Image Steganography Using Frequency Domain

Dr. MAHESH KUMAR, MUNESH YADAV

Abstract: Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Technologies that are closely related to steganography and watermarking and fingerprinting . High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm. Quantized-frequency Secure Audio Steganography algorithm. Integer Transform based Secure Audio Steganography algorithm.

Keywords: Genetic Algorithm, Audio Steganography algorithm

1. Introduction

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” [1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [2]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [2]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [3]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are “marked” in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [4]. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [3]. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial [5].

- *Dr.Mahesh Yadav , Associate Professor, Department of Computer Science & Engineering, M.R.K. Institute Of Engineering Technology, Saharanwas, Rewari , Haryana , India ,Guide or supervise me to complete the project.*
- *Munesh Yadav , M.Tech. Scholar, Department of C.S.E, M.R.K. Institute Of Engineering Technology, Saharanwas, Rewari ,Haryana , India , student with the help of my gudie I have complete the project.*

A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [3]. Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [6]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [7]. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems” [8]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [9]. Hiding the secret message/image in the special domain can easily be extracted by unauthorized user. As in image domain there are some drawbacks exist so that this thesis is done using Frequency domain. Frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message.

2.Description of Techniques

2.1 Block-DCT and Huffman Encoding

Hiding the secret message/image in the special domain can easily be extracted by unauthorized user[10]. 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.

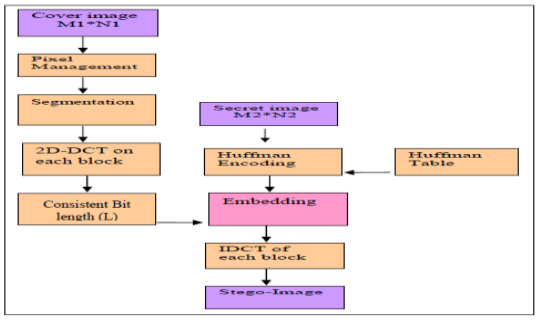

Figure 2.1 Block Diagram of

Embedding Technique
The schematic/ block diagram of the whole process is given in figure (a) and (b)

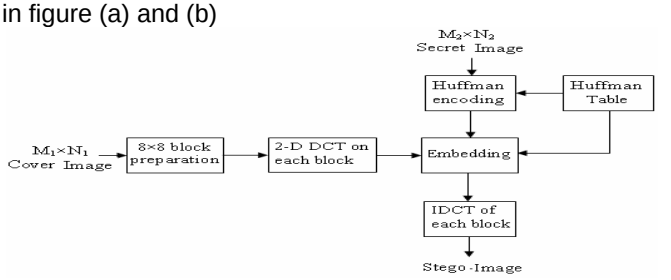

Figure 2.2 (a) Insertion of a Secret image (or message) into a Cover image[11]

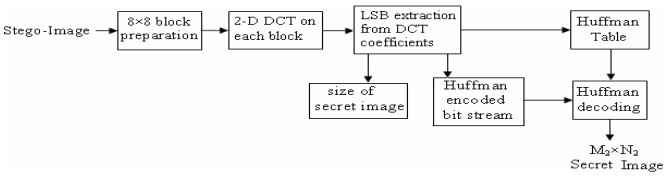

Figure 2.3 (b) Removal of Secret Image (or message)[11]

Advantages
- Improvement in security & image quality
- A good invisibility
- Less distortion after embedding process
- Expected to be practical
- Provides three layers of security

Disadvantages
- Robustness is not achieved
- Can be distorted by unintended users

2.2 Labeling method in stegnography
In this method tried to find binary value of each character of text message and then in the next stage, tried to find dark places of gray image (black) by converting the original image to binary image for labeling each object of image by considering on 8 connectivity. Then these images have been converted to RGB image in order to find dark places. Because in this way each sequence of gray color turns into RGB color and dark level of grey image is found by this way if the Gary image is very light the histogram must be changed manually to find just dark places. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of stegnography[12]

Advantages
- Applicable for unobtrusive communications
- Easy to implement
- More Effective & efficient
- Reduce manual work load
-

Disadvantages
- Less secure
- Require skillful & intelligent programmer
- Need an Enhanced technique to make use of Palette and composition of the gif image for better results

2.3 DWT(Discrete Wavelet Transform)
Steganography technique using DWT (Discrete Wavelet Transform) 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 using DWT is to alter the magnitude of the DWT coefficients of three sub-bands, HH, HL, and LH of cover image.

3. Proposed Techniques
New algorithms keep emerging prompted by the performance of their ancestors (spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain.

