A Novel Technique for Image Steganography Based On Block-DCT and Huffman Encoding

Arunima Kurup P& Poornima D Sreenagesh
S8, Department of Information Technology,
Mohandas College Of Engineering And Technology,Anad,Thiruvananthapuram

Abstract

Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Firstly a gray level image of size M× N is divided into no joint 8 × 8 blocks and a two dimensional Discrete Cosine Transform(2-d DCT) is performed on each of the P = MN / 64 blocks. Then Huffman encoding is also performed on the secret messages/images before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches. Furthermore, satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table.

Introduction

With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. However, message transmissions over the Internet still have to face all kinds of security problems. Therefore, how to protect secret messages during transmission becomes an essential issue for the Internet.

Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include DES (Data Encryption Standard) , AES (Advanced Encryption Standard) and RSA. These methods scramble the secret message so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper's attention. Hence, a new scheme, called "steganography", arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files) so that it cannot be observed. Steganography differs from cryptography in the sense that where Cryptography focuses on concealing the contents of a message, steganography focuses on concealing the existence of a message.Two other technologies that are closely related to steganography are watermarking and fingerprinting. Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself. Steganography is the art and science of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. The word steganography in Greek means "covered writing"(Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing")]. The main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer.

That is unwanted parties should not be able to distinguish in any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that containing secret message).

Thus the stego-image should not deviate much from original cover-image. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Related Work

Steganography is a branch of information hiding in which secret information is camouflaged within other information. A simple way of steganography is based on modifying the least significant bit layer of images, known as the *LSB technique*. The LSB technique directly embed the secret data within the pixels of the cover image. In some cases, LSB of pixels

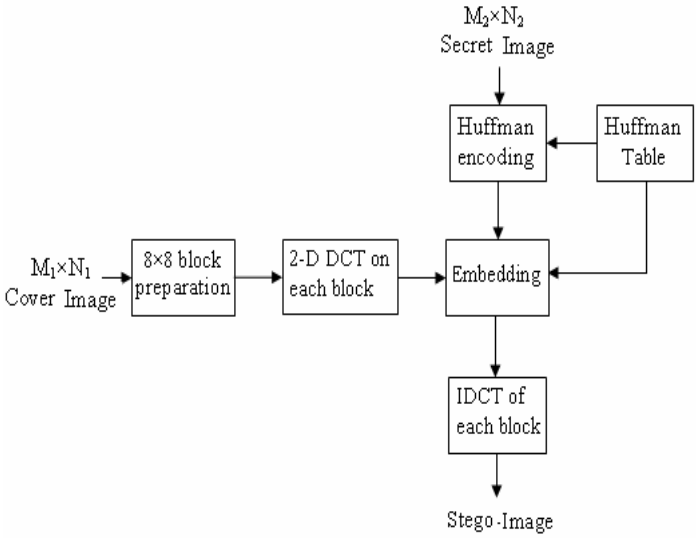
visited in random or in certain areas of image and sometimes increment or decrement the pixel value. Some of the recent research studied the nature of the stego and suggested new methodologies for increasing the capacity. Habes proposed a new method (4 least Significant) for hiding secret image inside carrier image. In this method each of individual pixels in an image is made up of a string of bits. He took the 4-least significant bit of 8-bit true color image to hold 4-bit of the secret message /image by simply overwriting the data that was already there.The schemes of the second kind embed the secret data within the cover image that has been transformedsuch as DCT (discrete cosine transformation). The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data. Tseng and Chang in proposed a novel steganography method based on JPEG. The DCT for each block of 8×8 pixels was applied in order to improve the capacity and control the compression ratio. Capacity, security and robustness , are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

PSNR (Peak Signal to Noise Ratio)

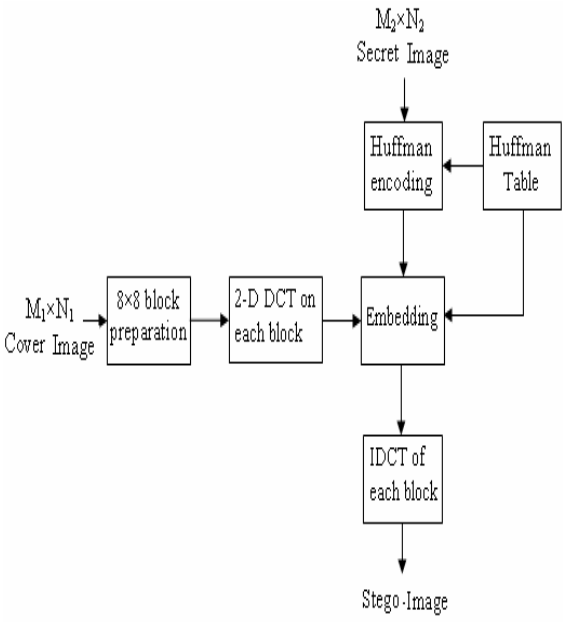
The PSNR is expressed in dB's. The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stegoimage.

