International Journal of Engineering &Technology, 7 (3.12) (2018) 1202 -1204

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Robust Watermarking using Genetic Algorithm in DCT Domain

Raj Vikram Singh[1], Subodh Waria[2], Rajiv Kumar Singh[3], Harsh Vikram Singh[4]

[1, 2, 3]Department of Electronics & Communication, IET Lucknow
[4]Department of Electronics, KNIT Sultanpur

Abstract

In this paper, a novel and efficient data hiding using Genetic Algorithm in DCT Domain implemented. Watermarking is an essential zone of research as of late including various applications. It is the investigation of inserting data into the cover picture viz., content, video, and picture (payload) without making measurably huge change the cover picture.

Keywords: Least Significant Bit (LSB), 5th Significant Bit, Discrete Cosine Transform (DCT), Digital Watermarking

1. Introduction

The word steganography (Data Hiding) is gotten commencing the ancient Greek vocabulary stegos means cover and graaphia means hiding [1]. In image hiding the data is concealed only in images. The uniqueness can be alluded to as cover content, cover picture, or cover sound. After embedding the mystery data it is alluded to as stegomedium. A stegokey is utilized for concealing/encoding procedure to limit location or extraction of the implanted message [2].
Imperceptible hiding for a dependable device. So pictures are caught with a computerized camera for later incorporation in news articles. Here, it is the craving of a news organization to confirm that a picture is consistent with the first catch and has not been altered to adulterate a scene [3-8]. For this situation, an undetectable watermark is installed at catch time; its quality at the season of distribution is planned to show that the picture has not been gone to since it was caught [9-12].
Numerous specialists have utilized DCT, DWT and different strategies for watermarking yet at the same time there is an expansive extent of change for concealing the information in Images. At first, existing calculations will be utilized for watermarking and further vigorous calculations will be proposed through this work for information stowing away in Images. The result of research will be valuable for different applications, for example, Military, Network security, information verification and so on [13-18].
In this paper Section 2 provides the definitions and algorithms of all three methods i.e. LSB Insertion Method, 5th Significant Bit Insertion Method and DCT Method. Section 3 provides simulation Results using MATLAB and comparative chart for analysis. Finally section 4 concludes the paper.

2. Proposed Methods and their Algorithms for Digital Watermarking

2.1 Least Significant Bit (LSB)

Digital Watermarking based on LSB is simplest method, used to embed the secret data into the least significant bits of the pixel.

Here number 240 is embedded into first eight bytes of the grid and but practically only 5 bits are changed.

Part 1: Embedding Algorithm
(i) Read the cover image
(ii) Read the Secret text message
(iii) Read the Secret key
(iv) Convert the secret text into binary form
(v) Encoding : Hide stream of bits of secret text message into the image at LSB (8th bit) positions sequencely.
(vi) Save the Watermarked image.

Part 2: Algorithm to Extract
Extracting is done as follows:
(i) Read the Watermarked image.
(ii) Read secret key
(iii) Convert secret key into binary form
(iv) Extract stream of bits of the Secret Key
(v) Compare both the secret keys
(vi) If both secret keys are same, Extract stream of bits of secret text message from Watermarked image by extracting the LSBs sequencely.
(vii) Rearrange the extracted bits and regenerate the ASCII secret text.

2.2 5th Significant Bit Insertion Method

In this method, the 5th significant bit of each 8-bit pixel of a cover image is used to hide the binary data.
To hide 240 (11110000) can be hidden in the first eight bytes of 8-bit grayscale image.

00100111 11101001 11001000 00100111
11001000 11101001 11001000 00100111
240: 11110000

Result:

00101111 11101001 11001000 00101111
11000000 11100001 11000000 00100111

Part 1: Embedding Algorithm
(i) Read Cover
(ii) Read the hidden message

(iii) Read the Secret key
(iv) Convert the secret text into binary form
(v) Encoding: Hide stream of bits of secret text message into the image at 5th significant bit positions sequencely.
(vi) Save the Watermarked image
Original as well as hidden Watermarked images are shown in Figure 3 and Figure 5 respectively.

Part 2: Algorithm to Extract Secret Text Message
Extracting is done :
(i) Read the Watermarked image.
(ii) Read the Secret Key
(iii) Convert the secret key into binary form
(iv) Extract stream of bits of Secret key
(v) Compare both the secret keys
(vi) If both secret keys are same, Extract stream of bits of secret text message from Watermarked image by extracting the 5th significant bits sequencely.
(vii) Rearrange the extracted bits and regenerate the ASCII secret text.

