Secure Bilinear Zooming Steganography for Enhancing QR Code Image Quality and Information Security

Nuur Alifah Roslan
Multimedia Department
Universiti Putra Malaysia, Malaysia
nuuralifah@upm.edu.my

Adnan Gutub
Cybersecurity Department,
Umm Al-Qura University, Saudi Arabia
aagutub@uqu.edu.sa

Rahmita Wirza Rahmat
Multimedia Department
Universiti Putra Malaysia, Malaysia
rahmita@upm.edu.my

Fatimah Khalid
Multimedia Department
Universiti Putra Malaysia, Malaysia
fatimahk@upm.edu.my

Nur Izura Udzir
Computer Science Department
Universiti Putra Malaysia, Malaysia
izura@upm.edu.my

Abstract: *The convenience and high data storage capacity of Quick Response (QR) codes have contributed to the ubiquity of these codes in this era of advanced technological advancement. However, there have been growing security concerns in the application of QR codes for communicating private data. Therefore, the current study proposed a secure Bilinear Zooming Steganography Quick Response Code (BZSQRC) algorithm that can manipulate QR code images by encoding a secret message using a secure Least Significant Bit (LSB) algorithm. The Peak Signal-to-Noise Ratio (PSNR) of the BZSQRC algorithm was 6.5% higher than that of the conventional LSB two-bit technique, which indicated enhanced steganographic image quality. An average noise reduction evaluation yielded a mean squared error as low as 0.0025. The proposed algorithm effectively compressed the module size of the QR code before embedding, which allowed QR codes with different module sizes in this study to be embedded into the same area. This study successfully demonstrated that the developed BZSQRC algorithm enhanced the PSNR and retained the readability and robustness of the QR code. It is recommended for future research to further augment the security layer by integrating secret keys and encryption*.

Keywords: *QR code steganography; QR code; image manipulation; information security; steganography*.

Received February 04, 2025; accepted .December 02, 2025
https://doi.org/10.34028/iajit/23/4/1

1. Introduction

The practicality and high data storage capacity of Quick Response (QR) codes have contributed to their extensive application in daily routines [41]. QR codes can be read and transmitted publicly using smartphones, but the current QR code solutions are associated with critical security concerns related to user privacy [3, 24, 55, 59]. Although QR codes serve as a necessary and powerful means to deal with product counterfeiting based on recent wireless technology advancements [11], the integrity of these codes remains in question.

Scanning tools (e.g., barcode, smartphone, and tablet) are utilised to promptly decode the QR codes that come with encoding and decoding criteria. Hence, the authenticity of the QR codes can only be established by manipulating the codes and embedding the essential information. There have been studies on digital image ownership or embedding secret messages into digital images for concealing sensitive information, but steganography methods based on traditional media are preferred over immediate embedding or QR-code safeguarding [18, 22, 23, 28, 29, 32, 38].

Steganography, which is derived from the ancient Greek root words of steganos (“covered” or “protected”) and graphei (“writing”), refers to “covered writing” [40]. Essentially, the foundational method of steganography consists of cover medium, confidential information, and the embedding process. Digital steganography method is capable of dealing with information in different forms of digital media, including text, audio, images, and videos.

The secure Least Significant Bit (LSB) approach is regarded as the most basic steganographic technique when it comes to utilising the QR code images [33]. This approach involves the substitution of the secret information bit with the least important piece of container files [9]. Unlike the original approach, a modified version of the LSB pixel or bit-planes has been increasingly utilised in today’s steganographic techniques. Optimised payload and enhanced visual quality and undetectability based on the simplicity of LSB embedding concurrently have propelled the development and expansion of these techniques [23]. Furthermore, in order to enhance the security level of the LSB approach, numerous prior studies integrated it with random parameters, Advanced Encryption

Standard (AES) compression method, and encryption algorithms Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography encryption [9, 33, 40].

Conventional QR code scanners should not be able to detect the embedded data, which makes the effectiveness of steganography highly crucial. Achieving this necessitates seamless incorporation of data in advanced algorithms without any visible artefacts or distortions [58]. However, when cameras are utilised to print and scan QR codes, frequency domain QR code steganography [17, 53] is susceptible to distortion issues. The excessive complexities of other approaches using homomorphic encryption [36] or stego-crypto techniques [34] have made them not practical for real-time use. Despite the improved robustness, spatial domain methods and QR error correction embedding possess limited data capacity. Additionally, the open nature of QR code scanning comes with security risks, especially when sensitive information are involved [49].

In view of the above, the current study proposed a secure Bilinear Zooming Steganography Quick Response Code (BZSQRC) algorithm that can manipulate QR code images by encoding a secret message using a secure LSB algorithm. Unlike frequency-based methods, the proposed BZ method does not introduce scanning distortion and even improves image manipulation. Its combination with LSB in this study served to introduce secure and lightweight data embedding, making it highly practical for real-time use. The proposed method introduced data embedding in a less detectable manner, optimising payload and strengthening confidentiality. More importantly, the proposed method in this study served to maintain the visual and functional integrity of QR codes, making it highly applicable for secure transactions, identity verification, and other sensitive applications.

The following sections review related literature, describe the methodology adopted in this study, and present and discuss the obtained results, conclusion, and recommendations for future research.

2. Related Works

Prior studies employed different image processing techniques, such as Discrete Wavelet Transform (DWT) [32, 36], Discrete Cosine Transform (DCT) [17], and the Discrete Fourier Transform (DFT) [17, 53], to assess the security of QR codes. These techniques involve converting QR code images into frequency domain and incorporating watermarks into the unique variables of these QR code images. The conventional techniques do not cater for printed QR codes on printed materials (e.g., posters or hard paper), as the scanning environment of cameras may distort the resulting QR code images.

Mittal *et al*. [36] employed the DWT technique for the steganography process to enhance the encryption layer. The Nth Degree Truncated Polynomial Ring Unit (NTRU) homomorphic encryption algorithm was utilised to encrypt the client's data. Through this encryption technique, QR codes and cover pictures were utilised to prevent attackers from reading the data.

In another study, QR codes were proposed as vessels for hidden data, and the DWT technique was utilised to break down the cover image into frequency components for discreet data embedding [32]. The data embedding process was directed by machine learning, particularly Recurrent Neural Networks (RNNs), for enhanced imperceptibility and durability, which ensured the close resemblance of the stego image to the original data without compromising the precision of data extraction.

Meanwhile, Mathivanan and Balaji Ganesh [34] regarded QR codes as the first-level encryption procedure and employed the stego-crypto technique. The process then involved substituting the dynamic bit approach as part of the second-level security by embedding individual QR codes into the colour image components of Red (R), Green (G), and Blue (B) prior to their integration with a randomisation function for added security.

Besides that, Sun., *et al*.'s [49] JSteg steganography method for embedding and extracting QR codes was found effective against noise attacks and facilitated the retrieval of QR codes after they were destroyed. The study further noted the prospects of correctly embedding and retrieving every QR code image generated by various input data information.

A novel type of colour QR code, specifically known as the Halftone Multifunctional Colour QR (HMC-QR) code, was proposed in one of the prior studies [23]. This technique was reported to have the capacity to integrate multiple types of information into a single QR code, combining both hidden (for traceability and anti-counterfeiting information) and visible (for advertisements or public queries).

Another prior study attempted to incorporate hybrid halftone dots into QR codes [22], which allowed the scanning of these dots that were invisible to the human eye from a distance. Amplitude Modulation (AM) dots represented the black modules of the QR codes, whereas Frequency Modulation (FM) dots represented the white modules of the QR codes. The study described the substantial dependence of both methods on the precise control of the dot area percentages. QR codes may be unreadable if the balancing appeared to be off. In other words, any minor printing errors or variations in the printing process can result in critical usability issues.