Proposed Image Steganography Algorithm

Image steganography schemes can be classified into two broad categories: spatial-domain based and transform-domain based . In spatial domain approaches, the secret messages are embedded directly. On spatial domain, the most common and simplest steganographic method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels is replaced by the message which bits are permuted before embedding. However, the LSB insertion method is easy to be attacked. In a new steganography technique, named, "modified side match scheme" was proposed. It reserves the image quality, increases embedding capacity but is not robust against attack because it is a spatial domain approach and no transfer is used. Based on the same embedding capacity, our proposed method improves both image quality and security.Hiding the secret message/image in the special domain can easily be extracted by unauthorized user. In this paper, we proposed a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image. The 2-D DCT convert the image blocks from spatial domain to frequency domain. The schematic/ block diagram of the whole process is given in figure 2((a) and (b)).



(a) Insertion of a Secret image (or message) into a Cover image.



(b) Removal of Secret Image (or message)

Figure 2: Block diagram of the proposed steganography technique.

Discrete Cosine Transform

Let I(x,y) denote an 8-bit grayscale cover-image with x = 1,2,……..,M1 and y = 1,2,……..,N1. This M1×N1 cover-image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of L =M1×N1 / 64 blocks..

Huffman encoding and Huffman table (HT)

Before embedding the secret image into cover image, it is first encoded using Huffman coding Huffman codes are optimal codes that map one symbol to one code word. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2 image is converted to a 1-D bits stream with length LH < M2 × N2. Huffman table (HT) contains binary codes to each intensity value. Huffman table must be same in both the encoder and the decoder. Thus the Huffman table must be sent to the decoder along with the compressed image data.

8-bit block preparation

Huffman code H is decomposed into 8-bits blocks B. Let the length of Huffman encoded bits stream be LH.Thus if LH is not divisible by 8, then last block contains r = LH % 8 number of bits.

Embedding of Secret Message / Image

The proposed secret message/image embedding scheme comprises the following five steps:

Step 1: DCT.
Divide the carrier image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks ofthe cover image f to obtain F.
.

Step 2: Huffman encoding.
Perform Huffman encoding on the 2-D secret image S of size M2 × N2 to convert it into a 1-D bits streamH.

Step 3: 8-bit block preparation.
Huffman code H is decomposed into 8-bits blocks B.

Step 4: Bit replacement
The least significant bit of all of the DCT coefficients inside 8×8 block is changed to a bit taken from each 8 bit block B from left to right. The method is as follows:

For k=1 ; k_1; k=k+1
LSB((F(u,v))2) ← B(k) ;

Where B(k) is the kth bit from left to right of a block B and (F(u,v)2) is the DCT coefficient in binary form.

Step 5: IDCT.
Perform the inverse block DCT on F using eqn (2)and obtain a new image f1 which contains secret image.

Embedding Algorithm

Input: An M1×N1 carrier image and a secret message/image.
Output: A stego-image.

1. Obtain Huffman table of secret message/image.
2. Find the Huffman encoded binary bit stream of secret-image by applying

Huffman encoding techniqueusing Huffman table obtained in step 1.

3. Calculate size of encoded bit stream in bits.
4. Divide the carrier image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the cover image.
5. Repeat for each bit obtained in step 3
6. Insert the bits into LSB position of each DCT coefficient of 1st 8×8 block found in step 4.
7. Decompose the encoded bit stream of secret message/image obtained in step 2 into 1-D blocks of size 8 bits.
8. Repeat for each 8-bit blocks obtained in step 6 (a) Change the LSB of each DCT coefficient of each 8×8 block(excluding the first) found in step 4 to a bit taken from left(LSB) to right(MSB) from each 8 bit block B.
9. Repeat for each bit of the Huffman table
    (a) Insert the bits into LSB position of each DCT coefficient
10. Apply inverse DCT using identical block size.
11. End

Extraction of the secret message / Image

The stego-image is received in spatial domain. DCT is applied on the stego-image using the same block of size 8 × 8 to transform the stego-image from spatial domain to frequency domain. The size of the encoded bit stream and the encoded bit stream of secret message/image are extracted along with the Huffman table of the secret message/image.

Extraction Algorithm

Input: An M1×N1 Stego-image.
Output: Secret image.

