

A Steganographic Approach Based on Spatial Frequency Layering

¹Dr. Sarab M. Hameed

Computer Science Department, College of Science, University of Bagdad

Abstract

This paper presents a steganographic approach capable of concealing a piece of critical information (grayscale image) in a cover RGB image. The critical information is first enciphered, and then embedded into the cover image layers that retain only pixels in area with similar spatial frequency characteristics to that of corresponding enciphered data. Results show that Image Quality Measures (IQM) such as Mean Square Error (MSE) and Correlation of the proposed approach are acceptable. By comparing the mechanism of the proposed approach with least significant bit replacement method, we can draw that our method provides an extra layer of security.

Introduction

The rise of the Internet and multimedia techniques in the mid-1990s has prompted increasing interest in hiding data in digital media. Early research concentrated on watermarking to protect copyrighted multimedia products (such as images, audio, video, and text) [1, 2]. Data embedding has also been found to be useful in covert communication, or steganography. The goal was and still is to convey messages under cover, concealing the very existence of information exchange.

Compared to watermarking, steganography has drawn less attention until recently, as computer specialists, signal-processing researchers, and multimedia product vendors concerned about information security have recognized that illicit use of the technique might become a threat to the security of the worldwide information infrastructure [3]. Researchers have thus begun to study steganalysis, or the detection of embedded information. Detecting secret data hidden in millions of multimedia items downloadable from online sites is recognized as an especially difficult task [4].

The idea and practice of hiding information exchange has a long history. Traditional techniques of steganography, or covered writing in Greek, ranged from tattooing the shaved head of a trusted messenger during ancient times (as reported by the 5th century Greek historian Herodotus) to using invisible ink during the two World Wars in the 20th century. Modern steganography employs digital media content as camouflage, powerful computers and signal-processing techniques to hide secret data, and methods to distribute stego-media throughout cyberspace, thus posing a serious challenge to scientists and professionals alike in the field of information security.

Common approaches to hide information in digital images include least significant bit (LSB) insertion which means there is enough information in the seven bits preceding it to ensure that the correct color will be established. When embedded data's bits are substituted into the least significant bits location it will have little to no effect on the images appearance to the human eye [4]. Other approaches are masking (in a manner similar to paper watermarks), and information hiding in transformations. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize large-capacity embedding for steganography. Candidate transforms include discrete cosine transform (DCT), discrete wavelet transforms (DWT), and discrete Fourier transforms (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. Various methods are available. For example, we can perform a block DCT and, depending on payload and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo-randomly scrambled and undergoes a second-layer transformation. Modification is then carried out on the double transform domain coefficients using various schemes [5, 6].

In this paper, new approach for image steganography has been proposed referred to as Frequency Layered- Based Steganography (FLBS). At the sender's side, the embedded image is encrypted by exclusive or (xor) operation using a specified key. Then, the encrypted image is hidden in cover image layer that retain only pixels in area with similar spatial frequency characteristics. The advantage of FLBS method is that provides an extra layer of security over the conventional one.

The proposed data hiding method is detailed in section two. Experimental results and conclusions are provided in section three and four respectively.

The FIBS General Layout

The purpose of the steganography is, in general, to hide data well enough that unintended recipients do not suspect about steganographic medium of containing hidden data. Cryptography, on the other hand, encodes data so that an unintended recipient cannot understand its intended meaning. Most steganographic methods also encrypt the data so even if the presence of the data is detected, deciphering (decrypting) the data will still be required. Hence forth, steganography is complementary to cryptography because it adds an extra layer of security. The purpose of this paper is to combine steganography and cryptography in one scheme. While, steganography scheme depends on decomposing the steganographic medium (a cover image) into layers each of them contains those pixels in areas with specified laplacian magnitude (sharpness/roughness magnitude), a simple cryptography scheme, on the other hand is used to encrypt the hidden data (an embedded image). The steps of Frequency Layered- Based Steganography (F.L.B.S) approach are explained as follows:

Step1: decompose the cover image (x) into various frequency components (layers). Each layer consisting of an image the same size as the original one, but only pixels in area with a certain spatial frequency range (i.e. a band pass filtered version of the original one). This decomposing process can be done as follows (figure (1) [7]):

- *Convert to de-correlated color space:* Convert x form correlated RGB color space to de-correlated color space (e.g. YIQ, where Y is a measure of luminance and I and Q components are the chromatic information). Figure (2) depicts this step on an image example.



