QR code based Image Steganography with Enhanced Image Quality and Compression

Poonam Survase
Department of Electronics & Communication Engineering
RSCOE, Pune, Maharashtra

Abstract

Steganography is the art of covered or hidden writing. The main purpose of steganography is covert communication-to hide the existence of a message from a third party. Steganography is generally used to hide important information in a visible media mostly an image. A good approach to steganography must provide two attributes: high security against the different attacks called steganalysis, which is nothing but a technique used for detecting hidden information using steganography method and second is compression. Image compression not only reduces storage but also benefits transmission. In this paper the image steganography is achieved with enhanced security due to QR code and compression using DWT transform, without affecting the actual cover image due to addition of secret information which is in form of QR codes. The process for embedding the QR codes has been carried out using Embedding and Extraction algorithm which insures secure and fast transmission of stego image. These results validate the practical feasibility of the proposed method for security applications.
Keywords: QR code, Stego, DWT, Image embedding, extraction

I. INTRODUCTION

With the advancement of network technologies and digital devices makes the delivery of digital multimedia fast and easy. However, distributing digital data over public networks such as Internet is not reliable because of copyright violation, counterfeiting, forgery, and fraud. Therefore, methods for protecting digital data, especially sensitive data, are extremely essential. The growing possibilities of modern communications need the special means of security especially on computer network. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding area, which encompasses applications such as copyright protection for digital media[3].

Hence they need some form of security from the third person during transmission which is provided by employing information hiding techniques. Generally, information hiding includes digital watermarking and steganography. Watermarking is different from steganography in its main goal. Watermarking is used for copyright protection, broadcast monitoring, transaction tracking, and similar activities .A watermarking scheme alters a cover object, either imperceptibly or perceptibly, to embed a message about the cover object (e.g. the owner's identification). Steganography where refers to the science of invisible communication.

The word steganography is derived from the Greek words stegos meaning cover and graphic meaning writing. In image steganography the information is hidden exclusively in images. Successful steganography depends upon the carrier medium not to raise attention

There are three main issues to be considered when studying steganographic systems: capacity (or bitrates), security and robustness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data[1] .

The human visual system is adaptive enough to be "fooled," seeing a lossy compressed image and confusing it and accepting it for the original. In fact, most pictures can be processed to remove 97% of the original data, and the human eye would have a very hard time at noticing any degradation. Compression is very important in reducing the costs of data storage and transmission in relatively slow channels[5]. There is a strong interest in developing data encoding and decoding algorithms that can obtain higher compression ratios while keeping image quality to an acceptable level[4].

Quick response (QR) codes have rapidly emerged as a widely used inventory tracking and identification method in transport, manufacturing, and retail industries[3]. Their popularity is due to the proliferation of smart phones, capable of decoding and accessing on line resources as well as its high storage capacity and speed of decoding. QR codes are used in a variety of applications, such as accessing websites, download personal card information, post information to social networks, initiate phone calls, reproduce videos or open text documents. This versatility makes them a valuable tool in any industry that seeks to engage mobile users from printed materials. Not surprisingly QR codes have been widely adopted in the marketing and publicity industry thanks to the advantage they provide in tracking the performance of publicity campaigns.

An important problem of QR codes is its impact on the aesthetics of publicity designs. The square shapes and limited color tolerance, severely impairs their integration into billboard designs or printed materials. This challenge has generated great interest for algorithms capable of embedding QR codes into images without losing decoding robustness. There have been several efforts to improve the appearance of such embeddings which can be classified in two categories, methods that modify the luminance or color of image pixels and methods that replace QR modules[1].

In this paper Image steganography is achieved with compression and enhanced security . Which maintains the visibility of cover image with good compression rate for fast transportation and less storing capacity and also enhanced security. Thus this will serve the dual requirement of minimal compression and concealing confidential images, considering the issues related to security. The organization of rest paper is as follows, Section II Related Work and details discussion on techniques used Section III proposed method and Section IV presents detailed simulation results and discussions of performance parameters. Finally conclusion is given in Section V.

