International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Enhanced Data Security in Quick Response (QR) Code Using Image Steganography Technique with DWT-DCT-SVD

Anupriya Arya[1], Sarita Soni[2]

[1]M-tech Scholar Student, Department of Computer Science Engineering, BBAU Central University, Lucknow, UP, India

[2]Assistant Professor, Department of Computer Science Engineering, BBAU Central University, Lucknow, UP, India

ABSTRACT

In this paper, we have proposed a novel hybrid invisible steganography scheme based on DWT, DCT and SVD. The encoding and decoding operation in the spatial domain is proposed. The text message is hidden in the QR-code image. The QR-code image is hidden into the singular value component. Reversible data hiding is an approach to extract the information embedded covertly as well as the host image. We introduce a novel Steganography method to embed QR codes in digital images. Here we use Least Significant Bit to embed the QR code into the image. Data Security using QR code uses the latest technique of QR code encoding of data and the encoded data is communicated through an insecure channel by means of digital watermarking techniques.

Keywords: Cover image Steganography, Quick response (QR) code, DWT, DCT, and SVD.

I. INTRODUCTION

In today's growing world of digital technology, access to the multimedia content is very easy and for some sensitive applications such as medical imaging, military system, legal problems, it is very essential to not only reinstate the original media without any loss of information but also to increase content's security. Reversible data hiding is an approach to extract the information embedded covertly as well as the host image. In this paper, we have proposed a novel hybrid invisible watermarking scheme based on DWT, DCT and SVD. We introduce a novel Steganography method to embed QR codes in digital images. Here we use Least Significant Bit to embed the QR code into the image. Data Security using QR code uses the latest technique of QR code encoding of data and the encoded data is communicated through an insecure channel by means of digital watermarking techniques. The data or secret message, also known as "Plain Text" is first converted to QR code image using QR code generation tool in MATLAB, and finally the QR code is used to embed in an image using Least Significant Bit Steganography Technique. Thus the technique adds to data security of 3 distinct levels. The digital data in terms of images are transmitted through any of the noise channels or insecure channels. An attacker cannot decode the information, though the message the communicated via an insecure channel [1], [2].

In this scheme, we have provided double layer of security by utilizing the multi-resolution property of wavelet and strong features of DCT and SVD. In the proposed scheme, watermark is embedded into the singular values of all high frequency sub-bands obtained by wavelet decomposition of the original image and at the time of extraction, watermark bits are used along with singular vectors to obtain the original image. Our scheme provides high security as

even after the extraction of watermark, without knowing the extraction algorithm, original image cannot be recovered in its entirety. The proposed scheme is tested on various test images and the obtained results show the effectiveness of the proposed scheme [3].

The significant bits of each pixel in the cover image can be used to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image.

This paper is organized as follows: Section II steganography overview Section III Least significant bit (LSB) method. Section IV LSB Method for 8 & 24 Bit color images, Section V Simulation Results and Discussion, Section VI conclusion and future work of research work.

II. PROPOSED METHODOLOGY

1.1 QR code

QR Code is a matrix symbol as shown in figure (1). QR Code holds information stored both in horizontal and vertical dimensions. A QR code can be read from any direction in 360° through position detection patterns located at the three corners. The error correction capability against dirt and damage can be up to 30%.

Quick Response (QR) codes are versatile, 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 consist of different areas that are reserved for specific purposes. Finder, separator, timing patterns and alignment patterns comprised function patterns. Function patterns shall not be used for the encoding data. At three corners of the symbol, finder patterns are used to assist in easy location of its position, size and inclination. The encode procedure of QR Code include following steps. Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into code words. QR codes are free create and many inventive uses of a QR code that make it a very versatile technology. The QR code is accessible in specifies 40 versions (sizes) of the QR code from the small 21 × 21 up to 177 × 177 modules in size [4], [5].

