International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 8, pp 37-48, August-2024

https://doi.org/10.47001/IRJIET/2024.808005

Review "The Digital Revolution for the Security of Hiding Information inside the Quick Response Code"

[1]Afraa Zidane Younis, [2]Ahmed Sami Nori

[1]Computer Science Department, College of Computer and Mathematics & Mosul University, Iraq
[2]Cyber Security Department, College of Computer and Mathematics & Mosul University, Iraq

***Abstract* - The Digital Revolution has significantly transformed secure and transmitted information, with QR codes emerging as a powerful tool in this landscape. QR codes that stands for Quick Response codes are 2D barcodes that can contain a vast amount of information; they have great opportunities to encrypt information, so they provide reliable solutions in terms of data hiding and data transfer. The described confrontation of the Digital Revolution insists on enhancing and changing ways to ensure information security, and the application of QR codes is a good example of how technological advancements can offer efficient ideas for concealing and protecting information. As encryption and QR code technology evolve, their role in securing data will undoubtedly expand, offering new levels of security in our increasingly digital world.**

Keywords: Digital Revolution Quick Response, Hiding Information, Security.

I. INTRODUCTION

Development has its advantages in ease, speed, and high technologies and this is what is available in the best digital innovations called the quick response code (QR). other primitive codes that developed starting in 1970, UPC symbols that were developed by IBM spearheaded the use of numbers arranged in thirteen various digits to allow mechanical input to computers. These UPC symbols are continued to use for Point-of-Sale (POS) system. In subsequent year's different codes with increasing storage capacities, and the figure given the nature of this invention, it would be remiss not to mention the dominant figures behind computing in its formative years. Figure 1 illustrates these stages of development; people have demanded aspects such as IDs that can store more digits of information and non-English languages symbols. To allow this, a symbol of even greater density than the multistaged symbols was needed. Therefore, making it possible for the QR Code to, at maximum, contain 7,000 digits of characters including the Kanji characters which are Chinese used in Japan and which was invented in the year 1994 [1]. QR is superior to linear bar codes, supports Kanji/Chinese characters; it can be used by anybody free of charge as Denso has released the patent into the public domain. Data structure standard is not a prerequisite for current usages. Most mobile phones equipped with cameras that enable the reading of QR Codes can access Internet addresses automatically by simply reading a URL encoded in the QR Code.

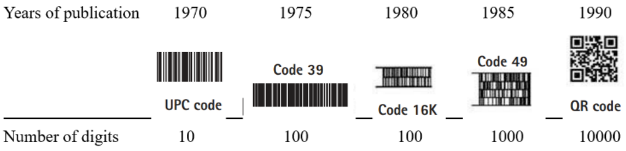
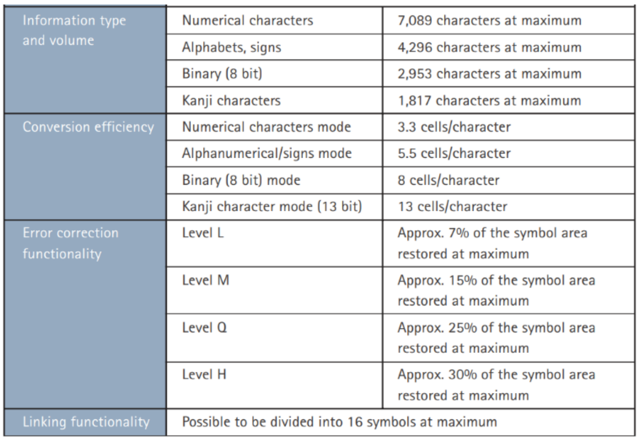


Figure 1: The History of Symbols

Addition to the characteristics of two-dimensional symbols such as large volume data (7,089 numerical characters at maximum), high-density recording (approx. 100 times higher in density than linear symbols), and high-speed reading, QR Code has other superiority in both performance and functionalities aspects distinguish. All-direction (360°) High-Speed Reading, resistance to Distorted Symbols, data Restoration Functionality (Resistant to Smudged or Damaged Symbols), masking Process, The Confidentiality of the Code, and Direct Marking. The most important feature of QR code is as shown in the table 1.

Table 1: The Specifications of the QR



Information type and volume	Numerical characters	7,089 characters at maximum
	Alphabets, signs	4,296 characters at maximum
	Binary (8 bit)	2,953 characters at maximum
	Kanji characters	1,817 characters at maximum
Conversion efficiency	Numerical characters mode	3.3 cells/character
	Alphanumerical/signs mode	5.5 cells/character
	Binary (8 bit) mode	8 cells/character
	Kanji character mode (13 bit)	13 cells/character
Error correction functionality	Level L	Approx. 7% of the symbol area restored at maximum
	Level M	Approx. 15% of the symbol area restored at maximum
	Level Q	Approx. 25% of the symbol area restored at maximum
	Level H	Approx. 30% of the symbol area restored at maximum
Linking functionality	Possible to be divided into 16 symbols at maximum	

II. THE STRUCTURE OF QR CODE

The QR Code can be described as a matrix-type symbol featuring a cell structure that is meticulously arranged in a square format. It encompasses distinct functionality patterns designed to facilitate effortless reading, along with a designated data area where information is stored. Within the QR Code, one can identify finder patterns, alignment patterns, timing patterns, and a quiet zone [2-3]. Throughout its evolution, the QR Code has undergone various stages of development aimed at enhancing its physical dimensions and storage capacity. Noteworthy advancements include the introduction of colored quick response codes, enabling a substantial increase in information retention compared to the traditional black and white response codes, all while maintaining a relatively similar physical footprint [4-5-6].

