International Journal of Computational Intelligence and Informatics, Vol. 3: No. 1, April - June 2013

QR- DWT Code Image Steganography

M Ramesh
Computer Science & Engineering,
AVS College of Engineering & Technology,
Nellore, Andhra Pradesh, India.
mramesh2609@yahoo.co.in

G Prabakaran
Computer Science & Engineering,
FEAT, Annamalai University,
Tamil Nadu, India
gpaucse@gmail.com

R Bhavani
Computer Science & Engineering,
FEAT, Annamalai University,
Tamil Nadu, India
Shahana_1992@yahoo.co.in

***Abstract*- Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. The proposed algorithm is a hybrid Steganography scheme based on Quick Response (QR-code) and Discrete Wavelet Transform (DWT). This technique includes encoding and decoding operation in frequency domain. The text message is hidden in the QR-code image. The QR code image is hidden into the Discrete Wavelet Transform. This technique performed well and additional security given to the information. The performance evaluation done by using statistical parameters. This work was compared to other techniques. The proposed method achieved high security and more imperceptibility.**

Keywords-Steganography, Discrete Wavelet Transform, Quick Response code

I. INTRODUCTION

The Steganography is of Greek source and Means "enclosed or hidden writing". Data Hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Steganography is implemented in different fields such as military and Industrial applications. The original practice dates back to ancient times when messenger‘s concealed tattooed messages on their scalps that were revealed by shaving. Since the 1980s, computer technologies have made steganography easier. Today everything from voice over IP to digital filing systems can be exploited to hide more information in ever more sophisticated ways.

Hundreds of computer programs can read and encode messages in digital files. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. In this paper, we focus on frequency domain technique. The DWT has received Considerable attention in various signal processing applications, including image Watermarking. The main idea DWT results from multi resolution analysis. This involves decomposition of an image in frequency channels of constant bandwidth on a logarithmic scale. With many useful applications in signal processing and statistics. Quick Response Code is the trademark for a type of matrix barcode QR Code has become a focus of advertising strategy, since it provides quick and effortless access to the brand's website. Popular methods include storing URLs, addresses and various forms of data on posters, signs, business cards, public transport Vehicles, etc. Indeed, this mechanism has a vast number of potential applications.

II. RELATED WORK

Z. Xiong et al., [1] have presented a scheme embeds a larger-sized secret image while Maintaining acceptable image quality of the stego-image and also improved image hiding Scheme for grayscale images based on Integer Wavelet Transformation. Mamta Juneja et al., [2] Proposed a robust image steganography A technique based LSB insertion and encryption. Sabyasachi Pattnaik et al., [3] proposed the performance comparison of robust steganography based on multiple transformation techniques. This technique ensures more security than individual transformation techniques, which has excellent Peak Signal to Noise Ratio (PSNR) with high levels of security. Sushil Kumar et al., [4] presented a multi-layered Secure, robust and high capacity image steganography Algorithm. This algorithm achieved three layers of security, better in terms of imperceptibility, robustness and embedding capacity compared with corresponding algorithms based on DWT.

Espejel-Trujillo et al., [5] have proposed a scheme allows using the security capacity of the Visual Secret Sharing Scheme (VSS scheme) together with robustness and easy acquisition of QR code. This technique was performed ID-document authentication with secure and easy way without using sophisticated equipment. Mutoo S.K et al., [4] presented a multilayered secure, robust and high capacity image steganography algorithm. This algorithm achieved three layers of security, better in terms of imperceptibility, robustness and embedding Capacity compared with corresponding algorithms based on DWT.

Shanjun Zhang et al., [6] have proposed a robust method of embedding QR code into the DWT domain of divided blocks of the still image. This technique was embedded information and extracted correctly even if the images are compressed to less percentage of the original according to the contents of the images.

ISSN: 2349 - 6363

The paper is organized as following sections. Methodology is described in section 3. Section 4 introduced the proposed model. Testing and statistical analysis is discussed in section 5. Experimental results are illustrated in section 6. The conclusion is given in the last section.

III. METHODOLOGY

A. Steganography

Steganography vs Cryptography - Steganography is not an alternative to cryptography. Steganography is the dark cousin of cryptography. While cryptography provides privacy, steganography is intended to provide secrecy. In other words, cryptography works to mask the content of a message; steganography works to mask the very existence of the message. The purpose of steganography is covert communication to hide a message from a third party.

Steganography is often confused with Cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; the human senses are not trained to look for files that have information hidden inside of them.

Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it. Steganography are used to achieve data privacy over secrecy.

