Performance Improvement In Discrete Wavelet Transform Based Digital Image Steganography By The Use Of Integer Wavelet Transform

[1]Parul Sehgal, [2]Vijay Kumar Sharma
[1]M.Tech (p), Rajasthan Institute of Engineering and Technology, Jaipur.
[2]Assistant Professor, CS Deptt., Rajasthan Institute of Engineering and Technology, Jaipur.

Abstract

A novel steganography method has been proposed for digital images based on Integer Wavelet Transform (IWT). The proposed method consists of two processes- the encoding process and the decoding process. The encoding process is used by the sender for embedding the secret message in the cover image resulting in a stego image. This stego image is send to the intended recipient. The decoding process is used by the recipient for extracting the secret message that is hidden in the stego image. We have successfully implemented the proposed steganography method on digital images based on integer wavelet transform and compared the performance of proposed method with discrete wavelet transform based digital image steganography by using statistical parameters such as peak-signal-to-noise-ratio (PSNR), mean square error (MSE) and normalized cross correlation (NCC). The experimental results demonstrate that the quality of stego image is improved in the proposed method by the use of integer wavelet transform.

1. Introduction

All The word steganography is of Greek origin and means “concealed writing” from the Greek words steganos meaning "covered or protected", and graphymeaning "writing”. 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 that there is a hidden message. There are many different carriers that can be used to hide the information such as digital images, videos, sound files and other computer files but digital images are the most popular.

Image Steganography can be achieved using a number of techniques. There are two popular schemes used for image steganography: spatial domain embedding and transform domain embedding. In spatial domain embedding, the processing is applied on the image pixel values directly. The advantage of these methods is simplicity. The disadvantage is that they are highly susceptible to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. In many cases even the small changes resulting out of lossy compression systems lead to total information loss. Least Significant Bit Insertion methods, Pallete based methods come under this category. In transform domain embedding, the first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. These changed coefficients are transformed back into spatial domain to get stego image. The advantage of transform domain methods is the high ability to face signal processing operations. It has been observed that embedding information in the frequency domain of a signal can be much more robust than the embedding in time domain. Most robust steganographic systems known today actually operate in some form of transform domain. Transform domain methods hide information in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping and some image processing. Many transform domain variations exist. One method is to use the Fourier and cosine transforms such as Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) to embed the information in the images. Another is the use of wavelet transforms such as Discrete Wavelet Transform (DWT) or Integer Wavelet Transform (IWT). We have used Integer Wavelet Transform in our proposed method.

2. Integer Wavelet Transform (IWT)

The wavelet transform is an advanced technique of image analysis. In recent years, the wavelet transform has emerged in the field of image processing as an

alternative to the well-known Fourier Transform and its related transforms. Formally, the wavelet transform is defined as a mathematical technique in which a particular signal is analysed (or synthesized) in the time domain by using different versions of a dilated (or contracted) and translated (or shifted) basis function called the wavelet prototype or the mother wavelet. Wavelet transforms are now being adopted for a vast number of applications, e.g. internet, color facsimile, printing, scanning, digital photography, remote sensing, mobile applications, medical imagery, digital library, military applications and e-commerce. The wavelet transform is an upcoming technology within the field of image compression. Wavelet based coding provides significant improvements in picture quality at higher compression ratios.

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH). Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system [9]. To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image [10] and in this case there will be no loss of information through forward and inverse transform [9]. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL sub band is distorted. Lifting schemescan be used to perform integer wavelet transform. The following is an example showing how we can use lifting schemes to obtain integer wavelet transform by using simple truncation and without losing inevitability.

The Haar wavelet transform can be written as simple pair wise averages and differences:

$$S_{1,n} = (S_{0,2n} + S_{0,2n+1})/2$$
$$d_{1,n} = S_{0,2n+1} - S_{0,2n} \quad (1)$$

where $S_{i,1}$, $d_{i,1}$ is the nth low frequency and high frequency wavelet coefficients at the ith level respectively.

