International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 03, Issue – 02, February 2018, PP – 19-24

Image Steganography with Compression using Integer Wavelet Transform

B. Nageshwar Rao[1], N. Umamaheswar[2]

[1]*Department, CSE-IT University, College of Engineering Osmania University , India*

[2]*BSNL Osmania University, India*

Abstract: Wavelet transforms have become increasingly important in image compression since wavelets allow both time and frequency analysis simultaneously. Wavelet transforms that map integers to integers have important applications in lossless coding. It has many advantages over other transforms in terms of the performance of image steganography and lossless image compression. The purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as an image. Data is embedded in pixel intensity values with less mean square error. Image compression is used to represent the image in the smallest number of bits while maintaining the essential information of the image. Most wavelet transforms generate float-point coefficients that are not very suitable for lossless image compression. Integer-to-integer wavelet transforms are more practical for lossless image coding with minimal memory usage and low computational complexity. This transformation technique yields better compression ratio.

Key Words: Steganography, Loss less compression, Integer to integer wavelet transforms,.

I. INTRODUCTION

Steganography means to conceal messages existence in another medium (audio, video, image, communication). In simple words it would be like that, hiding information into other information. The purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as an image. Data is embedded in pixel intensity values with less mean square error. After hiding process cover object and stego-object (carrying hidden information object) are similar. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography[1]. Often we wish to process signals in time domain, but in order to process them more easily, other information such as frequency may be required. For example, Fourier transform converts a signal between time and frequency domains, such that the frequencies of a signal can be seen. However the Fourier transform cannot provide information on which frequencies occur at which times in the signal as frequencies and time are viewed independently. To solve this problem the Short Term Fourier Transform (STFT) introduced the concept of windows through which different parts of the signal are viewed. But according to Heisenburg's Uncertainity Principle, as the resolution of signal improves in time domain, the frequency resolution gets worse. Ideally, a method of multi-resolution is needed, which allows certain parts of the signal to be resolved well in time, and other parts to be resolved well in frequency. The power and magic of wavelet analysis is exactly this multi-resolution[2].

- **Steganography Techniques:**

Steganography Techniques are classified into many categories based on embedding method used and are described as follows:

- **Spatial Domain Technique:**

In spatial domain steganography techniques image pixels values are converted in binary values and some of the bits are changed for hiding secret data. There are many categories of Spatial domain Techniques which differ mainly on the basis of manipulation of different bits in pixel values. Least significant bit (LSB)-based technique is one of the simplest and most widely used techniques that inserts or hides the secret message in the LSBs of pixel values without much visual distortion in the cover image. Another technique employs embedding of message bits at randomly chosen pixels. This technique is Pseudorandom LSB in which random pixels are chosen using algorithm where bits of secret data are embed.

- **Transform Domain Technique:**

In transform domain the message is embedded in cover image which is transformed in frequency domain. The message bits are inserted into transformed coefficients of image. Many different transformations can be used for cover image before hiding the secret data [3]. This method of steganography gives more robustness against attacks, as the secret data is stored in image at those areas which are not directly exposed and will remain unchanged after cropping or resizing of image.

Transform domain techniques are broadly classified into:

1. Discrete cosine transformation technique (DCT).
2. Discrete Wavelet transformation technique (DWT) [2].

- **Distortion Techniques:**

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion .Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit .The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

II. PROPOSED METHOD

2.1 Visual Cryptography (VC) Technique:

Instead of using image directly to embed data, it is broken into two or more parts called shares. Message is broken into bits and inserted into shares which in turn are transmitted via different paths. An intruder can't recover complete until data all the shares are received and combined in particular order. At the intended receiver side all the shares are received and stacked to recover the original data. Thus this technique provides a simple and robust method to embed data.

Performance Metrics:

The performance of the various techniques is evaluated based on various performance metrics which are defined as follows. Mean Square Error (MSE): The MSE stands for cumulative squared error between the stego image and the original image[5]. Lower the value of MSE means lower error. It is defined by the relation given below any m x n monochrome image. For coloured image size of image will be m x n x 3. Peak Signal Noise Ratio (PSNR): It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. The PSNR is defined as: Where, MAXI represents maximum value of pixel of the image. In the images with pixel having 8 bits per sample, its value is 255.

