A DCT-based Image Steganographic Method Resisting Statistical Attacks[1]

Rufeng Chu, Xinggang You, Xiangwei Kong, Xiaohui Ba

Department of Electronic Engineering, Dalian University of Technology, Dalian, China

ABSTRACT

The aim of steganography is to conceal the very existence of hidden communication, so its demand on security is serious. The security includes both imperceptibility and undetectability. But most steganographic methods didn't pay enough attention to the undetectability. In this paper, we propose a novel DCT-based steganographic method for images. The method takes advantage of the similarities of DCT coefficients between the adjacent image blocks and makes the embedding distortion spread to the adjacent image blocks. Experimental results demonstrate that this proposed method can not only preserve good image quality, but also resist some typical statistical attacks.

1. INTRODUCTION

The purpose of steganography is to hide the very presence of communication by embedding messages into innocuous-looking cover objects, such as digital images. To accommodate a secret message, the original cover image is slightly modified by the embedding algorithm to obtain the stego image.

The early steganographic schemes focused on introducing as little distortion in the cover image as possible utilizing the seemingly intuitive heuristics that the smaller the embedding distortion is, the more secure the steganographic scheme becomes. The Least Significant Bit embedding (LSB) with sequential or random message spread is a representative method of the idea, some famous steganographic software, such as Steganos, S-tools and Hide4PGP[1], are all based on the idea of LSB. In addition, researchers proposed some improved LSB replacement methods [2,3], based on characteristics of human visual systems (HVS) and spatial complexity measure, in order to increase the capacity. However, recent advances in steganalysis clearly showed that this is not the case. The LSB method has been successfully attacked even for very short messages [4,5]. In essence, the LSB embedding is so easily detectable because it introduces distortion that never naturally occurs to images and creates an imbalance between appropriately defined statistical quantities.

To enhance the security and improve the undetectability of steganographic method, some researchers attempt to design new steganographic schemes that embed messages by adding Gaussian noise to the image. Lisa M. Marvel describes a high-capacity method for embedding message bits in uncompressed raw image formats [6]. The hidden messages are modulated to Gaussian signals adding to the cover image. Faisal Alturki's approach [7] is a simple bit-replacement of quantized DCT coefficients calculated from a randomly permuted image. In the method, the distortion distribution is approximately a generalized Gaussian distribution. With the development of the steganalysis, a new steganalytic method has been proposed by Jeremiah J. Harmsena in 2003 [8], which is based on the fact that noise adding in the spatial domain corresponds to low-pass filtering of the histogram. Thus, the histogram of stego images has less power in high frequencies than the same histogram for cover images. Based on this statistical property, a classifier can be established to distinguish between cover images and stego images.

In this paper, we propose a novel DCT-based steganographic method for images, which can not only preserve good image quality, but resist some typical statistical attacks proposed in [4,8].

The rest of this paper is organized as follows. In the next section we analysis the statistical distributions of DCT coefficients at first. Then a detailed description of the new DCT-based steganographic method is given. The experimental results are shown in section 3. Finally, conclusions and future works are drawn in section 4.

2. NEW DCT-BASED STEGANOGRAPHIC METHOD

Hiding information within an image requires modification of redundant bits in the image. In general, such distortion cannot be sensed by human vision, but it may change media data properties. For example, statistical properties of

[1] This work was supported by National High Technology Research and Development Program of China and Science Foundation of Education Department of Liaoning Province (No. 20111029)

the cover image may be changed since information is embedded. As a result, statistical analysis is one of many steganalystic approaches. It may reveal the hiding traces or facts. Perhaps, this is also one of the foundations for steganalysis. On the contrary, for steganography, we should avoid making predictable changes to the data properties of the image. So we need analyze both the statistical distributions of the DCT coefficients and the characteristics of the typical statistical attacks [4,8].

2.1. Statistical Properties of DCT Coefficients

In our algorithm, we divide an image into 8×8 blocks of pixels firstly. Then we transform each image block into DCT (discrete cosine transform) domain. Over the past two decades, there have been various studies on the statistical distributions of the DCT coefficients for images. Figure 1(b) shows a typical plot of the histograms of the DCT coefficients. The image used here is the "bridge" image shown in Figure 1(a) from the standard image processing library. We find that distributions of the DCT coefficients between the adjacent image blocks are similar. Through further observation, we also find that the coefficients in the same position of the adjacent image blocks are also similar to some extent. In order to preserve good image quality and security, we need to take advantage of the similarity of the coefficients.