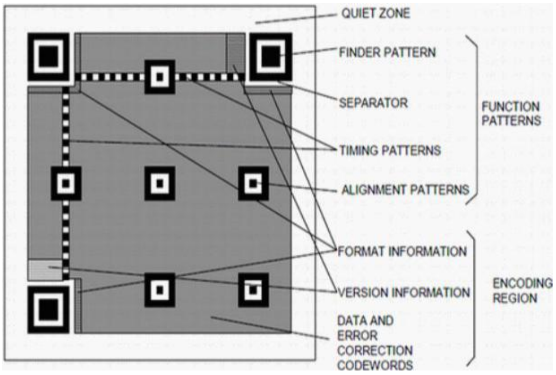


Figure 2: Structure of QR Code

2.1 Enhancement of QR Code Capacity

The enhancement of a QR code's capacity can be achieved through the refinement of its design to accommodate a greater amount of information while ensuring readability and reliability. Methods to augment the size of a QR code include: Elevating Version: The dimensions and capacity of QR codes are dictated by the different versions available. Higher versions possess the ability to contain more data and incorporate additional modules (squares). Opting for a higher version can amplify the storage capacity of the QR code. Selection between Numeric and Alphanumeric Modes: QR codes have the capability to be encoded in byte, Kanji, alphanumeric, or numeric modes. Certain data types can be encoded more efficiently in numeric and alphanumeric formats. Activation of Error Correction: In instances where a QR code is partially damaged or obstructed, its error correction mechanisms will ensure readability [7].

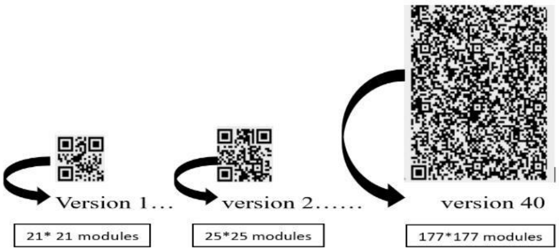


Figure 3: Stages of QR Development

Enhancing mistake correction at a higher level may allow for an increase in the storage capacity of the QR code without compromising readability. Optimisation of Data Compression refers to the attempt to decrease over-arching patterns or extra details that may be encoded, while converting into lesser dimensions. This process can potentially allow the QR code to hold more data within the box of its structure. Segmentation is method used to encode data that cannot fit into a single QR code since it is divided into segments. By doing this, the data can be spread to different QR codes meaning that the total capacity of data that a QR code can hold can increase. Micro QR Codes are slightly smaller than the standard QR codes and may be used in places where there is very little space. As they are capable of holding lesser amount of data as compared to the generally developed QR codes, they can still serve helpful when space is restricted through the application of these techniques.

2.2 Hiding inside the QR Code

There are several methods to encoding security information into QR codes. One method is the use of error repair data which is used to help in the read process even if the code is defective. According to the literature, the contents can be written twice and the visible data can be changed while the error correction data remains the same and thus the hidden information can be encoded into the QR code [8]. Also, to include information, the color of the code or the particulars in relation to the pixel of the code can also be altered. Selective graphic designs can contain text or other data of the user’s choice as part of the design in the code. With steganographic techniques, this message can be embedded in the QR code such that; it will be almost impossible to detect that something is hidden there. Another method is to place information within a perimeter around the QR code symbol [9-10]. Yet another method entails the use of steganography where extra information is written in such a way that they do not interfere with the scanning of the code [11-12-13-14-15]. Everyone has a right to privacy and security, so there is need to incorporate steganography in QR codes as it is applied in security, tracking, and communication where it is used to embed metadata, authentication markers, or even secret messages [16-17-18-19]. But it has to be borne in mind that the data that feeds into QR codes has to be compatible with QR codes in digital media [20-21]. However, user security and privacy threats are a major drawback of QR codes that are commonly implemented, currently QR codes are used in phishing attacks, to distribute malware and redirect users to unfamiliar domains [22-23-24-25-26-27]. Some strategies to deal with these threats are use of encryption, scanning applications and user consciousness to minimize any threat [28-29-30-31]. Lack of protection strategies for QR code security also poses different risks to its users who could be easily exploited by attackers. It

ISSN (online): 2581-3048
Volume 8, Issue 8, pp 37-48, August-2024
https://doi.org/10.47001/IRJIET/2024.808005

is important to strengthen the protection measures if QR codes are to be used and this is because some people may misuse the codes [32]. This makes risks to user security higher mainly because users do not distinguish between the two either. The suggested methods and systems were evaluated for performance to ensure safety maxims in different levels [33-34-35-36].

III. RELATED RESEAGHES

A study by Hazim Noman Abed [37] focused on a main research that did not lose security and protection with the image steganography technique using LSB and encryption along with QR Code for the safe transmission of data. Furthermore, the study included the selection of the bat algorithm in hiding messages to increase security aspects into the work. In addition, the study supported security measures by ensuring the elusive positions for the messages within the cover images. The effectiveness of the method was confirmed by using messages of different sizes and various cover pictures that showed the efficiency of the introduced security features. The adoption of this proposed technique could go a long way in preventing cases of leaked data and maintaining the confidentiality of the data while in transit thus improving security on the data in general.

