SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Enhancing Secure QR Code Steganography through Artificial Intelligence: A Conceptual Framework

Nuur Alifah Roslan[1,*], Maya Silvi Lydia[2], Adnan Gutub[3]

[1] Department of Multimedia, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia
[2] Department of Computer Science, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia
[3] Cybersecurity Department, College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia

ARTICLE INFO

Keywords:
QR code; steganography; convolution neural network; deep learning; artificial intelligence

ABSTRACT

The incorporation of modern barcode decoding technology into smartphones allows for the extraction of data contained inside QR codes. The use of QR codes for transmitting confidential information, such as e-tickets, discounts, and other sensitive data, raises worries about potential security risks. It is imperative to employ resilient QR code algorithms to guarantee the security of QR code applications in response to this challenge. This study presents a method for achieving product authentication through data concealing. The strategy involves using user data to generate a QR (Quick Response) code, which is then embedded into the product logo picture. The embedded QR code is not visible to the human eye. QR codes are renowned for their robust error-correcting system and excel in concealing random information. Convolutional neural networks (CNN) are a type of deep neural networks that enable the analysis of visual images and the recognition of patterns. The aim of this article is to employ the CNN method to conceal a QR code within the logo picture of a user's products. The suggested model consists of two Convolutional Neural Networks (CNNs), namely an encoder CNN and a decoder CNN. The role of the encoder Convolutional Neural Network (CNN) is to integrate the QR code into the user's product logo picture and produce an output image that closely resembles the original user image. The job of the decoder convolutional neural network (CNN) is to take the output of the encoder CNN as input and produce the embedded QR code picture as output. Our technique incorporates advanced security measures and conceals sensitive information, thereby preventing the unauthorized replication and misuse of the QR code.

1. Introduction

Technology is evolving at such a rapid pace that innovation is outpacing our ability to adapt. Changes occur constantly in this era of rapidly developing technology, and the creation of smartphones has cultivated such improvements as people are more connected now than ever before due to the Internet. The surge in online activity since Industry 4.0, coupled with quick technological advancements, highlights the imperative for safe data transmission in an age of incessant digital

* *Corresponding author.*
E-mail address: nuuralifah@upm.edu.my

https://doi.org/10.37934/araset.62.4.224231

communication [1]. Today's barcode decoders on smartphones can retrieve the data contained in QR codes. The other issues addressed is where with the emerging trends in mobile and wireless technology, QR code provide a powerful tool for combating the practice of product counterfeiting [2]. There are also many emerging research and development using the QR codes as the authenticity of a products in market [3].

Current QR code solutions, however, are unable to solve the security issues when the information needs to remain private for the user [4]. Mobile devices can read the data contained from the QR code and transmit it to the public. However, the crucial issues are the integrity of the QR code could be the challenge. The ownership of digital images or the embedding of secrets into digital images, however, has been the focus of several studies on the concealment of sensitive information [5-7]. Instead of immediately embedding or safeguarding the QR code, we proposed a strategy used steganography methods based on traditional media by enhancing the security through Convolutional neural networks (CNN) in the approach. Additionally, QR codes must be promptly decoded by scanning tools like cell phones, tablets, or barcode scanners because they have set encoding and decoding criteria. Therefore, by manipulating the QR code and then embedding the ownership information will be tagged the QR code authenticity to who it's belong or referenced.

Steganography is a method employed to securely convey information, conceal data, and avoid interception by embedding it inside pictures and delivering them discreetly [8]. It is observed as the primary method of protecting information security by concealing a confidential message (payload) within an innocuous file (container) in order to covertly transport the payload without detection by the adversary. Steganographic techniques just utilize the container to conceal the payload [9]. Therefore, we are proposing a technique which using the user data (ownership information) to build a QR code, which is embedded into the product logo. The embedded QR code is invisible. QR codes are known for its error-correcting system and random information concealment [10]. Meanwhile, the deep neural network like CNN is able to automatically extract a variety of visual characteristics [11]. Therefore, we employ the CNN method to implement a steganographic method.

The structure of this paper is as follows; Section 2 provides a Literature Review, with subsections discussing Conventional Neural Network (CNN) Steganography and QR Codes. Section 3 presents the Proposed Framework, which includes a detailed explanation of the framework and the settings of the proposed training model. Finally, the Conclusion outlines future directions for the proposed framework.

