International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Design and Development of Semi-Blind Image Steganography Algorithm using DCT for Securing Text Documents which Resist against JPEG Compression

Darshan Mehta, Dharmendra Bhatti

Abstract: ***Semi-blind Image Steganography algorithm development proposed by using DC coefficients of DCT technique. Create KEY vector and potential block matrix while embedding the secret data. Embed one secret character in one DCT block using the DC value of each block. Convert DC coefficient to binary representation and store positions for secret data. Apply JPEG compression on Stego Image. While extracting the secret data from compressed Stego Image, with the use of a KEY vector extracts secret data bits from potential blocks. After creating simulation, perform some test on a standard dataset and compare the results with target results.***

Keywords: DCT, Image Steganography, JPEG Compression, Key Vector, Potential Block Selection, RLE

I. INTRODUCTION

As far as development is a concern, three types of Image Steganography: Non-blind, Semi-blind and Blind [15]. In Non-blind techniques, Cover Image is available at the receiver side or Extraction phase. In Semi-blind, part of a cover image or some computation, vectors are shared between parties. In Blind techniques, Cover Image is not available at receiver side or Extraction phase. The main challenge in Image Steganography is to extract embedded secret data in any situation even though Stego Image suffers through any Intentional/non-intentional image processing and manipulation operations/attacks [16]. To develop an Image Steganography algorithm which withstands against all the attacks in one is almost an impossible task [11]. Out of many attacks, JPEG lossy image compression attack on Stego Image is one of the most challenging attacks concerning Image Steganography. It is considered as one of the difficult tasks to extract secret data from Stego Image after it suffers from JPEG compression attack. As JPEG compression algorithm work on DCT technique, it is most likely to employ/develop Image Steganography techniques, which utilize the properties of DCT techniques with an understanding of that what JPEG compression algorithm does with the Image to compress it. Image Steganography algorithm performance constrained by three parameters: Payload, Imperceptibility, and Robustness [8]. The payload in terms of a secret message as a bits insert into Cover Image. Imperceptibility in terms of visibility difference between Cover Image and Stego Image technically measured by PSNR and MSE.Robustness term refers in context to survive algorithm against intentional/unintentional JPEG Image lossy compression attack. We have developed a Semi-blind Image Steganography algorithm for securing text document which resists against JPEG compression.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Darshan Mehta*, Computer Science and IT, VNSGU, Surat, India.
Dr.Dharmendra Bhatti, Computer Science, UTU, Bardoli, India.

II. LITERATURE REVIEW

As per paper[1] proposed a robust blind image watermarking scheme with the use of a combination of DCT, SVD, and DWT transform domain with using a logistic chaotic map and least-square curve fitting. As per paper [2] presents a digital watermarking technique using DCT and psycho visual threshold which achieves good imperceptibility and robustness for copyright protection.

As per paper [3] propose a watermarking scheme of images with utilizing joint two transforms namely DWT and DCT and its properties. As per paper [4] implemented a data hiding technique on a digital image with combining cryptography and steganography by utilizing PN-Sequence, Discrete Cosine Transform (DCT) and One Time Pad (OTP). As per thesis [5] proposed A novel approach to robust digital image watermarking algorithms using artificial intelligence techniques. As per paper [6], the proposed method in a compressed Digital Color Image provides hiding a binary watermark. The given Color Image is transformed from RGB color space to YCbCr and then a middle band of DCT, the luminance (Y) component is used for watermarking processes. As per paper [7] propose a scheme of watermark embedding and extracting based on DCT transform and JPEG quantization table. The image is divided into non-overlapping 8*8 blocks, and each block is transformed by DCT. Then, a pair of points with the same quantization value is selected by the JPEG quantization table to embed one watermark bit, and the adjustment coefficients are adaptively selected by using the visual masking property of HVS.

As per paper [14] used edge entropy methods, optimal DCT psychological threshold, and visual entropy. Edge entropy and Visual entropy methods provide the most significant part to embed secret data. Cover image divides into 8*8 blocks, select blocks based on the lowest entropy values and modifies middle frequency coefficients of selected blocks.