In this study, Pei-Yu Lin *et al* [38] have put forward a new approach that show a remarkable improvement in terms of capacity with respect to concealing confidential information into QR codes when compared with other strategies. This improvement is realized based on the use of error correction capability that is in-built into QR code systems. It makes a higher inclusion of sensitive data into QR tags that directly manipulate data modules, as well as the readability of QR data and the privacy of the sensitive data included. This can be done through a methodology that involves parting the images into pixel pairs, in which secret bits are then hidden. It includes the identification of the allowed load of concealed information, identification of the digit pairs, placement of secret bits, and modification of the data modules in QR codes. People allowed to it can reveal the hidden information which is written in the annotated QR codes using the predefined secret key.

Malathi and colleagues [39] undertook a study that focused on this possible elimination of smart cards and PINs through the use of QR codes that are encoded in machine data. This involves the real-time encryption of the data field in the QR code of the ATM, which is decrypted by a mobile application for user identity verification and to perform the actual transaction. This is because encryption is very vital in enhancing the defense of the ATM operations, making it possible for users to withdraw cash without the physical cards. Consequently, users gain confidence, and clients obtain secure and reliable operations in banking services. The form of encryption helps in maintaining security in the transactions, the users' anonymity, and their financial details.

Iulian Aciobăniţei and colleagues [40] made a research that involved cloud computing domain and highlighted the aspects regarding security access to services and data. Light weight authentication using mobile device with Bro has been described as an efficient solution, where cryptographic techniques are applied to secure the interaction while access is facilitated using QR code. As for the action performed by the user at this stage, QR codes act as a means of exchange of authentication data between a user and the cloud service. By implementing the concepts of asymmetric and symmetric encryption, there must be a certainty that only the relevant authorities are capable of both reading the QR codes as well as generating them. Credentials are requested within the cloud environment, tasks related to cryptographic processes are accomplished in the same environment, and possibilities of the growth in the volume of requests are considered. Lightweight algorithms and the restriction of data transmission improve the particular flow of the authentication procedure, which is more appropriate for mobile devices and compartments with scarce power source. Thus, it reduces the need for multiple complex passwords and more- step verification methods or codes. This strategy applies to the essential need for safe, efficient, and effortless access to cloud services, and, therefore, presents the prospect of presenting solutions to modern authentication issues.

In this paper by P. M. Siva Raja *et al.* [41] the lifting wavelet transform (LWT) and the variable step size firefly algorithm (VSSFA) are used in wavelet domain steganography for improved security and invisibility. Three primary steps are involved in the process: choosing the best parameters, encoding the secret message, and retrieving the message. To incorporate QR coded messages and ensure data security, high-frequency sub-bands use LWT coefficients of the Least Significant Bit (LSB). The efficacy of the suggested steganography technique is evaluated using performance measures such as Mean Square Error (MSE), Tamper Assessment Factor (TAF), Normalize Correlation (NC), Bit Error Rate (BER), and Peak Signal to Noise Ratio (PSNR). The technique preserves the quality of the stego-image at an average PSNR of 63.76 dB and an embedding capacity of 5624 bits, showcasing its efficiency and reliability.

EasyStego is a new cross-domain steganography system that leverages QR barcodes in order to preserve information in literal and digital realms. Zhenhao Luo *et Al.*, [42] proposed a work on EasyStego which provides robust protection against physical distortions and capable of storing larger secret

ISSN (online): 2581-3048
Volume 8, Issue 8, pp 37-48, August-2024
https://doi.org/10.47001/IRJIET/2024.808005

messages while scaling up more in different situations making the physical and cyber security of data more robust. Employing AE encryption algorithm, the approach then limits secret messages' permissions and enhances security by reducing the likelihood of data leakage. The feasibility and effectiveness of EasyStego has been proved in this study's tests while showing that it can decode hidden messages under different types of physical distortions and challenges including different angles and distance, natural textures and quantitative error bits.

In the analysis of two unique anti-counterfeit apps based on VSSQR recommended for QR payment verification, Song Wan *et al.*, [43] offered the following multiple factors in the verification process: Visual secret sharing (VSS) that allows one to reconstruct the secret image visually without computation Thus, a method of dividing an initial secret image into noise-like shares is called visual secret sharing. In order to apply the VSS schemes, the information has to be protected from disclosure to other than the correct combination of shares. Currently, there are suggested methods and solutions to implement the security authentication of QR code payment through the integration of VSS with QR codes aimed at resisting counterfeiting of the payments. The VSSQR system involves establishing QR code sharing that could be well decoded and implementing secret information into two- way QR codes to secure.

ER. Luo, Harpreet, and others [44] this research investigates the use of QR codes for safe digital content transmission in image steganography. The technique minimizes major changes to the cover image while offering further resistance to lossy compression methods by using mid-band frequencies for embedding. Watermarking algorithms in the DCT mid-band and spatial domains are compared; the DCT mid-band is shown to be more dependable. The study highlights how crucial it is to steer clear of low frequencies while inserting hidden data in order to maintain the integrity of QR codes.

The objective of the study by Mathivanan, P., and others [45] is to ensure that ECG steganography is safe through the use of QR codes and ensure that patient information will only be embedded within ECG signals, and this shall not affect significant diagnostic markers on the signal. The ECG data is encoded and embedded into QR codes using various techniques of steganography. In other words, primary content is ECG data while the QR code is the hidden message. Employing the Daubechies 4 wavelet and one level one level discrete wavelet transform, does the cover ECG signal. For an actual embedment, the data concerning the patient is converted into QR code. The original ECG signal with watermark is got after applying the inverse DWT. The security aspect of this method has been confirmed in ECG steganography with the help of QR codes.