It is obvious that the output is not integer, the Haar wavelet transform in (1) can be rewritten using lifting in two steps to be executed sequentially:

$$d_{1,n} = S_{0,2n+1} - S_{0,2n}$$
$$S_{1,n} = S_{0,2n} + d_{1,n}/2 \quad (2)$$

From (1) and (2) we can calculate the integer wavelet transform according to:

$$d_{1,n} = S_{0,2n+1} - S_{0,2n}$$
$$S_{1,n} = S_{0,2n} + d_{1,n}/2 \quad (3)$$

Then the inverse transform can be calculated by

$$S_{0,2n} = S_{1,n} - d_{1,n}/2$$
$$S_{0,2n+1} = d_{1,n} + S_{0,2n} \quad (4)$$

3. Scrambling based on Arnold transformation

Arnold transformation, also known as cropping transformation, was proposed by V.J.Arnold while his research of ergodic theory. By representing digital image as a matrix, it becomes "chaotic" after Arnold transformation. The distinct digital image is corresponding to a class of special matrices in which there is a correlation between the elements. After the Arnold transformation of this matrix a new matrix can be obtained in order to achieve image scrambling processing. Setting the image pixel coordinates, N represents the order of the image matrix, i, j $\in$ (0,1,2,.....,N-1) and the Arnold Transform is as in (5):

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \text{ (Mod N)} \quad (5)$$

The above transformation is of one-to-one correspondence; the transformation can be done iteratively, iteration number can be used as a private key for extracting the secret image. This transformation gives more security and robustness to our algorithm.

4. Alpha Blending

Alpha Blending is the technique of blending or mixing of two images together to form a final output image. According to the alpha blending formula, the final image is given by (6):

$$FI = I_1 + \alpha * I_2 \quad (6)$$

where FI - Final Image

I_1 - First Image

I_2 - Second Image

α can have value between 0 and 1.

5. Proposed Method

The proposed method consists of the encoding and decoding processes which are described as follows:

5.1. Encoding Process

First the secret image is scrambled (with security key) using the Arnold transformation. Then Integer Wavelet Transform (IWT) is applied on the cover image and the Arnold scrambled secret image, which is followed by the alpha blending operation. Then the Inverse Integer Wavelet Transform (IIWT) is applied to obtain the stego image. This is done using the following algorithm (see figure 1):

Step 1: Obtain the cover image C and the secret image S.

Step 2: Apply a 1-level 2-D IWT on the image C.

Step 3: Apply Arnold transformation with private security key on image S to obtain the Arnold transformed secret image SS.

Step 4: Apply a 2-level 2-D IWT on the image SS.

Step 5: Extract the approximation coefficient and detail coefficients of 1-level 2-D IWT of the image C.

Step 6: Extract the approximation coefficient and detail coefficientsof 1-level 2-D IWT of the image SS.

Step 7: Apply Alpha Blending operation on image C and image SS.

Step 8: Perform 2-D IIWT to obtain the stego image SI.

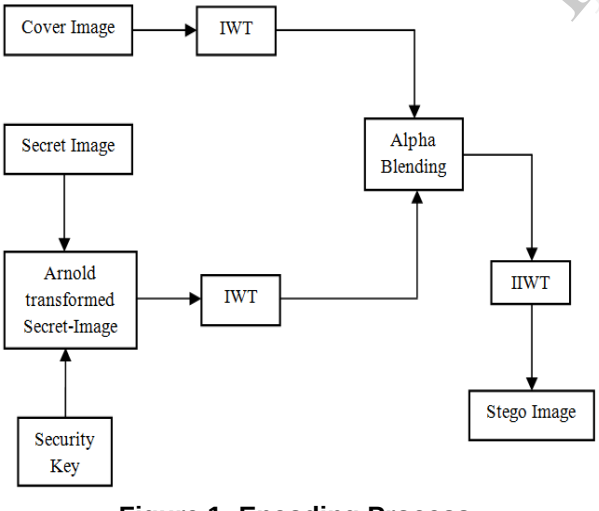

Figure 1: Encoding Process

5.2. Decoding Process

The decoding process is done in two steps:

A.In the first step, we have to recover the cover image from the received stego image. This is done using the following algorithm (see figure 2):