B. QR Code

QR codes are much related to barcodes, but with one difference added advantage, they have a matrix format that allows them to store a large volume of unique data. Normal linear barcodes are one-dimensional and can only hold up to 20 alphanumeric digits, but QR codes are two-dimensional (2D) so they can hold up to 7,089 numeric characters and up to 4,296 alphanumeric letterings worth of data.

QR codes are free to create and to use and there are many inventive uses of a QR code that make it a very versatile technology. The usual specifies 40 versions (sizes) of the QR code from the small 21x21 up to 177x177 modules in size. An improvement with QR code is also there relatively small size for a given amount of data The QR code is accessible in 40 different square sizes each with a user selectable inaccuracy correction level in four steps (referred to as inaccuracy correction level L, M, Q and H).

C. Discrete Wavelet Transform

An image that undergoes Haar wavelet transform will be divided into four bands at each of the transform level. The work presented in this paper is based on frequency domain processing in image hiding mechanism provides imperceptibility and robustness. The first band represents the input image filtered with a low pass filter and compressed to half. This band is also called approximation‘. The other three bands are called details, where the high pass filter is applied. These bands contain directional characteristics. The size of each of the bands is also compressed to half.

Specifically, the second the band contains vertical characteristics, the third Band shows characteristics in the horizontal direction and the last band represents diagonal Characteristics of the input image. Conceptually, Haar wavelet is very simple because it is constructed from a square wave. Moreover, the Haar wavelet computation is fast since it only contains two coefficients and it does not need a temporary array for multilevel transformation. Thus, each pixel in an image that will go through the wavelet transform computation will be used only once and no pixel overlapping during the Computation

IV. PROPOSED MODEL

A. Proposed Steganography Encoding Process

During the embedding process first read cover image and secret images. Apply Discrete Wavelet Transform on the cover image and a secret image to get a DWT cover image. Then apply fusion process on both DWT cover image and QR-code secret image to get composite image and get stego image. The schematic diagram of the proposed embedding process is shown in Figure 1.

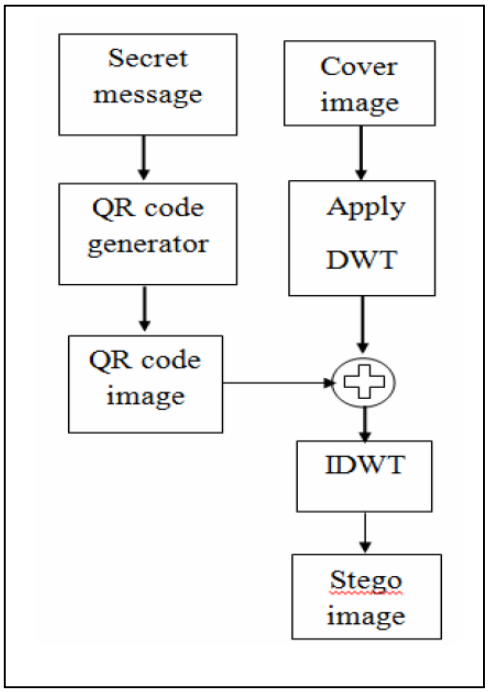

Figure 1. Encoding Model.

B. Embedding Algorithm

Step 1: Read the cover image as a cover image.

Step2: Generate a QR code with a secret Message.

Step 3: Apply DWT on both cover and QR Code image.

Step 4: Embed the QR code image into cover Image.

Step 5: Reconstruction of cover image to apply Inverse Discrete Wavelet Transform (IDWT).

Step 6: Finally get a stego image.

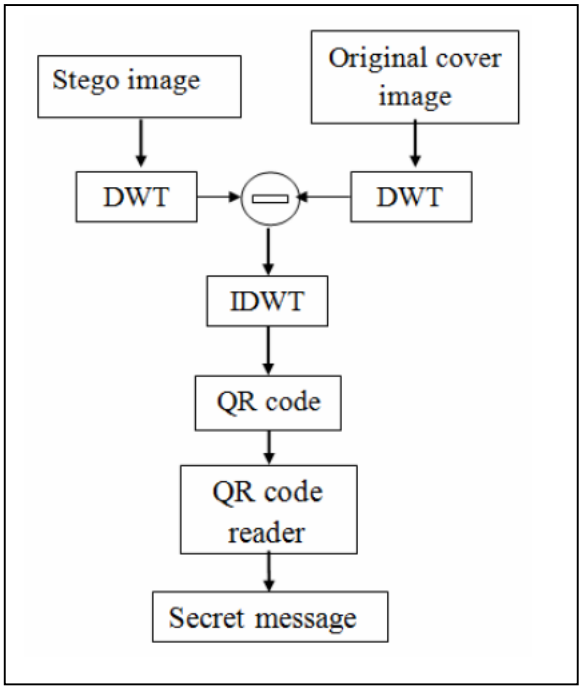

Figure 2. Decoding Model

C. Proposed Steganography Decoding Process

The decoding process is the reverse process of the proposed steganography embedding process. Here to read the cover image and stego image first and apply Subtract stego image coefficients with cover image components and reconstructed the image. The Schematic diagram of the proposed decoding process is shown in Figure 2.