2. Literature Review

2.1 Conventional Neural Network Steganography (CNN)

The rapid advancements in the field of artificial intelligence encouraged the researcher to redirect their interest towards deep learning-based steganography [12]. In deep learning, a neural network is optimized to minimize the amount of error in an objective function. This is often accomplished by employing large number of neural network layers. A neural network that is frequently utilized is known as a convolutional neural network (CNN). This neural network is frequently utilized with pictures to recognize and respond to a variety of spatial patterns [13]. Convolutional Neural Networks (CNNs) are neural networks that are known for their high effectiveness and are typically regarded as a type of regularised Multilayer Perceptrons (MLPs) [14]. The phrase "convolutional neural network" indicates that these networks employ a mathematical technique called convolution. Convolution is a precise linear process that measures the extent of overlap between one function as it moves over another.

In Convolutional Neural Networks (CNNs), the process of convolution is used instead of general matrix multiplication in at least one layer of the network. It is possible for the system to acquire the capability of recognising prominent patterns in images by utilising a Convolutional Neural Network (CNN) or any other type of deep neural network. As a consequence of this, the network is able to identify and maximise the usage of data that is kept in regions that are not necessary. In this way, it is possible to increase the amount of information that is concealed. Due to the fact that the system and credentials may be generated in a random manner, individuals who do not possess the relevant credentials are unable to obtain the concealed information [14].

CNN-based image steganography draws influence from encoder-decoder design. The encoder uses the cover picture and secret image as inputs to build the stego image, which is then used by the decoder to output the embedded secret image. The core premise remains the same, with the exception that different techniques have experimented with various structures. The way the input cover picture and secret image are concatenated varies depending on the technique, thus changes in the convolutional and pooling layers are to be expected. The number of filters, strides, filter size, activation function, and loss function vary between methods. It's vital to notice that the cover image and secret image must be the same size. This ensures that every pixel of the secret image is dispersed within the cover image [15].

There are numerous advantages that CNN-based architectures offer in the field of steganography, as demonstrated by studies [16-19]. There are numerous advantages that CNN-based architectures offer in the field of steganography. These advantages include greater payload capacity, robust security features, and the ability to generalise over a wide range of data formats. The SteganoCNN approach in previous study by Duan *et al.,* [16] utilises a dual-branch encoder to incorporate two secret images into a single carrier image. The encoder employs convolutional layers to acquire hierarchical information, which are subsequently merged and integrated into the carrier image. The decoder branch utilises convolutional and deconvolutional layers to restore the original pictures from the encoded carrier. This technique demonstrates great generalisation abilities and accommodates multiple data formats, resulting in high fidelity in reconstructed images.

CNNs have the potential to be used in a variety of applications, including steganography and cybersecurity, as demonstrated by the excellent accuracy achieved by the CNN-based architecture in network attack detection. For the aim of improving the efficiency of intrusion detection systems, Mohammad *et al.,* [17] makes use of a straightforward CNN-based architecture that is extended with data augmentation approaches. Convolutional layers are utilised by the CNN for the purpose of feature extraction, and later on, fully linked layers are utilised for classification.

The encoder Convolutional Neural Network (CNN) identifies distinctive characteristics from both the secret and carrier images and merges them to create a steganographic image. The decoder Convolutional Neural Network (CNN) reconstructs the hidden image from the steganographic image [18]. CNNs are shown to be effective in securely embedding and extracting concealed data, as demonstrated by the method's ability to attain high payload capacity and robust steganalysis resistance. Through the utilisation of an encoder-decoder architecture, Mohammad *et al.,* [17] proposes a CNN-based steganography technique that is both effective and efficient. In the encoder, the secret image is embedded into the carrier image through the use of many convolutional layers. On the other hand, the decoder is responsible for reconstructing the secret image through the use of deconvolutional layers. The approach provides better performance in terms of payload capacity and image quality, ensuring minimum distortion and great security in steganographic operations.

2.2 QR Code

Denso Wave, a Toyota company, created QR codes mainly to monitor automobiles as they were being made. The capacity to hold more data and scan quickly from any angle was the original selling point of quick response (QR) codes compared to more conventional barcodes [9]. This increased data capacity and scan speed made QR codes highly versatile and efficient. QR codes can encode various types of information, such as alphanumeric and control codes. A phone number, a URL and an ID are examples of information that can be embedded in QR codes. It's can hold typically 50 characters long, but the new, denser format allows for up to 1264 characters [19].