2.3 Proposed DCT Algorithm

Part 1: Embedding Algorithm
Embedding is done as:
(i) Reading original cover image I of size (M,N) in BMP .
(ii) Read the Secret text message
(iii) Read the Secret Key.
(iv) find the length of the secret text (T)
(v) Find the maximum text length which can be embedded in the Image(T_{max})
(vi) If $T_{max} > T$
(vii) Convert cover image into Blocks. Each Block consists of 64 pixels (8x8).
(viii) Perform DCT to convert spatial Domain into Transform Domain and get 64 DCT coefficients of each (8x8) pixels block.
(ix) Convert the secret text into n-bit binary form (D_d).
(x) For D_d =1 to n,
Hide the D_d^{th} bit of the secret message into D_d^{th} DCT block of the cover image as follows :.
a) If bit of binary message = = '0',
B(i,j) should be greater than B(u,v). If B(i,j) is less than B(u,v) than interchange the value of these two coefficients.
b) If bit of binary message = ='1',
B(u,v) should be greater than B(i,j), If B(u,v) is less than B(i,j) than interchange the value of these two coefficients.
Where B(i,j) and B(u,v) are the two mid-band DCT coefficients of D_d^{th} block of the cover image .
(xi) Apply Inverse DCT to reconstruct the image by recombining all the blocks.
(xii) Save the Watermarked image I(M,N) in BMP format of size MxN

Part 2: Extracting Algorithm
The extracting is done as:
(i) Reading the Watermarked image I of size MxN.
(ii) Read the secret key.
(iii) Convert the secret key into binary form
(iv) Extract stream of bits of secret key
(v) If both secret keys are same, Convert Watermarked image into Blocks. Each Block consists of 64 pixels (8x8).
(vi) Perform DCT to convert spatial Domain into Transform Domain and get 64 DCT coefficients of each (8x8) pixels block.
(vii) for D_d^{th} = 1 to n ,
Extract the D_d^{th} hidden bit 'b_d', using relationship given below :

$$\begin{cases} b_d = 0, \text{ if } B(i,j) > B(u,v) \\ \quad\;\; 1, \text{if } B(i,j) < B(u,v) \end{cases}$$

Where, 'b_d' is the bit of the secret text.
(viii) Rearrange the extracted bits and regenerate the ASCII secret text.

3. Results and Analysis

Peak Signal to Noise Ratio (PSNR) as well as Mean Square Error (MSE) are mostly applicable parameters for feature measure and their corresponding equations are also given below. [9] Consider two images, x (a, b) and y (a, b) of M×N dimensions. The formula for mean square error is [12]

$$MSE=\frac{1}{MN}\sum_a\sum_b[x(a,b)-y(a,b)]^2$$

$$PSNR=10\log\left(\frac{255}{\sqrt{MSE}}\right)$$

Fig. 1: lena.bmp (Original Image)

Fig. 2: lena.bmp (Watermarked Image) using LSB Method

Fig. 3: lena.bmp (Watermarked Image) using 5th significant bit Insertion Method

Fig. 4: lena.bmp (Watermarked Image) using DCT Method

Frome figure 5, it can be obersevered that, for the same length of the secret text, the PSNR values are not same. In LSB Method, the PSNR values are comparatively high. It shows that the imperceptibility of hidden picture is comparatively high. In 5th significant bit insertion method, the PSNR values are less than the LSB Method but more than the DCT Method. It shows that the imperceptibility of the watermarked image is better than the DCT

Method but less than LSB Method. In case of the DCT Method, the PSNR values are comparatively low.
From figure 7, it can be oberserved that, using the LSB Method or using the 5th significant bit insertion method, the bit error rates are almost same . In case of the DCT Method, the BERs are comparatively high. It shows that, for the same length of the secret text, DCT Method changes more number of bits of the image.