II. RELATED WORK

This section briefly reviews two techniques: (1) QR code and (2) Wavelet transform.

A. QR Code

Denso Wave (1994) developed a code called QR (“Quick Response”) code which is similar to the barcode. A QR code is a two-dimensional (2D) barcode and it is a square which consists of black square dots arranged on a white background. It encodes the information in both horizontal and vertical direction that stores more data than a bar code. QR can encode numeric character, alphanumeric character and kanji characters. The proposed method uses the QR code as a secret message mainly to increase the information security and embedding capacity of the steganography. QR code is generated from the QR code generator available in the inter-net. The secret message can be retrieved from the QR code by scanning the QR code using QR code scanner. Fig. 1 shows the QR coded secret message used for the experiment[9].

Fig. 1: QR code used for experimental Setup

The patterns and structures inside a QR code have well defined functions which include symbol alignment, sampling grid determination, and error correction. The information is encoded in square black and white modules of several pixels wide. Finder patterns play a central role in the speed and success of decoding and are located in three corners of the symbol. Fig. 2 shows the three main regions in the QR symbol structure: function pattern region, encoding region and the quiet zone which is a guard region located on the outside of the symbol.

1) Function Pattern Region

Finder and alignment structures are essential to locate, rotate and align the QR code. The former ones are designed to have the same ratio of black and white pixels when intersected by a line at any angle, allowing to easily detect rotated or inverted codes. Alignment patterns are used to determine the sampling grids from which code words are extracted and they are easily identifiable as concentric square structures evenly distributed along the code area.

2) Encoding Region

The code area delimited by finder patterns is denoted as the encoding region, where data, parity modules and decoding information is stored. This area is divided into code words consisting of blocks of 8 QR modules. Two dimensional shapes of these code words depend on the version of the code and are designed to optimize area coverage[9].

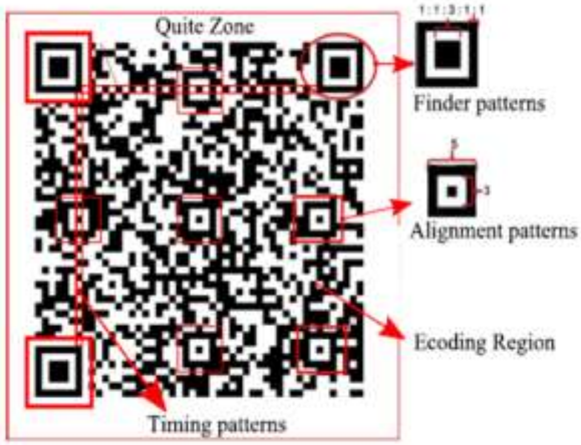

Fig. 2: QR code regions with the location of finder and alignment patterns highlighted in red[9].

B. Image Compression

Compression is one of the major image processing techniques. It is one of the most useful and commercially successful technologies in the field of digital image processing. Image compression is the representation of an image in digital form with as few bits as possible while maintaining an acceptable level of image quality[5].

Data compression is the technique to reduce the redundancies in data representation in order to decrease data storage requirements and hence communication costs. Reducing the storage requirement is equivalent to increasing the capacity of the storage medium and also increases the speed of transmission and hence communication bandwidth. The efficient ways of storing large amount of data but due to the bandwidth and storage limitations, images must be compressed before transmission and storage .After receiving the compressed image it is decompressed and to reconstructed to the original image or approximation of it.

There are several methods of image compression available today that is lossless and lossy image compression. In lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored. Medical imaging, technical drawings, and astronomical observations typically use lossless compression techniques. The Graphics Interchange File (GIF) is an image format used on the Web that provides lossless compression. In lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. Pictures and videos from digital cameras are examples of digital files that are commonly compressed using lossy methods. A simple method of lossy image compression is to reduce the color space to a smaller set of colors. The JPEG image file is the example of lossy compression.