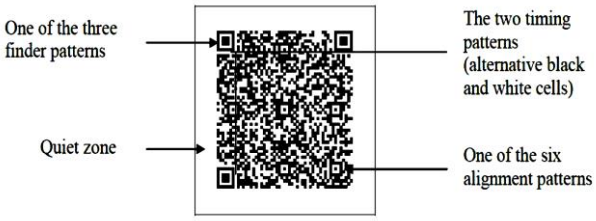


Figure 1. QR Code

1.2 Discrete wavelet transform (DWT)

A **discrete wavelet transform** (**DWT**) is a wavelet transform in which the wavelets are discretely sampled. The advantage over other wavelet transforms is, it has temporal resolution: it captures both frequency and location information (location in time).

2-D Discrete Wavelet Transform is widely used transform in image processing. DWT is based on the concept of wavelets. It is localized both in frequency and time domain. This reveals spatial and frequency aspects simultaneously [6]. It is used for analyzing an image at different resolutions into different frequency components. Due to multi-resolution property, features that may go unnoticed at one resolution may be easily detected at another. Multi-resolution analysis comprises image pyramid and sub-band coding theory. For obtaining 2-D wavelet decomposition, 1-D DWT can be applied on image first in horizontal and then in vertical direction using different filters. 2-D DWT decomposes the image into two parts: Approximation and Detailed part. Approximation part contains one low frequency sub-band LL and detailed part contains three high frequency sub-bands LH, HL and HH. Decomposed sub-bands can be used to reconstruct the original image using Inverse DWT. High frequency sub-

bands of wavelet decomposition have Laplace distribution and this property can be utilized for the data embedding [7].

1.3 Discrete cosine transform (DCT)

A transformation function which transforms image from spatial domain to frequency domain which makes the analysis of a signal simple. DCT Steganography is done by using direct application of transform to entire image or block wise. One dimensional DCT is used in audio compression method. Two dimensional DCT is used in image compression, where vertical and horizontal dimensions are considered. Formulae for calculating DCT is given by equation 1. DCT is used in many standardized image, audio, and video compression methods. It has shown its superiority in reduction of the redundancy of a wide range of signals. An image is subdivided into 8x8 block of samples. Each of these 8x8 blocks of samples of the original image is mapped to the frequency domain [8]. It is represented as a composition of DCT basic functions with appropriately chosen 64 coefficients, representing different horizontal and vertical intensities. The discrete cosine transforms is a technique for converting a signal into elementary frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to Equation.1 shown below. In the equation, x, is the input image having N x M pixels, x (m, n) is the intensity of the pixel in row m and column n of the image, and y (u, v) is the DCT coefficient in row u and column v of the DCT matrix [9].

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_m\alpha_n\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left\{x(m,n)*\cos\frac{(2m+1)u\Pi}{2M}\cos\frac{(2n+1)u\Pi}{2N}\right\}$$

…..(1)

Where

$$\alpha_u=\begin{cases}\frac{1}{\sqrt{2}} & u=0\\ 1 & u=1,2,\ldots M-1\end{cases};\quad \alpha_v=\begin{cases}\frac{1}{\sqrt{2}} & v=0\\ 1 & v=1,2,\ldots N-1\end{cases}$$

1.4 Singular Value Decomposition (SVD)

The Singular Value Decomposition is one of the most useful tools of linear algebra with several applications to multimedia. Applications including Image compression, Steganography and other Signal Processing. Given a real matrix, A (m,n); 1≤ m ≤M, 1≤ n ≤ N, it can be decomposed into a product of three matrices given by equation (2)

$$A=USVT \qquad \ldots\ldots(2)$$

Where U and V are orthogonal matrices, U TU = I, V TV = I, and S = diag (λ1, λ2, ….. λr). The diagonal entries of S are called the singular values of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the Singular Value Decomposition (SVD) of A, and can be written as shown in equation (3),

$$A=\lambda_1U_1V_1T+\lambda_2U_2V_2T+\ldots\ldots+\lambda_rU_rV_rT \qquad \ldots. (3)$$

Where r is the rank of matrix A, It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer. An important property of SVD based Steganography is that the largest of the modified singular values change very little for most types of attacks like transpose, flip, rotation, scaling and translation [10].

