A NOVEL TECHNIQUE USED FOR IMAGE STEGANOGRAPHY BASED ON FREQUENCY DOMAIN

Kirti Gautam M.Tech* JIET , Jind , KUK Kurukshetra[1]

Sapna Aggarwal Assistant Professor JIET, Jind , KUK Kurukshetra [2]

Kirtigautam078@gmail.com[1] Er.sapna.aggarwal@gmail.com[2]

Abstract :- 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. 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 is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files.

Index Terms— Steganography, MSB, LSB, USENET,DCT, DWT, Image Processing, PSNR, MSE, Coefficients Selection and Frequency Hopping

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 defining it as "covered writing". In image steganography the information is hidden exclusively in images. In general, steganographic algorithms rely on the replacement of some noise component of a digital object with a pseudo-random secret message . In digital images, the most common noise component is the least significant bits (LSB's). To the human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. 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 . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.

2. Related work

Image steganography schemes can be classified into two broad categories: spatial-domain based and transform-domain based. Frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The description of the frequency domain stegnography is as follows:-

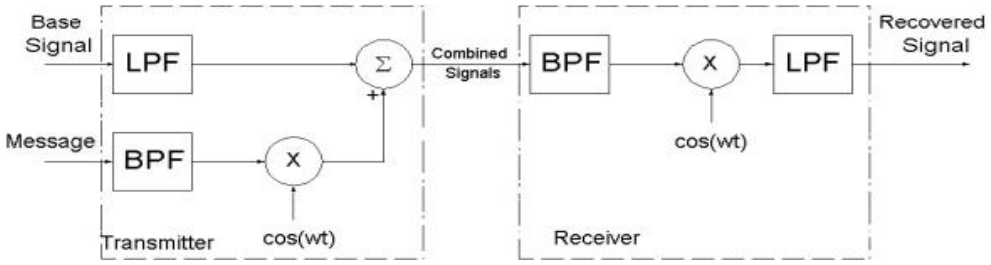

Figure 1 Block Diagram for frequency domain stegnography[4]

We begin with two signals, such as the ones below. These will be called the "base", which contains the hidden message, and the "message", which will be hidden in the base. Next, we take the base signal and lowpass filter it to 18 kHz, which will clear up the upper 4 kHz. we will bandpass filter the message signal which will be a small enough band to fit in the upper portion of the filtered base. We modulate the filtered message using a cosine with carrier frequency band. We then combine the modulated, filtered message with the filtered base signal and we get a signal with a hidden message in it. This process is a fairly simple one, requiring only filtering and amplitude modulation in order to hide the signal in the base. It is very much a physically realizable process and one that we could accomplish with our current knowledge of electrical engineering techniques [15]. This ease of implementation will more than make up for the small amounts of distortion in the combined signals, as well as the limited frequency range of the recovered signal. Like as,

Figure 2 Example of stegnography technique using frequency domain[5]

Secret Image Cover Image f of size N×N Stego Image g of size N×N

Peak signal to noise ratio(PSNR)

The measurement of the quality between the cover image f and stego-image g of sizes N × N shown in fig is defined as:

$$PSNR = 10 \times \log(255^2 / MSE)$$

$$\text{where } MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y) - g(x,y))^2 \Big/ N^2$$

Where f(x,y) and g(x,y) means the pixel value at the at position (x, y) in the cover-image and the

corresponding stego-image respectively. 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 stego image .

Capacity

- The larger the cover message is (in data content terms — number of bits) relative to the hidden message, the easier it is to hide the latter.
- For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media.

Security

- The objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible. That is to say, the changes are indistinguishable from the noise floor of the carrier.
- From an information theoretical point of view, this means that the channel must have more capacity than the 'surface' signal requires, that is, there must be redundancy
- In digital image, there is noise from the imaging element; & digital audio, there is noise from recording techniques or amplification equipment, which should avoidable .
- In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise, and shot noise.
- This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data.

3. Proposed image steganographic method

In this method firstly colored (RGB) image is divided the image into (4 x 4) sub images. Then the position is determined in which the data is being hidden. The position is determined by using a random generator function. The region where the frequency is high is selected & then hide the secret message at that position.

Algorithm used for Embedding

Step 1- Read a colored (RGB) image, divide the image into (4 x 4) 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 (4x4) 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 message 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

Extraction Process or Steganalysis Process

Step 1. Read the Stegano image

Step 2. Divide the image into (4 x 4) 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 4. For each sub image Gi, the following process will be done:

(Repeat the following process)

- Read the data area from the sub matrix and retrieve 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

4. Simulation results

In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 7 program on Windows 7 platform.