In wavelet image compression, parts of an image is described with reference to other parts of the same image and by doing so, the redundancy of piecewise self-similarity is exploited. There are a number of problems to be solved in image compression to make the process viable and more efficient. A lot of work has been done in the area of wavelet based compression. That is, different compression ratios are applied to the wavelet coefficients belonging in the different regions of interest, in which of either each wavelet domain band of the transformed image[5].

3) Discrete Wavelet Transform

We have basically four types of wavelets

- Haar wavelet transform
- Daubechies wavelet transform
- Symlet wavelet transform
- Biorthogonal wavelet transform

As computational complexity increases, compression ratio also increases. Haar wavelet transform is the simplest transform for image compression, the principle behind this is very simple as calculating averages and differences of adjacent pixels. The Haar DWT is more computationally efficient than the sinusoidal based discrete transforms, but this quality is a tradeoff with decreased energy compaction compared to the DCT. "The Haar transform operates as a square matrix of length N = some integral power of

Implementing the discrete Haar transform consists of acting on a matrix row-wise finding the sums and differences of consecutive elements. If the matrix is split in half from top to bottom the sums are stored in one side and the differences in the other. Next operation occurs column-wise, splitting the image in half from left to right, and storing the sums on one half and the differences in the other. The process is repeated on the smaller square, power-of-two matrix resulting in sums of sums. The number of times this process occurs can be thought of as the depth of the transform. In our project, we worked with depth four transforms changing a 256x256 images to a new 256x256 image with a 16x16 purely sums region in the upper-left hand corner[6].

The advantages of Haar Wavelet transform as follows:
1) Best performance in terms of computation time.
2) Computation speed is high. Called lossless compression.
3) Simplicity (e.g., if, = 0).
4) HWT is efficient compression method.
5) It is memory efficient, since it can be calculated in place without a temporary array.

III. PROPOSED METHOD

Frame work of proposed method is as shown in fig:3 The embedding phase embeds the QR coded secret message into the pre-processed source image. The extraction phase extracts the source image and QR coded secret message separately. The algorithm for embedding and extraction phase is given below.

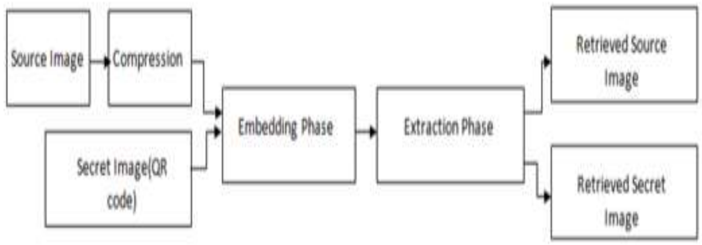

Fig. 3: Framework of proposed method.

A. Embedding Phase

The embedding phase of the proposed work is shown in Fig. 4. The embedding phase is explained in the following steps
1) Check how many images you embed.
Formula: i/p - 1, as 1 image is source image.
2) Get size embed image.
3) Check limit that is how many images you can save in source image.
Formula: (100*8(size of embed image+4*number of images+1)) to calculate size of source image.
4) Reshape source image.
Formula: 2.*floor (source image, 8, length of image/8)/2
5) Convert embedded image into binary add in first column(number of i/p images are in first column)
6) Add embed image into source image.
7) Add(replace) it to each column. as we make source image 8 * length image.
8) Formula: for i, Source image column(next+i)+ binary embedded image.
9) Finally reshape image as it's original size.
10) Write image.

Fig. 4: Block diagram of embedding phase.

B. Extraction Phase

The extraction phase is explained in the following steps:

1) Reshape image (8*length of image/8)
2) Calculate number of images embedded.

Formula: sum(all column of images .* (0-7)square) reason: as we add number of images into pixel of 2 range.

3) var next=4*number of images + 1
4) Extract image : for i=read image

Formula: sum(image column of i+next).*power(2,0.7).

5) Reason: pixel position & binary conversion at the time image embedded.

