Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Approach to Reduce Distance Error between Cover and Stego Image Based on GA and IWT Algorithm

Ria Gandhi, Er. Girish
CSE, PTU (Punjab Technical University)
Punjab, India

Abstract*— Embedding maximum information in a stego-image with minimum change in its appearance has been a major concern in image-based steganography techniques. In this paper, we present a strategy of attaining maximum embedding capacity in an image in a way that maximum possible neighboring pixels are analyzed for their frequencies, to determine the amount of information to be added in each pixel. The technique provides a seamless insertion of data into the carrier image and reduces the error assessment and artifacts insertion required to a minimal. Present study attempts to reduce the error difference between the cover image and the stego image and to improve PSNR(peak signal to noise ratio) i.e the quality of the image and the hiding capacity with low distortion will be improved using two algorithms i.e GA(Genetic algorithm) and IWT(integer wavelet transform). The stegnographic methods used to hide information securely in an image file is LSB(Least Significant Bit), and transform domain embedding.We justify our approach with the help of an experimental evaluation on implementation of the proposed model. Steganography is the term used to describe the hiding of data in images to avoid detection by attackers. It is an emerging area which is used for secured data transmission over any public media

***Keywords*— Steganography, Cover Image, Payload, Stego Image, Discrete Cosine Transform (DCT), Inverse Discrete cosine transformation (IDCT) ,LSB, Bit length.**

I. INTRODUCTION

Adding maximum information in a stego-image with minimum change in its appearance has been a major concern in image-based steganography techniques.We present a strategy of getting maximum embedding capacity in an image in such way that the maximum possible neighboring pixels are analyzed for their frequencies,to determine the amount of information to be added in each pixel.The technique provides a seamless insertion of data into the carrier image and reduces the error assessment and artifacts insertion required to a minimal. Present study attempts to reduce the error difference between the cover image and the stego image and to improve PSNR(peak signal to noise ratio) i.e the quality of the image and the hiding capacity with low distortion will be improved using two algorithms i.e GA(Genetic algorithm) and IWT(integer wavelet transform).The stegnographic methods used to hide information securely in an image file is LSB(Least Significant Bit), and transform domain embedding.We justify our approach with the help of an experimental evaluation on implementation of the proposed model. Steganography is used to describe the hiding of data in images to avoid detection by attackers. It is an emerging area which is used for secured data transmission over any public media

II. THE PROPOSED ALGORITHM

Steganography is a way of transferring message in a way that the existing message is concealed. Steganography can utilize various medium as carriers of the message. These mediums can include various methods of steganography using text, like character marking, invisible ink, using pin pictures, type-writer correction), images, and audio, video signals. Most of the steganography techniques use images as a stego-medium. We can hide Information in images through many different ways. The most common approaches used to hide information in images are: Least significant bit (LSB) insertion, Masking and filtering techniques, Algorithms and transformations. Masking and filtering techniques hide information by marking an image in a manner similar to paper watermarks. Because watermarking techniques are more integrated into the image, they may be applied without fear of image destruction from lossy compression. The least significant bit insertion (LSB) is the most widely used image steganography technique. It embeds message into the least-significant bits of each pixel.To increase the embedding capacity, two or more bits in each pixel can be used to embed message, which has high risk of delectability and image degradation. The LSB techniques might use as a fixed least significant bit insertion scheme, in which the bits of data added in each pixel remains constant, or a variable least significant bit insertion, in which the number of bits added in each pixel vary on the surrounding pixels, to avoid degrading the image fidelity In the paper we discuss the embedding of text into image through variable size least significant bit insertion. The process of insertion of text in our proposed approach is not sequential, rather it follows a random order, based on a random algorithm. This technique aims at providing not only maximum insertion capacity, but also performs a maximum analysis of surrounding pixels to determine the embedding capacity of each pixel. The process results in a stego-image which is very much similar in appearance to the original image. we propose a steganography model that ensures maximum embedding of information in both gray scalable and colored images, and also ensures that

maximum pixels are analyzed to determine the embedding capacity. This leads to a reduction of the overall error induction in the image. The stego-image obtained after application of this analysis would not only have maximum amount of information, but would also have the minimum difference in appearance with the original image.