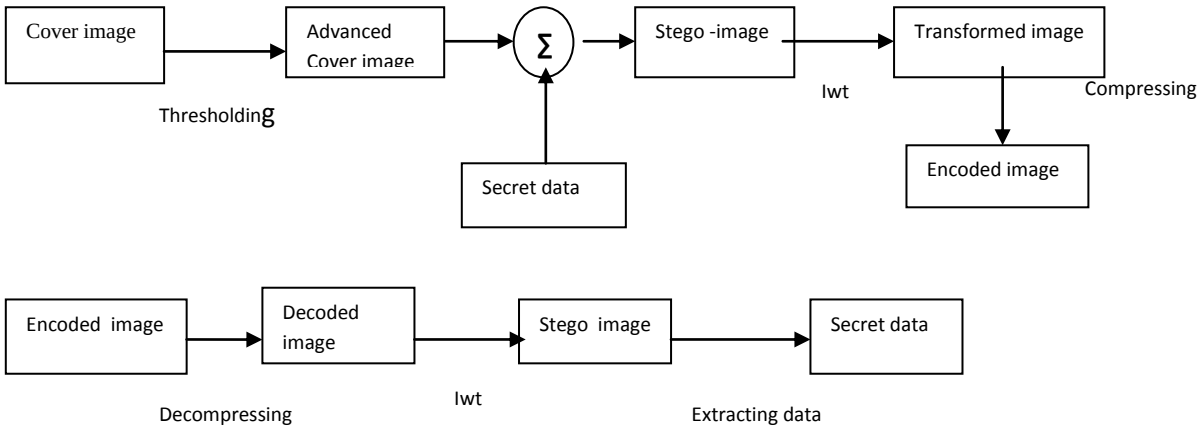
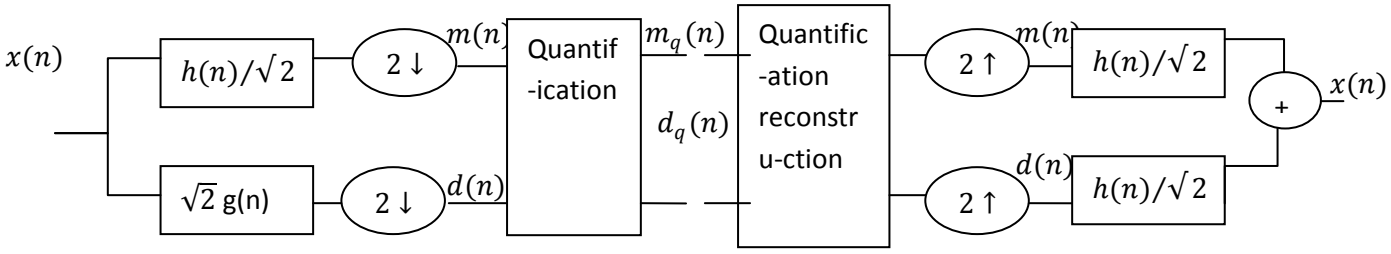


Fig1. Proposed Block diagram of Visual Cryptography

Integer Wavelet Transform

Integer wavelet transform is gaining its popularity among the family of wavelets as it is considered to be the best way to compress losslessly [4]. Integer Wavelet Transform is much faster than the floating point arithmetic in almost all general purpose computers because the floating point wavelet transform demands for longer data length than the integer wavelet transform does. Another benefit of using integer wavelet is the reversibility. That is, the image can be reconstructed losslessly because all the coefficients are integers and can be stored without rounding off errors[6].



Forward Integer Haar Transform Inverse Integer Haar Transform

For the implementation of IWT , we use the Haar Perfect Reconstruction Filter Banks, with scaled low pass and high pass filter coefficients.If x(n) is the input sequence[7], by using Fast wavelet transform ,then the filtered coefficients are given by

$$\begin{bmatrix} m(n) \\ d(n) \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x(2n) \\ x(2n+1) \end{bmatrix} \quad (1)$$

$$m_q(n) = [m(n)] \quad (2)$$

$$d_q(n) = [d(n)] = d(n) \quad (3)$$

From the filtered coefficients, the sequence can be reconstructed as

$$m(n) = m_q(n)\ if\ d_q\ \ even$$

$$m(n) = m_q(n) + 0.5\ if\ d_n(n) is\ odd$$

$$d(n) = d_q(n)$$

2.2 Comparison of steganography techniques

- Mean Square Error (MSE): The results of applying various techniques and image sizes on MSE are given below. From the results the following inferences can be drawn: MSE is highest for DCT transform technique.In comparison to this technique MSE for other techniques is very small (negligible)[8].