1. Divide the stego-image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the stego-image.
2. The size of the encoded bit stream is extracted from 1st 8 × 8 DCT block by collecting the least significant bits of all of the DCT coefficients inside the 1st 8×8 block.
3. The least significant bits of all of the DCT coefficients inside 8×8 block (excluding the first) are collected and added to a 1-D array.
4. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
5. Construct the Huffman table by extracting the LSB of all of the DCT coefficients inside 8×8 blocks excluding first block and the block mentioned in step 3.
6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
7. End.

Conclusion

In this paper, we propose a steganography process in frequency domain to improve security and imagequality compared to the existing algorithms which are normally done in spatial domain. According to the simulation results the stego-images of our method are almost identical to other methods' stego-images and it is difficult to differentiate between them and the original images. Our proposed algorithm also provides additional three layers of security by means of transformation (DCT and Inverse DCT) of cover image and Huffman encoding of secret image. The demand of robustness in image steganography filed is not requested as strongly as it is in watermarking filed. As a result, image steganography method usually neglects the basic demand of robustness. In our proposed method, the embedding process is hidden under the transformation i.e. DCT and inverse DCT. These operations and Huffman encoding of secret image keep the images away from stealing, destroying from unintended users and hence the proposed method may be more robust against brute force attack.

References

[1] DES Encryption Standard (DES), National Bureau of Standard (U.S.). *Federal Information Processing Standards Publication 46*, National Technical Information Service, Springfield, VA, 1997.

[2] Daemen,J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard", Dr. Dobb's Journal, March 2001.

[3] R. Rivest, A. Shamir, and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communication of the ACM*: 120-126.

[4] Pfitzmann, B. 1996. Information hiding terminology," *Proc. First Workshop of Information Hiding Proceedings*, Cambridge, U.K., Lecture Notes in Computer Science, Vol.1174: 347-350.

[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,
47:10, October 2004

[6] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999.

[7] Moerland, T, "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*,
www.liacs.nl/home/ tmoerl/privtech.pdf
[8] N. F. Johnson and S. Katzenbeisser, A survey of steganographic techniques., in S. Katzenbeisser and F.
Peticolas (Eds.): *Information Hiding*, pp.43-78. Artech House, Norwood, MA, 2000.

[9] Li, Zhi., Sui, Ai, Fen., and Yang, Yi, Xian. 2003 "A LSB steganography detection algorithm", *IEEE Proceedings on Personal Indoor and Mobile Radio Communications*: 2780-2783.

[10] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.

[11] Alkhrais Habes , "4 least Significant Bits Information Hiding Implementation and Analysis" , ICGST Int. Conf. on Graphics, Vision and Image Processing (GVIP-05), Cairo, Egypt, 2005.

[12] Krenn, R., "Steganography and Steganalysis",
http://www.krenn.nl/univ/cry/steg/article.pdf

[13] C.-C. Chang, T.-S. Chen and L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification", *Information Sciences,* vol. 141, 2002, pp. 123-138.

[14] R. Chu, X. You, X. Kong and X. Ba, "A DCT-based image steganographic method resisting statistical attacks", *InProceedings of (ICASSP '04), IEEE International Conferenceon Acoustics, Speech, and Signal Processing*, 17-21 May.vol.5, 2004, pp V-953-6.

[15] H.-W. Tseng and C.-C. Chang, "Steganography using JPEG-compressed images", *The Fourth International Conference on Computer and Information Technology, CIT'04*, 14-16 Sept 2004, pp. 12-17.

[16] Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding.IEEE Trans. Inform. Theor., 47: 1423-1443. DOI: 10.1109/18.923725.

[17] Chan, C.K. and Cheng. L.M. 2003. Hiding data in image by simple LSB substitution. Pattern Recognition, 37: 469 – 474.

[18] Chang, C.C and Tseng, H.W. 2004. A Steganographic method for digital images using side match. Pattern Recognition Letters, 25: 1431 – 1437.

[19] SWANSON, M.D., KOBAYASHI, M., and TEWFIK, A.H.: 'Multimedia data embedding and watermarking technologies', Proc. IEEE, 1998, 86(6), pp. 1064-1087

[20] Chen, T.S., Chang C.C., and Hwang, M.S. 1998. A virtual image cryptosystem based upon vector quantization. IEEE transactions on Image Processing, 7,10: 1485 – 1488.

[21] Chung, K.L., Shen, C.H. and Chang, L.C. 2001. A novel SVD- and VQ-based image hiding scheme.
Pattern Recognition Letters, 22: 1051 – 1058.

[22] Iwata, M., Miyake, K., and Shiozaki, A. 2004. Digital Steganography Utilizing Features of JPEG Images, IEICE Transfusion Fundamentals, E87-A, 4:929 – 936. International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010 112

[23] Chen, P.Y. and Wu, W.E. 2009. A Modified Side Match Scheme for Image Steganography,
International Journal of Applied Science and Engineering, 7,1: 53 – 60.