Apart from that, there have been studies on blind QR code steganographic approaches based on error correction capability [15, 17, 53, 54, 56]. These prior studies addressed the correction properties of QR codes and enhanced the QR module to embed secret messages. In most cases, a standard scanning device is first utilised to read the QR code data content from recently generated QR codes. Secret messages can then be

extracted by authenticated recipients from these tagged QR codes. However, the maximum payload of the secret messages equals to the error tolerance of the QR codes although this proposed scheme is applicable to standard mobile and scanning devices. Addressing that, Luo *et al.* [31] proposed a method to increase the payload of embeddable secrets. The study assessed QR codes as containers and payload encoding within the QR codes and found a high PSNR and successful decoding of the QR codes.

With the expanding landscape of Artificial Intelligence (AI), the integration of these technologies into QR code steganography has also been explored in numerous studies. For instance, one of these studies [57] introduced a novel approach of concealing information without perceptibly modifying the images, but the proposed methodology was found to be susceptible to image blurriness, require superior image quality and computational requirements, and involve system complexity. Taking the case of utilising machine learning models like RNNs, significant computational power is required, especially during the training phase using techniques like Back Propagation Through Time (BPTT) [32]. Higher computational cost may result in time-consuming preparation, causing delays for real-time applications like online communication or surveillance. This poses a more critical limitation as compared to simpler steganography methods.

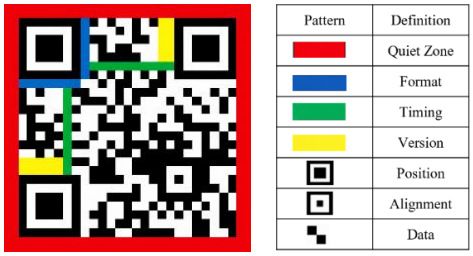
In view of the above, this study observed a significant research gap in protecting confidential information when it comes to QR codes. It is highly challenging to protect private data considering how QR code data content can be easily scanned and retrieved using barcode readers [15, 31, 54]. Moreover, traditional image hiding or steganography methods display critical drawbacks that require additional image processing processors or computers compatible with real-time scanning to directly retrieve QR codes. This has clearly called for a secure QR code-based steganography algorithm, which was addressed in this study by integrating a BZ method in LSB, with the emphasis on developing a novel secure approach of concealing critical message within QR code images.

2.1. Background of Study

2.1.1. QR Code

Back in 1994, Denso-Wave, a Japanese business, introduced the Two-Dimensional (2D) structure of QR barcode concept, which initially served for inventory control in the automotive component manufacturing industry [36]. Today, there are dedicated application programmes in most smartphone brands to scan QR codes. Utilising QR codes to conceal the embedded information is deemed suitable [54]. QR codes are squares with black and white image blocks that are presented in the black (or dark) module (represented as "1") and white (or bright) module (represented as "0") types. These codes possess minimal data, encoding text in numeric, alphanumeric, bits, and Kanji character sets [16]. Figures 1 and 2 show an example of a QR code and its structure [6].

Figure 1. An example of a QR code. Reproduced with permission from reference [6].



a) QR Code structure. b) Legend.

Figure 2. The structure of a QR code. Reproduced with permission from reference [6].

A QR code consists of various key components, such as the quiet zone, formatting information area, timing pattern section, QR code version, position and alignment patterns, and data section [6]. The quiet zone facilitates the detection of symbols, while the vacant region (white space) within the code plays a crucial role for the scanning and interpretation of the QR code. The formatting information area presents the mask pattern and the error correction level employed, whereas the timing pattern section displays a distinctive alternating arrangement of black and white patterns, which facilitate the identification of the central coordinating of individual cells. Likewise, the central coordination of the cell is rectified in instances of distortion or errors within the cellular domain. The subsequent iterations of QR codes also range from versions 1 to 40, with each iteration exhibiting distinct cellular quantities and arrangements.

The QR code image yields a fundamental and significant pattern. The accurate placement of the QR code is determined based on the positioning pattern. Strategic placement of the pattern at its three corners establishes the position, size, and angle of the QR code. This phenomenon can be perceived in a full range of directions, encompassing a complete 360-degree circumference. The black and white cells within the QR code are converted from the encoded data containing binary values of "1" or "0". QR code distortion (particularly nonlinear distortions) is rectified through an alignment pattern, and error correction is made by augmenting the data with Reed-Solomon coding [47]. As for the current study, the structural components of a QR code and its potential as a high-capacity payload for

concealing steganographic information within an image were examined.

2.1.2. Bilinear Zooming Interpolation

In the case of Bilinear Zooming (BZ) interpolation, the nearest 2×2 neighbourhood of four nearest known pixel values surrounding the unknown pixel is computed. The weights are based on the relative distances between the unknown pixel and its neighbours along the x- and y-axes. The calculation of the final interpolated value involves computing a weighted average of: 1) Top-left, 2) Top-right, 3) Bottom-left, and 4) Bottom-right pixels. The row and the column of the resulting image are then expanded by determining the average pixel value between two pixels.

Assuming the pixel value at a point of (x, y)(x, y)(x, y), located between the following four known pixel values in a grid, $f_{00}=f(x_1, y_1)$, $f_{10}=f(x_2, y_1)$, $f_{01}=f(x_1, y_2)$, $f_{11}=f(x_2, y_2)$, as well as $dx=(x-x_1)/(x_2-x_1)$ and $dy=(y-y_1)/(y_2-y_1)$, then the interpolated value f(x, y) is as follows:

$$f_{(x,y)}=(1-dx)(1-dy)\, f_{00}+dx(1-dy)\, f_{10}+(1-dx)dyf_{01}+dx\cdot dy\cdot f_{11}$$

Overall, this method produces good-quality photos and higher smoothness upon zooming [46]. When uniform scaling (e.g., double enlargement) are concerned, the process then simplifies to averaging four surrounding pixel values, which enable efficient and visually appealing image enlargement with enhanced continuity and smoothness. As compared to the nearest-neighbour interpolation, the BZ interpolation offers smoother transitions and reduces pixels.

2.1.3. Image Steganography

Concealing one image within another image is performed through image steganography. The cover image in the image steganography field is manipulated, ensuring the imperceptibility of the concealed information. This technique differs from encryption, as the process avoids suspicion [48]. LSB steganography is a conventional technique of manipulating image pixels [9]. The process identifies the lowest bit in a binary number known as LSB. Fundamentally, it serves to imperceptibly alter the LSB of pixels within the form of an image, audio, or video file to the human eye or ear but still can be detected with specialised software.

In LSB steganography, the LSB of pixels are substituted with the secret message bits that need to be concealed [37]. As the LSB have minor effect on the colour of pixels, the difference is typically imperceptible to the human eye. This allows concealing substantial amounts of data within the image using multiple bits in each pixel.