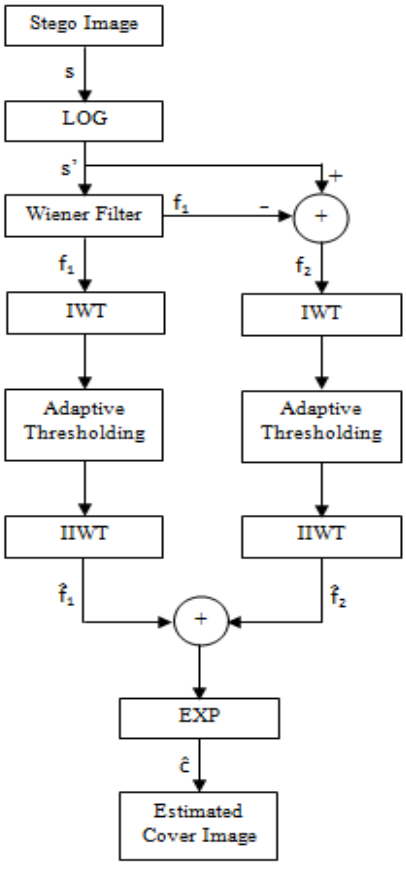

Figure 2: Process of obtaining the cover image from the stego image

Step 1: Receive the stego image s.

Step 2: Take the logarithmic transform of the received stego image s, to yield another image s'.

Step 3: Using Wiener filter, generate two images f_1 and f_2. Image f_1 is the output of Wiener filter and image f_2 is obtained by subtracting image f_1 from s'.

Step 4: Apply 2-D IWT on the images f_1 and f_2.

Step 5: Perform an adaptive denoising method on the coefficients of images f_1 and f_2 to suppress the noise (secret-image).

Step 6: Apply 2-D IIWT on these denoised images to yield $\hat{f}_1$ and $\hat{f}_2$, the denoised versions of f_1 and f_2.

Step 7: Add $\hat{f}_1$ and $\hat{f}_2$.

Step 8: Apply the exponential transform to the resulted image so as to obtain the final cover image $\hat{c}$ (image

obtained by denoising the stego image) which is in fact an estimation of c(the original cover image).

B. In the second step, we actually decode the secret image by using the received stego image and the estimated cover image obtained in the above step. First apply 2-D IWT at level 1 on the estimated cover image and the stego image, followed by alpha blending process. Then apply IIWT to obtain the Arnold scrambled secret image. Finally, by applying the Arnold transform with the security key the original secret image is obtained. This is done using the following algorithm (see figure 3):

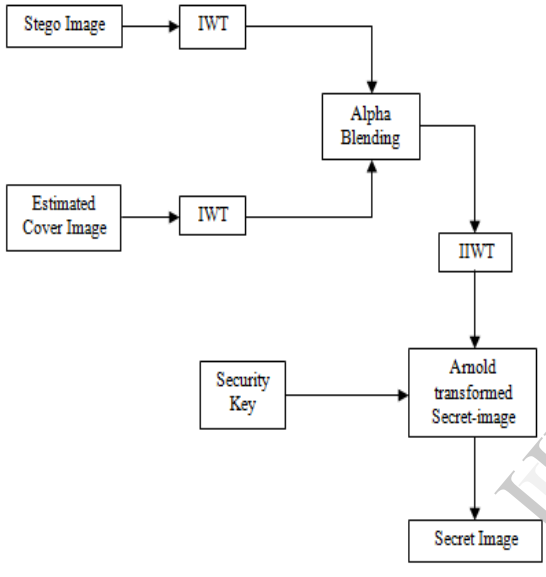

Figure 3: Process of obtaining the secret image

Step 1: Apply 1-level 2-D IWT on the stego image SI and obtained estimated cover image C.

Step 2: Apply Alpha blending operation on image SI and image C.

Step 3: Separate the wavelet coefficients and apply IIWT to get the Arnold transformed secret image SS.

Step 4: Perform the Arnold transformation with private security key on image SS to get the original secret image S.