III. PROPOSED ALGORITHM

MATLAB R2017a is use for experiments and simulation. Standard JPEG Images used like Lena, Baboon, and Cameraman etc. with dimensions of 512*512, Gray Scale- 8 bit depth per pixel. AMD A10-9600p RADEON R5 processor with 6GB RAM and Windows 10 Home – 64 bit OS is use.

Proposed Algo. (Embedding):

Algorithm: Embedding Algorithm

Input: Cover Image as JPEG Image, Secret Message

Output: Stego Image

1. Input cover image 512*512(gray scale 8- bit depth), standard images like Lena, baboon etc...

   1.1 IF cover image= color image THEN

   Convert to Gray scale

   Store cover image in (I) matrix

2. Input Secret data file

   2.1 Read secret data from .txt file

   2.2 store secret date in (sm) vector

3. Store the dimensions (M, N) of cover image

4. Transform Cover Image into 8*8 blocks

   4.1 convert each block in DCT

   4.2 consider DC coefficients of each block

   4.3 create DC coefficients Matrix

   4.4 Estimate the to be compressed cover image with JPEG compression on QF=50 with decoding JPEG algorithm and its quantization matrix

   4.5 create DC coefficients Matrix of step 4.4

   4.6 Store the size of both DC coefficient Matrix(R, C, R1, C1) respectively

   4.7 Initialize Key Vector as NULL, Initialize potential_block = zeros(R, C)

   4.8 For each i=1: R
   For each j=1: C

   4.8.1 IF first 4 bits of Cover Image DC coefficients==Estimated DC coefficients && contain atleast one '0' and one '1' bit THEN

   Potential_block (i, j) =1

   4.8.2 REPEAT for Each Character (sm (smindex)) i.e. 8 bits

   Append index position of desired bits sequence in KEY Vector

   END 4.8.2

   END 4.8.1

   END 4.8

5. Compress secret KEY vector with RLE and make it shared global variable

6. Make potential_block matrix as shared global variable

7 Apply IDCT and write the image

8. Got Stego Image

9. Apply JPEG Compression attack with different QF=50

10. Got Compressed/Attacked Stego Image

Proposed Algo. (Extraction):

Algorithm: Extraction Algorithm

Input: Compressed Stego Image, KEY Vector, potential_block matrix

Output: Secret data

1. Input Compressed Stego Image and utilize shared global variables KEY Vector, potential_block matrix

2. Initialize (data) and (secstr) vectors as NULL

3. Decompress secret KEY vector with RLE (which was compressed in embedding process) and store (key) variable

4. Apply DCT and create DC coefficients Matrix of attacked/compressed stego image

5. Store the size of DC coefficients matrix in (R1,C1)

6. For each i=1:R1
   For each j=1:C1

   6.1 IF potential_block (i, j) ==1 THEN

   6.2 REPEAT for Each Character i.e. 8 bits

   6.2.1 According to Key Vector Position

   6.2.2 Extract secret data binary bit (one at a time)

   6.2.3 Append each binary bit to (data) variable

END 6.2

6.2.4 Convert 8 bits to its equivalent secret data character

6.2.5 Append each secret character in (secstr) vector

6.2.6 Make (data) to NULL in each iteration

END 6.1

END 6

7. Write secret data (secstr) vector to .txt file and create the file.

8. Check the similarities/difference of original secret data and extracted secret data

IF CC=1 THEN

Secret data are identical

ELSE

Not identical

IV. RESULTS AND DISCUSSION

Parameters:

1. PSNR and MSE: Compute Peak Signal to Noise Ratio between Images in Decibels between two Images. Higher PSNR means the quality of a reconstructed image is better. The MSE represents the cumulative squared error between the reconstructed and the original Image. Lower MSE means lower error.

