DWT Based QR Steganography

K. Priya¹, S. Mohamed Mansoor Roomi², P. Uma Maheswari³, R. Suganya⁴

¹²Research Scholar, ECE, Thiagarajar College of Engineering, Madurai, India.
²Professor, ECE, Thiagarajar College of Engineering, Madurai, India.
³Associate Professor, IT, Thiagarajar College of Engineering, Madurai, India.

E-mail: priya5586@gmail.com

Abstract. Data security pays more attention in most of the communication fields. Image steganography is one of the leading data security techniques that provides confidentiality with high embedding capacity and high steganography image quality. This work proposes Discrete Haar Wavelet Transform (DWT -H) and bitwise operations-based embedding technique to embed secret QR-code message in the cover image and extraction of QR-code secret message is also carried out by the same methodology. The efficiency of the proposed method is estimated by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). This technique provides less MSE and PSNR in the range of 31dB to 44dB and extracts QR code image up to version 40. The results of the proposed method provide the practical feasibility for QR-coded-based security applications with less time and high accuracy.

1. Introduction

Steganography plays an important role in the copyright field, text or image communication, military, digital rights management for secure communication. In these fields, confidentiality in exchanging of information should be maintained securely between two parties or any intelligence organization. Image steganography is one of the recently emerging technology for secrecy maintenance and it hides the secret message inside the cover message for security reasons and protects the message from any attacks over the internet. Most of the techniques are developed for information security and at similar time attacks and unofficial access are also increased.

Huang et. al. [1] presented DCT based steganography approach for JPEG images. Sarreshtedari et.al. [2] proposed the pixel reduction technique that achieves good embedding capacity. Pharwaha [3] suggests the randomly selected bit for embedding the data. Gutte et.al [4] suggested LSB based technique, but the computational complexity is high. Swain [5] proposed two different techniques that work in the spatial domain. Soni et.al [6] investigated a discrete version of fractional Fourier transform for image steganography. Jordi et al [7] presented a technique to hiding information in steganographic capabilities using QR Code reader and writer for voting application. Discussed various attacks in the voting system that influence the QR code in steganography and found a solution for these attacks.

Another application of QR code cover is distributing shares, using cryptographic keys. In the secret-sharing method, the public receives the normal message but authorized people can decrypt secret shares using the required credential key. The protocol of the secret-sharing was investigated along with many miscellaneous secret share QR methods [8]. The QR code generation and methods to hide QR code in a color image were discussed and some basic embedding methods such as halftoning to decrease the rough effect of the square in QR code and enhance the quality of steganography image
have experimented. The error minimization in QR code decryption was found in decoding methods [9].

2. QR Code
Quick Response (QR) code is a type of two-dimensional bar code that is used to encode the message like letters, numbers, and binary, etc. It is a machine-readable code that contains information about the product that is hidden in a QR code. The size of the QR code varies from version 1 to version 40. The module size of the version is in the range of 21*21 to 177*177. QR code holds 4296 characters called the capacity of storage and its memory storage capacity is more compared to any other one-dimensional bar code. In this paper, a text message that is hidden in a QR code image and that image is used as a hidden message to increase content safety and embedding capacity of the message in the carrier image.

The shape of the QR code is square with three-position detection and alignment pattern located at three corners of the QR code such as top left, top right, and bottom left. The data type information is located around QR code detection and version information is located around pattern detection. Version detection is used to find the capacity of QR codes. The hiding message and error corrections are arranged in blocks which are composed of 8-bit number code words. QR code data depends on the input character, QR code module range, and level of error correction. This proposed methodology used QR Draw Ad software released by DENSO Wave Incorporation for QR code image generation. The output QR code image from the extraction phase is scanned by a QR code scanner called Gomin android software which is downloaded from the google play store. The flow of QR code generation and scanning is shown in figure 1.

3. Discrete Wavelet Transform (DWT)
DWT is used in various applications like denoising, compression techniques, detecting self-similarity in signal and image processing. The DWT is shown time and frequency domain details simultaneously. This transform divides the content of the image into approximation and detail sub-images using the low pass and high pass filtering. This process is repeated up to many times and each time the signal is down sampled. The structure of one-level decomposition is shown in figure 2. The approximation sub-image contains the information of pixel values and the remaining three sub-images contain the details about changes of horizontal, vertical, and diagonal respectively as shown in figure 3. DWT operated on two sets namely scaling and wavelet. Scaling used low pass and wavelet used high pass filtering for image decomposition. This proposed method used Haar wavelet DWT for image decomposition.