$$MSE = \frac{1}{kl}\sum_{x=0}^{k-1}\sum_{y=0}^{l-1}[I(x,y) - K(x,y)]^2 \quad (4)$$

Table 1: Comparison of steganography techniques in terms of MSE

Image Size	LSB Technique	Pseudo Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual Cryptography Technique	
						Share 1	Share 2
64X64	0.035	0.029	121.00	8.1e-004	0.013	0.18	0.18
128X128	0.009	0.008	122.00	4.5e-004	0.004	0.17	0.17
192X192	0.004	0.003	59.90	1.7e-004	0.002	0.17	0.17
256X256	0.002	0.002	34.08	1.3e-004	8.7e-004	0.17	0.17
320X320	0.001	0.001	22.12	5.2e-004	6.5e-004	0.17	0.17

- Peak Signal To Noise Ratio(PSNR):The result of applying various techniques and image size on PSNR are given below. The following inferences can be drawn from the results: PSNR is highest for distortion technique and minimum for DCT technique. Spatial domain techniques have high signal to noise ratio in comparison to DCT transform technique but lower than DWT transform technique. VC technique have PSNR value lower than spatial and DWT Technique but higher than DCT transform technique[9].

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

Image Size	LSB Technique	Pseudo Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual Cryptography Technique	
						Share 1	Share 2
64X64	62.72	63.36	27.30	79.03	67.17	55.60	55.60
128X128	68.80	69.09	27.30	81.60	71.58	55.70	55.70
192X192	72.28	72.93	30.35	85.78	75.16	55.80	55.80
256X256	74.89	75.62	32.80	87.08	78.70	55.80	55.80
320X320	76.76	77.24	34.68	90.96	80.00	55.80	55.80

Based on the visual quality and MSE of the stego-images in the above observations, LSB technique is chosen as the best technique for this project.

Least Significant Bit Substitution Technique (LSB): In this technique, the LSBs of the pixel values of cover image are modified according to bits of message. The simplest of LSB steganography techniques is LSB replacement for all pixels of image[10]. Since only LSB is changed, difference between the cover (i.e. original) image and the stego-image is hardly noticeable. Advantages of LSB are the picture quality of cover image is hardly affected. Hiding capacity is good. Very simple in implementation. Disadvantages are Robustness is less, the hidden data is subject to alternation due image manipulation. Detection of secret data is easy because of easy algorithm[11]. More information storage requires large image size thus requires high transmission rate due to large size of stego image.

Embedding Algorithm:

Step 1: Read the cover image and secret message.
Step 2: Break message in bits called secret bits. The message to be written can be available in either text message
or binary data. Text message is required to be converted to binary value first and then it can be embedded
into cover image.
Step 3: Image is converted to matrix of pixels where each pixel value can be accessed. Each pixel value in decimal
form is converted to binary and then its LSB is accessed.
Step 4: Each secret bit is checked sequentially. As per the value of bit, LSB of pixel will be modified. LSB of pixel of cover image is modified by each bit of secret message in sequence.
Step 5: This modified pixel value is fed back to its respective position. As per the size of message data LSBs of image pixels are modified.
Step 6: Write stego image.
Step 7: Performance evaluation of the stego-image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Obtain the stego image in matrix of pixels values.
Step 2: Access the LSB of pixel of stego image containing data. These bits are combined to form bytes and bytes
are combined to form the complete message data. For this step each pixel value of stego image is converted to binary and then its LSB is accessed which is secret bit.
Step 3: Retrieve bits and convert each set of 8-bits into character i.e. text message. This is required secret information.

III. RESULT ANALYSIS

The results obtained with Integer Wavelet Transform based Image Steganography are present below in terms of High capacity, MSE, PSNR, Coding efficiency, Compression ratio and redundancy