The simplicity and high embedding capacity are what drive the popularity of the spatial domain for LSB steganography [13, 26, 39, 45]. Its implementation and capability of embedding large amounts of data are generally straightforward as the pixel values of the cover image are directly modified [8, 20]. However, it should be noted that its simplicity leads to certain drawbacks. Firstly, the embedded data are at risk of minimal tampering or compression due to the inherently fragile nature of the LSB modifications. Moreover, the concealed data can be easily extracted or destroyed by statistical or visual steganalysis attacks if there are robust protective mechanisms. These drawbacks reflect the technique's lack of resilience, especially in hostile environments involving data integrity and security [40]. Immamuddinkhan and Kanahasabapathys' [25] method employs bidirectional circular shifting in dual stego-images to achieve reversible steganography. It maps secret data to minimum shift values, optimized via histogram-based transformations before pixel-pair embedding. This achieves superior PSNR and perfect reversibility, ensuring significantly higher image fidelity than traditional spatial techniques. However, its capacity is limited by the exclusion of pixels with high or low intensities to avoid overflow and underflow, and extraction is entirely dependent on the availability of both dual stego-images and the specific histogram transformation data.

Meanwhile [43] method integrates 6-D chaotic encryption with Tabu search to optimize LSB steganography. It achieves improved security via a massive key space and fast processing. However, LSB embedding remains statistically vulnerable to detection. Nevertheless, high PSNR and entropy validate its practical effectiveness.

There have been various recommendations proposed to enhance the LSB steganography, including making use of the transform domain like the DCT [12], DWT [2, 44, 52], and DFT [4, 35]. As compared to spatial techniques, these proposed techniques enhance data robustness by manipulating the frequency components of the image, making them less susceptible to detection and attacks [20].

For instance, the Haar DWT, which was deemed efficient in embedding concealed information, was employed to deal with both cover and payload images [50]. The technique combined the multiresolution features of DWT. The study also incorporated the alpha blending technique, where the alpha parameter served as the scaling factor that regulated the combination of cover and payload image elements. In another study, the integration of DWT and bit-plane slicing method was proposed, which involved breaking down the image into eight different planes, each corresponding to a bit in the pixel's binary representation [19]. Through Elliptic Curve Cryptography (ECC), the most significant bit plane image was scrambled, yielding higher security with smaller key sizes. The scrambled image was embedded into the high-frequency sub-bands of the carrier image, underscoring the substantial role of DWT in the study.

In another study, DWT was implemented to support the generation of a strong hash that can withstand various image processing attacks, such as scaling, low pass filtering, Joint Photographic Experts Group (JPEG) compression, rotation, noise addition, and median/mean filtering [27]. The hashing technique was employed to generate a hash sequence specifically for an image. Besides that, Huffman encoding and image wavelet hashing were employed for the coverless image steganography approach.

Studies have presented evidence on the significant advantages of Haar DWT in steganography. Its capability for multiresolution analysis enables substantial embedding capacity without compromising visual fidelity [2, 7, 52]. Data embedding in the frequency domain contributes to its robustness, strengthening its resistance to compression and image-processing attacks. Moreover, the integration of DWT with other techniques like alpha blending, bit-plane slicing, and image hashing ensures data integrity and invisibility [19, 27, 50]. Besides that, its integration with encryption algorithms like ECC further strengthens payloads at minimal overhead [27]. These attributes boost the efficacy of DWT for secure and high-performance applications in steganography.

The [44] proposed a comparative methodology that evaluates the LSB, DCT, and DWT techniques. LSB possesses a considerable capacity; however, it is inadequate in terms of resilience against alterations. Concurrently, they integrate the method with DCT to improve image quality, while DWT ensures optimal security. Consequently, the choice of a technique is contingent upon achieving a balance between payload requirements and requisite robustness.

Therefore, the BZSQRC algorithm based on the wavelet transform domain of the LSB algorithm was employed in this study. The following section describes the methodology adopted in this study to generate the BZSQRC algorithm.

3. Methodology

As discussed, this study employed the BZ method in LSB to embed essential information. The 2D barcode (QR code) served as the matrix barcode trademark. The secret message and input image in greyscale attributes were defined as the QR code and cover image, respectively. The embedding process of the proposed BZSQRC algorithm is depicted in Figure 3. In this process, QR codes were embedded into the processed input images following the BZ resizing and verification, wavelet transformation, and bit-plane slicing.

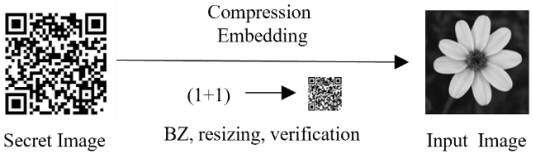


Figure 3. The module size compression used in the proposed BZSQRC algorithm.

Several input data types were encoded through these QR codes. Various attributes could influence the data storage capacity of these code symbols, such as datatype, version (overall symbol dimension), and error correction levels [10]. As shown in Table 1, there were four error correction levels in the QR codes, which indicated the percentages of codewords that could be restored during any disruption. Through imaging devices and repeated application of the Reed-Solomon error correction method [10], the process ensued until these image could be aptly interpreted. Meanwhile, the block diagram of the proposed BZSQRC algorithm (Figure 4) consisted of two main phases, which involved the pre-processing process for the secret and input images and the embedding process.

Table 1. Summary of the QR code symbol attributes.

Attribute	Value
Input data	Numeric, alphanumeric, and binary
Data type	Mode and input character set
Version	1 to 40
Error correction level	Low (7%), medium (15%), quartile (25%), and high (30%)

The framework was designed to embed a QR code as secret message within a cover image by leveraging the frequency-domain transformation and bit-level embedding techniques. In the first phase, the input image, which served as the carrier (cover image), was processed. Through DWT, the input image was decomposed into Low-Low (LL), Low-High (LH), High-Low (HL), and high-high (HH) frequency sub-bands, which enhanced the capacity for imperceptible data hiding. Each of these sub-bands represented different frequency components. DWT facilitated the conversion of the input image from the spatial domain to the frequency domain, which enabled embedding in perceptually less sensitive regions (e.g., higher frequencies) and resultantly, improved both invisibility and robustness.

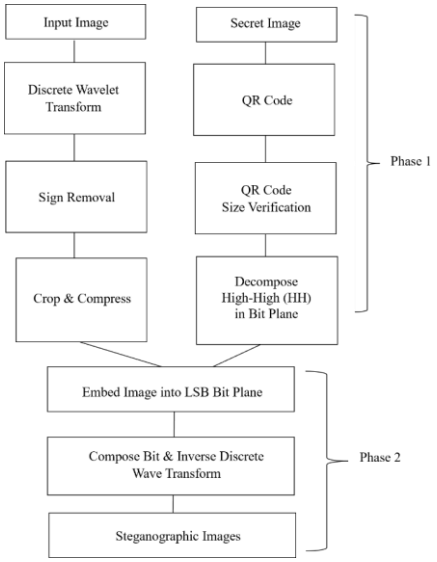


Figure 4. The block diagram of the proposed BZSQRC algorithm.

The process then ensued with sign removal. The presence of positive or negative values (signs) for wavelet coefficients may introduce noise-like behaviour in the embedded data. The removal or normalisation of the signs functioned to simplify the coefficient structure, which ensured no abrupt artifacts in the embedded data, resulting in reduced variability in bit patterns and streamlined LSB embedding process. Following that, crop and compress operations were employed. The process ensured dimensional compatibility between the input image and the secret image (through cropping) and reduced redundancy and control data size (through compression). This particular process was deemed particularly crucial in the case of limited capacity of the host image or for real-time or bandwidth-sensitive applications.

At the same time, the secret image, which was represented as a QR code, was subjected to its own preprocessing pipeline. The process of QR code size verification was augmented with the BZ interpolation to ensure smooth transitions and minimal pixelation. In other words, the structural integrity of the code was retained for readability and accuracy upon extraction, particularly after the compression and embedding operations. The process then ensued with the decomposition of the resized QR code via wavelet analysis, which involved isolating the HH frequency band containing fine details. The sub-band was further broken down into bit planes for embedding.