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

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

2. Payload: Size of / No. of Bits

i.e. Payload = no. of bits of secret message/no. of bits of cover image

3. CR: CR=Stego Image size / Compressed Stego Image Size, as CR increases IQ/QF decreases.

Mapping formula to IQ/QF: QF*100/Stego Image size=Comp. Stego Image size

4. IQ/QF: Max.=100% Min.=1%, as percentage reduces Image quality decreases and CR increases

Mapping formula to CR: CR*Comp. Stego Image size= Stego Image Size

5. ER (NCC): Max = 100% or NCC=1, as percentage reduces Extraction Rate decreases

Table 1. Target Result Set

Sr.No.	Cover Image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER	Ref.
1	512*512 (gray scale 8 bit depth)	1024	40.07	IQ=10, 20, 30, 50, 70	0.8382, 0.8502, 0.8867, 0.9449, 0.9859	[1]
2		1024	45.689	IQ=30, 40, 50, 60, 70	0.7769, 0.8733, 0.9990, 1, 1	[2]
3		1024	43	IQ=60	0.9734	[3]
4		1024	54.362	IQ=50, 75	0.934, 0.995	[4]
5		1024	44.85	IQ= 100, 90, 80, 60, 40,20	0.8957, 0.8347, 0.8173, 0.5726, 0.5654, 0.3931	[5]
6		4096	40.16	IQ= 50, 60, 70, 80, 90	1 for all IQ	[6]

Sr.No.	Cover Image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER	Ref.
7		4096	37.392	IQ= 45, 55, 65, 75, 85, 99	0.7482, 0.8137, 0.9403, 0.9967, 0.9983, 0.9983	[7]

Table 2. Proposed Algorithm Result

Cover Image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER	Ref.
512*512 (gray scale 8 bit depth)	24768	79.60	IQ=50	1	Proposed scheme