Figure (2) a: RGB Image b: Y Channel of Image

- *Apply Gaussian or mean filter:* The y is filtered by low-pass filter (we use 3×3 Gaussian filter with coefficient (0.05, 0.25, 0.4, 0.25, and 0.05) or 3×3 mean filter). The resulted image is called $f(y)$. Figure (3) depicts low-pass filtering on channel Y.



Figure (3) Low-pass Filtering for Channel Y (left low-pass filter with Gaussian filter, right low pass filtering with mean filter)

- *Apply Laplacian filter:* Subtract the low-passed image $f(y)$ from the channel y . The difference is then rectified (i.e. by taking the absolute values). Multiple thresholds are applied (we use three thresholds, i.e. four layers). The magnitude of the image indicates the sharpness of the image area. A busy area, which contains many sharp changes, will result in large difference between the cover image and the smoothed image. A flat area will result in small difference between the original and smoothed image. Therefore the magnitude in the laplacian is an indication of the roughness of the image area surrounding the pixel. The scheme therefore effectively classified pixels in area with similar roughness into the same layer. Figure (4) depicts effect of laplacian filter with three thresholds (15, 35, and 65) on $f(y)$.



Figure (4): Frequency Classified layer for Image in Figure 2.a. A White Color Indicates that the Pixel is absent from that Position.

- *Sort Layers:* Sort the layers obtained from the step in descending order (according to the number of pixels each contains). Each of these layers can be used to indicate the pixel path on which the critical data is concealed.

Step 2: Once we have classified pixels into different layers and arranged layers in descending order, the following operations are performed to hide the grayscale image:

- *Scan embedded image:* Scan the grayscale image (embedded information) from top to bottom and from left to right in steps of one byte (B) at a time.
- *Encrypt embedded image:* B will be encrypted simply using XOR operation with the key K (K is a secret key shared by the sender and the receiver).
- *Hide embedded image:* Largest layer is scanned in scan-line order so that, B will be hidden in the two least significant bits of four byte of the RGB pixel that belong to that layer. Continuing this process for all bytes of the embedded information and if this layer was not sufficient to hide the embedded information then we use the second layer and so on.

Results

The proposed approach satisfy steganographic requirements: including security, size of payload, and imperceptibility.

First, in order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically. This requirement was satisfied by encrypting the embedded information and hiding it in different layers based on spatial frequency.

Second, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. This method consumes four bytes of the cover image to embed one byte of the embedded grayscale image.

Finally, in order to quantitatively the success of the proposed approach, some of Image Quality Measures (IQMs) are employed such as Mean Square Error (MSE) and Correlation Coefficient (Corr).

The MSE is calculated as demonstrates in equation 1 [8].

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (Y_{ij} - S_{ij})^2 \quad (1)$$

Where M, and N are the height and width of the cover image, Y_{ij} is the pixel value of the cover image, S_{ij} is the pixel value of the stego-image.

Correlation Coefficient is given by equation 2 [8].

$$Corr = \frac{\sum \sum (S - \bar{S})(Y - \bar{Y})}{\sqrt{\sum \sum (S - \bar{S})^2} \sqrt{\sum \sum (Y - \bar{Y})^2}} \quad (2)$$

Where

$$\bar{S} = \frac{\sum \sum S}{MN} \quad (3)$$

$$\bar{Y} = \frac{\sum \sum Y}{MN} \quad (4)$$

S represents the pixels of the cover image and Y represents the pixels of the stego image.