1.5 Proposed model

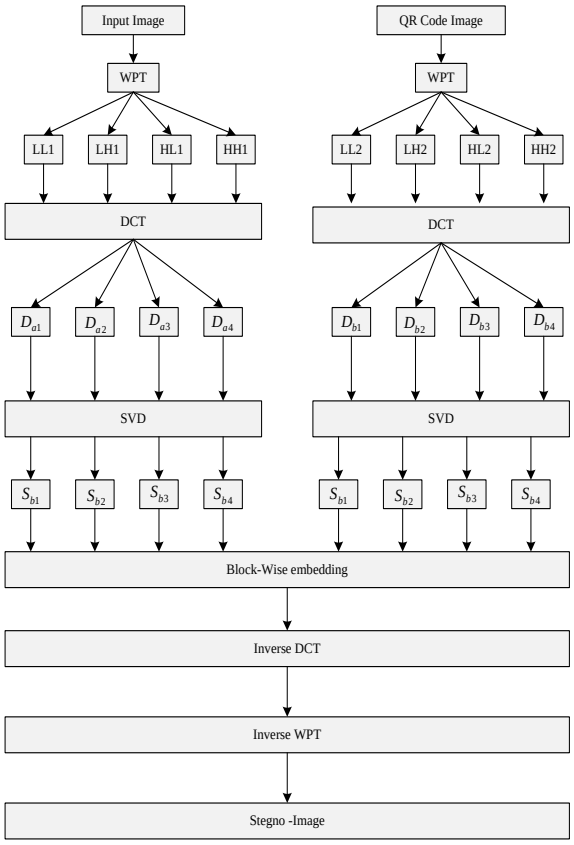


Figure 2. Steganography Process Flowchart

1.6 Proposed Steganography encoding and decoding process

Encoding Process:

The Steganography encoding process is described below:

The Steganography embedding procedure is briefly described in the following steps:

Step-1: Apply wavelet packet decomposition to input image as well as Steganography image.

Step-2: The blocks (N) are selected based on the threshold value which depends upon the high frequency components of the respective blocks.

Step-3: SVD is applied to each 16x16 blocks to obtain the SVs (Singular Values) of each block called as 'Si' matrix.

Step-4: Binary Steganography logo is added to the Si matrix of each block.

Di = Si + αW Where 'α' is a gain factor ……(4)

Step-5: SVD is applied on each Di matrix to obtain the SVs of each (Swi matrix) block. Di = UwiSwiVwi T.

Step-6: Use the Swi matrix of each block to build the Steganographyed blocks

Bwi = UiSwi Vi T ……(5)

Step-7: Combined the Steganography and un-Steganography blocks into a single matrix.

Step-8: Applied Inverse DCT (idct2) and the Steganography image (Iw) is obtained.

Step-9: Apply Inverse wavelet packet transform to get the Steganography image.

Decoding Process:

The Steganography decoding procedure is briefly described in the following steps:

Step-1: Apply WPT to decompose into approximation and detail parts.

Step-2: Apply DCT to Steganography image and divide the Steganography image into 16 x 16 blocks.

Step-3: SVD is applied on any one of the selected Steganographed block

Bwi ' = Ui ' Swi ' Vi T'. ……(6)

Step-4: Obtain the matrices that contain the Steganography using Uwi, Vwi T and Swi ' matrices Di ' = UwiSwi ' Vwi T.

Step-5: Extract the Steganography (W' matrix) from the Di '

Matrix Wi '= (Di' – Si) / α (10) ……(7)

Step-6: The process is repeated to all the 16x16 blocks until the extracted Steganography nearly matches with the original one.

1.7 Evaluation of Image Quality:

For comparing stego-image with cover image results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio [12] and histogram. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

1.7.1 Mean-Squared Error:

The MSE represents the cumulative squared error between the compressed and the original image. The lower the value of MSE, the lower the error. The block calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}\left[I_1(m,n) - I_2(m,n)\right]^2}{M * N}$$

……(8)

M and N are the number of rows and columns in the input images, respectively.