Present recent research discuss the practical application of detection algorithms and the mechanisms for getting around them.Applying LSB technique during discrete cosine transformation (DCT) on cover image.

III. EXPERIMENTAL RESULTS

In this technique, the colour image is decomposed into three components R, G and B. Watermark information will be embedded in the G plane using equation 1 to produce G'. Assume that f (i, j) represents the pixel of the component of the RGB representation of the colour host image, w (i, j) represents the binary pixel of the watermark.

$$F_k(u,v) = DCT\{f_k(i,j)\},$$

If w(i,j)=1 then

$$F_k(x,y) = \begin{Bmatrix} \Delta Q_e(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{Bmatrix}$$

If w(i,j)=0 then

$$F_k(x,y) = \begin{Bmatrix} \Delta Q_o(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{Bmatrix}$$

Where Qe is the quantization to the nearest even number and Qo is the quantization to the nearest odd number Δ is a scaling quantity and it is the quantization step used to quantize either to the even or odd number. The predefined coefficients in each 8x8 sub block are represented by NHB. The binary watermark digits are randomly scrambled using a secret key; this scrambling process is essential to reduce the spatial correlation between the host image and the embedded watermark. After the scrambling process, a shuffle scheme is applied for each binary watermark copy before embedding. Different shuffle schemes can be applied. Simple shuffle technique is used to reshape the watermark copy as vector and shift the vector by different shifts before the binary watermark digits are randomly scrambled using a secret key; this scrambling process is essential to reduce the spatial correlation between the host image and the embedded watermark. After the scrambling process, a shuffle scheme is applied for each binary watermark copy before embedding. Different shuffle schemes could be applied. Simple shuffle technique is to reshape the watermark copy as vector and shift the vector by different shifts before the .Where WSB is the number of watermark shifted bits, The shift is necessary to reduce the spatial relation and to increase the robustness against vertical cropping attacks.

The embedded information w (i,j) can be extracted by performing 8x8 DCT transform for the watermarked host image and indicate the same coefficients of the host image that carries the 16 bits of the embedded watermarks using the same secret key in the initial scrambling operation. The scrambled watermarks are descrambled to get the original watermarks. The watermark information can be retrieved by using a reverse process to the shift scheme which has been applied in the embedding process.It will yield the original bits order.Although the proposed scheme is blind since it does not require the original host image for reconstruction, but it needs the information such as the sizes of both host image and watermark image. Finally, discard the totally degraded copy of the extracted watermarks and then calculate the average by summing the resultant watermark copies divided by their number, select the resultant average watermarks as the final reconstructed watermark or choose one copy of the extracted watermarks as the final watermark if it provides better result than the resultant average watermark. The bit extraction formula is shown in equation.

$$If \quad Q(\frac{F_k(x,y)}{\Delta}) \text{ is odd} \quad \text{then } w(i,j)=0$$

$$If \quad Q(\frac{F_k(x,y)}{\Delta}) \text{ is even then } w(i,j)=1$$

Where Q is rounded to the nearest integer, the scaling quantity is the same as the one used in the embedding process.

The following steps are followed in this case: -

1. The Image is broken into data units each of them consists of 8 x 8 block of pixels.
2. Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.
3. After applying DCT, one DCT Coefficient is generated for each pixel in data unit.
4. Each DCT coefficient is then quantized against a reference quantization table.
5. The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.
6. Encoding is applied to each modified quantized DCT coefficient to produce compressed Stego Image.

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir andLeonard Adelman.

IV. EXPERIMENTAL RESULTS

The proposed method is applied on SI2xSI2 8-bit image "Lena". The simulation is implemented on 2.SGHZ Core 2 Duo processor, 4GB RAM and Windows Vista OS and Matlab7.6. The messages are generated randomly with the same length as the maximum hiding capacity.