All these processes conditioned the cover image to accept the secret message with minimal perceptual disturbance and maximised embedding efficiency. This established the needed foundation for a high-quality steganographic image synthesis in the next phase. In particular, the second phase involved embedding the bit-level representation of the secret image (typically a high-frequency HH sub-band from a wavelet-decomposed QR code) image into the LSB bit plane of the host image's transformed coefficients. This was where the actual steganographic hiding took place. The method achieved high level of imperceptibility by targeting the LSB of the transformed coefficients.

This study specifically opted for the LSB plane for its perceptual insignificance any changes to these bits result in minimal (often imperceptible) distortion to the visual quality of the image. This careful placement ensured the needed balance between imperceptibility, robustness, and payload capacity. Moreover, bit-level embedding provided a structured pathway for later retrieval, which supported the systematic bit-plane removal during the extraction process.

The process then ensued with the reconstruction of the full set of wavelet coefficients from the modified bit planes containing both the original host data and the embedded secret message. This process was crucial to regenerate a coherent and analysable image structure. The final spatial-domain image was subsequently synthesised through the inverse discrete wavelet transform (IDWT) (references).

Finally, all frequency-domain information, which included the embedded data, were effectively consolidated into a standard image format that visually resembled the original input image. Through IDWT, the stego image containing the encoded secret QR code would be visually indistinguishable from the original data and retain high visual fidelity. The following subsections detail the embedding and extraction processes.

3.1. Embedding Process

As illustrated in Figure 5, there were several steps involved when it comes to embedding the secret message within the QR code into a static image in this study. The process begins with the cover image undergoing (DWT), which decomposes it into four frequency sub-bands, namely LL, LH, HL, and HH. This decomposition enables selective embedding in perceptually less sensitive regions, thereby preserving overall visual quality.

BZSQRC Embedding Algorithm Pseudocode

```
def text_to_binary():
    Convert text to a binary string
    return ''.join(format(ord(char), '08b') for char in text)

def embed_text_into_coefficients(text, coefficients, bit_len):
    embedded_text = text_to_binary(text)
    text_len = len(embedded_text)
    if text_len > len(coefficients):
        raise ValueError("Text too long to embed")
    for i in range(text_len):
        coefficients[i] = (coefficients[i] & ~1) | int(embedded_text[i])
    return coefficients

def process_image(image):
    Convert image to grayscale if needed
    return grayscale_image

def wavelet_transform(image):
    Perform 2D DWT on grayscale image
    return LL, LH, HL, HH

def embed_data(text, image):
    gray = process_image(image)
    LL, LH, HL, HH = wavelet_transform(gray)

    # Embed into approximation coefficients (LL)
    LL_flat = LL.flatten()
    LL_embedded = embed_text_into_coefficients(text, LL_flat, len(LL_flat))
    LL_new = LL_embedded.reshape(LL.shape)

    return LL_new, LH, HL, HH

def inverse_wavelet(LL, LH, HL, HH):
    Reconstruct image using inverse DWT
    return reconstructed_image

def embed_pipeline(text, image):
    LL_new, LH, HL, HH = embed_data(text, image)
    reconstructed_image = inverse_wavelet(LL_new, LH, HL, HH)
    return reconstructed_image
```

Figure 5. The pseudocode of the BZSQRC embedding algorithm.

In parallel, the secret message is encoded into a QR code and pre-processed. This pre-processing stage includes: 1) Validation of QR code dimensions, 2) Removal of redundant quiet zones (typically four modules from each boundary), and 3) Resizing using BZ interpolation. The use of BZ interpolation is critical to maintain structural fidelity of the QR code during scaling, ensuring that its readability is not compromised after embedding.

Next, the processed QR code is also subjected to wavelet decomposition, from which the HH sub-band is extracted. This sub-band is then decomposed into eight distinct bit-planes, allowing fine-grained control over the embedding process at the binary level.

The embedding phase is performed in the HH sub-band of the cover image, specifically targeting the LSB plane. This choice is motivated by the need to minimize perceptual distortion while maintaining sufficient capacity. The embedding is executed by replacing the LSBs of the cover image's HH coefficients with corresponding bits from the QR code bit-planes. Additionally, the embedding follows a defined offset strategy, ensuring spatial consistency and avoiding structural clustering that could raise suspicion or degrade robustness.

After embedding, the modified HH sub-band is recombined with the unchanged LL, LH, and HL sub-bands. Finally, the (IDWT) is applied to reconstruct the stego image, which visually resembles the original cover image while securely containing the embedded QR code.

Overall, in the embedding process a dual-domain processing approach which we combining spatial precision (bit-plane substitution) and frequency-domain robustness (wavelet decomposition) in order to achieve a balance between imperceptibility, capacity, and structural integrity of the hidden QR code.

3.2. Extraction Process

As depicted in Figure 6, the extraction process aimed to ensure the accurate retrieval of the embedded QR code from the stego image without compromising the structural integrity and readability of the secret message. In the extraction process, the hidden message was separated from the steganographic image. Imaging devices, such as barcode scanners and smartphones, would be able to read the inverted information in its textual or data format. Through DWT, the stego image was decomposed into LL, LH, HL, and HH frequency sub-bands. Following that, the HH sub-band containing the embedded information was isolated for further analysis.

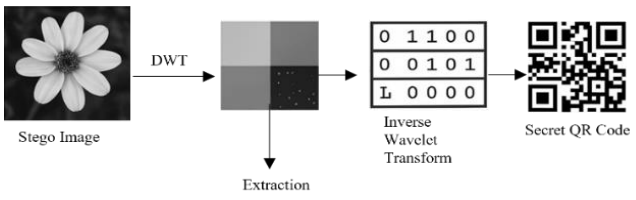


Figure 6. Extraction process of the BZSQRC algorithm.

For consistency, the previously sign normalisation was reversed by referencing a stored or regenerated sign matrix, thereby restoring the original coefficient polarity where necessary. The HH sub-band was decomposed into bit-planes and LSB plane, which was where the secret message was embedded. It should be noted that the extraction process started from the predefined embedding offset.

Through the reassembled bits, the wavelet-domain representation of the QR code's HH sub-band was reconstructed prior to being subjected to the inverse wavelet transform for the regeneration of the spatial-domain QR code. In the case where resizing was involved during embedding, the extracted QR code would be resized to its original dimensions through the inverse BZ (or simply interpreted at its resized scale, depending on the application requirements). Following that, standard decoding procedures were applied on the final QR code for the retrieval of the secret message.

4. Results and Discussion

Through an objective quality measure (PSNR), the proposed BZSQRC algorithm in this study was validated for different QR code versions with various dimensions and volume of retained information [51]. The number of characters encoded by a QR code would influence the QR code version and the data type. Table 2 summarises the maximum storage capacity values for different data types at the maximum QR code level (version 40, low error correction level). Meanwhile, the recorded PSNR values for the original and steganographic versions of three different images (in correspondence to the test cover images in Figure 7) are summarised in Table 3.

Table 2. Summary of the QR code storage capacity values (at max.).

Input	Characters (max.)	Translation capacity (max. char)	Bits/char	The possible set of characters
Numeric	7089	23,664	3.3	0, 1, 2, 3, 4, 5, 6, 7, 8, and 9
Alphanumeric	4296	25,776	5.5	A-Z, 0-9, space, $, %, +, -, *, ., /, and :
Binary/Byte	2953	23,624	8	ISO8859-1 (Latin-1) and ASCII
Kanji	1817	29,072	13	Kanji characters from Shift JIS X 0208

Figure 7. The test cover images.