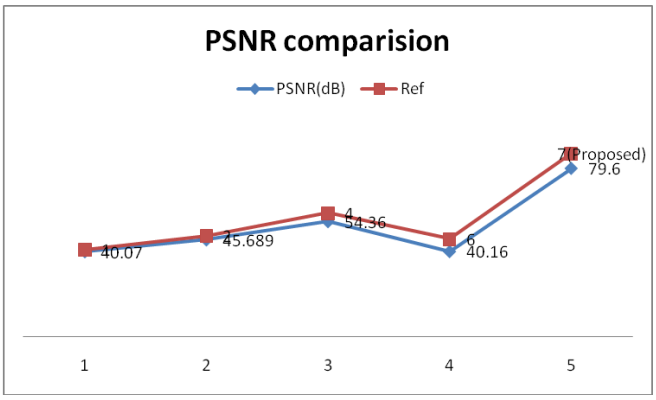

Fig 1. PSNR comparison chart

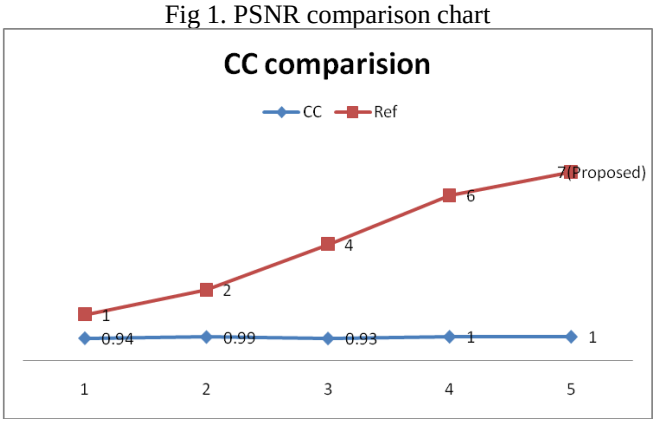

Fig 2. CC comparision chart

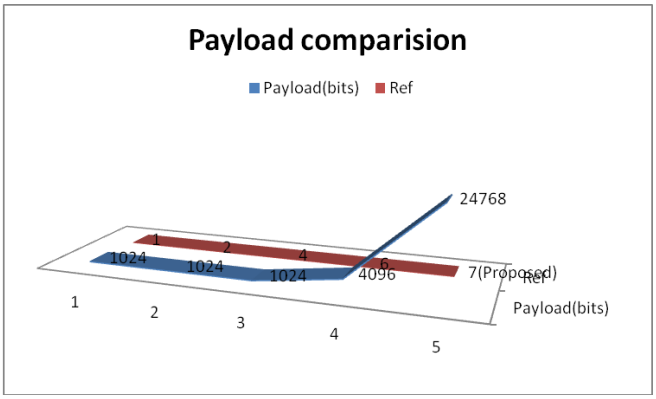

Fig. 3 Payload comparison chart

V. CONCLUSION

We have proposed Image Steganography algorithm development using DCT techniques. It is considered as Semi-blind Image Steganography technique. We have implemented and compared our results with other results. Our results prove that our system outperforms the existing techniques available in the targeted comparison data set. In the future, one can improve our proposed results and aims to reach Blind Image Steganography development with improving all the considered three parameters like robustness, payload, and imperceptibility.

REFERENCES

1. Xiao-bing Kang et al. (2017) A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength.CrossMark- Springer Science+Business Media,Multimedia Tools Application,Springer.
2. Ferda Ernawan M et al.(2018) A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold.IEEE Access.Volume 6 :20464-20480.
3. Salah Mokhnache et al. (2018) A Robust Watermarking Scheme Based on DWT and DCT Using Image Gradient. International Journal of Applied Engineering Research.13 (4):1900-1907.
4. Setia A et al. (2017) An Improved Secure Image Hiding Technique Using PN-Sequence Based on DCT-OTP. 1st International Conference on Informatics and Computational Sciences: 47-52.
5. Jagadeesh B, A novel approach to robust digital image watermarking algorithms using artificial intelligence techniques, Jawaharlal Nehru Technological University, Anantapuram.2016: http://hdl.handle.net/10603/175659
6. Yesilyurt M. (2013) A New DCT Based Watermarking Method Using Luminance Component. Elektronika IR Elektrotechnika.19 (4):47-52.
7. Yun-Ping ZHENG et al. (2017) A Watermarking Algorithm Based on DCT and JPEG Quantization Table. ITM web of conferences. Open access article,ITA-2017-China:1-5.
8. Nagalinga R, Robust digital image steganographic schemes, Manonmaniam Sundaranar University.2015: http://shodhganga.inflibnet.ac.in
9. Sipi.usc.edu, 'standard image dataset' ,2018.[online]. Available: http://sipi.usc.edu/database/database.php?volume=misc .[Accessed: 28 – jul – 2018].
10. Imageprocessingplace.com, 'standard image dataset' ,2018.[online]. Available:http://www.imageprocessingplace.com/root_files_V3/image_databases.htm .[Accessed: 28 – jul – 2018].
11. Rejani R et al. (2015) Comparative Study of Spatial Domain Image Steganography Techniques. Int. J. Advanced Networking and Applications.7 (2):2650-2657.
12. L.Baby Victoria et al. (2015) A Study on Spatial Domain and Transform Domain Steganography Techniques used in Image Hiding. International journal of innovative technology and creative engineering.5 (5):273-276.
13. Mali S et al. (2012) Robust and secured image-adaptive data hiding. Elsevier- Digital Signal Processing.22:314-323.

14. Ernawan F et al. (2018) A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold.IEEE Access. Volume 6: 20464-20480.
15. Karan Nair et al. (2015) Implementing Semi-Blind Image Steganography with Improved Concealment . International Journal of Computer Applications, International Conference on Computer Technology,ICCT: 14-19.
16. Setiadi D et al. (2017) Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System. 2 (1) : 1-11

AUTHORS PROFILE

Darshan M. Mehta, Serving as a Assistant Professor in UCCC and SPBCBA and SDHG College of BCA & IT affiliated to VNSGU, Surat and Research Scholar at UTU, Bardoli. Completed M.C.A in 2006 and having 2 Yr Industry Experience and 10 Yrs Academic Experience.

Dr.D.G.Bhatti, serving as a Professor and IT Head at UTU, Bardoli. 2 Yr Industry Experience and more than 20 Yrs Academic Experience.