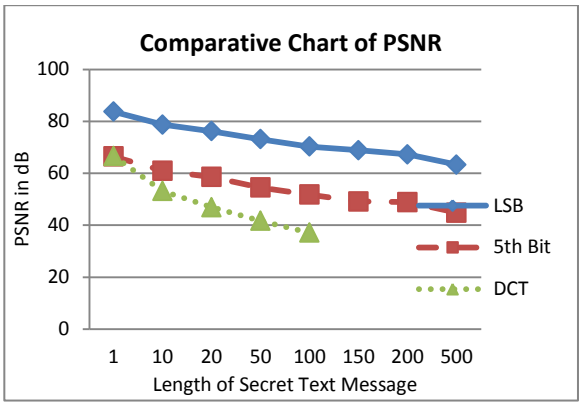

Fig. 5: Comparative chart of PSNR verses character length of the secret text

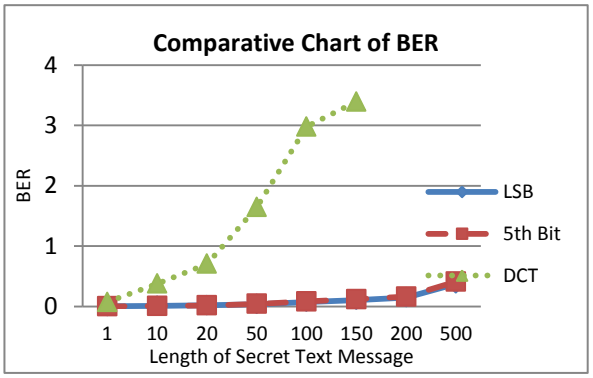

Fig. 6: Comparative chart of MSE verses character length of the secret text

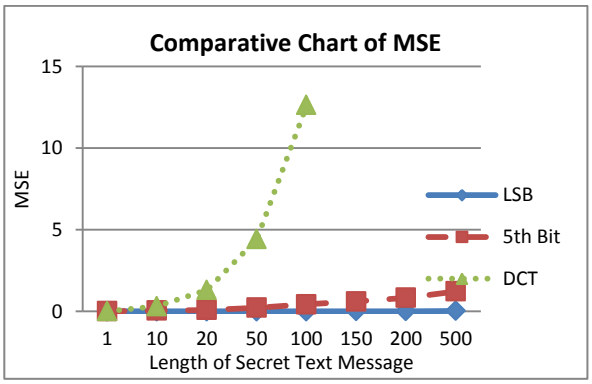

Fig. 7: Comparative chart of MSE verses character length of the secret text

The conclusion of the analysis, that have been conducted in this section, is tabulated in following table.

Table 1: The Conclusion of all analysis

Items	LSB insertion method	5th significant bit insertion method	DCT method
Domain	Spatial	Spatial	Frequency
Security	Weak	Moderate	Strong
Detection	Suspicious	Difficult to be suspected	Very difficult to be suspected
Required size of the image (for same length of the Secret Text)	Small	Small	Large
Robustness	Low	Moderate	High
Image degrading	Low	Moderate	High
Imperceptibility	High	Moderate	Low
Length of the Secret Text (for same image size)	High	High	Low

4. Conclusion

This paper has presented three algorithms i.e. LSB insertion Method, 5th Significant Bit Insertion Method and DCT Method for data hiding. It can be concluded from table that present method is very useful for watermarking.

References

[1] R. Anderson, "Information Hiding," Proceedings of the First International Workshop on Information Hiding, LNCS, vol. 1174, pp. 137-150, Cambridge, U.K., May 1996.
[2] A. Shizaki, J. Tanimoto, and M. Iwata, "A Digital Image Watermarking Scheme Withstanding Malicious Attacks," IEICE Transaction on Fundamentals of Electronics, Communications and Computers, pp. 2015-2022, October, 2000.
[3] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proceedings of IEEE, vol. 86, no. 6, pp. 1079-1107, June, 1998.
[4] M. D. Swanson, B. Zu, and A. H. Tewfik, "Robust Data Hiding for Images," 7th IEEE Digital Signal Processing Workshop (DSP 96), pp. 37-40, Loen, Norway, September, 1996.
[5] N.J. Hopper, J. Langford, and L. Ahn, "Provably Secure Steganography," Proc. of the 22nd Annual International Cryptography Conference, vol. 2442, pp. 77-92, California, U.S.A., August, 2002.
[6] E.J. Delp and R.B. Wolfgang, "A Watermark for Digital Images," Proc. of International Conference on Image Processing, pp. 219-222, 1996.
[7] W Bender et al, "Techniques for data hiding," IBM Systems Journal, vol. 35, pp. 313-336, 1996.
[8] R.B. Wolfgang, and E.J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies," Proc. of the International Conference on Imaging, Systems and Technology, pp. 279-287, USA, 1997.
[9] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Proc. of the 3rd International Workshop on Information Hiding, LNCS, vol. 1768, pp. 61-76, Germany, 1999.
[10] M.S. Hsieh D.C. Tseng, and Y.H. Huang "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," IEEE Transactions on Industrial Electronics, vol. 48, pp.875-882, 2001.
[11] S. Bhama, H. Singh, and N.D. Phadte, "Parallelism for Faster Implementation of the K-L Transform for Image Compression," Pattern Recognition Letters, vol. 14, no. 8, pp. 651-659, 1993.
[12] Y.L. Guan and J. Jin, "An Objective Comparison Between Spatial and DCT Watermarking Schemes for MPEG," Proc. of the International Conference on Information Technology: Coding and Computing, pp. 207- 211, Las Vegas, U.SA.
[13] A.G. Tescher, Transform Image Coding, Academic Press, New York, 1979.
[14] J.R. Hernandez, M. Amado, and F. Perez Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and A New Structure," IEEE Transactions on Image Processing, vol. 9, pp. 55-68, 2000.
[15] P.K. Amin, N. Liu, and. K.P. Subbalakshmi, "Statistically Secure Digital Image Data Hiding," Proc. of the IEEE 7th Workshop on Multimedia Signal Processing, Shanghai, pp. 1- 4, 2005.
[16] S.A. Khayam, "The Discrete Cosine Transform (DCT): Theory and Application," ECE 802 – 602: Information Theory and Coding, Michigan State University, March, 2003.
[17] J. Wang and L. Ji, "A Region and Data Hiding Based Error Concealment Scheme for Images," IEEE Transactions on Consumer Electronics, vol. 47, no. 2, pp. 257-262, 2001.
[18] R.C. Gonzalez and R.E. Woods, Digital Image Processing, Pearson Education, 2004.