Another interesting work that tries to address the problem of practical application of QR codes is the three-layered QR code using the theories of secret sharing and linear block codes by Bin Yu and her group [46]. The said foregoing also means that the first character of the layer 1 data must be included in the QR code. THEY apply a linear error correcting code of the Reed Solomon type to the input data. In layer 2, split the encoded data into multiple shares by separating the disabilities each with a secret sharing algorithm such as Shamir's Secret Sharing. In layer 3, develop the barcodes, and then split them into portions. The studied approach enhances QR codes' security and reliability, making them suitable for use in settings where data authenticity and secrecy are paramount.

To avoid counterfeit currency, Asha Durafe [47] introduced a study that explains why it is necessary for criminal records to remain concealed. It flags steganography, a security technique where messages' existence is concealed, on information shared between criminal sectors. In steganography technique, criminal images and crime scene images are hidden in other files that can act as carriers. Digital steganography is the most beneficial in this aspect as discussed earlier. To enhance the level of security in the proposed Criminal Record Security System (CRSS), the RSA encryption and LSB steganography are used. It also employs a Raspberry Pi and GSM module for data transfer and is highly secure. It encrypts data in the use of RSA to reduce the visibility of sensitive criminal records, including photos, when passing to the recipient where it'll be decrypted. In addition, the gadget sends an oppressive QR code with the needed details.

Yanfei Sun *et al.* [48] the research paper is intent on describing QR Code Steganography based on JSteg in Discrete Cosine Transform (DCT) domain. The JSteg algorithm reconstructs the secret information into binary code format and embed it into the pixel data of cover image to achieve information security as well as easy transmission JSteg algorithm use JPEG format to embed the data in the image files The JPEG format uses the lossy compression method to expel redundant and less significant data in the image files and can support different compression levels to meet the different needs for data transmission across the networks.

Combination of advanced partitioning based on specific relationship for improving B-VisSS with respect to the conventional VisSS techniques was presented by researchers Jyoti Rao *et al.* [49] which specially involve a method to embed the secret image as hidden image in the QR codes. This

ISSN (online): 2581-3048
Volume 8, Issue 8, pp 37-48, August-2024
https://doi.org/10.47001/IRJIET/2024.808005

implementation technique is characterized by high security, anonymity, and reliability, which makes it ideal for any application in which data integrity and security are paramount. Thus, defining such new opportunities for VSS and employing the potential of Advanced partitioning, this method further develops the QR codes' perspective function and safety, as well as opens new possibilities for secure communication and data protection.

A study by Pengcheng Jiang *et al.* [50] a study presents a mechanism for improving security utilising QR codes for secret-sharing It intends to assimilate secret data into QR codes which cannot be tampered with or leaked thereby providing strong decryption and attack discovery, also achieve optimum concealed capacity and concealment from disguised attackers which provides the safety and sanctity of the codes to be shared among the receivers Based on two dimensional code structure, error correction function.

Suseendran Surendran *et al.* [51] have published a research paper which points out that integration of cryptography and QR codes in steganography offers a sound and secure way of concealing and transmitting data. The methodology for improving security in steganography by combining cryptographic techniques with Quick Response (QR) codes involves several key steps: data encryption, QR code generation, data embedding, error correction, and data retrieval. This methodology affords the desired additional layer of protection over the hidden data making it very appropriate for security sensitive and data integrity demanding uses.

Adinath Sangale *et al.* [52] introduced a study that described the three-tier security system that embraced the steps of cryptography, steganography, and a QR code feature for the protection of messages so as to secure sensitive information and ensure the differentiation of the data's originality A method of recommending asymmetric encryption algorithms in an attempt to improve information security and functionality in prospective use Suggests an approach to increasing the security of messages; each The first level of security is achieved by employing RSA technique to encipher the private message after which the enciphered digital message is concealed within a QR barcode in the second level Finally the QR barcode image containing the concealed information is hidden behind the mask image in the third and final level using a developed image encoding technique thereby creating a multilayer security system through a combination of cryptography and steganography. A quantitative and a qualitative analysis on this system revealed a positive impact through the enhancement of security features of data transmitted. Also, the outcomes concerning the application of these techniques mitigated risks and ensured the protection of valuable assets as information transmitted across the internet network; additionally, guaranteeing the integrity of shared data.

Nikita Bhoskar and colleagues [53] provided an investigation that presents an innovative methodology to enhance the security of QR codes through sophisticated partitioning algorithms. The study concentrates on enhancing the current sharing method to tackle security issues and puts forward a plan for (k, n) access structures that are grounded on particular relationships. The primary objective is to effectively conceal secrets inside QR codes by utilizing a visual sharing arrangement that is exclusively accessible to authorized users possessing the private key. The suggested approach aims to categorize all k-member subsets into different groupings to diminish the quantity of examples needed as n rises, thereby bolstering the security of the QR codes. Subsequent research directions recommended in the article involve devising tactics to deploy (k, n) access structures based on specific relationships to heighten security. However, the paper points out potential challenges in practical execution due to the emphasis on specific relationships for access structures.

Chorade Prit *et al.* [54] presented a study focuses on enhancing data security in QR code-based message sharing systems through the integration of cryptography and steganography Cryptography involves encrypting the message to secure it, while steganography hides the encrypted message within an image to provide an additional layer of security Researchers aim to combine cryptography and steganography effectively to ensure secure data sharing the proposed system encrypts the message using RSA encryption, generates a QR code representing the encrypted text, and then hides this QR code within an image using steganography techniques the first layer utilizes RSA encryption to encode the data, the second layer employs image steganography to hide the encrypted message in a QR code image, and the third layer encodes the QR code image using a mask image for additional security the study extensively evaluates asymmetric encryption algorithms, with a focus on RSA, for their security, adaptability, and encryption performance.