Haar wavelet first operates horizontally and then vertically on adjacent elements. Haar wavelet scaling function is given in equation 1. This is an orthogonal basis for certain vector space.
DWT-Haar on an image is explained in equation 2. Where \( f(x,y) \) is the image coordinates and \( \text{haar}(k,x) \) and \( \text{haar}(m,y) \) is the one level haar wavelet. \( S(k,m) \) is the single-level DWT-Haar transformation image. Inverse DWT Haar on DWT-Haar image is given by equation 3 which gives the original image.

\[
\varphi(t) =\begin{cases} 
1 & 0 \leq t \leq 1 \\
0 & \text{otherwise}
\end{cases}
\]

\[
\varphi(t) =\begin{cases} 
1 & 0 \leq t \leq 1 \\
0 & \text{otherwise}
\end{cases}
\]

\[
s(k,m) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \times \text{haar}(k,x) \times \text{haar}(m,y)
\]

\[
f(x,y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s(k,m) \times \text{haar}(k,x) \times \text{haar}(m,y)
\]

4. Proposed Methodology
In this proposed methodology, first, the secret text message is converted to a QR code by a QRDraw Ad software. The steganography image is created in the embedding phase by masking the QR code image in the carrier image. In the extraction phase, the secret QR code image is retrieved from the steganography image. Then the secret text message is decoded using a QR code scanner, that scans the retrieved QR code image. The overall block diagram is shown in figure 4.
Figure 4. Overall Block Diagram of Proposed Methodology

Text Message

QR Code Image Generation

1 Bit Right Shift

Cover Image

Check Size

Not Same

Same

Take DWT on Cover Image

Horizontal Component

Bitwise Complement

Bitwise AND Operation

Bitwise OR Operation

Take Inverse DWT

Stego Image

Resize the Cover Image to double the size of QR code Image
The embedding process is shown in figure 5 of a secret message in the form of a QR code. Generate QR code image from a QR Draw Ad software. Take a cover (C) image and QR code (QR) image and check the size of both. If the cover image size is equal to double the size of the QR code image, keep the cover image size as it is otherwise changing the cover image size to double of QR code image size. Take 1-bit right shift to QR-code image named as $(QR)_{1RS}$ shown in equation 4.

$$QR >>> = QR_{1RS} \quad (4)$$

Decompose the cover image by using DWT-Haar ($C_{DWT}$) to get sub-images ($cA$, $cH$, $cV$, $cD$) depicted as specifies in equation 5. Of these four sub-images, take horizontal changes in the wavelet domain for further processing as shown in equation 6.

$$C_{DWT} = DWT_{HAAR}(C) = (cA, cH, cV, cD) \quad (5)$$

$$C_{DWT-ch} = cA \quad (6)$$

Take bitwise complement of $cH$ cover sub-image$(\sim C_{DWT-ch})$. Apply bitwise AND operation on $cH$ cover sub-image ($C_{DWT-ch}$) and Then the output image called $C_{AND}$ depicted in equation 7.

$$C_{AND} = (C_{DWT-ch}) \& = (\sim C_{DWT-ch}) \quad (7)$$

Then apply bitwise OR operation on $C_{AND}$ and $(QR)_{1RS}$ called Stego1 shown in equation 8. Take Inverse DWT on $C_{AND}$ and $QR_{1RS}$ called stego image shown in equation 9.

$$Stego_1 = C_{AND}QR_{1RS} \quad (8)$$

$$Stego = IDWT(C_{AND}, QR_{1RS}) \quad (9)$$

The extraction process of QR code image retrieval using a stego image is shown in figure 6. Decompose the stego image by using DWT-Haar. Four sub-images ($sA$, $sH$, $sV$, $sD$) are obtained shown in equation 10. Take horizontal component of stego sub-image ($sH$) for further processing depicted in equation 11.

$$S_{DWT} = DWT_{HAAR}(S) = (sA, sH, sV, sD) \quad (10)$$

$$S_{DWT-sh} = sH \quad (11)$$

Apply 1 bit left shift on the horizontal component of stego sub-image called $S_{DWT-sh-1LS}$ shown in equation 12.

$$S_{DWT-sh} >>> = S_{DWT-sh-1LS} \quad (12)$$

Apply bitwise AND operation on $S_{1LS}$ and 255 called $S_{AND}$ (equation 13).

$$S_{AND} = (S_{DWT-sh-1LS} \& = 255) \quad (13)$$
Assign maximum intensity values of $S_{AND}$ image to 255 and otherwise assigned to zero called as retrieved QR coded image ($R(QR)$) as shown in equation 14. The text message that is hiding in the QR code can be recovered using a QR code scanner.

$$R(QR) = \begin{cases} \max(S_{AND}) = 255 \\ \text{otherwise} = 0 \end{cases} \quad (14)$$

**Figure 6.** Flow Chart of Extraction Phase

5. **Results and Discussions**
In this proposed methodology, the experimental results were obtained using Matlab2020a in the Asus ROG Strix G731GT laptop with Intel i7 ninth-generation processor, Nvidia GeForce GTX 1650 graphics card, and 8 GB DDR4 RAM.
5.1. Experimental Results of Embedding Phase
In the embedding phase, the default inbuilt Matlab image namely “peppers.png” is taken as the cover image, and the QR code image is taken as a secret message. The cover image and QR code image act as the input to the system. DWT- Haar transform is applied over the cover image. It generates four sub-images namely, approximation image, changes of horizontal, vertical, and diagonal image. Figure 7, shows the input cover image (7.a), QR code image (7.b), the four sub-images of DWT-Haar for the image of the cover (7.c), and stego image (7.d).

