

A Novel Technique Used For Image Steganography Based On Frequency Domain

Suman goyat

Guide Rajkumar Yadav Prof. MDU Rohtak

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. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. It does not replace cryptography but rather boosts the security using its obscurity features. Here this paper provides a new and efficient approach to image steganography. The key objectives of this paper are: 1) a new image encryption method tailored to digital images and steganography, 2) a new, efficient and real-time algorithm and 3) a new embedding method using the Reflected Binary Gray Code, RGB, in the wavelet domain.

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” [1] 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 [10]. 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 [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 [6]. 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].

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 steganography is as follows:-

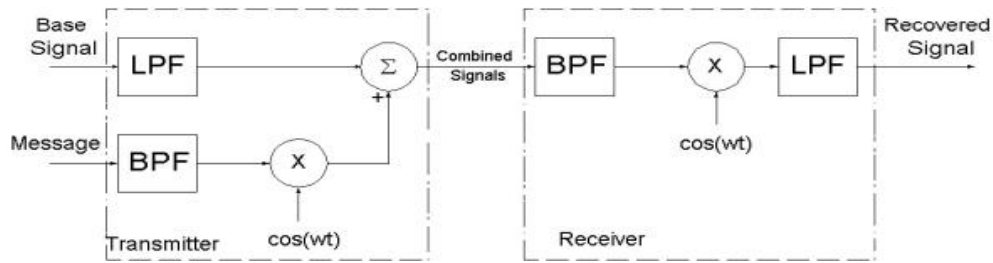


Figure 1 Block Diagram for frequency domain steganography[4]

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 steganography technique using frequency domain[5]

Secret Image

Cover Image f of size $N \times N$

Stego Image g of size $N \times N$

2.1 Data embedding security schemes

The choice of embedding algorithm in the most cases is driven by the results of the steganographic channel robustness analysis . One of the areas that improves steganographic robustness is usage of a key scheme for embedding messages. Various key steganographic schemes have various levels of protection. Key scheme term means a procedure of how to use key steganographic system based on the extent of its use [5]. However, when the steganographic robustness is increased a bandwidth of the whole embedding system is decreased. Therefore the task of a scheme selection for achieving the optimal values of the steganographic system is not trivial [8].

Embedding messages in steganographic system can be carried out without use of a key or with use of a key. To improve steganographic robustness key can be used as a verification option. It can make an impact on the distribution of bits of a message within a container, as well as an impact on the procedure of forming a sequence of embedded bits of a message.

The first level of protection is determined only by the choice of embedding algorithm. This may be the least significant bits modification algorithm, or algorithms for modifying the frequency or spatial-temporal characteristics of the container. The first level of protection is presented in any steganographic channel. Steganographic system in this case can be represented as shown at *The First Protection Level Scheme* figure. There following notations are used: c - is a container file; F - steganographic channel space (frequency or/and amplitude container part, that is available for steganographic modification and message signal transmission); SC - steganographic system; m - message to be embedded; E - embedding method; \hat{c} - modified container file.

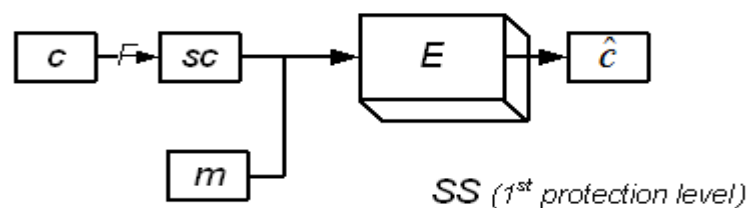


Figure 3 1st level protection[8]

The second protection level of the steganographic system, as well as all levels of protection of the higher orders, is characterized by the use of Key (password) via steganographic modification. An example of a simple key scheme, which provides a second level of protection, is to write the unmodified or modified password in the top or bottom of the message; or the distribution of the password sign on the entire length of the steganographic channel. Such key schemes do not affect the distribution of messages through the container and do not use a message preprocessing according to the defined key (see figure *The Second Protection Level Scheme*). This kind of steganographic systems are used in such tasks as, for instance, adding a digital signature for proof of copyright [8]. Data embedding performance is not changed in comparison with the fastest approach of the first protection level usage.