Yixiang Fang *et al.* [55] the research study proposed to investigate the phenomenon of concealed messages by the adoption of a high degree of error correction (for instance; level Q or H) and security measures in QR codes. As part of the detail of the idea, the study suggests the application of additional techniques using projection matrices and image segmentation to conceal information within the QR code design. This way ensures that the QR code remains open and comprehensible to normal scanner technologies; however, it also demands a separate process of extracting the concealed information.

John Blesswin *et al.* [56] has pointed out the problem of security breaches in communication with QR codes, which is why researchers have prepared a proposed set of measures to increase security. The paper introduces the visual cryptography as an effective cryptographic technique to solve these security challenges as the confidential information is encoded by means of the shadow. There are works proposed to counter these aspects of threats in QR code security models – self-authentication models, complementary visual cryptography, and adaptive techniques. Thus, the EIIPVC methodology turns out to be a progressive model for secure image transfer in modern digital communication, as evidenced by theoretical proofs and empirical data observed in the current study. This variety of methodology involves encoding a grayscale secret image into shadows on the sender end while the same is decrypted on the receiver end without involving actual decryption keys. It involves cast shadow generation, transmission, overlapping, and decryption whereby the individual shadows that is combined should be able to reconstruct the grayscale secret image to its original form.

S. Dhivyalakshmi Narayanan *et al.* [57] carried out a research study focusing on enhancing the security and anti-counterfeit features of QR codes by the integration of multi-encryption algorithm technique. First, the information to be embedded with the QR code is encrypted using a symmetric key encryption technique like advanced encryption standard (AES). Therefore, the output of the first encryption process is once more encrypted for the second time using the asymmetric encryption algorithm such as RSA. This extra step increases the level of security as compared to the standard version of PGP, the reason being that decryption requires a set of keys. Moreover, coming up with a hash of the encrypted data is accomplished through the use of a hash function such as SHA-256. This hash has the objective of providing validity of data and facilitating authenticity confirmation. The use of multiple encryptions especially improves on the measures of security. If one of the layers has been compromised, an extra layer of encryption and a hash function make the task of an unauthorized user nearly impossible.

See Table 2 it contains a summary of the previous studies that were cited in this research in terms of the algorithm used, the work, and the result that was drawn from each research.

Table 2: A Summary of the Previous Studies

	References	Method	The Work and Result
1	[37] 2017	Least Significant Bit (LSB)	1. Steganography technique using 2. Encryption with QR Code for secure data transmission, and bat algorithm. 3. Implementing the proposed technique can help in mitigating data breaches and ensuring the integrity of confidential information during transmission.
2	[38] 2017	Using (QR)'s error correcting capability	1. Breaking up photos into 2-pixel groups and concealing secret bits inside them, together with specifying the secret's tolerance limit. 2. Using a secret key, extract the embedded secret from tagged QR codes.
3	[39] 2017	Dynamic encryption	Involves dynamic encryption of information in the ATM's QR code, decoded by a mobile app for user validation and transaction processing, allowing users to withdraw money without physical cards.
4	[40] 2018	Lightweight authentication protocols based on QR codes	The advantages of cloud computing, cryptographic security, and user-friendly authentication techniques are combined when using cryptography in the cloud for lightweight authentication protocols based on QR codes.

5	[41] 2018	Utilizing a variable step size firefly algorithm (VSSFA) and lifting wavelet transform (LWT)	1. The procedure consists of three primary stages: choosing the best parameters, encoding the secret message, and message extraction. QR coded messages are embedded using LWT coefficients of the Least Significant Bit (LSB) in high-frequency sub-bands. 2. The technique keeps the quality of the stego-image, demonstrating its effectiveness and dependability.
6	[44] 2019	DCT mid-band domain	1. The "DCT" transform domain-based technique aids in the efficient embedding of the hidden secret message. 2. An 8*8 DCT block's middle band frequency coefficients. 3. Two files are needed; the QR code is one of them. The concealed information is contained in the first and second images.
7	[45] 2019	One-level Daubechies Four wavelet DWT	1. ECG signals are modified to conceal patient data without affecting crucial diagnostic areas. 2. The cover ECG signal is broken down using the Daubechies 4 wavelet and a one-level DWT.
8	[42] 2019	Cross-domain steganography scheme with an AES encryption algorithm	1. A novel cross-domain steganography scheme using QR barcodes to protect secret messages in both physical and cyber domains. 2. Employs AES encryption for enhanced security, and reducing the risk of sensitive-information leakage.
9	[43] 2019	QR codes with Visual Secret Sharing (VSS)	In order to provide safe information transmission, the VSSQR system entails embedding secret information between two QR codes and creating shares that can be accurately deciphered.
10	[46] 2019	Three-Layer QR Code Using Liner Code and Secret Sharing Scheme	1. The first bit of layer 1 data that the QR code will encode Apply a linear error-correcting code (like Reed-Solomon) to the input data. In layer 2, divide the encoded data into numerous shares using a secret sharing technique (like Shamir's Secret Sharing). In layer 3, generate QR codes and segment and distribute them. 2. Fit for high-stakes applications where secrecy and data integrity are crucial.
11	[48] 2020	The Discrete Cosine Transform (DCT) domain's JSteg algorithm.	1. Will see the release of the Discrete Cosine Transform (DCT) algorithm, or JSteg.1. The JSteg algorithm embeds hidden information into the cover image's pixel data by converting it into a binary string. 2. To remove unnecessary or redundant data from image files, the JPEG standard uses lossy compression.
12	[47] 2020	Uses a Raspberry Pi, a GSM module, RSA encryption, and LSB steganography to increase security.	1. Steganography uses digital steganography to conceal criminal and crime scene photos inside carrier files. 2. Makes use of RSA encryption and LSB steganography for increased security, as well as a Raspberry Pi and GSM module for safe data transfer. 3. The technology seeks to encrypt data and conceal private criminal records, such as photos.