QR codes are a convenient and simple method to transmit information. To scan the QR code, simply take a photo with your mobile. They achieved great success in the advertising and marketing industry. They may be seen everywhere, including food labels and large advertising signs [9]. The majority of QR-related research [9,20-23] that has been conducted in recent times has utilised the conventional method of image concealment or the conventional steganography approach. Alajmi *et al.,* [9] describes a system that efficiently combines encryption with steganography, employing QR codes to hide and communicate hidden data safely. The approach's novel use of legitimate, decoy-containing QR codes improves its resilience, making it a potential solution for secure information transmission. The potential of it to create genuine QR codes that are indistinguishable from regular ones, hence reducing the probability of discovery, is one of its main benefits. Furthermore, providing deceptive communications adds an extra layer of protection, possibly misleading adversaries and strengthening the system's overall adaptability.

Furthermore, Mathivanan [24] present a novel color picture stego-crypto approach that improves data embedding capacity, security, and robustness. The suggested method uses base64 encoding to turn secret data into a QR code, which is then embedded into a color picture's red, green, and blue components via a dynamic bit replacement methodology. This approach employs three layers of protection, including pixel permutation and logistic chaos-based encryption, to provide significant resistance to brute force, statistical, and differential attacks. The suggested stego-crypto technique provides a strong way to protect data in colour images, allowing for the inclusion of a lot of data while remaining undetectable and resistant to attacks. Meanwhile, Andrejčík *et al.,* [20] proposed a method in which a QR code containing a confidential message is inserted into the least significant bit (LSB) of a cover picture, creating a steganographic image. The procedure entails altering the dimensions of the QR code, transforming it into a binary format that is appropriate for LSB embedding, and employing an XOR operation to merge the QR code with the cover picture.

The recent research proposed by previous researchers [21-23]. Narayanan *et al.,* [21] research utilises several encryption techniques to provide layered security. It also incorporates the encrypted data into QR codes to provide increased protection. On the other hand, the technique separates the input text into segments encoded in different modes, using empty segments to hide data and guaranteeing resilience through error correction [23]. Narayanan *et al.,* [21] approach provides enhanced security and flexibility, but it may require significant computational resources and pose difficulties for individuals without expertise in the field. Meanwhile, Koptyra and Marek [22] technique is characterised by its effective use of space and its high level of resilience in mistake correction. However, it may be susceptible to discovery through sophisticated analysis and requires a complex implementation process. The pros and limitations of each technique are determined by the unique security, stealth, and technological capabilities required for a particular application.

Besides, Narayanan and Prabhu [23] use several encryption methods to improve QR code security against counterfeiting. It combines the Advanced Encryption Standard (AES) algorithm, the Rubik's Cube Principle, and visual steganography. AES encrypts 128-bit data blocks with keys of variable

lengths, utilising rounds of replacement, permutation, and mixing to provide durable encryption. Then, by implementing the Rubrik's Cube principals, it scrambles picture pixels in the same way that you would manipulate a Rubik's Cube, considerably boosting the complexity and security of the encrypted image. picture steganography conceals data under a cover picture, making the QR code's existence less obvious.

The QR code picture is split into RGB channels, each channel is encrypted using AES using the Rubik's Cube Principle, and the channels are then recombined into a single encrypted image. This multilayer encryption provides robust security and data hiding. The suggested multi-encryption solution has improved security since it combines AES, Rubik's Cube scrambling, and steganography, making decryption impossible without specialised keys and algorithms. It obtains a high NPCR (Number of Pixel Change Rate) of 99.79%, showing great resilience to statistical assaults and a strong defence against unauthorised data extraction.

However, the technique has limitations, such as computational complexity due to its multi-layered process, increased processing time and resource consumption, key management issues, and potential difficulties in applying the Rubik's Cube Principle to multi-tone images like RGB, which complicates encryption and decryption. Addressing these issues can help to enhance the security and efficiency of the proposed multi-encryption method for QR code anti-counterfeit measures. Based on past research, we can conclude that the QR Code properties may be useful for picture steganography. As a result, our goal is to offer QR Code CNN Steganography to improve the security of QR Steganography by using the CNN Steganography technique.