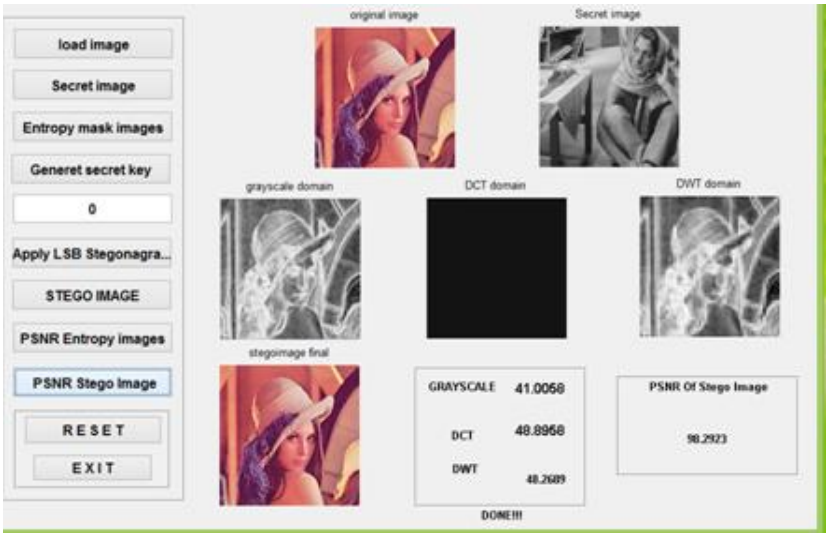

Fig. 1.application of proposed algo on lena image.

Table I shows the stego image quality by PSNR Human visual system is unable to distinguish the grayscale images with PSNR more than 3S dB. The paper embedded the messages in the 4-LSBs and received a reasonable PSNR. "Fig. 1" shows the images after and before embedding. Table I shows the capacity and the PSNR of the proposed method.

Table I: Proposed values of capacity and psnr

Image name	Hiding capacity	PSNR
Lena Image	32768000	94.7777
Baboon image	9730000	98.2923
Blue hills colour image	25281000	91.4802
Pepper colour image	12510000	92.4116

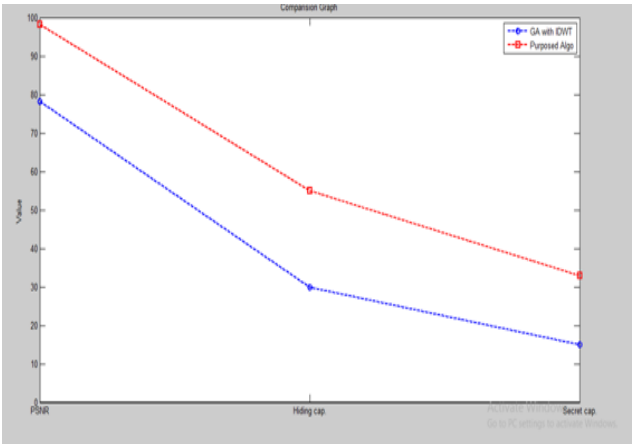

Fig. 2 Comparison performance analysis of Lena for two methods.

"Fig. 3" shows that when the size of message increases, the histogram tends to be smoother.

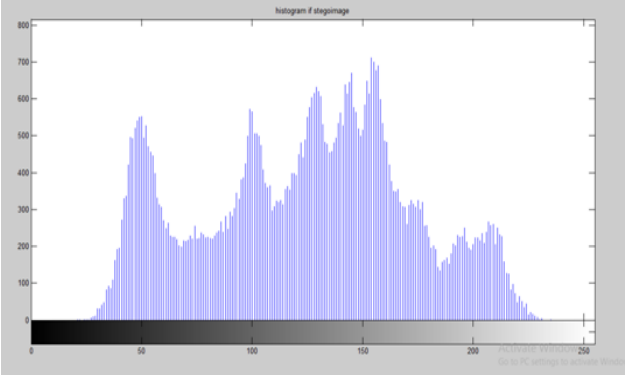

Fig. 3 Histogram of Lena

V. CONCLUSION

The steganography is used in the covert communication to transport secrete information. In this paper Bit Length Replacement Steganography using Segmentation and DCT is proposed. The cover image is segmented into smaller matrix of size 8x8 and converted to DCT domain. The MSB bits of payload in spatial domain are embedded into each DCT coefficients of cover image based on the coherent length L which is determined by the DCT coefficient values. GA is used in various techniques to obtain an optimal mapping function to reduce the error difference between the cover and the stego image The performance results in terms of PSNR for different kinds of images and dimensions are better in the proposed algorithm compared to the existing algorithm. In future the technique can be verified for robustness. We added the RSA algorithm process with it.