1.7.2 Peak Signal-to-Noise Ratio:

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image

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

……(9)

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc.

1.7.3 Histogram:

Histograms are a type of bar plot for numeric data that group the data into bins. After you create a Histogram object, you can modify aspects of the histogram by changing its property values. This is particularly useful for quickly modifying the properties of the bins or changing the display.

III. SIMULATION RESULTS AND DISCUSSION

The proposed method, are simulated using MATLAB R2013a. Phantom image with different conditions are discussed for Enhanced Data Security in Quick Response (QR) Code Using Image Steganography Technique with DWT-DCT-SVD which are as follows:

Image-1: Phantom

The Image-1 experiment was performed on the Phantom image, embedding a secret text message, the embedding was performed using the proposed technique, in this section, Mean Error, Entropy Difference, correlation coefficients, PSNR and SSIM parameters are calculated after the embedding process for each technique as shown in figure (3).

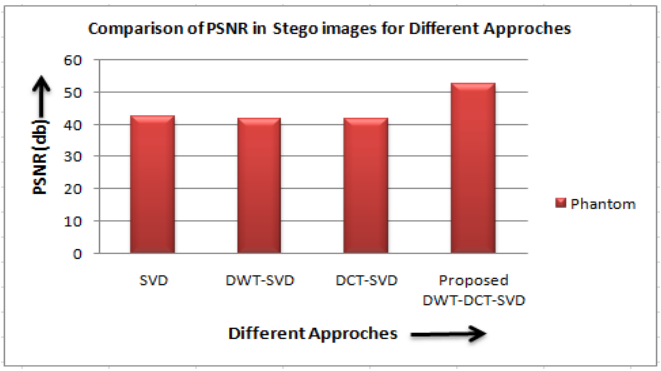


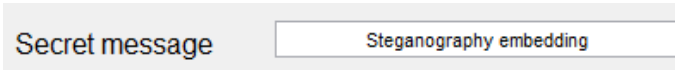
Figure 3. PSNR (dB) of Stego Images for different methods

Table 1 shows the values of the studied parameters after secret text message inside phantom image using the proposed QR based technique with DWT-DCT-SVD.

Table 1. Statistics for Image-1 experiment **Phantom** image after embedding.

Methods / Quality Metrics	SVD [13]	DWT-SVD [14]	DCT-SVD [15]	Proposed Method
Mean Error	0.0139	0.0453	0.0907	0.0029
Entropy Difference	0.1023	0.7902	0.2723	0.0178
Correlation Coefficients	0.86	0.82	0.81	0.91
PSNR	42.67	41.61	41.63	52.67
SSIM	0.8623	0.8721	0.8277	0.8813

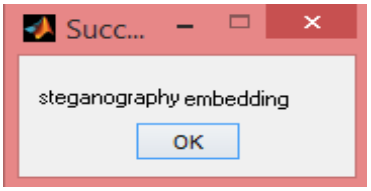
Figure 3 (a) shows the secret text message which is given as a input figure 3 (b) shows generated QR code of the secret text message, figure 3 (c) shows the input cover image, figure 3 (d) shows the stegno-image which is combination of generated QR image and cover image, figure 3 (e) shows decoded QR code image and figure 3(f) shows the decoded Secret message.



(a) Secret Text Message

(b) Secret message QR Code image **(c)** Cover Image

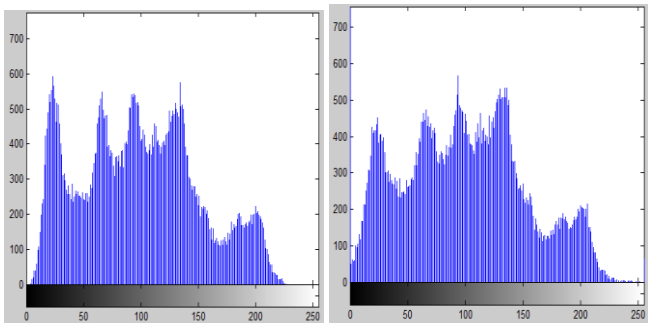
(d) Stego Image **(e)** Recovered QR code image



(f) Recovered secret message

Figure 3. Shows the Gray phantom image before and after embedding

Figure 4 is the histogram of phantom image before and after embedding the secret message in the first experiment using the proposed technique.



