A Review on Steganography and Data Hiding in QR Code

Abhinav Agarwal
Department of Computer Science
Singhania University
Jhunjhunu Rajasthan
Abhinavkiot2410@gmail.com

Dr. Sandeep Malik
Department of Computer Science And Engineering
Oriental University
Indore , Madhya Pradesh
smaliknnl@gmail.com

Abstract*— Steganography is regarded as the first line of defence in information security because it conceals a secret message (payload) within an innocent-looking file (container), allowing the payload to be transferred under the opponent's nose without the adversary realising what is going on. All steganographic technologies do is conceal the payload by hiding the container in plain sight. A steganographic system is described in this study, which exploits the container not only to hide the payload but also to provide false information to the opponent. In this way, visualising the smart combination of steganography methods might give an increased degree of protection for information transmissions. Quick Response (QR) codes are widely employed as a result of their many advantageous properties. In addition to resilience, readability and error correction capabilities, it also has a larger data capacity than regular barcodes, among other advantages. This study investigates the steganography method of embedding QR code (QRC) holding secret data into the cover image, which is built on the JSteg technique, to assure information security & ease of transmission. Numerous alternative cover pictures have been used to test secret messages of various sizes, and standard metrics have been established to evaluate their effectiveness.

I. INTRODUCTION

Information hiding is a new study topic that includes applications like watermarking, cryptography, steganography, and copyright protection for digital material, among others. Steganography is concerned with the hiding of secret communications between data-hiders as well as data-receivers. A large number of steganography methods have been developed, including LSB, JSteg, Outguess, and F5 among others. JSteg is a steganographic method that is used in JPEG pictures and is one of the most widely used. The implementation of JPEG steganography, which makes use of the Discrete Cosine Transform (DCT) to transform images into the frequency domain, is shown. The reason for its widespread usage and popularity is because image recovery methods such as these are resistant to JPEG compression. When it comes to communication security, methods such as steganography and cryptography as well as Quick Response (QR) Codes have all been employed. A QRC is a type of matrix barcode that has been utilised in a variety of social media apps, including Facebook and Twitter. It allows users to quickly and easily access URLs, geo-locations, and other types of data. A message encoded in a QRC, on the other hand, maybe read by any QRC reader with relative ease. The use of a QRC in collaboration with steganography may help to strengthen the secrecy and security of secret information while it is being sent. Lin and colleagues developed a high-payload secret concealing solution for data security that makes use of QR codes and steganography to conceal the payload. Zhou and colleagues suggested an attacking approach that is capable of not only detecting stego-images but also extracting the messages that are buried inside them. In this study, a unique method for encrypting QR codes and steganography is presented, which combines the two technologies. It is necessary to include the QRC data in the DCT coefficient matrix to achieve a secret data message, as well as the steganographic picture is created by inverse quantization as well as inverse DCT transformation to achieve secret data transmission (Jude Hemanth *et al.*, 2017).

The container is a steganography feature that has not yet been completely used to its full potential. A picture, e.g., is utilised to hide payload, & which is all there is to it. We need to figure out how to make better use of the container. For illustration, a container might be used to provide false information to the enemy if the adversary is not paying attention. This may be accomplished via the use of Quick QRC. QRC are 2D bar codes that can be scanned by cameras & are machine-readable by computers. They are capable of encoding a variety of different forms of information, including alphanumeric and control codes. Data such as a phone no., a URL, as well as an ID are examples of the types of data that may be stored in QR codes. Denso-Wave, a Japanese firm that is now a part of Toyota, was the first business to introduce QR codes in 1994. QR codes were utilised to track automobile components in a short amount of time. From then, they proliferated around the globe, mostly in the marketing and commercial sectors, among other places. QR codes are a handy and simple method of disseminating information. Nothing more complicated than taking your mobile and taking a photo of the QR code. When it came to the advertising and marketing industries, they were great successes. These symbols may be seen almost everywhere, on anything from food labels to large advertising signs. Figures 1 and 2 depict an instance of a QRC & its structural elements respectively (Alajmi *et al.*, 2020)

Figure 1

(a) QR code structure

Pattern	Definition
	Quiet Zone
	Format
	Timing
	Version
	Position
	Alignment
	Data