Proposed method in Image steganography using frequency domain is as follows:
The image is converted into frequency domain after applying wavelet transform. The cover image is converted from RGB to Grey scale which is more suitable format for data hiding. The secret message or image which is to hide is then processed to know the size of that secret message or image. A key is used to provide secrecy which generates the PN sequence for hiding secret message in cover image. Apply suitable algorithm for hiding the message. The secret message is being hidden at the edges of the cover image. PSNR is calculated by applying mathematical operation.

$$PSNR = 10*\log10\ (C^2_{max} / MSE)$$

Where MSE denotes means square error which is given as:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$

Where x and y are the image coordinates , M and N are the dimensions of image , Sxy is generated stegoimage and Cxy is the cover image. Also C max holds the maximum value in the image for example:

$$C^2_{max} \leq \begin{cases} 1, & \text{double precision} \\ 255, & \text{unit 8 bit} \end{cases}$$

4. ALGORITHM USED FOR EMBEDDING
Step 1- Read a colored (RGB) image, divide the image into (2 x 2) sub images Gi, (i=1,2,..) ; (each sub image contains 16 pixels).

Step 2- Determine the position in which we will start hiding the data; This is determined by using a random generator function.

Step 3- For each sub image Gi, the following process will be done:

- **Step 3-1**- Convert the least three bits from the blue color byte to decimal for each pixel P(r,c) in Gi, the results will be saved in Bi (2x2) decimal matrix. All elements of Bi are in the range (0…2m -1).
- **Step 3-2** - To hide the following bits 0101101011100….., convert each three bits to the equivalent decimal number (i.e 010 is converted to D= 2), then find V and the sign S
- **Step 3-3** If the sign S is negative, add the value of V to one of the pixels P(r,c) in the sub image Gi, the values of (r,c)
- **Step 3-4** Otherwise (if S is positive) subtract the value of V from the pixel P(r,c) in the sub image Gi, the values of (r,c) are calculated depending on the values of (i,j) of the point Bi are calculated depending on the values of (i,j) of the point Bi This process will force the value of modulation function to be equal to the embedded data.

This algorithm is used to embed secret image into cover image. The secret message can be any text, image or any other medium. After embedding process msg is sent to the receiving party. At receiving side the stego image is again applied to reverse embedding process for extracting the original message. The extraction process is as follows :-

4.1 Extraction Process or Steganalysis Process

Step 1. Read the Stegano image

Step 2. Divide the image into (2 x 2) sub images Gi, (i=1,2,..) ; (each sub image contains 16 pixels).

Step 3. Determine the position in which we will start hiding the data; This is determined by using a random generator function

Step 2. For each sub image Gi, the following process will be done:
(Repeat the following process)

- Read the data area from the sub matrix and retrive as an array of bits
- Reverse the Encoding Process by reperforming the Ex-or operation on data bits.
- 0101101011100….., convert each three bits to number (i.e 010 is converted to D= 2), then find V and the sign S
- If the sign S is negative, add the value of V to one of the pixels P(r,c) in the sub image Gi, the values of (r,c) of (i,j) of the point Bi
- Otherwise (if S is positive) subtract the value of V from the pixel P(r,c) in the sub image Gi, the values of (r,c) are calculated depending on the values of (i,j) of the point Bi the equivalent decimal are calculated depending on the values

Step 5. Convert the data back in Text format

Step 6. Store the data in the form of file

5. Implementation of Mechanisms Existing Techniques Basic techniques

- A novel technique for image steganography based on Block-DCT and Huffman Encoding
- High Capacity Image SteganographyusingWavelet Transform and Genetic Algorithm
- A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images
- Labeling method
- JPEG and particle swarm optimization
- Quantized-frequency Secure Audio Steganography algorithm
- Integer Transform based Secure Audio Steganography algorithm

5.1 Block-DCT (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 / 62 blocks. The mathematical definition of DCT is:
Forward DCT:

$$F(u,v)=\frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$$

for $u=0,...,7$ and $v=0,...,7$

where $C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases}$

Inverse DCT :

$$f(x,y)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)F(u,v)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$$

for $x=0,...,7$ and $y=0,...,7$

Algorithm

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

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 stream H.

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

Step 2: 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.

Advantages

- Improvement in security & image quality
- A good invisibility

- Less distortion after embedding process
- Expected to be practical
- Provides three layers of security

Disadvantages

- Robustness is not achieved
- Can be distorted by unintended users

5.2 DWT (Discrete Wavelet Transform) Embedding algorithm of Secret Message / Image

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

Step 1: Decompose the cover image by using Haar wavelet transform.

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 stream H.