(a) (b)

Figure 4 . Histogram of (a) cover Image and (b) Stego Image

IV. CONCLUSION

A new scheme on reversible Steganography is presented in this thesis, to deal with the extraction of Steganography and also the recovery and security of the original image. The Scheme proposed in this paper is based on the concept of discrete wavelet

transform and singular values of high frequency sub-bands. Proposed scheme is tested on various images and the experimental results are obtained which are visually good and PSNR values are also high. The high PSNR values at maximum embedding capacity indicate that our proposed scheme is good enough to produce high quality Steganography images.

V. REFERENCES

[1]. E. Vahedi, R.A. Zoroofi and M. Shiva, "Toward a new wavelet-based Steganography approach for color images using bio-inspired optimization principles", Digital Signal Process. Vol. 22, pp. 153–162, 2012.

[2]. O. Fındık, I. Babaoˇglu and E. Ülker, "A color image Steganography scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm", Opt. Communication, vol. 283 (24), pp. 4916–4922, 2010.

[3]. R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao andR.-J. Chen, "An improved SVD-based watermarking technique for copyright protection", Expert System Application, vol. 39, pp. 673–689, 2012.

[4]. Y.-R. Wang, W.-H. Lin and L. Yang, "An intelligent watermarking method based on particle swarm optimization", Expert System Application, vol. 38 (7), pp. 8024–8029. 2011.

[5]. G. Bhatnagar and R. Balasubramanian, "A new robust reference Steganography scheme based on DWT-SVD", Computer. Stand. Interfaces vol. 31 (5) pp. 1002–1013, 2009.

[6]. A. Nikolaidis and I. Pitas, "Asymptotically optimal detection for additive Steganography in the DCT and DWT domains", IEEE Trans. Image Process. Vol. 12 (5) pp. 563–571, 2003.

[7]. E.E. Abdallah, A.B. Hamza and P. Bhattacharya, "Improved image Steganography scheme using fast Hadamard and discrete wavelet transforms", J. Electron. Imaging vol. 16 (3) pp. 0330201–0330209, 2007.

[8]. F. Huang and Z.-H. Guan, "A hybrid SVD-DCT Steganography method based on LPSNR", Pattern Recognition Lett. Vol. 25 (15) pp.1769–1775, 2004.

[9]. F. Liu and Y. Liu, "A Steganography algorithm for digital image based on DCT and SVD", Process of IEEE Congress on Image and Signal Processing pp. 380–383, 2008.

[10]. E. Ganic and A.M. Eskicioglu, "Robust DWT-SVD domain image Steganography: embedding data in all frequencies", in: Process of the ACM Multimedia and Security workshop, pp. 166–174, 2004.

[11]. C. Song, S. Sudirman and M. Merabti, "A robust region-adaptive dual image Steganography technique", J. Vis. Commun. Image R vol. 23 pp. 549–568, 2012.

[12]. Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Power and Computing Technologies, pp. 1197-1200, March 2013.

[13]. A. Phadikar, S.P. Maity, B. Verma, "Region based QIM digital Steganography scheme for image database in DCT domain", Computer. Electr. Eng. Vol. 37 pp. 339–355, 2011.

[14]. M. Ouhsain and A.B. Hamza, "Image Steganography scheme using nonnegative matrix factorization and wavelet transform", Expert System Application vol. 36 (2) pp. 2123–2129, 2009.

[15]. S. Alexander, D. Scott and M.E. Ahmet, "Robust DCT-SVD domain image Steganography for copyright protection: embedding data in all frequencies", Process of the 13th European Signal Processing Conference (EUSIPCO2005), pp. 4–8, 2005.