Table 3. Summary of PSNR values.

Image (512×512)	A			B			C		
QR code version	**V1**	**V20**	**V40**	**V1**	**V20**	**V40**	**V1**	**V20**	**V40**
QR code size	84×84	388 × 388	708 × 708	84 × 84	388 × 388	708 × 708	84 × 84	388 × 388	708 × 708
PSNR (dB)	71.38	59.48	54.33	71.11	59.42	54.32	71.44	59.46	54.31

The proposed BZSQRC algorithm recorded higher PSNR with greater QR code storage capacity. The

results in Table 3 further demonstrated the correlations between PSNR and the version (size) of the embedded secret message. Furthermore, these QR code versions were validated using the default error correction level (level L) and a module size of 4×4 bits: a) version 1 (V1), b) version 20 (V20), and c) version 40 (V40). The sizes of the secret message in binary form for these QR code versions were 136 bits (version 1), 6,864 bits (version 20), and 23,624 bits (version 40).

4.1. Advantages

The compression of the module size of the QR code prior to embedding was one of the key advantages of the proposed BZSQRC algorithm. This advantage allowed the embedding of QR codes with different module sizes into the same area. In this study, the comparison of the proposed algorithm with other steganographic tools in Xiong *et al*. [55], Hung *et al*. [24] and Bala Krishana and Dugar [11] revealed the ease of modification for embedding into additional sub-images or bit planes for the case of the proposed BZSQRC algorithm, which enhanced its embedding capacity. The QR code in this study was embedded into the seventh and eighth bit planes of LDWT sub-images (HH, HL, and LH). The comparison results in terms of PSNR and embedding capacity are presented in Table 4.

Table 4. Comparison of PSNR and embedding capacity values with prior studies.

Image/Size		Proposed BZSQRC algorithm	Chen *et al*. [14]	Luo *et al*. [31]	Lin *et al*. [30]
A	PSNR [dB]	50.24	37.23	38.8	37.7
	Capacity [kbits]	141.744	99.947	66.064	129.791

Referring to Table 4, the proposed BZSQRC algorithm (version 40 with low error correction level) achieved an embedding capacity of 141,744 bits and attained PSNR of 50.24 dB between the cover and steganographic images (A). This study's proposed algorithm clearly demonstrated superior PSNR outcomes as compared to other verified tools with similar or higher embedding capacity characteristics. The significance of steganographic communication was retained given the aim of steganography to attain high capacity for embedding essential information at high level of imperceptibility. This observation demonstrated capacity (the number of secret bits that could be hidden per pixel in the cover image) as a key criterion of performance measurement, which can be calculated as follows [20]:

$$Capacity = \left(\frac{total\ number\ of\ bits\ embedded\ into\ image}{total\ number\ of\ pixels\ on\ image}\right)(bits/pixel) \quad (1)$$

Meanwhile, a high PSNR value implies minimal difference between the original and resulting images. The obtained results demonstrated PSNR as another key criterion of performance measurement in terms of the imperceptibility of a steganographic image. After all, it is challenging for the human eye to discern the original and steganographic images in the case of PSNR exceeding 35 dB [5]. With that, PSNR for eight-bit images can be calculated as follows [20]:

$$PSNR = 10\,log_{10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

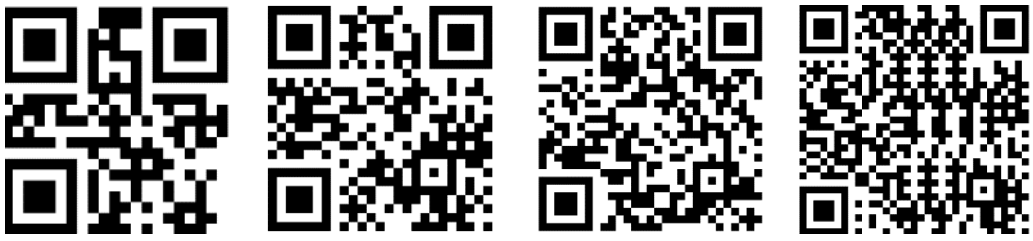
where MSE denotes the mean square error between the cover and steganographic images, and MSE is computed as follows [20]:

$$MSE = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I_{ij-}\, I'_{ij}\right) \quad (3)$$

where W denotes the image width (pixels); H denotes the image length (pixels); i denotes the image row; j denotes the image column; I_{ij} denotes the pixel value of the cover image; I'_{ij} denotes the pixel value of the steganographic image.

Accordingly, the increasing resemblance of steganographic image to the cover image would reduce MSE and subsequently increase PSNR [5, 21, 48].

The effectiveness of the proposed BZSQRC algorithm was examined in several tests, which included the utilisation of four QR code images (Figure 8). The dataset for image processing was retrieved from an online data set centre on the Kaggle platform [42]. QR code images of versions 1 to 4 were retrieved from this particular platform, with each containing QR code data of four random digits [1]. The study proceeded to evaluating PSNR and MSE in reference to the same secret message in Alajmi *et al*. study [6], which utilised the following embedded information: "Scan to RSVP for our event: June 15th, 2024, Location: Quack Avenue 79 Florida". The obtained results of the proposed BZSQRC algorithm and LSB two-bit method are summarised in Table 5.



a) QR code data: 1101 Version: 10 Size: 290 px×290 px. b) QR code data: 1101 Version: 20 Size: 330 px×330 px c) QR code data: 1101 Version: 30 Size: 370 px×370 px d) QR code data: 1101 Version: 40 Size: 410 px×410 px

Figure 8. The QR codes of versions 10, 20, 30, and 40 as cover images.

Table 5. Summary results of PSNR and MSE values.

Stego image	PSNR		MSE	
Method	LSB two-bit method	BZSQRC algorithm	LSB two-bit method	BZSQRC algorithm
QR code V1	73.974	81.251	0.00444	0.00072
QR code V2	75.097	79.106	0.00342	0.00120
QR code V3	76.090	80.099	0.00273	0.00095
QR code V4	76.982	81.100	0.00222	0.00096
Average	**75.5**	**80.4**	**0.0032**	**0.0025**

Meanwhile, the results of PSNR and MSE are illustrated in Figures 9 and 10, respectively. This study's proposed BZSQRC algorithm recorded higher PSNR and substantially lower MSE than that of the LSB two-bit method.

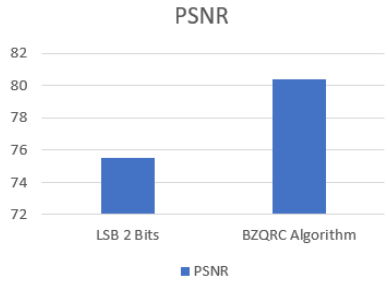


Figure 9. The PSNR evaluation results.

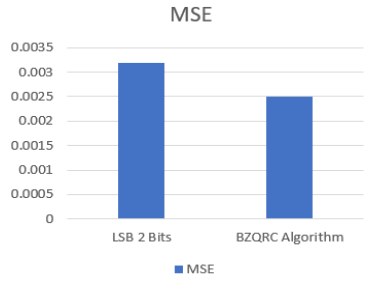


Figure 10. The MSE evaluation results.

4.2. Remarks

This study tested the validity of the steganographic image containing a QR code. For the detection of the QR code data from the steganographic image, different QR code scanner applications for an Android smartphone were considered. The search for the most highly rated application was conducted back in August 2024. QR code scanner, which recorded the highest user rating (a score of above 4.5), was selected.

