Deepak Sharma, International Journal of Advanced Trends in Computer Applications (IJATCA)
Volume 3, Number 1, January - 2016, pp. 1-3
ISSN: 2395-3519

International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A robust Image Steganography Technique Using DCT and Neural Network

[1]**Deepak Sharma**
Assistant Professor (CSE)
B.B.P.U.C.C. Balachaur
ddbbpucc@gmail.com

Abstract: *Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. During communication process LSB steganography based on Huffman encoding algorithm does not provide full security and good compression. So a secure DCT-based steganographic algorithm is proposed in integration with neural network. This algorithm provides more security and compression by combining cryptography with DCT-steganography. The proposed technique has two main algorithm i.e. Embedding Algorithm and Extraction algorithm. The whole simulation has taken place in MATLAB environment. The performance parameters are PSNR and MSE.*

Keywords: *PSNR, MSE, DCT, Neural Network, Steganography.*

I. INTRODUCTION

With the development of internet technologies, digital media can be transmitted conveniently over the internet. So image transmission has to face many problems. So protection of this plays very big role in digital world. Privacy is another issue when digital communication is considered. Steganography and Cryptography are the two technologies related with security and privacy. Cryptography means to secure the way of transmission and it does not indicate the message in secure form. So to provide security, Steganography has been used. Steganography is the art of hiding information that prevent the detection of hidden messages.

The difference between Steganography and Cryptography is that the cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret. Steganography and cryptography both are ways for protecting information from unwanted parties. In this paper, Steganography can be done using DCT and BPNN method.

The remaining paper is organized as Section II introduces the Proposed Work, Section III includes the Results and evaluation and Finally Section IV will contain Conclusion.

II. PROPOSED ALGORITHM

Embedding Algorithm

1. Start K =0
2. Initialization= 0 ; read cover Image
3. Initialization= 1: read hidden message
4. For every carrier image selected from image pool = true
5. For K =1 : Binarisation then DCT
6. If Image. DCT application. Compression. quantization matrix
7. Table allocated = TRUE, K = K+1
8. Calculate LSB (Set DC = secret message)
9. For i = LSB; collection of bits.
10. If LSB.bit = true
11. Image.Feasible.Carrier= true
12. If image size = true
13. Selection Procedure = true
14. Set image = stego image
15. Stop

The above algorithm shows the Embedding algorithm for the Steganography. Initially, Cover image and Hidden message is taken. In the next step, Both cover image and Hidden message is converted to binary. After this the cover image is broken into 32 * 32 block of pixels . Then after this DCT is applied to each block. Each block is compressed through quantization table. After this Calculate LSB of each DC coefficient and replace with each bit of secret message. Finally write stego image.

Extraction Algorithm

1. Start K= 0
2. Initialisation = 0 ; Read stego image
3. For i= o to I = n ; traverse image

4. If i = n , then check matrix value
5. If I = true, extract LSB.
6. If I ≠ true, move next
7. If LSB. Extraction = TRUE
8. Merge.Image = true
9. If merge.Image = TRUE
10. Call Neural Network
11. Neural network = 0
12. For Neural network = TRUE
13. (i=input layer, j= Hidden Layer, k= Outpt layer:
    Input.Layer. Set Value= 0;
    If output.layer.value= error;
    Then Move. Back=0;
    Continue for I.value = O.value)
14. Set = Extraction.Image
15. Stop

The above algorithm shows the extraction process for the Steganography, In this We have collection of LSB bits, now check the LSB bits feasibility. If the feasibility of LSB bits matched then they will be merged. After this binarisation takes place. The BPNN is applied for extraction of message.