13	[49] 2020	Advanced Partitioning and Visual Secret Sharing	1. Advanced Partitioning and Visual Secret Sharing1. To effectively integrate hidden data within QR codes, combine Visual Secret Sharing with smart partitioning based on specified relationships. 2. This technique improves QR codes' security and functionality.
14	[50] 2021	Error correction mechanisms, and XOR operations	1. A distributed secret sharing method using QR codes for enhanced security It aims to embed secret information in QR codes to prevent tampering and leakage. 2. Maximizing the capacity of hidden data and preventing attacks by disguised attackers ensuring the safety and integrity of shared secrets among receivers.
15	[51] 2021	Cryptographic techniques with Quick Response (QR) codes	Data encryption, QR code generation, data embedding, error correction, and data retrieval
16	[52] 2022	Asymmetric encryption algorithms	1. Proposed 3-layered architecture that integrates cryptography, steganography, and QR code technology. 2. The results indicated that the combination of these techniques effectively safeguarded valuable data transmitted over the internet.
17	[53] 2022	Partitioning algorithms	1. Proposes a strategy for (k, n) access structures based on specific relationships. 2. Methodology aims to group all k-member subsets into various collections to reduce the number of examples required as n increases, enhancing the security of the QR codes.
18	[54] 2023	RSA encryption and steganography techniques	1. RSA encryption is used by the suggested system to encrypt the message. 2. Creates a QR code that represents the encrypted text, conceals it inside an image using steganography techniques, with an emphasis on RSA because of its encryption performance, security, and adaptability.
19	[56] 2023	Inverse Pixel Visual Cryptography Caused by Errors (EIIPVC)	It involves encoding a secret B/W image in to shadows at the sender's side and decoding the same without applying any of the conventional decryption keys at the receiver's side.
20	[55] 2023	Image Segmentation	1. For concealing the data to remain as inconspicuous as possible, use a high error correction level, for example, level Q or H. 2. Techniques of hiding the secret data within the framework of the QR code with the usage of projection matrices and picture segmentation. 3. Applying this strategy helps to ensure that the created QR code remains functional and soluble by other relative Traditional QR codes.

21	[57] 2024	Multi-encryption algorithm	1. Undefined First of all, it is encrypted using one of the symmetric encryption algorithms such as AES. 2. Undefined the first encrypted message is then encrypted again using an asynchronous algorithm such as RSA. 3. Undefined at the end using a hash function like SHA-256 to prevent exposure of the original plain text data.

IV. CONCLUSION

Thus, QR codes can be considered as one of the key drivers of the Digital Revolution that changed the very nature of Information Security. These concise and multipurpose codes provide sturdy performances handy for concealing and conveying confidential data, utilizing peculiarities such as high density, capability to work with errors, and encryption. QR codes have multiple layers of security that can implement with other authentication methods and new generation technologies like block chain and dynamic content updates. Their uses cover various industries such as health, finance, smart city, and learning where they improve functionality and secure data integrity. Further into the digital age, the need for QR codes in protecting data will only increase from this, it is evident that the use of QR codes in. Standardization, user awareness as well as the protection from malicious codes are issues that need to be resolved if their possibilities are to be fully exploited. Thus, it is possible to ensure the progressive development of innovative approaches and the effective application of QR code technologies, along with confident creation of a solid information security system, reliable and resistant to constant new threats. Thus, the Digital Revolution has equipped us with something like QR codes, which is a giant leap toward a safer and linked society.

REFERENCES

[1] Mishra, A., & Mathuria, M. (2017). A review on QR code. *Int. J. Comput. Appl*, *164*(9), 17-19.

[2] Galiyawala, H. J., & Pandya, K. H. (2014, December). To increase data capacity of QR code using multiplexing with color coding: An example of embedding speech signal in QR code. In *2014 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.

[3] Taveerad, N., & Vongpradhip, S. (2015, November). Development of color QR code for increasing capacity. In *2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)* (pp. 645-648). IEEE.

[4] Lim, Z. Y., & Sim, K. S. (2022). Multi-Color Code with High Data Capacity. *International Journal on Robotics, Automation and Sciences*, *4*, 35-45.

[5] Ruan, C., & Huang, P. (2023, November). High capacity secret embedding strategy for QR codes based on EMD. In *Third International Conference on Artificial Intelligence, Virtual Reality, and Visualization (AIVRV 2023)* (Vol. 12923, pp. 569-577). SPIE.

[6] Aravindh, G., Piraisudan, R., Murali, L., Silwin, B. R., & Nithish, T. (2024, April). A Visual Cryptographic Scheme for Colour QR Codes in Defence. In *2024 International Conference on Science Technology Engineering and Management (ICSTEM)* (pp. 1-6). IEEE.

[7] Arya, A., & Tiwari, S. K. (2023). A survey paper on quick response codes and its image pre-processing methods based on steganography. *Int J Innovat Res Growth*, *12*, 17-24.