Figure 7. Experimental Results of Embedding Phase

5.2. Experimental Results of Extraction Phase
The results of the retrieved QR code image shows in figure 7. The input of this extraction phase is stego image shown in figure 8.a. Then the extracted horizontal change sub-image cH is shown in figure 8.b. Figure 8.c shown AND operated DWT-cH image and figure 8.d shown retrieved QR code image.
5.3. Performance Evaluation using Distortion Measurement

Table 1: Performance Evaluation using MSE, PSNR

| Cover Image | Stego Image | MSE  | PSNR (dB) |
|-------------|-------------|------|-----------|
| Onion       | Onion       | 1.29 | 43.14     |
| Lena        | Lena        | 1.87 | 39.54     |
| Peppers     | Peppers     | 1.86 | 37.89     |
| Baboon      | Baboon      | 3.45 | 33.27     |

Figure 8. Experimental Results of Embedding Phase
The performance evaluation of the proposed work is measured using the estimation of the distortion level of stego image. The distortion of stego image can be calculated by the Peak Signal to Noise Ratio (PSNR). The PSNR is greater than 30 decibels (dB), the visibility of the stego image is acceptable. The mean square error (MSE-equation 15) used to calculate the PSNR value is shown in equation 16. Quality estimation can be measured from Mean Square Error (MSE) in performance evaluation. The range of MSE is always a non-negative value and it is near to zero.

\[
MSE = \frac{1}{m \times n} \sum_{p=1}^{m} \sum_{q=1}^{n} (S_{pq} - C_{pq})^2
\]  

(15)

\(S_{ij}\) is the stego image and \(C_{pq}\) cover image, where \(p\) and \(q\) are the image coordinates and \(n\) and \(m\) are the dimensions of an image.

\[
PSNR = 10 \log_{10} \frac{255^2}{MSE}
\]  

(16)

The MSE and PSNR values for the cover image and the stego images are depicted in table 1. The MSE values vary in the range of 1.29 to 3.45 and PSNR values vary in the range of 31dB to 44dB shows the visual quality of the stego image.

6. Conclusions

This work proposed a DWT and bitwise operations-based image steganography technique using QR code as a secret message. This method provides better confidentiality with high stego image quality. The efficiency of this method involves that the embedded data is not perceptible to any viewers and is further proved by distortion measurements calculated between the cover and stego image. This method successfully extracted QR code image from stego image up to QR version 40 in the extraction phase.

References

[1] F. Huang, J. Huang and Y. Shi, 2012, New Channel Selection Rule for JPEG Steganography, in IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1181-1191.

[2] Saeed Sarreshtedari, Mohammad Ali Akhaee, 2014, One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme. IET Image Process. Vol 8(2), pp 78–89.

[3] A. P. S. Pharwaha, 2010, Secure data communication using moderate bit substitution for data hiding with three layer security, IE(I) Journal-ET, vol.91, pp.45-50.

[4] Gutte, Chincholkar, and Lahane, 2013, Steganography for two and three LSBS using extended substitution algorithm. ICTACT J. Commun. Technol. 4, 685–690.

[5] Gandharba Swain, 2016, Digital Image Steganography Using Variable Length Group Of Bits Substitution, Procedia Computer Science, Volume 85, Pages 31-38.

[6] Soni, A. Jain, J. Roshan, R., 2013, Image steganography using discrete fractional Fourier
transform, *International Conference of Intelligent Systems and Signal Processing (ISSP)* pp.97-100.

[7] Jordi Cucurull, Sandra Guasch, Alex Escala, Guillermo Navarro-Arribas and Victor Acin, 2014 QR Steganography- A Threat to New Generation Electronic Voting Systems. *In Proceedings of the 11th International Conference on Security and Cryptography*, pages 484-491.

[8] Yang-Wai Chow, Willy Susilo, Joseph Tonien, Elena Vlahu-Gjorgjevska and Guomin Yang, 2018 Cooperative Secret Sharing Using QR Codes and Symmetric Keys, *Symmetry, 10, 95*.

[9] Akshara Gaikwad, K.R.Singh, 2015, Information Hiding using Image Embedding in QR Codes for Color Images: A Review, *(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1)*, pp. 278-283.