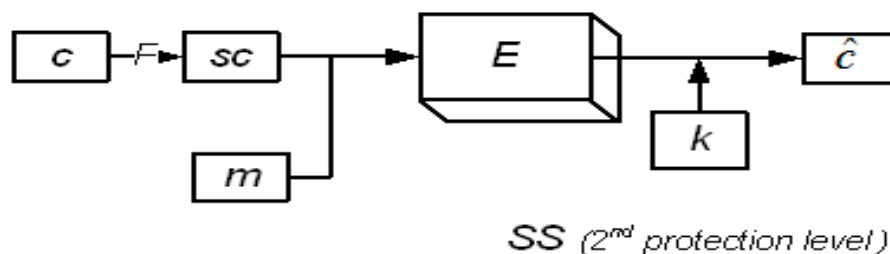


Figure 4 2nd Level protection [8]

Steganographic data channels that use key schemes based distribution of a message through the container and or preprocessing of an embedded message for data hiding are more secure. When the third protection level key scheme is used it affects the distribution of a message through the container (see figure *The Third Protection Level Scheme*, where $F(P, L)$ – distribution function of a message within a container; P – minimum number of container samples that are needed to embed one message sample; L – step of a message distribution within a container). Accordingly, the performance of container processing will be lower than in the case of the first and the second key schemes. Taking into account that $P \geq L$, the simplest representation of the $F(P, L)$ function could be as following:

$$F(P, L) = cycle * L + step * P,$$

where *cycle* is a number of the current L section and *step* is a number of the embedded message sample.

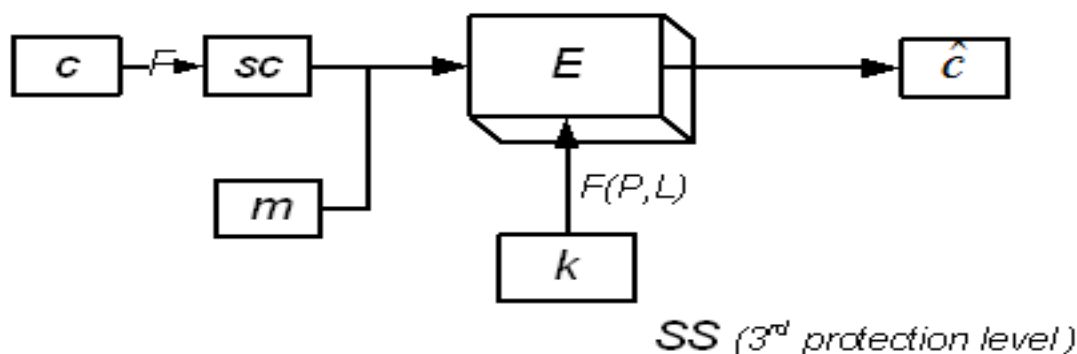


Figure 5 3rd Level protection[8]

Capacity, security and robustness, are the three main aspects affecting steganography and its Usefulness[17]. 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.

Peak signal to noise ratio(PSNR)

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

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

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

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 [12].

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[13].

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 G_i , ($i=1,2,..$) ; (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 G_i , 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 G_i , the results will be saved in B_i (4×4) decimal matrix. All elements of B_i are in the range $(0 \dots 2^m - 1)$.
- **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 G_i , 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 G_i , the values of (r,c) are calculated depending on the values of (i,j) of the point B_i are calculated depending on the values of (i,j) of the point B_i 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 G_i , ($i=1,2,..$) ; (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 G_i , 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 G_i , the values of (r,c) of (i,j) of the point B_i
- Otherwise (if S is positive) subtract the value of V from the pixel $P(r,c)$ in the sub image G_i , the values of (r,c) are calculated depending on the values of (i,j) of the point B_i 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

Steganalysis

Steganalysis is the science of attacking steganography in a battle that never ends. It mimics the already established science of Cryptanalysis [7]. Note that steganographers can create a steganalysis system merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques, e.g., image filtering, rotating, cropping, and translating. More deliberately, it can be achieved by coding a program that examines the stego-image structure and measures its statistical properties, e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction) [9].