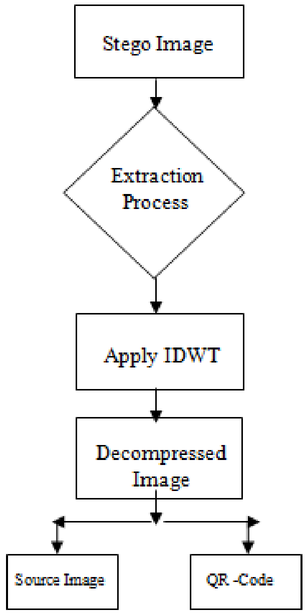

Fig. 5: Block diagram for Extraction Process

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Outputs for Beak Image (1)

1) Original Source Image and Original QR code Image

Fig. 6: Original Source Image and Original QR code Image

2) Compressed Beak Image

Fig. 7: Compressed Beak Image

3) Embedded Image

Fig. 8: Embedded Image

4) Extracted Original Beak Image and QR code

Fig. 9: Extracted Original Beak Image and QR code

B. Output for Flower Image (2)

1) Original Source Flower Image and QR code Image

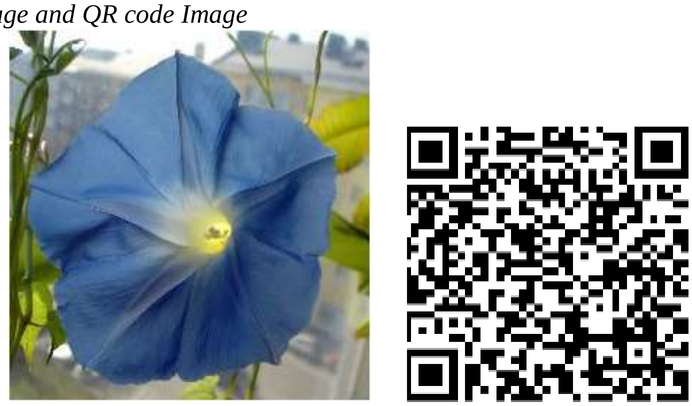

Fig. 10: Original Source Flower Image and QR code Image

2) Compressed Flower Image

Fig. 11: Compressed Flower Image

3) Embedded Image

Fig. 12: Embedded Image

4) Extracted Original Flower Image and QR code

Fig. 13: Extracted Original Flower Image and QR code

C. Output for Polar Bear (3)

1) Original Source Polar bear Image and QR code Image

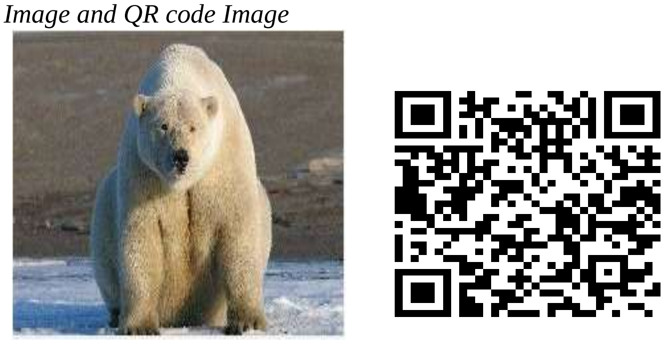

Fig .14: Original Source Polar bear Image and QR code Image

2) Compressed Polar Bear Image

Fig. 15: Compressed Polar Bear Image

3) Embedded Image

Fig. 16: Embedded Image

4) Extracted Original Polar bear Image and QR code

Fig. 17: Extracted Original Polar bear Image and QR code

D. Snapshot of Original QR Code Extracted From Source Image and Secret Message Retrieved From It Successfully

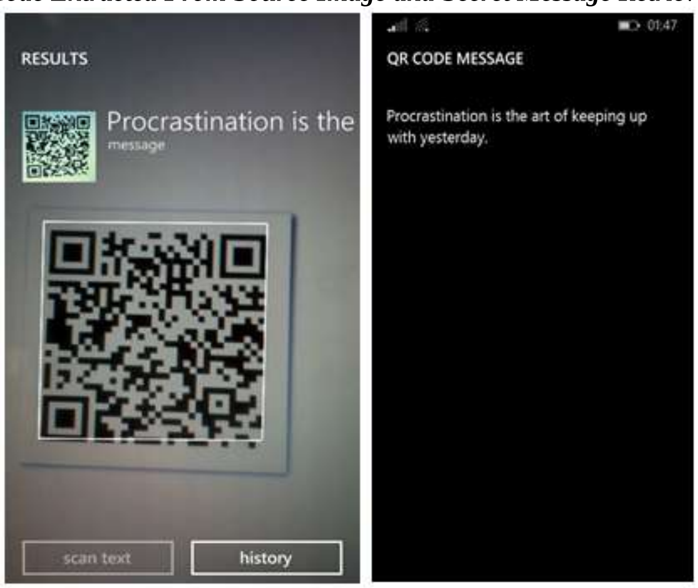

Fig. 18: Snapshot of Original QR code Extracted from Source Image and Secret Message Retrieved from it successfully

Table – 1
Compression Result using DWT for three different images

Size of the Original Image	Size of the compressed Image With DWT	Compression ratio
Beak(3.16 MB)	568KB	8.0523:1
Flower(2.84 MB)	600KB	8.0523:1
Polar(4 MB)	865KB	8.0523:1

Table – 2
PSNR and Embedding capacity values for three different images

Image	PSNR Value in DB	Embedding Capacity in Bits
Beak	51.386	5218.706
Flower	51.047	9756.678
Polar	50.162	20667.554

V. CONCLUSION