How different scanning software and applications identified and interpreted QR codes concealed using the proposed BZSQRC algorithm in this study was examined using the following outcomes:

1) Yes (indicated by "/") for successful detection and reading of the QR code.
2) No (indicated by "X") for the failure to detect and read the QR code.

This study employed the following steganographic image detection techniques for the validation of the QR code data:

1) QR and barcode scanners can read standard QR codes, including QR codes embedded in images with minor modifications.
2) QR code scanner and scanner app are specifically designed to detect and decode QR codes, including QR codes embedded within images using steganography techniques.
3) QR and barcode readers are similar to general QR and barcode scanners.
4) QR scanner or barcode scanner typically provides robust QR code detection capabilities, making it likely to read the steganographic QR codes.
5) Google lens possesses advanced image recognition capabilities and can detect and read QR codes embedded within images.

The results of the QR code analysis are summarised in Table 6. The proposed BZSQRC algorithm contained separate inputs of QR code data and embedded information. Despite that, with the utilisation of any QR code scanner, the QR code data were successfully retrieved without any failure.

Table 6. Summary of the QR code data validity analysis.

Steganographic image detection	Steganographic QR code V1	Steganographic QR code V2	Steganographic QR code V3	Steganographic QR code V4
QR and barcode scanners	/	/	/	/
QR code scanner and scanner app	/	/	/	/
QR and barcode readers	/	/	/	/
QR scanner or barcode scanner	/	/	/	/
Google Lens	/	/	/	/

4.3. Limitations

There were several limitations to the proposed BZSQRC algorithm in this study. Firstly, the BZ process may lead to data loss or image quality loss when it comes to zooming in on QR codes, which may affect the readability and robustness of the QR codes. Secondly, scaling up the size of the QR code may cause blurring and pixelation. This may affect its effectiveness and robustness due to the wrong extraction of LSB data or the incorrect hiding of steganographic information. Lastly, the proposed BZSQRC algorithm did not incorporate any security mechanism, which potentially increase the susceptibility of the LSB data or steganographic content to detection by adversaries or automated algorithms.

5. Conclusions

Through the BZ technique to manipulate QR code images, a novel BZSQRC algorithm was successfully developed and validated in this study. A secure LSB

algorithm was utilised to enclose the secret message within a QR code, while DWT was employed to incorporated the image. In the proposed algorithm, the secret message served as the payload for the steganographic process. The QR code image was utilised as a cover medium to conceal the payload of the BZSQRC algorithm when it comes to generating QR steganographic images. Analysis revealed that the proposed BZSQRC algorithm performed better in terms of PSNR, which was about 6.5% higher than that of the LSB two-bit method, suggesting the effectiveness of the former in enhancing the steganographic image quality. Additionally, the proposed algorithm displayed low average noise reduction, with MSE of as low as 0.0025. Moreover, the proposed BZSQRC algorithm separated the QR code image from the secret message through the inverse process. These results confirmed the validity of the QR code if scanned. It is recommended for future research to make use of a secret key and an encryption layer to enhance the security of the proposed BZSQRC algorithm.

Acknowledgement

This work was supported by Geran Inisiatif Putra Muda (GP-IPM) Research Grant [Grant No. 9740200].

References

[1] Adeniran A., My AI QR Code Decoder, Kaggle, https://www.kaggle.com/discussions/general/529026, Last Visited, 2025.

[2] Akhtarkavan E., Majidi B., and Mandegari A., "Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A_5 Lattice Vector Quantization," *IEEE Access*, vol. 11, pp. 9701-9715, 2023. DOI: 10.1109/ACCESS.2023.3238575

[3] Al Dallal H. and Al Mukhtar W., "A QR Code Used for Personal Information Based on Multi-Layer Encryption System," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 9, pp. 44-56, 2023. DOI: 10.3991/IJIM.V17I09.38777

[4] Aladwan F., Shukla R., Abroshan H., Islam S., and Al-Haddad R., "From Spatial to Frequency Domain: Defending Medical Image Classification Against Steganography-Based Adversarial Attacks," *in Proceedings of the IEEE International Conference on Big Data*, Washington (DC), pp. 4466-4473, 2024. DOI: 10.1109/BIGDATA62323.2024.10825959

[5] Al-Aidroos N. and Bahamish H., "Image steganography based on LSB matching and image Enlargement," *in Proceedings of the 1st International Conference of Intelligent Computing and Engineering*, Hadhramout, pp. 1-6, 2019. DOI: 10.1109/ICOICE48418.2019.9035172

[6] Alajmi M., Elashry I., El-Sayed H., and Farag Allah O., "Steganography of Encrypted Messages Inside Valid QR Codes," *IEEE Access*, vol. 8, pp. 27861-27873, 2020. DOI: 10.1109/ACCESS.2020.2971984

[7] Almawgani A., Alhawari A., Hindi A., Al-Arashi W., and Al-Ashwal A., "Hybrid Image Steganography Method Using Lempel Ziv Welch and Genetic Algorithms for Hiding Confidential Data," *Multidimensional Systems and Signal Processing*, vol. 33, no. 2, pp. 561-578, 2022. DOI: 10.1007/S11045-021-00793-W

[8] Alyousuf F., Din R., and Qasim A., "Analysis Review on Spatial and Transform Domain Technique in Digital Steganography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 573-581, 2020. DOI: 10.11591/EEI.V9I2.2068

[9] Aslam M., Rasid M., Azam F., Alotaibi S., and et al., "Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review," *in Proceedings of 2nd International Conference on Computing and Information Technology*, Tabuk, pp. 32-38. 2022. DOI: 10.1109/ICCIT52419.2022.9711628

[10] Bajaj B., "Reliability on QR Codes and Reed-Solomon Codes," *arXiv Preprint*, vol. arXiv:2407.17364v1, pp. 1-21, 2024. https://arxiv.org/pdf/2407.17364

[11] Bala Krishna M. and Dugar A., "Product Authentication Using QR Codes: A Mobile Application to Combat Counterfeiting," *Wireless Personal Communications*, vol. 90, pp. 381-398, 2016. DOI: 10.1007/s11277-016-3374-x

[12] Baziyad M. and Obaidat M., "On the Importance of the DCT Phase for Image Steganography Schemes," *in Proceedings of the IEEE 5th International Conference on Computing Communication and Automation*, Greater Noida, pp. 791-795, 2020. DOI: 10.1109/ICCCA49541.2020.9250849

[13] Cevik T., Cevik N., Rasheed J., Asuroglu T., and et al., "Reversible Logic-Based Hexel Value Differencing-A Spatial Domain Steganography Method for Hexagonal Image Processing," *IEEE Access*, vol. 11, pp. 118186-118203, 2023. DOI: 10.1109/ACCESS.2023.3326857

[14] Chen W., Li Q., Tang X., and Pan Q., "A Digital Watermarking Method for Medical Images Resistant to Print-Scan Based on QR Code," *Multimedia Tools and Applications*, vol. 83, pp. 52197-52218, 2024. DOI: 10.1007/s11042-023-17155-2

[15] Chiang Y., Lin P., Wang R., and Chen Y., "Blind QR Code Steganographic Approach Based Upon Error Correction Capability," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 10, pp. 2527-2543, 2013. DOI:

10.3837/tiis.2013.10.012

[16] Chou G. and Wang R., "The Nested QR Code," *IEEE Signal Process Letters*, vol. 27, pp. 1230-1234, 2020. DOI: 10.1109/LSP.2020.3006375