[8] Wan, S., Lu, Y., Yan, X., Ding, W., & Liu, H. (2018). High capacity embedding methods of qr code error correction. In *Wireless Internet: 9th International Conference, WICON 2016, Haikou, China, December 19-20, 2016, Proceedings 9* (pp. 70-79). Springer International Publishing.

[9] Arora, A., Garg, H., & Shivani, S. (2023). Privacy Protection of Digital Images Using Watermarking and QR Code-based Visual Cryptography. *Advances in Multimedia*, *2023*(1), 6945340.

[10] Wu, D. C., & Wu, Y. M. (2020). Covert communication via the QR code image by a data hiding technique based on module shape adjustments. *IEEE Open Journal of the Computer Society*, *1*, 12-34.

[11] Ohana, D. J., & Shashidhar, N. (2013). QR code steganography. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[12] Hajduk, V., Broda, M., Kováč, O., & Levický, D. (2016, April). Image steganography with using QR code and cryptography. In *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)* (pp. 350-353). IEEE.

[13] Pramanik, S. A. B. Y. A. S. A. C. H. I., & Raja, S. S. (2020). A secured image steganography using genetic algorithm. *Advances in Mathematics: Scientific Journal*, *9*(7), 4533-4541.

[14] Andrejčík, S., Ovseník, Ľ., & Oravec, J. (2023). The Influence of Steganographic Methods and QR Code

Resolutions on Data Hiding in Cover Images. *Acta Electrotechnica et Informatica*, *23*(4), 10-16.

[15] Koptyra K, Ogiela MR. Steganography in QR Codes—Information Hiding with Suboptimal Segmentation. *Electronics*. 2024; 13(13):2658. https://doi.org/10.3390/electronics13132658

[16] Rani, M. M. S., & Euphrasia, K. R. (2016). Data security through qr code encryption and steganography. *Advanced Computing: An International Journal (ACIJ)*, *7*(1/2), 1-7.

[17] Usama, M., & Yaman, U. (2022). Embedding information into or onto additively manufactured parts: a review of qr codes, steganography and watermarking methods. *Materials*, *15*(7), 2596.

[18] Sahu, S. K., & Gonnade, S. K. (2013). Encryption in QR code using stegnography. *International Journal of Engineering Research and Applications*, *3*(4), 1738-1741.

[19] Masoud, Alajmi., Ibrahim, F., Elashry., Hala, S., El-sayed., Osama, S., Farag, Allah. (2020). Steganography of Encrypted Messages Inside Valid QR Codes. IEEE Access, doi: 10.1109/ACCESS.2020.2971984

[20] Soon, T. J. (2008). There are several types of 2D codes in use by the industry, one of which is QR Code. This article provides an overview of QR Code, the standardisation activities on this technology and its applications in the various sectors. *Foxdesignsstudio. com.[Online]. Available: https://foxdesignsstudio. com/uploads/pdf/Three_QR_Code. pdf.[Accessed: 10-Feb-2023]*.

[21] Coleman, J. (2011). QR codes: What are they and why should you care?. *Kansas Library Association College and University Libraries Section Proceedings*, *1*(1), 16-23.

[22] Krombholz, K., Frühwirt, P., Rieder, T., Kapsalis, I., Ullrich, J., & Weippl, E. (2015, August). QR Code Security--How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 230-237). IEEE.

[23] Mavroeidis, V., & Nicho, M. (2017). Quick response code secure: a cryptographically secure anti-phishing tool for QR code attacks. In *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7* (pp. 313-324). Springer International Publishing.

[24] V. Sharma, ‘‘A study of malicious QR codes,’’ Int. J. Comput. Intell. Inf. Secur., vol. 3, no. 5, pp. 1–15, 2012.

[25] Yong, K. S., Chiew, K. L., & Tan, C. L. (2019, June). A survey of the QR code phishing: the current attacks and countermeasures. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)* (pp. 1-5). IEEE.

[26] Averin, A., & Zyulyarkina, N. (2020, November). Malicious QR-Code threats and vulnerability of blockchain. In *2020 Global Smart Industry Conference (GloSIC)* (pp. 82-86). IEEE.

[27] Venkat Krishnapur. Fab 4, 2021. What is QR code phishing and how to protect yourself from it. https://indianexpress.com/article/technology/opiniontechnology/what-is-qr-code-phishing-and-how-to-protect-yourself-from-it7174553/

[28] Julien Maury. February 21, 2022. QR Codes: A Growing Security Problem. https://www.esecurityplanet.com/threats/qr-code-security-problem/

[29] Narayanan, A. S. (2012). QR codes and security solutions. *International Journal of Computer Science and Telecommunications*, *3*(7), 69-72.

[30] Song, J., Gao, K., Shen, X., Qi, X., Liu, R., & Choo, K. K. R. (2018). QRFence: A flexible and scalable QR link security detection framework for Android devices. *Future Generation Computer Systems*, *88*, 663-674.

[31] Al-Zahrani, M. S., Wahsheh, H. A., & Alsaade, F. W. (2021). Secure Real-Time Artificial Intelligence System against Malicious QR Code Links. *Security and Communication Networks*, *2021*(1), 5540670.

[32] Pawar, A., Fatnani, C., Sonavane, R., Waghmare, R., & Saoji, S. (2022, August). Secure QR Code Scanner to Detect Malicious URL using Machine Learning. In *2022 2nd Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-8). IEEE.

[33] Wahsheh, H. A., & Luccio, F. L. (2019, February). Evaluating Security, Privacy and Usability Features of QR Code Readers. In *ICISSP* (pp. 266-273).