Steganography must provide two attributes security and good compression rate. In this paper steganography with average compression ratio 8.0523:1 is achieved using DWT and also have enhanced security of stego Image which avoids the uneven embedding capacity using QR code. The proposed scheme maintains the stego Image quality with an average PSNR value of 50.226 DB.

Experimental results also validate practical feasibility of proposed method for security applications. As future work ,the intelligent optimization technique can be used to enhance the quality of embedded Images

REFERENCES

[1] S. Uma Maheswari “Frequency domain QR code based image steganography using Fresnelet transform” AEU - International Journal of Electronics and Communications 2014
[2] Ibaida, A,et.al ,Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems"Biomedical Engineering, IEEE Transactions 2014
[3] Reza Jafari, Djemel Ziou, Mohammad Mehdi Rashidi, "Increasing image compression rate using steganography", Expert Systems with Applications, Volume 40, Issue 17, 1 December 2013, ISSN 0957-4174
[4] Jayachandran, M.; Manikandan, J., "SAR Image Compression Using Steganography," Advances in Computer Engineering (ACE), 2010 International Conference on , vol., noJune 2010 doi: 10.1109/ACE.2010.15.
[5] Seung-Won Jung, Adaptive post-filtering of JPEG compressed images considering compressed domain lossless data hiding, Information Sciences, Volume 281, 10 October 2014
[6] Prabakaran, G.; Bhavani, R.; Sankaran, S., "Dual Wavelet Transform Used in Color Image Steganography Method," Intelligent Computing Applications (ICICA), 2014 International Conference
[7] Hsiu-Lien Yeh, Shu-Tsai Gue, Piyu Tsai, Wei-Kuan Shih, Wavelet bit-plane based data hiding for compressed images, AEU - International Journal of Electronics and Communications, Volume 67, Issue 9, September 2013
[8] Ibaida, A.; Khalil, I., "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems," Biomedical Engineering, IEEE Transactions on , vol.60, no.12, pp.3322,3330, Dec. 2013
[9] Garateguy, G.J.; Arce, G.R.; Lau, D.L.; Villarreal, O.P., "QR Images: Optimized Image Embedding in QR Codes," Image Processing, IEEE Transactions on , vol.23, no.7, pp.2842,2853, July 2014.
[10] E. H. Miller, “A note on reflector arrays,” IEEE Trans. Antennas Propagat., to be published.