3. Proposed Framework

3.1 QR Code CNN Steganography

The QR code consisting of the user's product ownership information, and then we will embed the generated QR are into the user's product logo image such that the very existence of the QR will be invisible. The QR Code will embed with the ownership information as a value and identical data of the product. We proposed to employ the CNN method to conceal a QR code within the logo picture of a user's products. There are two stages in the proposed method: generating the QR Code and the CNN Encoding and CNN Decoding stage. Figure 1 below shows the model of our proposed work.

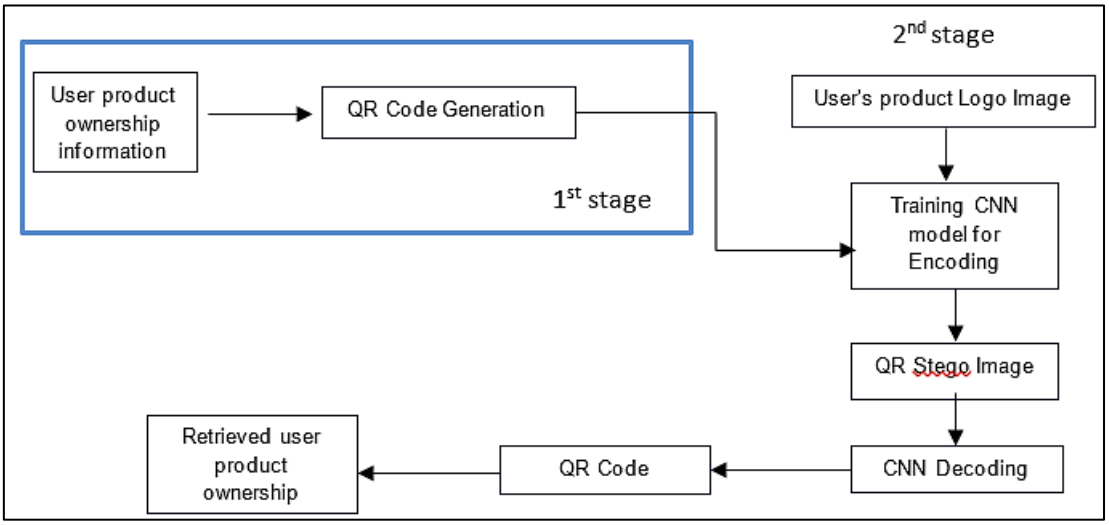

Fig. 1. QR code CNN steganography model

Figure 1 above show s QR Code CNN Steganography Model, divided into two primary stages: QR Code Generation and CNN-based Steganography. In the first stage, user product ownership information serves as the initial input, from which a QR code is generated. This stage ensures that the QR code accurately encapsulates the ownership details. In the second stage, the user's product logo image is utilized to hide the QR code. A Convolutional Neural Network (CNN) model is trained for encoding, which involves learning to embed the QR code into the product logo image in a manner that is not easily detectable. The result of this encoding process is the QR Stego Image, where the QR code is securely concealed within the product logo image.

For retrieval, the QR Stego Image undergoes CNN decoding to extract the hidden QR code. The extracted QR code is then retrieved from the QR Stego Image. Finally, this QR code is used to accurately restore the user product ownership information, ensuring that the original data is precisely recovered. This model employs a robust two-stage process for securely embedding and extracting QR codes within product logo images using CNN-based steganography, providing an effective method for concealing and retrieving ownership information.

3.2 Training CNN Model

The proposed CNN training model was suggested to use the subset of two thousand (2000) images from the Tiny ImageNet dataset, each image has dimensions 64x64x3. Two photos are randomly selected from the ImageNet dataset to train this model. Distributing these photographs 1:2, so this way; half are utilized as cover-pictures and the other secret image. On the dataset, we use Keras image library and Adam optimiser to start with processing. Fetching the secret image features: The Prep network of the Encoder CNN is used to extract the secret from an input, and we will use both as pairs for forming dataset using Hidden's output.