(b) Legend

Figure 2

1.1 Basic Steganographic methods Contains:

- **Substitution methods** – Numerous redundant elements of the cover picture have been employed to incorporate a portion of hidden data that is hidden from view. It is necessary to first detect repeated data over cover medium to implant secret message over all those repeating pixels data, which makes steganalysis very tough to do.
- **Transform domain methods –** In this approach, the frequency domain of the hidden picture is embedded into the cover media, and the cover medium is a transparent material. This increases the long-term viability and robustness of a stego item.
- **Spread spectrum methods –** This is a method of hiding information via the use of signal structure and spread spectrum technologies.
- **Statistical methods –** Some of the cover objects mathematical or numerical qualities may be changed to incorporate secret data messages in them, which is known as embedding. Most of the time, these strategies make use of testing based on assumptions when obtaining sensitive data.
- **Distortion methods –** The most effective method of data hiding is to detect the damaged signal from the cover medium and thereafter determine the instant when the cover picture is no longer visible.
- **Cover generation methods –** This is the most effective & straightforward method of embedding secret messages, provided that cover media is selected in a manner that is most appropriate for the upcoming embedding procedure (Ramya and Gopinath, 2015).

II. RELATED WORK

.

(Alajmi *et al.*, 2020), To do this, they will employ a QR code as a container. In contrast to the payload, the QR codes created by our suggested system may convey the system's standard message as well. Even though everybody may see the message, only those who possess a secret key will be able to access its payload. It is not necessary to link the message and the payload together; that is, any message may be created independent of the payload & vice versa. Researchers may make use of this by giving the opponent a communication that includes incorrect or misleading facts about oneself. Researchers put the recommended method thru the tests & establish that the created QR code is (valid), namely it is identical to such a regular QR code, which actually looks harmless and so less subject to an adversary's attack. Additionally, it is a resource, has a good level of noise immunity, and therefore is subject to steganalysis assaults, among several other features.

(Hajduk *et al.*, 2016), The purpose of this study is to provide a proposal for an image steganographic approach that is capable of inserting an encoded secret message utilising a QR code into an images data stream. The QR code embedding procedure is safeguarded by the AES encryption technique, which is utilised in conjunction with the DWT domain to provide maximum security. Furthermore, the encryption was successful in destroying the usual properties of the QR code, making the procedure more secure as a result. The purpose of this work is to build a picture steganographic approach that has a high degree of security while also having a high level of non-perceptibility. The relationship between security as well as the capacity of the approach was enhanced by compressing the QR code before it was embedded, which was done before the embedding procedure. The PSNR was used to assess the efficiency of the suggested approach, and the findings obtained were comparable to those obtained using existing steganographic tools.

(M and R, 2017), In this study, a unique technique for secret communication is given, which combines the principles of steganography with QR codes to achieve its goal. The recommended procedure is divided into two stages: (i) Encrypting the message using key values that are created using a genetic algorithm; and (ii) concealing the encrypted content behind a QR code. The simulation data demonstrates that it is possible to construct a better design of a safe algorithm that provides increased security and dependability.

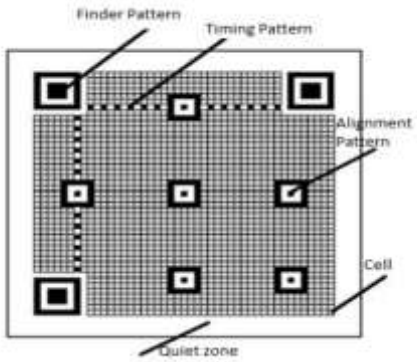
(Mendhe, Gupta and Sharma, 2018), So in this paper, they suggest a three-layered framework for safeguarding the process of message exchange, with the QR code picture serving as one of the layers. The cryptography and steganography methods used in this architecture are applied in both an empirical and strategic manner. The suggested system, based on quantitative as well as qualitative data, offers a greater degree of security than the existing method. In addition, researchers assess the system following the performance assessment criteria reported in the study.

(Sun, Yu and Wang, 2020), In this work, they investigate the steganography technique for embedding a QR code encoding a hidden message into a cover picture using the JSteg algorithm, which is based on the JSteg technique. Numerous alternative cover pictures have been used to test secret messages of varying sizes, & standard metrics have been established to evaluate their effectiveness. Following the experimental findings, all of the PSNR values are more than 47.6 dB in magnitude. The suggested solution provides great security while also being more imperceptible.