[17] Chung C., Chen W., and Tu C., "Image Hidden Technique Using QR-Barcode," *in Proceedings of the IIH-MSP 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kyoto, pp. 522-525, 2009. DOI: 10.1109/IIH-MSP.2009.119

[18] Dragoi I. and Coltuc D., "On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 187-189, 2020. DOI: 10.1109/TIFS.2020.3006382

[19] Ganavi M., Prabhudeva S., and Hemanth Kumar N., "An Efficient Image Steganography Scheme Using Bit-Plane Slicing with Elliptic Curve Cryptography and Wavelet Transform," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, pp. 43-59, 2022. DOI: 10.5815/ijcnis.2022.04.04

[20] Gnanalakshmi V. and Indumathi G., "A Review on Image Steganographic techniques Based on Optimization Algorithms for Secret Communication," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 44245-44258, 2023. DOI: 10.1007/S11042-023-15568-7

[21] Goel S., Rana A., and Kaur M., "A Review of Comparison Techniques of Image Steganography," *IOSR Journal of Electrical and Electronics Engineering*, vol. 6, pp. 41-48, 2013. DOI: 10.9790/1676-0614148

[22] Huang W. and Wang H., "QR Codes for Information Hiding by Hybrid Halftone Dots," *in Proceedings of the IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data*, Taipei, pp. 598-601, 2024. DOI: 10.1109/ICEIB61477.2024.10602696

[23] Huang Y., Cao P., and Lyu G., "A Directly Readable Halftone Multifunctional Color QR Code," *Chinese Journal of Electronics*, vol. 32, no. 3, pp. 474-484, 2023. DOI: 10.23919/CJE.2021.00.366

[24] Hung S., Yaw C., Fang Y., Tan P., and Lee R., "Micrography QR Codes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 9, pp. 2834-2847, 2020. DOI: 10.1109/TVCG.2019.2896895

[25] Immamuddinkhan M. and Kanahasabapathy S., "Bidirectional Circular Shift-Based Reversible Steganography Algorithm with Dual Stego-Images," *The International Arab Journal of Information Technology*, vol. 22, no. 4, pp. 709-721, 2025. DOI: 10.34028/iajit/22/4/6

[26] Jayapandiyan J., Kavitha C., and Sakthivel K., "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," *IEEE Access*, vol. 8, pp. 136537-136545, 2020. DOI: 10.1109/ACCESS.2020.3009234

[27] Kanzariya N., Jadhav D., Maltare N., and Gagani L., "A Coverless Image Steganography Based on Huffman Encoding and Robust Image Wavelet Hashing," *Journal of Electrical Systems*, vol. 20, no. 11, pp. 973-982, 2024. DOI: 10.52783/JES.7350

[28] Lin P., "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 384-392, 2016. DOI: 10.1109/TII.2015.2514097

[29] Lin P., "Imperceptible Visible Watermarking Based on Postcamera Histogram Operation," *Journal of Systems and Software*, vol. 95, pp. 194-208, 2014. DOI: 10.1016/j.jss.2014.04.038

[30] Lin P., Chen Y., Lu E., and Chen P., "Secret Hiding Mechanism using QR Barcode," *in Proceedings of the International Conference on Signal-Image Technology and Internet-Based Systems*, Kyoto, pp. 22-25, 2013. DOI: 10.1109/SITIS.2013.15

[31] Luo M., Wang S., and Lin P., "QR Code Steganography Mechanism with High Capacity," *in Proceedings of the IEEE International Conference on Communication Problem-Solving*, Taipei, pp 1-2, 2016. DOI: 10.1109/ICCPS.2016.7751131

[32] Manikanta Prasad J. and Pramod H., "QR DWT Guided Steganography Using Machine Learning," *in Proceedings of the 2nd International Conference on Advances in Information Technology*, Chikkamagaluru, pp. 1-6, 2024. DOI: 10.1109/ICAIT61638.2024.10690569

[33] Marghny M., Al-Aidroos N., and Bamatraf M., "Data Hiding Technique Based on LSB Matching Towards High Imperceptibility," *MIS REVIEW: An International Journal*, vol. 18, no. 1, pp. 57-69, 2012. DOI: 10.6131%2fMISR.201209_18(1).0003

[34] Mathivanan P. and Balaji Ganesh A., "QR Code Based Color Image Stego-Crypto Technique Using Dynamic Bit Replacement and Logistic Map," *Optik*, vol. 225, pp. 165838, 2021. DOI: 10.1016/j.ijleo.2020.165838

[35] Melman A. and Evsutin O., "On the Efficiency of Metaheuristic Optimization for Adaptive Image Steganography in the DFT Domain," *in Proceedings of the 17th International Symposium Problems of Redundancy in Information and Control Systems*, Moscow, pp. 49-54, 2021. DOI: 10.1109/REDUNDANCY52534.2021.9606459

[36] Mittal S., Kaur P., and Ramkumar K., "Achieving Privacy and Security Using QR-Code Through

Homomorphic Encryption and Steganography," *in Proceedings of the ICRITO 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, Noida, pp. 1-6, 2021. DOI: 10.1109/ICRITO51393.2021.9596265

[37] Pelosi M. and Easttom C., "Identification of LSB Image Steganography using Cover Image Comparisons," *The Journal of Digital Forensics, Security and Law*, vol. 15, pp. 1-48, 2021. DOI: 10.15394/jdfsl.2021.1551

[38] Puteaux P. and Puech W., "A Recursive Reversible Data Hiding in Encrypted Images Method with a Very High Payload," *IEEE Transactions on Multimedia*, vol. 23, pp. 636-650, 2020. DOI: 10.1109/TMM.2020.2985537

[39] Rafat K. and Sajjad S., "Advancing Reversible LSB Steganography: Addressing Imperfections and Embracing Pioneering Techniques for Enhanced Security," *IEEE Access*, vol. 12, pp. 143434-143457, 2024. DOI: 10.1109/ACCESS.2024.3468988

[40] Rahman S., Jamal Uddin., Zakarya M., Hussain H., and et al., "A Comprehensive Study of Digital Image Steganographic Techniques," *IEEE Access*, vol. 11, pp. 6770-6791, 2023. DOI: 10.1109/ACCESS.2023.3237393

[41] Rani M. and Rosemary E., "Data Security Through QR Code Encryption and Steganography," *Advanced Computing: An International Journal*, vol. 7, no. 1/2, pp. 1-7, 2016. DOI: 10.5121/acij.2016.7201

[42] Rustad S., Andono P., and Shidik G., "Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset)," *Signal Processing*, vol. 206, pp. 1-28, 2023. DOI: 10.1016/j.sigpro.2022.108908

[43] Sandhu M., Ahmed M., Hussain M., Head S., and Khan I., "Protecting Sensitive Images with Improved 6-D Logistic Chaotic Image Steganography," *The International Arab Journal of Information Technology*, vol. 21, no. 6, pp. 1064-1073, 2024. DOI: 10.34028/iajit/21/6/10

[44] Sharma V., Srivastava D., and Mathur P., "A Daubechies DWT Based Image Steganography Using Smoothing Operation," *The International Arab Journal of Information Technology*, vol. 17, no. 2, pp. 154-161, 2020. DOI: 10.34028/iajit/17/2/2

[45] Shyam Kishore G., Lakshman Kumar Y., Sravan Abhilash K., and Aparna E., "A Bitwise Operations-based Image Steganography Technique for LSB Replacement," *in Proceedings of the 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI*, Greater Noida, pp. 1-4, 2024. DOI: 10.1109/ICSCAI61790.2024.10866737