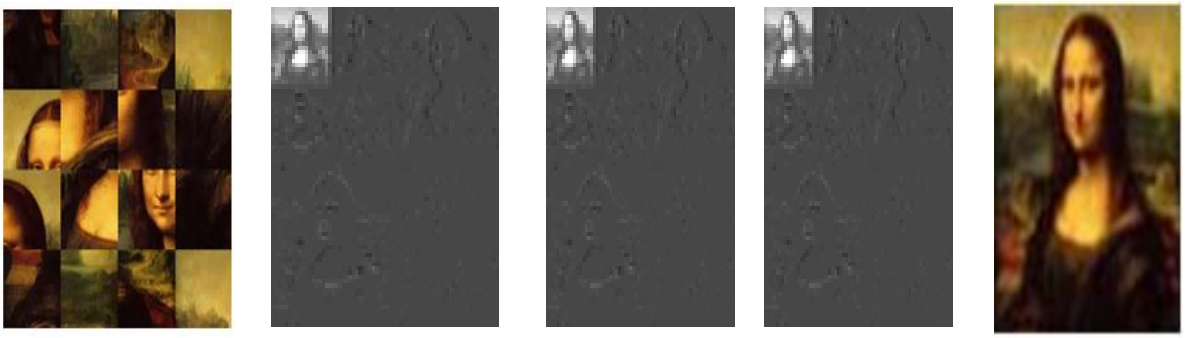
Cover image of size	64x64	128x128	256x256
high capacity	6141 symbols	24573 symbol	98301 symbol
mean square error	0.21	0.049	0.014
peak signal to noise ratio	255	255	255
coding efficiency	99.6%	94.16%	84.17%
compression ratio	1.808	2.77	3.66
redundancy	44.56%	63.96%	72.68%

	Color Image	**Gray Scale Image**
high capacity	98301 symbol	32765 symbol
mean square error	0.15	0.98
peak signal to noise ratio	255	255
coding efficiency	95.27%	98.62%
compression_ratio	3.5	1.96
redundency	67.29	49.07

Original image stego image given cover image adjusted over image

Steganography Psycho visual redundancy

Inter wavelet transform



Disordered image R-Component G-component B-component Obtained

Transformed image component

Psycho visual redundancy


Given cover image


adjusted cover image



Disordered image

Steganography Inter wavelet transform


Original image


Transformed image


Obtained information

IV. CONCLUSION

In this paper a secure and authentic image steganography technique is proposed to hide color images grayscale images and combination of both , which also tells how to hide data bits. The experimental results show that the technique produces good quality stego images with good mean square error, PSNR values, coding efficiency and compression ratio.

REFERENCES:

[1]. Samir K Bandyopadhyay, Debnath Bhattacharyya, DebashisGanguly, Swarnendu Mukherjee and PoulamiDas, "ATutorial Review on Steganography" (IC3–2008 UFL &JIITU, p. no. 105-114).

[2]. V.Srinivasa rao, Dr P.Rajesh Kumar, G.V.H.Prasad,M.Prema Kumar, S.Ravichand, "Discrete CosineTransform Vs Discrete Wavelet Transform: AnObjective Comparison of Image CompressionTechniques for JPEG Encoder", International Journal ofAdvanced Engineering & Applications, Jan. 2010.

[3]. M. F. Tolba, M. A. Ghonemy, I. A. Taha,, A. S. Khalifa"Using Integer Wavelet Transforms in Colored ImageStegnography",International Journal on IntelligentCooperative Information Systems, Volume 4, July 2004,pp 75-85.

[4]. Ahmed A. Abdelwahab and Lobna A. Hassaan, "ADiscrete Wavelet Transform Based Technique For ImageData Hiding", 25th National Radio Science Conference,2008.

[5]. Neda Raftari and Amir Masoud Eftekhari Moghadam,"Digital Image Steganography Based on Integer WaveletTransform and Assignment Algorithm", Sixth AsiaModelling Symposium, 2012, pp 87-92.

[6]. El Safy, R.O, Zayed. H. H, El Dessouki. A "An AdaptiveSteganographic Technique Based on Integer WaveletTransform", IEEE conference, 2009, pp 111-117.

[7]. Lai and L. Chang, "Adaptive Data Hiding for imagesBased on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319, 2006

[8]. Elham Ghasemi, Jamshid Shanbehzadeh and BahramZahirAzami, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm",IEEE conference 2011, pp 42-45.

[9]. Silvia Torres-Maya, Mariko Nakano-Miyatake andHéctor Perez-Meana, "An Image Steganography Systems Based on BPCS and IWT", 16th IEEE International Conference on Electronics, Communications And Computers, 2006.

[10]. Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi,Zhicheng Ni and Wei Su, "Distortionless data hiding based on integer wavelet transform", IEEE Electronicletters, December 2002 Vol. 38 No. 25, pp. 1646-1648.