At that stage, the two images are converted to a 64 x 64 resolution and normalisation occurs for the colour image with pixel values from between 0-255 is fed into the CNN. The implementation must design a canopy photo in an effort to have the hidden snap and make it visually consistent with that cap image. The second stage will comprise of taking the image from our output container and feeding it to Decoder CNN in order to retrieve what was initially hidden. At the same time, we will train both encoding and decoding convolutions of CNNs jointly updating their weights.

Once the model is tuned, it will be used to insert QR codes into colour photos for reuse. Tiny ImageNet is the source of the cover image, and we will a generate secret images for the QR code. These datasets will now be used to train the CNN model as we did earlier. This CNN model will allow us to embed our QR code image into the User logo Image, and from the container image, we will retrieve the embedded QR image. Initially, the User logo Image and QR code image are required to be given as input for the Encoder CNN. As a result, this CNN will generate the embedded image. Finally, this generated embedded image will then be inputted to the decoder CNN, generating the restored image.

4. Conclusions

This may potentially yield many alternative novel concepts but also with a significant contribution. We generated a system that merged steganography approaches from traditional media and, by integrating it with neural networks (CNN), provided robust security. This approach was offered as a compromise between embedding or protecting the QR code outright. Since QR codes have predetermined encoding and decoding attributes, they must be decoded quickly using scanners such as smartphones, tablets, or barcode readers. This will potentially link ownership or references

to the individuals when authenticating the QR code, if it remains valid after altering a part of it and appending their possession info. For a future works, we will look forward a trained data and analyse the results based on this proposed conceptual framework.

Acknowledgement
The authors wish to express they're thanks to one and all who supported them during this work. The authors received no specific funding for this study. The authors declare that they have no conflicts of interest to report regarding the present study. This research was funded by a grant from Universiti Putra Malaysia (GP-IPM Grant Project Code: GP-IPM/2022/9740200).

References

[1] Hassan, Md Maruf, R. Badlishah Ahmad, Naimah Yaakob, Ong Bi Lynn, and Nur Farhan Kahar. "An enhanced dual-layer video steganographic approach: Enhancing security and imperceptibility." *Journal of Advanced Research in Applied Sciences and Engineering Technology* (2024): 1-19. https://doi.org/10.37934/araset.58.1.119

[2] Bala Krishna, M., and Arpit Dugar. "Product authentication using QR codes: a mobile application to combat counterfeiting." *Wireless Personal Communications* 90 (2016): 381-398. https://doi.org/10.1007/s11277-016-3374-x

[3] Yang, Jing, and Ava Francesca Battocchio. "Effects of transparent brand communication on perceived brand authenticity and consumer responses." *Journal of Product & Brand Management* 30, no. 8 (2021): 1176-1193. https://doi.org/10.1108/JPBM-03-2020-2803

[4] Xiong, Lizhi, Xinwei Zhong, Neal N. Xiong, and Ryan Wen Liu. "QR-3S: A high payload QR code secret sharing system for industrial Internet of Things in 6G networks." *IEEE Transactions on Industrial Informatics* 17, no. 10 (2020): 7213-7222. https://doi.org/10.1109/TII.2020.3044006

[5] Lin, Pei-Yu. "Distributed secret sharing approach with cheater prevention based on QR code." *IEEE Transactions on Industrial Informatics* 12, no. 1 (2016): 384-392. https://doi.org/10.1109/TII.2015.2514097

[6] Dragoi, Ioan Catalin, and Dinu Coltuc. "On the security of reversible data hiding in encrypted images by MSB prediction." *IEEE Transactions on Information Forensics and Security* 16 (2020): 187-189. https://doi.org/10.1109/TIFS.2020.3006382

[7] Puteaux, Pauline, and William Puech. "A recursive reversible data hiding in encrypted images method with a very high payload." *IEEE Transactions on Multimedia* 23 (2020): 636-650. https://doi.org/10.1109/TMM.2020.2985537

[8] Devi, V. Anjana, I. Bhuvaneshwarri, C. Santhosh Kumar, V. Chandrasekar, V. Kalaichelvi, E. Anitha, and Jogendra Kumar. "Reliable and secure data transfer in IoT Networks using Knight-Tour and PHLSB Method." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 2 (2023): 107-118. https://doi.org/10.37934/araset.32.2.107118