REFERENCES

[1] Avinash K. Gulve[1] and Madhuri S. Joshi (2015),"An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach"11 pages.

[2] Zaid Al-Omari,Ahmad T.Al-Taani(2015)," A Survey on Digital Image Steganography",ICIT.

[3] P Chaturvedi, RK Bairwa (2014), "An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images",In:Int. J Recent Research and Review, Vol. VII, Issue 1,ISSN 2277 – 8322.

[4] Pratap Chandra Manda (2014)," A STUDY OF STEGANOGRAPHY TECHNIQUES USINGDISCRETE WAVELET TRANSFORM,JGRCS Vol 5

[5] Amrita Khamrui, J. K. Mandal (2014)," A Wavelet Transform Based Image Authentication Approach Using Genetic Algorithm (AWTIAGA)", Volume 248, 2014, pp 251-258.vol-1., Springer International Publishing.

[6] CR Gaidhani, VM Deshpande (2014),"Image Steganography for Message Hiding Using Genetic Algorithm",Vol-2,ISSN: 2347-2693.

[7] Tripathy, Abhishek; Kumar, Dinesh (2014)," Secured Cryptography cum Steganography Model with Large Message Embedding behind Colored Image by using Genetic Algorithm and OPA Process". International Journal of Computer Applications (0975 – 8887) Volume 85 – No 12, January 2014.

[8] Abhishek Tripathy, Dinesh Kumar (2014)," Image Steganography By Using Integer Wavelet Transform And Genetic Algorithm To Perform Text Based Hiding Behind Gray Scaled or Colored Image", International Journal of Recent Research and Review, Vol. VII.

[9] Stuti Goel, Arun Rana,Manpreet Kaur (2013), " A Review of Comparison Techniques of Image Steganography",Global J Computer Science and Technology,Vol 13

[10] S Atawneh, A Almomani, P Sumari (2013)," Steganography in digital images: Common approaches and tools",IETE ,Vol 30,pp 344-358.

[11] Shikha Sharda, Sumit Budhiraja (2013)," Image Steganography: A Review".,Int J Emerging Technology and Advanced Engineering Vol 3.

[12] N. Ajeeshvali,B.Rajasekhar (2012)," Steganography Based on Integer Wavelet Transform and Bicubic Interpolation", IJIGSP, vol.4,PP.26-33.

[13] Saeed Masaebi,Amir Masoud Eftekhary Moghaddam (2012),"A New Approach For Image Hiding Based On Contourlet Transform",Int j electrical and computer engineering,Vol 2.

[14] Raftari, N,Qazvin Azad Univ,Qazvin, Iran,Moghadam (2012)," Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT",A.M.E Dept. of Electr., Comput. & IT Eng.

[15] Shiva Kumar,K.B,Khasim,T.Raja,K.B (2011),"Dual Transform Technique for Robust Steganography", Computational Intelligence and Communication Networks (CICN),pp:310 – 314

[16] Ching-Yu Yanga ,Wu-Chih Hua and Chih-Hung Lin (2010)," Reversible Data Hiding by Coefficient-bias Algorithm", Journal of Information Hiding and Multimedia Signal Processing,vol 1.

[17] Nan-I Wu,Chung-Ming Wang ,Min-Shiang Hwang (2007)," Data Hiding: Current Status and Key Issues",Institute of Computer Science and National Chung Hsing University.

[18] Mehdi Kharrazi,Husrev T. Sencar,Nasir Memon,Edward J, Ping W. Wong (2005)," Benchmarking steganographic and steganalysis techniques",San Jose, CA.

[19] Chi-Kwong Chan ' L.M. Cheng (2001)," Improved hiding data in images by optimal moderately-significant-bit replacement",Department of Electronic Engineering, City University of Hong Kong,Vol 37, pp 1017 – 1018.

[20] Bender.W,Gruhl,D.Morimoto, N. Lu, A (1996)," Techniques for data hiding",IBM Systems Journal,Vol 3,pp:313–336.