The following diagram shows the process of embedding

Figure 6. Cover image

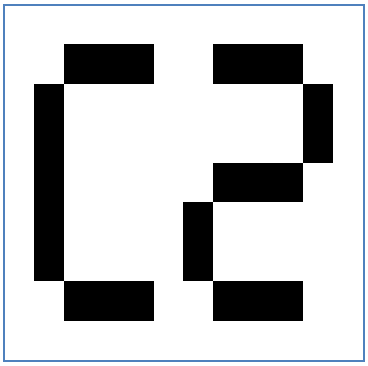

Figure 7. Secret image

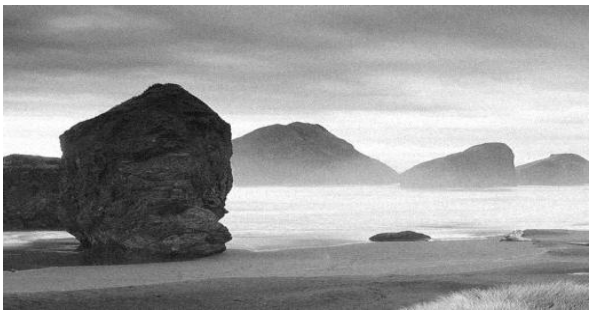

Figure 8. Stego image

The histogram is the intensity wise distribution of pixels in the image. This showa how the frequency is distributed throughout the image. The following diagram shows this distribution.

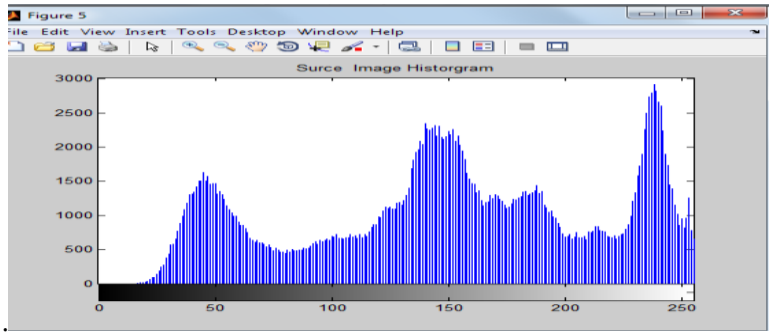

Figure 9 Histogram for cover image

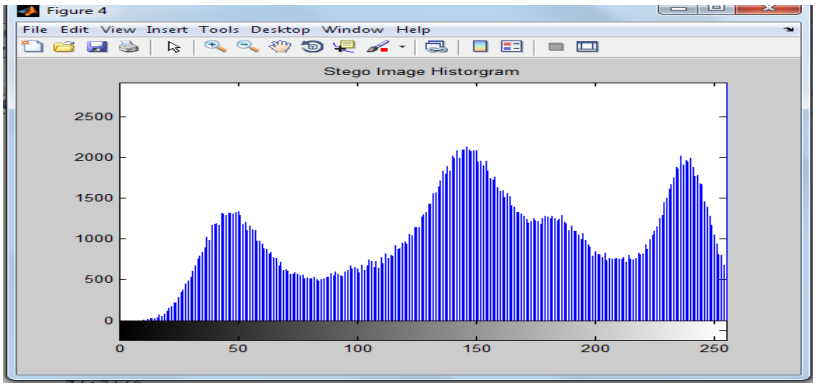

Figure 10. Histogram for stego image

PSNR values of Different Images

Images	**Size**	**Capacity**	**PSNR**
Lenna	256	299520	51.34
Baboon	256	299520	59.80
Airplane	256	299520	50.56
Boat	256	299520	59.05

Table 1 Different PSNR Value for different images

As a performance measurement for image distortion, the well known peak-signal-to-noise ratio(PSNR) which is classified under the difference distortion metrics can be applied on the stego-images. It is defined in table that the main parameter for the performance measurement is PSNR & in our proposed method the PSNR value is greater than the other technique so we can say that this method is somewhat better & efficient.

5. Conclusion

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. The PSNR value should be as maximum as possible; therefore it is basic requirement to increase it as much as possible. The drawbacks of the previous scheme are to be resolved in this proposed work. No technique is assuming to be best but tried to be best. Basic requirements are to be achieved like confidentiality, robustness, secrecy, accuracy etc. an easy & efficient method is to be populated to regenerate the solution of the security measurements.

6. Refrences

[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, 47:10, October 2004

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

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

[5] 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

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

[7] Moerland,T,"Steganography and Steganalysis", *Leiden Institute of Advanced Computing science*

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

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

[10]Richard Popa, An analysis of steganography techniques, Master's thesis, University of Timisoara,Timisoara, Romania, 1998.

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

[12] http://www.scribd.com/doc/49916571/5/system-objectives

[13] 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.

[14] 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.

[15]http://ticsp.cs.tut.fi/images/3/3d/Cr1020-riga.pdf