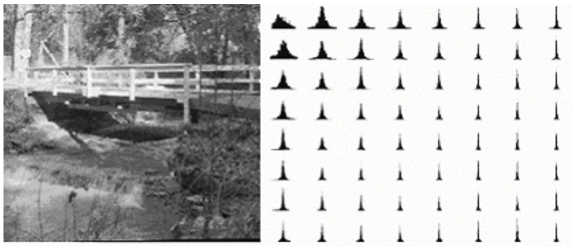


Fig.1 (a) Standard image "bridge" (b) DCT coefficients distributions of "bridge"

To improve the undetectability, we need to analyze the characteristics of the existing typical steganographic and steganalytic methods at first. The LSB replacement method as well as its improved methods [1,2,3] has a disadvantage, strong randomicity occurs in the bit-planes after messages embedding. Take advantage of this statistical property, steganalytic methods [4,5] can reveal exactly the existence of secret communications. In particular, Fridrich's RS Steganalysis can exactly estimate the message length even for very short messages. In addition, the method of adding Gaussian noise to images is also not available. The Gaussian noise is different from the device noise introduced during the image capturing process. If an image consists of much distinct Gaussian noise, it will be easy to be paid attention to. A novel statistical attack method has been proposed by Jeremiah [8], which can effectively attack the additive noise modelable steganography. From the viewpoint of Jeremiah's attack method, the Gaussian noise adding method [6.7] is one of the additive noise modelable steganography.

From the analysis above, we can see that the statistical properties in the bit-planes should not change much after embedding for a high performance steganographic method. In addition, we cannot apply simple Gaussian noise adding method. However, we still think the noise adding method has high performance. The noise just should be the content-dependent noise. In this paper, we present a novel DCT-based steganagraphic method, which take advantages of the similarity of the DCT coefficients in the same position of the adjacent image blocks. To embed message, we quantize the difference of the coefficients instead of the coefficients themselves. Thus the distortion spreads to the adjacent image blocks. Because quantized noise is produced by both of the DCT coefficients of the adjacent blocks, the magnitude of the noise is different according to different image contents. This is to say that the quantized-noise is not independent of the image contents. So our method cannot be considered as additive noise steganography model in which the additive noise must be independent of the image. This can help our method resist Jeremiah's statistical attack [8]. On the other hand, the quantized noise is scattered in different bit-planes after taking the inverse block DCT. Thus the randomicity of the bit-planes remains the same as natural images, which makes Fridrich's statistical attack failed. The experimental results will be given in the section 3 in detail.

2.2. Proposed Steganogaphic Method

Let I be a natural image of size $M\times N$. The embedding process starts by dividing the image into $n\times n$ blocks. Then we apply $n\times n$ DCT to each block, and classify the adjacent DCT block B_1 and B_2 as a group. $B_1(i,j)$ and $B_2(i,j)$ denote the DCT coefficients of the block B_1 and B_2 respectively, where $0\le i,j<n$.The difference of the DCT coefficients of adjacent DCT blocks is calculated as follows.

$$d(i,j)=B_2(i,j)-B_1(i,j)$$

To embed a " 1" , we quantize the $d(i,j)$ to be even multiple of S. To embed a " 0" , we quantize the $d(i,j)$ to be odd multiple of S. Detailed description of the process is shown in the following.

(1) Let $m=round(d(i,j)/S)$, where $round(\cdot)$ represents the round function. To embed a " 1" , we substitute m with a nearest odd integer to $d(i,j)/S$. To embed a " 0" , we substitute m with a nearest even integer to $d(i,j)/S$.

(2) Calculate the quantized difference, $d^{'}(i,j) = m \times S$.