[9] Alajmi, Masoud, Ibrahim Elashry, Hala S. El-Sayed, and Osama S. Farag Allah. "Steganography of encrypted messages inside valid QR codes." *IEEE Access* 8 (2020): 27861-27873. https://doi.org/10.1109/ACCESS.2020.2971984

[10] de Seta, Gabriele. "QR code: The global making of an infrastructural gateway." *Global Media and China* 8, no. 3 (2023): 362-380. https://doi.org/10.1177/20594364231183618

[11] Selvaraj, Arivazhagan, Amrutha Ezhilarasan, Sylvia Lilly Jebarani Wellington, and Ananthi Roy Sam. "Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning based techniques." *IET Image Processing* 15, no. 2 (2021): 504-522. https://doi.org/10.1049/ipr2.12043

[12] Ghamizi, Salah, Maxime Cordy, Mike Papadakis, and Yves Le Traon. "Adversarial Embedding: A robust and elusive Steganography and Watermarking technique." *Arxiv Preprint Arxiv:1912.01487* (2019). https://doi.org/10.48550/arXiv.1912.01487

[13] Havard, Andrew, Theodore Manikas, Eric C. Larson, and Mitchell A. Thornton. "CNN-Assisted Steganography--Integrating Machine Learning with Established Steganographic Techniques." *arXiv preprint arXiv:2304.12503* (2023). https://doi.org/10.48550/arXiv.2304.12503

[14] Sharma, Kartik, Ashutosh Aggarwal, Tanay Singhania, Deepak Gupta, and Ashish Khanna. "Hiding data in images using cryptography and deep neural network." *Arxiv Preprint Arxiv:1912.10413* (2019). https://doi.org/10.33969/AIS.2019.11009

[15] Subramanian, Nandhini, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane. "Image steganography: A review of the recent advances." *IEEE Access* 9 (2021): 23409-23423. https://doi.org/10.1109/ACCESS.2021.3053998

[16] Duan, Xintao, Nao Liu, Mengxiao Gou, Wenxin Wang, and Chuan Qin. "SteganoCNN: Image steganography with generalization ability based on convolutional neural network." *Entropy* 22, no. 10 (2020): 1140. https://doi.org/10.3390/e22101140
[17] Mohammad, Rasheed, Faisal Saeed, Abdulwahab Ali Almazroi, Faisal S. Alsubaei, and Abdulaleem Ali Almazroi. "Enhancing intrusion detection systems using a deep learning and data augmentation approach." *Systems* 12, no. 3 (2024): 79. https://doi.org/10.3390/systems12030079
[18] Kich, Ismail, Youssef Taouil El Bachir Ameur, and Amine Benhfid. "Image steganography by deep CNN auto-encoder networks." *International Journal* 9, no. 4 (2020). https://doi.org/10.30534/ijatcse/2020/75942020
[19] Amoah, Godwin Awuah, and J. B. Hayfron-Acquah. "QR Code security: mitigating the issue of quishing (QR Code Phishing)." *International Journal of Computer Applications* 184, no. 33 (2022): 34-39. https://doi.org/10.5120/ijca2022922425
[20] Andrejčík, Samuel, Ľuboš Ovseník, Jakub Oravec, Norbert Zdravecký, and Maroš Lapčák. "Image steganography with using QR code." In *2022 IEEE 16th International Scientific Conference on Informatics (Informatics)*, p. 29-32. IEEE, 2022. https://doi.org/10.1109/Informatics57926.2022.10083471
[21] Narayanan, S. Dhivyalakshmi, S. Prabhu, and E. Padma. "Improving QR Code security using multiple encryption layers." In *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS)*, p. 845-848. IEEE, 2024. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533884
[22] Koptyra, Katarzyna, and Marek R. Ogiela. "Information Hiding in QR Codes using Segment Manipulation." In *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, p. 397-400. IEEE, 2024. https://doi.org/10.1109/PerComWorkshops59983.2024.10502885
[23] Narayanan, S. Dhivyalakshmi, and S. Prabhu. "Strengthening QR code Anti-Counterfeit through Multi-Encryption Algorithm." In *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS)*, p. 864-866. IEEE, 2024. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533943
[24] Mathivanan, P. "QR code based color image stego-crypto technique using dynamic bit replacement and logistic map." *Optik* 225 (2021): 165838. https://doi.org/10.1016/j.ijleo.2020.165838