[34] Rafsanjani, A. S., Kamaruddin, N., Sjariff, N. N. A., Firdaus, N., Maarop, N., & Rusli, H. M. (2022). A Evaluating Security and Privacy Features of Quick Response Code Scanners: A Comparative Study. *Open International Journal of Informatics*, *10*(2), 197-207.

[35] S., D., Narayanan., Dr., S., Prabhu., E., Padma. (2024). Improving QR Code Security using Multiple Encryption Layers. 845-848. doi:10.1109/icc-robins60238.2024.10533884

[36] Agasthiya, Reni, Selvasingh. (2023). Implementing Number Theory in Visual Cryptography for Secure Online Transactions using QR Codes. International Journal for Research in Applied Science and

Engineering Technology, doi: 10.22214/ijraset.2023.56117.

[37] Abed, H. N. (2017). Robust and secured image steganography using lsb and encryption with qr code. *Journal of AL-Qadisiyah for computer science and mathematics*, *9*(2), 1-9.

[38] Lin, P. Y., & Chen, Y. H. (2017). High payload secret hiding technology for QR codes. *EURASIP Journal on Image and Video Processing*, *2017*, 1-8.

[39] Malathi, V., Balamurugan, B., & Eshwar, S. (2017, February). Achieving privacy and security using QR code by means of encryption technique in ATM. In *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)* (pp. 281-285). IEEE.

[40] Aciobăniței, I., Buhus, I.C., & Pura, M. (2018). Using Cryptography in the Cloud for Lightweight Authentication Protocols Based on QR Codes. *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 000539-000542.

[41] Raja, P. S., & Baburaj, E. (2018, February). QR code based image steganography via variable step size firefly algorithm and lifting wavelet transform. In *Proceedings of the 2nd International Conference on Machine Learning and Soft Computing* (pp. 114-121).

[42] Luo, Z., Xie, W., Wang, B., Tang, Y., & Xing, Q. (2019). EasyStego: robust steganography based on quick-response barcodes for crossing domains. *Symmetry*, *11*(2), 222.

[43] Wan, S., Yang, G., Qi, L., Li, L., Yan, X., & Lu, Y. (2019). Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code. *Mathematical Biosciences and Engineering*, *16*(6), 6367-6385.

[44] Singh, E.H. (2019). Implementation of Image Steganography in QR Code Using Mid-Band DCT. *Journal of emerging technologies and innovative research*.

[45] Mathivanan, P., Edward Jero, S., & Balaji Ganesh, A. (2019). QR code-based highly secure ECG steganography. In *International Conference on Intelligent Computing and Applications: Proceedings of ICICA 2018* (pp. 171-178). Springer Singapore.

[46] Yu, B., Fu, Z., & Liu, S. (2019). A Novel Three-Layer QR Code Based on Secret Sharing Scheme and Liner Code. *Security and Communication Networks*, *2019*(1), 7937816.

[47] Durafe, A. (2020). Securing criminal records using R-Pi, QR code and steganography. *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278*, *3075*(9), 6.

[48] Sun, Y., Yu, M., & Wang, J. (2020, November). Research and development of QR code steganography based on JSteg algorithm in DCT domain. In *2020 IEEE 15th International Conference on Solid-State & Integrated Circuit Technology (ICSICT)* (pp. 1-4). IEEE.

[49] Rao, J., & Chavan, N. Data Hiding under QR Code using Visual Secret Sharing and Advanced Partitioning Based on Specific Relationship.

[50] Jiang, P., & Xue, Y. (2021). A Distributed Secret Sharing Method with QR Code Based on Information Hiding. *Journal of Cyber Security*, *3*(4).

[51] Surendran, S., Palaniappan, R., & Nagaraj, V. (2021). Improved Security In Steganography By Amalgaming Cryptography And Quick Response Code. *Int. J. of Aquatic Science*, *12*(3), 1847-1853.

[52] Sangale, A., Taru, A., Gupta, R., Gandhas, V., & Deokar, R. SECURE MESSAGING USING CRYPTOGRAPHY, STEGANOGRAPHY AND QR CODE.

[53] Bhoskar, N., Ithape, P., Gavali, B., & Kasture, P. (2022). A Survey on secrete communication through QR code steganography for military application. *Int. J. Res. Appl. Sci. Eng. Technol*, *10*(1), 728-731.

[54] (2023). Secure QR-Code Based Message Sharing System Using Cryptography and Steganography. *International Journal for Research in Applied Science and Engineering Technology*.

[55] Fang, Y., Tu, K., Wu, K., Peng, Y., & Shi, Y. (2023). PROMISE: A QR Code PROjection Matrix Based Framework for Information Hiding Using Image SEgmentation. *KSII Trans. Internet Inf. Syst.*, *17*(2), 471-485.

[56] Blesswin, J., Mary, S., Gobinath, T., Divate, M., A, C.E., Shahbad, A.A., Patil, D., & S., S.R. (2023). Error-induced inverse pixel visual cryptography for secure QR code communication. *Journal of Autonomous Intelligence*.

[57] Narayanan, S. D., & Prabhu, S. (2024, April). Strengthening QR code Anti-Counterfeit through Multi-Encryption Algorithm. In *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS)* (pp. 864-866). IEEE.

Citation of this Article:

Afraa Zidane Younis, & Ahmed Sami Nori. (2024). Review “The Digital Revolution for the Security of Hiding Information inside the Quick Response Code”. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 8(8), 37-48. Article DOI https://doi.org/10.47001/IRJIET/2024.808005

****