content hosted on online platforms. These systems often require users to download linked virtual objects well in advance, and the inability to dynamically update markers or content reduces their flexibility and real-time effectiveness. Recent advancements in AR emphasize the need for dynamic, real time generated content that allows more interactive and responsive user experiences,

making it essential to overcome these constraints. The integration of QR codes with AR systems acts as a promising solution to these challenges. [24] In this approach, QR codes serve as markers that can be easily detected and tracked for their position and orientation. The encoded data within the QR code, typically a URL, is used to retrieve corresponding 3D virtual objects in real time. Once scanned, the AR system quickly estimates the marker's location and overlays the virtual content accordingly. This method eliminates the need for prior user registration or pre downloaded assets, thereby improving flexibility, scalability, and overall user experience. Furthermore, Augmented Reality QR Codes or AQR, represent an advance integration of the AR technology with QR Codes. Unlike traditional QR codes that simply redirect users to static content such as text or websites, these QR codes trigger real-time AR content when scanned.[25] These codes act as both data carriers and spatial markers, enabling the system to not only decode information but also accurately position and render virtual objects in the real-world environment. The use of AQR is expanding across various fields, like education, marketing, gaming, industrial training etc.[34][35]

B. QR in Education

QR Codes play an increasingly important role in modern education, as the help to make learning more interactive, efficient and most importantly accessible. Students are familiar with QR codes and find them useful for learning because they are simple and easy to use. They also like the clean and clear design, which makes accessing information quick and convenient. Alot of students prefer content that provides both short summaries for quick understanding and detailed explanations for deeper learning. This combination helps them learn at their own pace and improves their overall learning experience. In the field of education, Quick Response codes help to empower and utilise the concept of Portable learning. According to [27], the main highlight of portable learning is defined by the trilogy of 'Area freedom', 'Time autonomy' and 'Significant Substance'. As we know, that motivation plays a very crucial role in the process of learning, especially in today's world which is full of distractions. In such environments, maintaining interest and engagement can be challenging. QR code supported learning environments can help to address this issue, by providing quick access to interactive and engaging content such as videos, quizzes, and additional resources. This helps the students to stay motivated while being actively involved in their studies. The paper [26], also acknowledges the role of QR codes in education, highlighting the concept of 'Mobile Learning'. It is a teaching paradigm which incorporates the use of portable devices to improve traditional learning. As mentioned earlier, QR codes allow activities of AR, this helps to create games based on learning and study materials. Moreover, this technology can also be used to prevent the usage of unfair means in examinations. The authors of [28], presented a method to detect any kind of manipulations with the OMR sheets after the examination is conducted. In their proposed method, the details of the examinee, number of responses filled etc. are stored in an encrypted QR code, which will later be decrypted at the evaluation centre. The details will be checked for any sort of altering.

C. Cashless Payments

QR codes have become a popular way to make payments because they are simple, fast, and easy to use. With just a quick scan using a smartphone, users can complete transactions without needing cash or physical cards. This makes the payment process smooth and contactless, which is especially useful in busy environments and for everyday transactions. When connected to mobile wallets or banking apps, QR codes allow instant and hassle-free payments.[36] They are also very cost-effective for merchants, as they do not require expensive machines or complex setup—just a printed or digital QR code is enough to

start accepting payments. This makes it easier for small shops, street vendors, and local businesses to adopt digital payments without high investment. Another important advantage is accessibility, as QR codes help include more people in the digital payment system, even in remote or less developed areas.[29][30] In addition, newer features like dynamic QR codes[2], which change for every transaction, add an extra layer of security by reducing the risk of fraud or misuse. QR payments also help maintain digital records of transactions, making it easier for both users and businesses to track spending and manage finances. Overall, QR codes have made payments more convenient, affordable, secure, and widely accessible, benefiting both customers and businesses alike.

D. Internet of Things

QR codes make it easy to identify real-world objects and connect them to digital information, allowing users to instantly access details using their smartphones. Building on this idea the authors of [4] presented a concept called eQR codes (executable QR codes) in which we can embed small programs directly within the QR code itself. Unlike traditional QR codes that depend on an internet connection to retrieve data, eQR codes can perform certain actions and enable interaction even in offline environments, as the required logic or instructions are already stored within the code. This makes them more independent and reliable in situations where connectivity is limited. This capability allows even simple or "non-smart" objects to become interactive. For example, a QR code printed on a machine, product, or device can provide step-by-step instructions, safety guidelines, or troubleshooting support without needing internet access.[12] It can also guide users through processes, making complex tasks easier to understand and follow. This is especially helpful in industrial settings, educational environments, and remote locations where quick and clear guidance is required. Furthermore, eQR codes contribute to the broader vision of the Internet of Things (IoT) by embedding a level of intelligence directly into physical objects.[27] While they may not offer full IoT functionality, they create a partial IoT experience by enabling objects to guide, assist, and interact with users independently. This approach is cost-effective, easy to implement, and reduces dependency on network infrastructure. As a result, eQR technology opens up new possibilities for smarter interactions in areas such as manufacturing, maintenance, education, and everyday consumer products, making physical objects more informative and user-friendly.

6. Conclusion

In conclusion, QR code technology has evolved into a powerful and versatile tool, enabling efficient data sharing, seamless user interaction, and a wide range of applications across domains such as education, digital payments, security systems, and augmented reality. Its simplicity, low cost, and compatibility with smartphones have played a major role in its rapid and widespread adoption. Furthermore, advancements such as encrypted QR codes, steganography based techniques, and AR-integrated QR systems have significantly enhanced its capabilities, enabling more secure, interactive, and intelligent applications. These innovations have also opened new possibilities in areas like IoT, where QR codes can act as a bridge between physical objects and digital systems. However, despite these advantages, QR codes still face several important challenges that must be addressed. Limitations such as restricted data capacity, dependence on external links, and the absence of built-in authentication mechanisms make them vulnerable to misuse. Security threats including tampering, counterfeiting, and quishing attacks highlight the risks associated with blind trust in QR based systems. Additionally, issues related to scanning conditions, user awareness, and system interoperability can further impact their

effectiveness in real-world scenarios. These challenges emphasize the need for stronger security measures, improved design strategies, and greater user education. Looking ahead, the future of QR code technology lies in enhancing its security, flexibility, and overall reliability. Continuous improvements in encryption techniques, dynamic QR systems, and secure data handling can help address many of the current limitations. At the same time, increasing user awareness and promoting safe scanning practices will play a crucial role in minimizing potential risks. By combining technological advancements with better security measures and informed usage, QR codes can continue to evolve as 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, "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. G.-J. 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. Rani and E. K. Rosemary, "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 and D. Pöhn, "Hooked: A real-world study on QR code phishing," arXiv preprint arXiv:2407.16230, 2024, doi: 10.48550/arXiv.2407.16230.
19. [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. 15, 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/