(Jude Hemanth *et al.*, 2017), In this study, the bit-plane of transform coefficients is chosen as the location where the hidden communication will be embedded. Properties of four different transforms employed in steganography have been investigated, and outcomes of four different transforms have been evaluated & compared. This has been shown by the research observations. Using four transforms from the frequency domain, this research offers a data hiding-based

picture steganography approach that employs four transformations from the frequency domain to achieve image steganography. This study also discusses how the four transformations interact with steganography and how they operate together. It has been shown experimentally that the suggested strategy improves the quality of stego-images while simultaneously increasing the embedding volume. It keeps the stego-image quality at a PSNR of more than 47 dB while not interfering with the retrieval of the secret message in question. The employment of intelligent optimization approaches to improve the quality of the stego picture is possible in future as part of the improvement process, if necessary. Various transformations may be employed to improve the picture steganography systems in the future, which will be the subject of future research.

(Ramya and Gopinath, 2015) This report outlines the extensive research of QR codes, their structures, as well as the present condition, wherein the QR Codes are applied in the area of information security. Furthermore, using a pixel value-based data concealing approach, they investigate several imperceptibility features such as the PSNR, MSE, AD, MD, and NAE, and the results are provided. When comparing image quality metrics among Cover QR & Stego QR, this technique provides superior results since hidden data has been inserted to its matching pixel value of cover QRC.



In this paper, we analysis to the accompanying architecture of QRC provides us with an invigorating concept as to why we have the option of using QR as a cover medium for information concealment. Let's take a quick look at the architecture of the QR to get a better idea of how it may be able to better conceal information. Assembling Patterns This pattern was used to determine the QR code's location. The Quick Response Code Symbol's angle, as well as size, may also be appropriately identified with this code. The round all the clock angle of the QR code may be better detected with this pattern. These patterns come in handy after a QR code has been read to fix any distortions that may have occurred. Disturbance detection is made easy thanks to the centre black alignment mechanism. If an erroneous pitch is present, these more supporting patterns may be used to locate the cell's centre coordinates. Horizontal and vertical views reveal this. For the matrix embedding approach, this is more of a way to recognise the QR from its more complicated context. To put it another way, it's a This is the place where we can genuinely hide our secrets. The data can be hidden much more simply when the QRC is in binary format, which allows us to put O in the black module as well as ones in a white module that correlate. Incorporating Reed-Solomon codes as well as their error-correction capabilities into the embedding data.

(Lin and Chen, 2016), The principles of the QR barcode are quickly explained in this work. QR Barcode The QR standard specifies that there are 40 various versions of QR tags, every with four separate error correction levels, according to the QR standard (L, M, Q and H). As shown in Table 1, a greater degree of error correction may withstand more severe damage to the QR tag than a lower one. E.g., level L indicates that QR data may be properly restored by barcode reader while distortion of QR tag is kept to less than 7% of its original size. Whereas level H implies that QR data may be decoded by a barcode scanner, it also shows that 30% of the QR tag is destroyed. A codeword in this context denotes eight modules. Similarly, binary numbers zero and just one are represented by the white and black modules, correspondingly.

Table1 Error correction levels

Error correction Level	Recovery Capacity %
L	7 parcent
M	15 parcent
Q	25 parcent
H	30 parcent

Table 2. Complete comparison among related schemes & proposed schemes.

Approaches	[(Chung, Chen and Tu, 2009)],(Wang, 2009)	[12, 13]	Proposed
Applications	Image hiding	Image hiding	Secret hiding
Embedding	domain Frequency	Spatial	Spatial
Computational complexity	High	Low	Low
Operation upon QR code No	No	No	Yes
Module-based	No	No	Yes
Utilizing error correction capability	No	No	Yes
Robustness	-	-	High
Secret payload	-	-	Larger than tc bits

Table 2 depicts a complete comparison of the two methods under consideration. (Chung, Chen and Tu, 2009),(Wang, 2009) as well as the suggested scheme Unlike the standard concealing and watermarking strategies, this one is a little more creative. (Huang, Chang and Fang, 2011), Directly inside the QR tag's components, the new technique embeds the secret information. (Dey *et al.*, 2012). The secret extraction method of the proposed system is thus viable for barcode scanners. The novel technique has a low computing cost and may be used to develop apps for mobile device platforms. The secret payload of the planned technique is dynamic, & it can be expanded in response to higher settings for QR versions or error correction levels, among other factors. The developed technique is utilized for embedding secret bits into a QR tag in quantities more than tc, as seen in Table 2. As a result, the suggested approach has the potential to improve the embeddable secret payload over recent work.