The results of FLBS on a number of images are illustrated in figure (5). The 1st column demonstrates cover image, 2nd column illustrates embedded image, 3rd column stego image, presents 4th column MSE and 5th produces correlation. From results, we show that the MSE is very small, and the correlation is near one which mean that this method provide high imperceptibility.

Conclusion

The method presented here is capable of hiding information (grayscale image) in the given

RGB image. This approach has the following features: a secret key is used to hide the data in secure manner. An extra layer of security is accomplished by hiding the information in the encrypted form and in different layers. This scheme significantly enhances the security but at the same time retains its simplicity.

References

- [1] J. Fridrich "Applications of data hiding in Digital Images", Tutorial of the ISSI'99 Conference, Brisbane, Australia, August 1999, 22-25.
- [2] S. Katzenheisser and F. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Computer, 2000.
- [3] L. M. Marvel, "Image Steganography for Hidden Communication", Tech. Rep. ARL-TR, Army Research Laboratory, April, 2000.
- [4] Maeho, Romana, "How Stego Online Works, URL: <http://www.stego.com/howto.html>.
- [5] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding IBM Systems Journal, vol.35, no. NOS 3&4, 1996, pp 313-335.
- [6] N.F. Johnson and S. Jajodia, "Exploring steganography, seeing the unseen", IERF Computer, 1998, pp 26-34.
- [7] G. Qin and K. Lam, "Frequency Layered Color Indexing for Content-Based Image Retrieval", IEEE Transaction on Image Processing, Vol. 12, No. 1, 2003.
- [8] G.M. Kadhor NawaZ, G. Prakash, and Dr. K. Thiyayarajah " Data Hiding and Image Quality Measures(IQMs) a New Stego-Crypto Approach", Proceeding of the 4th International Multiconference on Computer Science and Information Technology, Vol 1, 2006, pp 251-256.

المستخلص

يقدم البحث طريقة لإخفاء المعلومات الخرجة (صورة رمادية) في صورة صورة. توفر المعلومات الخرجة أولاً بعد ذلك يتم إخفاءها في طبقات فصوصة التي تحتفظ بالنقاط التي لها نفس خصائص التردد المكتسب. أوضحت النتائج بأن مقاييس نوعية الصورة متوفرة مثل خطأ المعدل التربيعي (MSE) ومعامل الارتباط. أعطت هذه الطريقة المقترحة طريقة إحصائية من الأمانة مقارنة بالطريقة التقليدية.

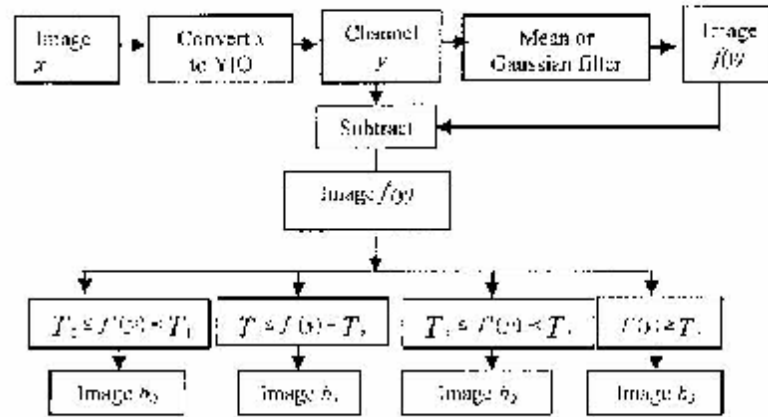


Figure (1) Layer classification method
















Cover Image	Embedded Image	Stego Image	MSR	Correlation
			4.467	0.998
			5.59	0.999
			2.4	0.998
			5.07	0.997
			6.03	0.997

Figure (5) Some Results of the FLBS with IQM