[46] Singh A. and Singh J., "Review and Comparative Analysis of Various Image Interpolation Techniques," *in Proceedings of the 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies*, Kannur, pp. 1214-1218, 2019. DOI: 10.1109/ICICICT46008.2019.8993258

[47] Soumya P. and Sreenivas B., "Embedding Color Image with QR Code Including Securing and Noise Removal of it," *Synthesis Journal*, vol. 3, no. 19, pp. 1-3, 2015. DOI: 10.17577/IJERTCONV3IS19051

[48] Subramanian N., Elharrouss O., Al-Maadeed S., and Bouridane A., "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409-23423, 2021. DOI: 10.1109/ACCESS.2021.3053998

[49] Sun Y., Yu M., and Wang J., "Research and Development of QR Code Steganography Based on JSteg Algorithm in DCT Domain," *in Proceedings of the IEEE 15th International Conference on Solid-State and Integrated Circuit Technology*, Kunming, pp. 1-4, 2020. DOI: 10.1109/ICSICT49897.2020.9278285

[50] Tevaramani S. and Ravi J., "Image Steganography Performance Analysis Using Discrete Wavelet Transform and Alpha Blending for Secure Communication," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 208-214, 2022. DOI: 10.1016/J.GLTP.2022.03.024

[51] Udvaros J. and Szabo L., "Recognize and decode QR Codes from Images," *in Proceedings of the IEEE 10th International Conference on Control, Decision and Information Technologies*, Vallette, pp. 1393-1397, 2024. DOI: 10.1109/CODIT62066.2024.10708606

[52] Varuikhin V. and Levina A., "Steganographic Information Hiding Method Based on Double Wavelet Transform," *in Proceedings of the 11th Mediterranean Conference on Embedded Computing*, Budva, pp. 1-5, 2022. DOI: 10.1109/MECO55406.2022.9797168

[53] Vongpradhip S. and Rungraungslip S., "QR Code Using Invisible Watermarking in Frequency Domain," *in Proceedings of the IEEE 9th International Conference on ICT and Knowledge Engineering*, Bangkok, pp. 47-52, 2012. DOI: 10.1109/ICTKE.2012.6152412

[54] Wu D. and Wu Y., "Covert Communication Via the QR Code Image by a Data Hiding Technique Based on Module Shape Adjustments," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 12-34, 2020. DOI: 10.1109/ojcs.2020.2984473

[55] Xiong L., Zhong X., Xiong N., and Liu R., "QR-3S: A High Payload QR Code Secret Sharing System for Industrial Internet of Things in 6G Networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7213-7222, 2021.

DOI: 10.1109/TII.2020.3044006

[56] Xue L., Chao Y., Liu L., and Zhang X., "Information Hiding Algorithm for PDF417 Barcode," *in Proceedings of the IEEE 5th International Conference on Natural Computation*, Tianjian, pp. 578-581, 2009. DOI: 10.1109/ICNC.2009.266

[57] Yamauchi K. and Kobayashi H., "Invisible QR Code Generator Using Convolutional Neural Network," *in Proceedings of the IEEE 46th Annual Conference of the Industrial Electronics Society*, Singapore, pp. 4009-4014, 2020. DOI: 10.1109/IECON43393.2020.9254709

[58] Ye H., Zhang S., Liao J., Gu S., and Wang C., "PPRSteg: Printing and Photography Robust QR Code Steganography via Attention Flow-Based Model," *arXiv Preprint*, vol. arXiv:2405.16414v1, 2024. https://arxiv.org/html/2405.16414v1

[59] Zhou Y., Hu B., Zhang Y., and Cai W., "Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and its Performance," *IEEE Access*, vol. 9, pp. 122362-122372, 2021. DOI: 10.1109/ACCESS.2021.3108189

Nuur Alifah Roslan received a PhD degree in Computer Security from the Universiti Putra Malaysia, Malaysia. She is currently a senior lecturer at University Putra Malaysia (UPM). She is a member of MyHCI-Ux Malaysia Associate, Human-Computer Interaction and an Associate Member of Information Security, UPM research group. Her current research interests include: Steganography, Digital Watermarking, Information Security, Multimedia Security and Human-Centric Security.

Adnan Gutub ranked as a Professor (since 2012) currently affiliated with the CyberSecurity Department at the College of Computing at Umm Al-Qura University (UQU), Makkah-Saudi Arabia. He received his PhD degree (2002) in Electrical and Computer Engineering from Oregon State University, USA. He had his BS in Electrical Engineering and MS in Computer Engineering, both from KFUPM, Saudi Arabia. Adnan's research work can be observed through his 200+publications (journals and conferences) as well as his 5 US patents registered officially by USPTO in information security linked to Cryptography, Steganography, Watermarking, Secret-Sharing, and Smart Systems. Administratively, Adnan Gutub filled many executive and managerial academic positions at KFUPM as well as UQU. He also worked as a local consultant for different academic programs in Dammam and Madinah, supervising 18 thesis researchers gaining graduate degrees in attractive cybersecurity explorations.

Rahmita Wirza Rahmat received B.Sc. and M.Sc. degrees in Science Mathematics from the University Science Malaysia. She received her PhD in Computer Assisted Engineering from the University of Leeds, U.K. At this moment, she is working in the Faculty of Computer Science and Information Technology as a lecturer (Prof in Computer Graphics). Among her focus research areas are Computer Graphics and Applications, Computer Assisted Surgery and Computational Geometry. Until now, she has led 15 research grants and published her work in more than 100 journals, 60 proceedings, seven chapters in books and two international books. She also managed to patent filed 8 of her research works. Since 2008, she has been one of the Panel Assessors for the Malaysian Qualifications Agency. She founded Computer Research Group, which later changed to Computer Graphics, Vision and Visualization Research Group. She is also a co-founder of Computer Assisted Surgery and Diagnostic Special Interest Research Group (CASD). She is one of the task force committee members in preparing the draft for the memorandum of agreement between UPM, UKM and IJN for Computer Assisted Surgery and Diagnostic special interest research group where the MOA was successfully signed by all parties on 15 February 2013, which last for 5 years.

Fatimah Khalid (Member, IEEE) obtained the B. Sc. In Computer Science from University Technology Malaysia (UTM) in 1992. From 1993 to 1995, she worked as a System Analyst at the University Kebangsaan Malaysia (UKM) and continued her Master's Degree at UKM. After getting her Masters Degree in 1997, she started involved in teaching at Sal College until 1999 and continued at the University Putra Malaysia in June 1999. She received her PhD in System Science and Management from the University Kebangsaan Malaysia in 2008. In January 2016, She was secondment to the Computer Science Department at Tabuk University, Saudi Arabia, for one and a half years. Currently, she is working in the Faculty of Computer Science and Information Technology as a lecturer with Associate Professor.

Nur Izura Udzir has been an Associate Professor at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM) since 1998. She received her Bachelor of Computer Science (1995) and Master of Science (1998) from UPM and her PhD in Computer Science from the University of York, UK (2006). Her areas of specialisation are computer security, intrusion detection systems, access control, secure operating systems, steganography, coordination models and languages, and distributed systems. For her contributions to academics and research, she has won various awards, i.e., the MIMOS Prestigious Award 2015 for the supervision of her student's doctoral thesis, the Young Scientist Award 2021, and seven Best Paper Awards at international conferences. In addition to keynote speeches and invited expert talks, she has also been invited as a visiting lecturer/foreign scientist at the M. Auzeov South Kazakhstan State University, Kazakhstan, in 2014, 2019 and 2020.