Step 3: 3-bit block (Bi) preparation Huffman code H is decomposed into 3-bits blocks and thus form a decimal value ranging from 0 to 7. For example, the binary sequence …. 110 001 010 111 100 000 011 will be changed to the decimal sequence (Bi) … 6 1 2 7 2 0 3.

Step 2: Bits replacement Select one sub-band for embedding the secret message. If we donate 'f ' as coefficients matrix of the selected sub-band, then using the following equation, the 3 least significant bits of wavelet coefficients is replaced by the 3 bits of Huffman encoded bit stream in the form of 3 bit block Bi.

$f'(x,y) = f(x,y) - f(x,y) \% 8 + Bi$ ----------(1)

Step 5: IDWT Apply the Haar inverse DWT (IDWT) on the DWT transformed image, including the modified sub band to produce a new image f1 which contains secret image.

6. Conclusion

Dissertation presented a background discussion on the major algorithms of steganography deployed in digital imaging. The emerging techniques such as DCT, DWT and adaptive steganography are not too prone to attacks, especially when the hidden message is small. This is because they alter coefficients in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. There are different ways to reduce the bits needed to encode a hidden message. Apparent methods can be compression or correlated steganography, as proposed by Zheng and Cox [12], which is based on the conditional entropy of the message given the cover. In short, there has always been a trade-off between robustness and payload. Scholars differ about the importance of robustness in steganography system design. In [13], Cox regards steganography as a process that should not consider robustness as it is then difficult to differentiate from watermarking. Katzenbeisser, on the other hand, dedicated a sub-section to robust steganography. He mentioned that robustness is a practical requirement for a steganography system. ''Many steganography systems are designed to be robust against a specific class of mapping.''. It is also rational to create an undetectable steganography algorithm that is capable of resisting common image processing manipulations that might occur by accident and not necessarily via an attack. Cox's view is formed based on his definition of steganography and its scope, while Katzenbeisser is looking at the process of steganography in a different way, preferring to view it as a robust secret communication mechanism. Steganography urges that the cover image must be carefully selected. A familiar image should not be used, it is better for steganographers to create their own images [14]. This thesis offered some guidelines and recommendations on the design of a steganographic system. Steganography methods usually struggle with achieving a high embedding rate. As an alternative channel to images, video files have many excellent features for information hiding such as large capacity and good imperceptibility. The challenge, however, is to be able to embed into a group of images which are highly inter-correlated and often manipulated in a compressed form [13]. Thesis also discusses with some detail the differences between steganography and watermarking. The various non-oblivious watermarking techniques available, which are highly resilient to image processing and geometric attacks, aim to detect the presence of a watermark using a correlation with an original template except in the rare watermarking blind detection scenario such as the work in [14]. This resilience can be seen for instance in the invariance proposed in the work of Deng et al. [15–18]. However, in steganography, this detection is not required as the aim is to correctly extract the hidden bits without the availability of any side information such as the original image and watermark. To the best of our knowledge it is first to discuss the complexity and hardness of the steganography embedding problem; in particular, we show that the decision version of the problem is NP-complete[19] We conclude that

- In this method major importance is given on the secrecy as well as the privacy of information
- The embedding process is hidden under the transformation (DWT and IDWT)[13] of cover image
- DWT operations provide sufficient secrecy
- Satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules

References

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 27:10, October 2002

[3] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[4] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[5] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001

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

[7] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 127:03, June 2000

[8] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April 1998

[9] Venkatraman, S., Abraham, A. & Paprzycki, M., “Significance of Steganography on Data Security”,Proceedings of the International Conference on Information Technology: Coding and Computing, 2002

[10] http://en.wikipedia.org/wiki/Steganography

[11] Gonzalez, R.C. and Woods, R.E., Digital Image Processing using MATLAB, Pearson Education, India,2006.

[12] Jamil, T., “Steganography: The art of hiding information is plain sight”, IEEE Potentials, 18:01, 1999.

[13] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, A new genetic algorithm approach for secure JPEG steganography, in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April 2006, pp. 1–6.

[14] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April

[15] Provos, N. & Honeyman, P., “Hide and Seek: An introduction to steganography”, IEEE Security and Privacy Journal, 2003

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

[17] C.-C. Chang, T.-S. Chen and L.-Z. Chung, “A steganographic method based upon JPEG and quantization table modification”, Information Sciences, vol. 121, 2002, pp. 123-138.

[18] R. Chu, X. You, X. Kong and X. Ba, “A DCT-based image steganographic method resisting statistical attacks”, InProceedings of (ICASSP '02), IEEE International Conferenceon Acoustics, Speech, and Signal Processing, 17-21 May.vol.5, 2002, pp V-953-6.

[19] http://www.datahide.com/BPCSe/applications-e.html

[20] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001