D. Decoding Algorithm

Step 1: Read the stego image and original image.

Step 2: Apply DWT on both images.

Step 3: Subtract stego image Discrete Wavelet Transform component with the original Image discrete Wavelet Transform Component and get the QR code image.

Step 4: By using QR code reader extract Secret message from the QR code image.

V. Testing And Performance Analysis

A. Matlab

Matlab is a high performance language for technical computer, integrates computation, visualization and programming in an easy to use environment. One of the aims for selecting to evaluate the performance of the proposed method, we implement the proposed method by using Matlab R2010a and 7.10 version. MATLAB is to fit perfectly in the necessities of an image processing research due to its inherent characteristics and helpful to solve problems with matrix and vector formulations.

B. Quality Metrics

Image Quality of watermarked image was tested on various quality parameters.

Mean Square Error (MSE): It is defined as the square of the error between cover image and watermarked image. The distortion in the image can be measured using MSE and is calculated using Equation.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{k=1}^{N} \left(x_{j,k} - x'_{j,k}\right)^2 \quad (1)$$

Where $x_{j,k}$ – cover I frame, $x'_{j,k}$ – watermarked frame.

Peak Signal to Noise Ratio (PSNR): It is the measure of the quality of the image by comparing the cover image with the watermarked image

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

i.e., it measures the statistical difference between the cover and watermarked image is calculated by using below equation.

C. Attacks

TABLE 1. QUALITY OF COVER VS STEGO IMAGE AFTER APPLY THE ATTACKS.

Attacks	Variance	PSNR
Contrest	0.001	58.32
Brightness	0.001	57.97
Rotations	0.001	58.01
Spicklnoise	0.001	57.56

VI. Results And Discussion

The image quality factors PSNR and MSE, other quality measurement are observed. The image quality of the proposed method has been completed, which is better than the most cases compared to the existing methods.

TABLE 2. THE QUALITY OF COVER VS STEGO IMAGE.

Cover Images	PSNR	MSE
Flower.jpg	59.47	6.166
Team.jpg	58.58	6.05
Real.jpg	60.05	5.12
Empty.jpg	59.45	5.21
Own.jpg	59.89	4.57

VII. CONCLUSION

In this paper, we have proposed a new image steganography scheme under DWT transform technique. Simulations are carried out on images of different formats viz. JPEG, TIFF and BMP using MATLAB. The encoding and decoding operation in the frequency domain is proposed. The text message is hidden in the QR-code image. The QR-code image is hidden into the Discrete Wavelet Transform. This technique performed well and additional security given to the information. Performance analysis of these two transforms is done based on parameters PSNR and MSE are better than the earlier techniques.

REFERENCES

[1] Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong, "Reversible image watermarking using interpolation techniques", IEEE Transactions on Information Forensics and Security, vol 5, no 1, Mar 2010, pp. 187–193.

[2] Ahkil Khare, Meenu Kumari and Pallavi Khatre, "Efficient algorithm for digital image steganography", journal of information knowledge and research in computer science an application, vol 10, issue 1, 0ct 2010, pp. 1-5.

[3] Sabyasachi Pattnaik, R K Chhotaray, K B Raja and K B Shiva Kumar, "Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques", International Journal on Computer Technology Applications, vol 2, 2011, pp. 1035 – 1047.

[4] Mutoo S.K. and Sushil Kumar, "A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm", World of Computer Science and Information Technology Journal, vol 6, 2011, pp. 239-246.

[5] Espejel-Trujillo A., Castillo-Camacho I., Nakano-Miyatake M., Perez-Meana H, "Identity Document Authentication Based on VSS and QR Codes", Iberoamerican Conference on Electronic Engineering and Computer Science, vol 3, 2012, pp. 241 – 250.

[6] Shanjun, Zhang Kazuyoshi, Yoshino, "DWT-Based Watermarking Using QR Code", Science Journal of Kanagawa University, 2008, pp. 3-6.

[7] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data hiding in H.264 encoded video sequences", IEEE 9th Workshop on Multimedia Signal Processing (MMSP07), Oct 2007, pp. 373–376.