6. Experimental Results and Performance Analysis

The performance of the proposed method is evaluated by implementing it using Matlab R2012a and 7.0.1 version. We analyse the performance of our proposed method by comparing the cover image and the stego image in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Normalized Cross Correlation (NCC).

PSNR is the measure of the distortion between the original cover image and the stego image. It is defined as follows in (7):

$$\text{PSNR} = 10 \log \frac{255^2}{\text{MSE}} \text{ DB} \qquad (7)$$

where MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N. If $x_{j,k}$ and $x'_{j,k}$ are the pixel located at the j^{th} row and k^{th} column of images x and x' respectively, then it is defined as follows in (8):

$$\text{MSE} = \frac{1}{M*N} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - x'_{j,k})^2 \quad (8)$$

A large PSNR value indicates that the higher image quality (which means there is only little difference between the cover image and the stego image). On the contrary, a small PSNR value indicates that there is great distortion between the cover image and the stego image. It is hard for the human eyes to distinguish between the original cover image and the stego image when the PSNR value is larger than 30db. Also the value of MSE should be as less as possible.

NCC is the measure of the similarity between the original cover image x sized M x N and the stego image x' sized M x N. A positive NCC value indicates the similarity between the cover image and the stego image and the negative NCC value indicates the dissimilarity. It is defined as follows in (9):

$$\text{NCC} = \sum_{j=1}^{M} \sum_{k=1}^{N} x_{j,k} \cdot x'_{j,k} / \sum_{j=1}^{M} \sum_{k=1}^{N} x_{j,k}^2 \quad (9)$$

We compared the proposed IWT based digital image steganography with the DWT based digital image steganography for the various cover images and secret images. Table-1 shows this comparison in terms of PSNR and NCC.

From Table-1, it can be observed that the value of PSNR and NCC is higher in case of IWT based digital image steganography. This means that the proposed IWT based digital image steganography provides a better visual quality of the stego image than the DWT based digital image steganography.

For cover image lenna.tiff and secret image PANGRAM.jpg, we have plotted the bar graph for the PSNR and NCC values obtained in IWT based digtal image steganography versus the PSNR and NCC values obtained in DWT based digital image steganography, using the data from Table-1. Figure 4 and Figure 5 shows these bar graphs from which it is clear that the proposed IWT based steganography method provides an improvement in the PSNR and NCC values.

Table-1. Comparison of IWT based digital image steganography with DWT based digital image steganography

Cover Image	Secret Image	IWT based digital image steganography		DWT based digital image steganography	
		PSNR	NCC	PSNR	NCC
flower.jpg 250X250	NAME.bmp 403X327	40.2143	0.9891	34.1068	0.9693
flower.jpg 250X250	PANGRAM.jpg 864X540	40.2822	0.9896	34.1742	0.9698
lenna.tiff 256X256	NAME.bmp 403X327	39.9728	0.9886	33.9689	0.9688
lenna.tiff 256X256	PANGRAM.jpg 864X540	40.0385	0.9889	34.0257	0.9691

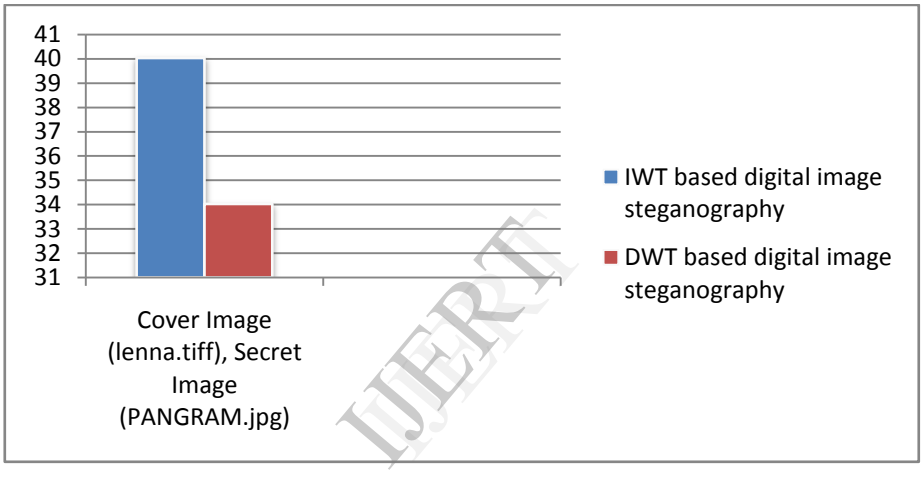

Figure 4: Bar graph for PSNR obtained in IWT based digital image steganography versus DWT based digital image steganography