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

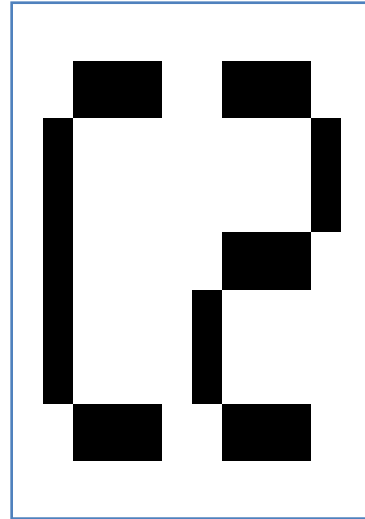


Figure 7. Secret image



Figure 8. Stego image

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

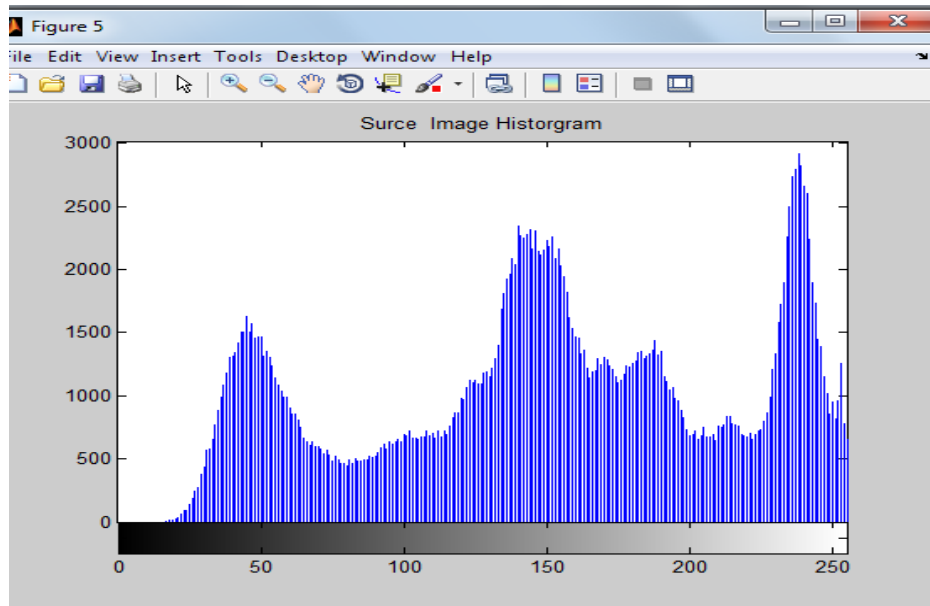


Figure 9 Histogram for cover image

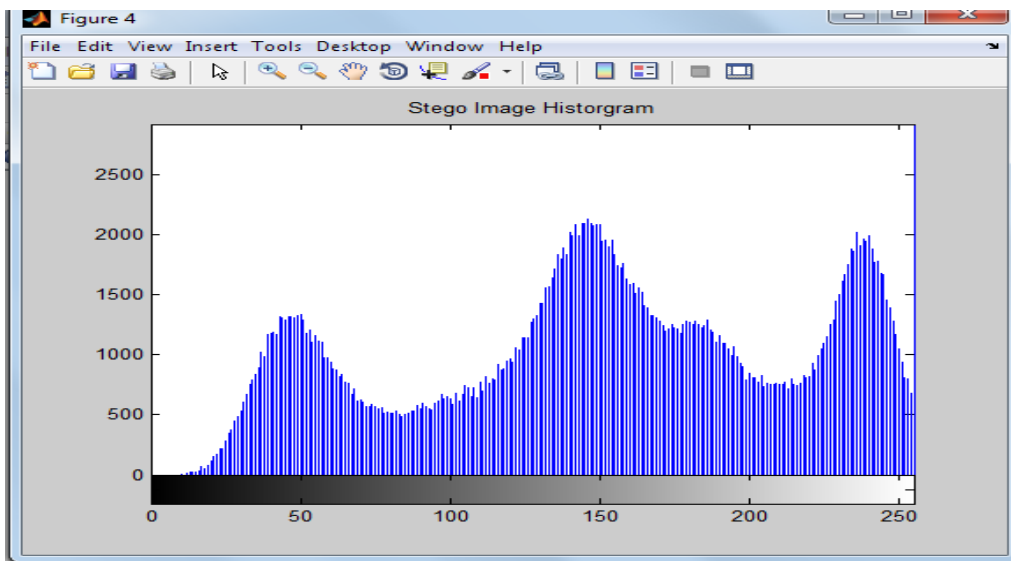


Figure 10. Histogram for stego image

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.

Issues of stegnography

The biggest problem steganography faces is that of size. There is a limit to the size of a file which you can embed information into. For instance if you take a 16 bit image where each pixel is 4 bytes in three colours RGB you can only reliable encode the lower byte before the colour changes become visible in the viewed image.[2] This means that the image you are embedding your data in has to be 1 quarter larger than the encrypted data itself.

Complexity Of Steganography Problem

A transformation from the knapsack problem to the steganography problem a show that the steganography problem is NP-complete.[3]

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.

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, 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", *In Proceedings of (ICASSP '04), IEEE International Conference on 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>