III. CONCLUSION

Private information encoded QR codes may be hidden using a variety of techniques. The majority of these strategies were covered in this study. Almost all of the approaches demonstrated acceptable performance metrics. When

Steganography is used in conjunction with encryption techniques such as AES and RSA, it is discovered that the results are much more promising. Private information is likewise protected by high-end data security measures using these. Numerous stenographic techniques in QR codes have become more efficient and easier as a result of the increasing usage of mobile phones & tablets. A colour QR code hidden inside a colour picture is called steganography. After being encrypted, the QR code picture containing the original data is watermarked and placed over a colour image. To retrieve the original data from a Stegoimage, De-Watermarking is used to retrieve and decode the colour QRC data image, which is then used to decrypt the actual information. It is proposed in this study to use QRC as containers in that payload may be hidden, hence enabling a steganographic system. Rather of putting the payload in a picture, we embed the payload inside a QR code instead. It is possible to read messages included inside the created QRC using any QR reader. A created QRC e is legitimate, meaning that it is identical to any other standard QRC, which creates it an excellent container for concealing the payload of a message or data. Aside from that, the message is completely separate from the payload, and it can be utilised to deceive the adversary. In testing, it was discovered that the QR codes created were almost indistinguishable from standard QR codes.

References

Alajmi, M. *et al.* (2020) 'Steganography of Encrypted Messages Inside Valid QR Codes', *IEEE Access*. doi: 10.1109/ACCESS.2020.2971984.

Chung, C. H., Chen, W. Y. and Tu, C. M. (2009) 'Image hidden technique using QR-barcode', in *IIH-MSP 2009 - 2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. doi: 10.1109/IIH-MSP.2009.119.

Dey, S. *et al.* (2012) 'Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm', *International Journal of Modern Education and Computer Science*. doi: 10.5815/ijmecs.2012.06.08.

Hajduk, V. *et al.* (2016) 'Image steganography with using QR code and cryptography', in *2016 26th International Conference Radioelektronika, RADIOELEKTRONIKA 2016*. doi: 10.1109/RADIOELEK.2016.7477370.

Huang, H. C., Chang, F. C. and Fang, W. C. (2011) 'Reversible data hiding with histogram-based difference expansion for QR code applications', *IEEE Transactions on Consumer Electronics*. doi: 10.1109/TCE.2011.5955222.

Jude Hemanth, D. *et al.* (2017) 'Analysis of wavelet, ridgelet, curvelet and bandelet transforms for QR code-based image steganography', in *2017 14th International Conference on Engineering of Modern Electric Systems, EMES 2017*. doi: 10.1109/EMES.2017.7980396.

Lin, P. Y. and Chen, Y. H. (2016) 'QR code steganography with secret payload enhancement', in *2016 IEEE International Conference on Multimedia and Expo Workshop, ICMEW 2016*. doi: 10.1109/ICMEW.2016.7574744.

M, M. and R, B. (2017) 'Hide and Seek: A New Way to Hide Encrypted Data in QR Code Using the Concepts Steganography and Cryptography', *IJARCCE*. doi: 10.17148/ijarcce.2017.6697.

Mendhe, A., Gupta, D. K. and Sharma, K. P. (2018) 'Secure QR-Code Based Message Sharing System Using Cryptography and Steganography', in *ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications*. doi: 10.1109/ICSCCC.2018.8703311.

Ramya, V. and Gopinath, G. (2015) 'Review on quick response codes in the field of information security (Analysis of various imperceptibility characteristics on grayscale and binary QR code', in *2014 International Conference on Advances in Engineering and Technology, ICAET 2014*. doi: 10.1109/ICAET.2014.7105222.

Sun, Y., Yu, M. and Wang, J. (2020) 'Research and Development of QR Code Steganography Based on JSteg Algorithm in DCT Domain', in *2020 IEEE 15th International Conference on Solid-State and Integrated Circuit Technology, ICSICT 2020 - Proceedings*. doi: 10.1109/ICSICT49897.2020.9278285.

Wang, J.-W. (2009) 'Nested image steganography scheme using QR-barcode technique', *Optical Engineering*. doi: 10.1117/1.3126646.