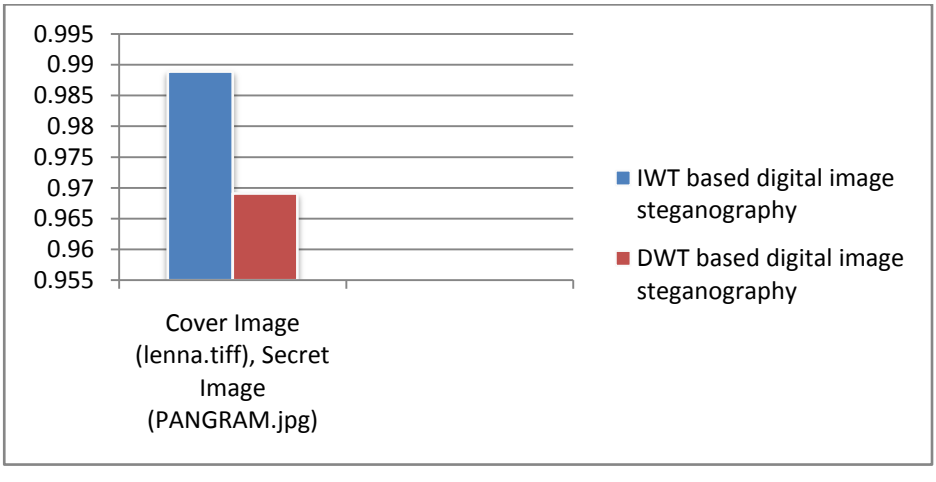

Figure 5: Bar graph for NCC obtained in IWT based digital image steganography versus DWT based digital image steganography

In this paper, a steganography method for digital images based on Integer Wavelet Transform has been implemented. The proposed method results in good visual quality of the stego image with perceptual invisibility of the secret image and high security. Experiments show that the proposed IWT based digital image steganography method results in improved PSNR and NCC values than the DWT based digital image steganography.

8. References

[1] S.Jayasudha, "Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm", International Journal Of Engineering And Science Issn: 2278-4721, Vol.2, Issue 4 (February 2013), Pp 31-35.

[2] V. Dinesh, M. R. Kiran & A. Nepolian, "Reversible Steganographic Technique based on IWT for Enhanced Security", International Journal of Advanced Electrical and Electronics Engineering,ISSN (Print) : 2278-8948, Volume-2, Issue-3, 2013, pp-38-42.

[3] Ms. K. Ramani, Dr. E. V. Prasad, Dr. S. Varadarajan, "Steganography using BPCS to the Integer Wavelet Transformed Image", International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007, pp-293-302.

[4] Prabakaran.G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", International Conference on Computing, Electronics and Electrical Technologies, pp. 1096-1100, 2012.

[5] ArashVosoughi and Mohammad. B. Shamsollahi, "Speckle Noise Reduction of Ultrasound Images Using M-band Wavelet Transform and Wiener Filter in a Homomorphic Framework", International Conference on BioMedical Engineering and Informatics, pp-510-515, 2008.

[6] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal,L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" International conference on Communication Systems Software, pp. 614-621, 2008.

[7] P.Chen, and H.Lin, "A DWT approach for image steganography", International Journal of applied Science and Engineering", volume.4, 3: pp 275:290, 2006.

[8] H S Manjunatha Reddy and K B Raja, "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), pp. 462-472.

[9] Lakshminarayan K, Prabhakaran G, Bhavani R, "A High Capacity Video Steganography Based on Integer Wavelet Transform", Journal of Computer Applications ISSN: 0974 – 1925,Volume-5, Issue EICA2012-4, February 10, 2012, pp-358-365.