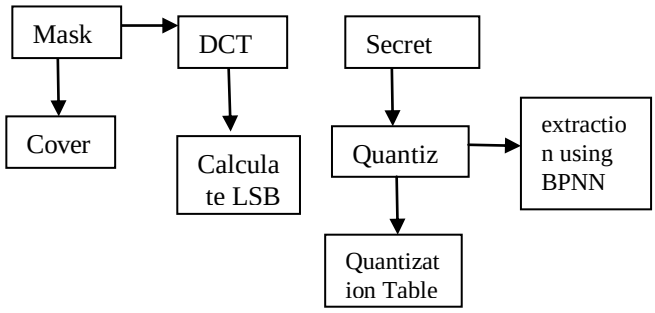

Figure 1: Proposed Model

III. RESULTS AND DISCUSSIONS

The results are taken in matlab programming. The PSNR and MSE values are calculated using equation (1) and (2) The Peak Signal-to-Noise Ratio (PSNR) is defined as:

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

eq.(1)

The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

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

eq (2)

Where M and N are the number of rows and columns in the input images, respective. The Peak Signal-to-Noise Ratio (PSNR) is calculated to measure the quality of stego image. The PSNR is calculated in db. Larger PSNR indicates better quality of an image. And we found the PSNR value 100.2 and calculated MSE is .033.

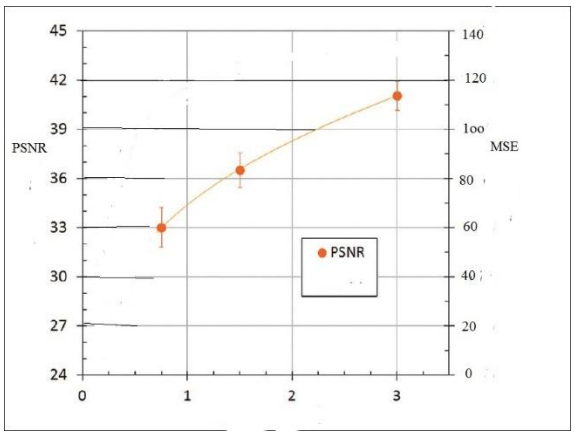

Figure 2: Performance Parameters.

IV. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. From the results it is clear that as PSNR in DCT is the best but as we know that security is much more important in today's communication system. So security wise DCT is the best. Also BPNN is used for the extraction of hidden message.

REFERENCES

[1] Chang, C.C., Chen, T.S. and Chung, L.Z., "*A steganographic method based upon JPEG and quantization table modification*", Information Sciences, 2002, 141(1-2), pp.123-38.

[2]T. Morkel, J.H.P. Eloff , M.S. Olivier,"*An Overview of Image Steganography*," *in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 .

[3] Ankur M. Mehta, Steven Lanzisera, and Kristofer S. J. Pister, "*Steganography 802.15.4 Wireless Communication".*

[4] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik,"*Authentication of Secret Information in Image Steganography"* Microprocessor Applications Laboratory, Indian Institute of Science,Bangalore.

[5] Proceedings of the 2006 International Conference on "*Intelligent Information Hiding and Multimedia Signal Processing* "(IIH-MSP'06)0-7695-2745-0/06 © 2006 IEEE.

[6] AsgharShahrzadKhashandarag and NaserEbrahimian, "*A new method for color image steganography using SPIHT and DCT, sending with JPEG format*", International Conference on Computer Technology and Development, IEEE, 2008

[7] CHEN Zhi-li, HUANG Liu-sheng, YU Zhen-shan, LI Ling-jun and YANG wei, "*A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words*", 3RD International Conference on Availability, Reliability and Security, IEEE, 2008..

[8] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" Microprocessor Applications Laboratory, Indian Institute of Science, Bangalore in 2008

[9] MamtaJunejaParvinder Singh Sandhu, "*Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption"*2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[10]KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka, ―A DCT based Mod4 Steganography Method‖ Signal Processing 87, 1251-1263, 2009.

[11] Yi- Zhen Chen, Zhi Han, Shu-ping Li, Chun- hui Lu, Xiao- Hui Yao , "*An Adaptive Steganography Algorithm Based on Block Sensitivity Vectors Using HVS Features* " 2010 3rd International Congress on Image and Signal Processing.