(3)We get the new DCT coefficients $B_1^{'}(i,j)$ and $B_2^{'}(i,j)$ using the formula,

$$B_1^{'}(i,j) = B_1(i,j) - (d^{'} - d)/2$$

$$B_2^{'}(i,j) = B_2(i,j) + (d^{'} - d)/2$$

To increase the capacity, we can embed two bits per quantization. The embedding process can be simulated in a similar way. For example, to embed " 00" the differences are quantized so that the result of the division by S followed by 2 results in even integers. To embed " 10" a subsequent division by S followed by 2 results in an even followed by an odd integer etc. And we can get $B_1^{'}(i,j)$ and $B_2^{'}(i,j)$ respectively. When the embedding process is completed we take the inverse block DCT and then get the stego image $I^{'}$ 。

The decoding process is straightforward. Similar with the encoding process, the stego image is partitioned into non-overlapping $n \times n$ blocks. Next, the block DCT is computed and each difference of the DCT coefficients in the same position of the adjacent blocks is calculated. Then each difference value is divided by S . The output of the first division is divided by 2 to obtain the second embedded bit. Fig.2 shows a block diagram of the decoding procedure.

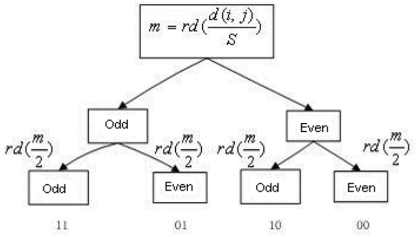


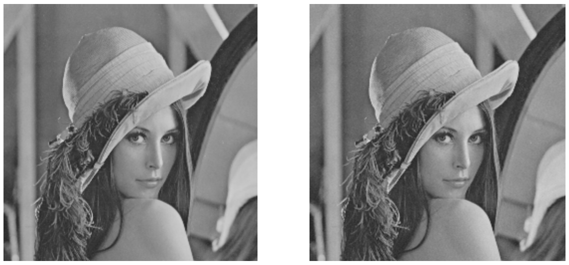
Fig.2. Structure of the extracting process

Here $d(i,j)$ represents the (i,j)-th received difference and $rd(\cdot)$ represents the round function.

3. EXPERIMENTAL RESULTS

3.1. Image quality

In this section we present an example to illustrate the technique. We use the popular image LENNA of size 256*256. Fig.3 shows the cover image and the stego image embedded with the maximum payload (4k bytes). The PSNR (Peek Signal and Noise Ratio) value of the stego image is 45.89 db.



(a) cover image (b) stego image

Fig.3. An experimental result of the proposed method

3.2. Security

As for security of the steganographic algorithm, the demand on undetectability is much serious. In the following, we will analysis our algorithm with some classic steganalysis techniques.

3.2.1. Jiri Fridrich's RS Steganalysis

Jiri Fridrich proposed a statistical steganalytic method in 2001[4], which can detect effectively the existence of secret messages embedded with LSB or some extended algorithms, such as Steganos[1], S-Tools[1], Hide4PGP[1], AMLSB[3] and BPCS[2]. By the method, an image is divided into disjoint pixel groups. The regularity of each group is computed by a discrimination function. By combining the function and an invertible operation, three types of pixel groups are defined: regular, singular, and unusable. Two complemental masks are used for simulating the act of different noise adding.

As for LSB-like algorithm, the test results can be indicated in the Fig.5. In the diagram, the x-axes depict the percentage of image pixels into which message data are embedded, and the y-axes depict the relative numbers (in percentage) of regular and singular pixel groups with masks m=[0 1 1 0] and –m=[0 -1 -1 0]. Such diagram is referred to as RS-diagrams. According to RS steganalysis[4], if more and more LSBs are replaced with random data, then the variety in the percentages Rm and Sm of the two pixel groups (regular and singular, respectively) in the diagram can be expressed by a curve model like Fig.4. Through the model, an equation can be deduced to estimate the length of the secret messages.

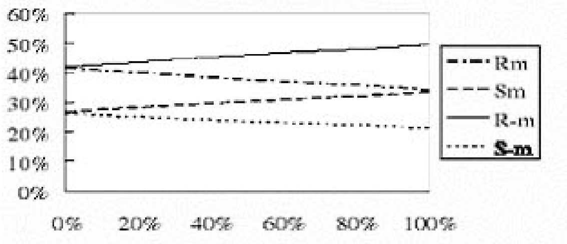


Fig.4. RS-diagrams for stego images produced by LSB-embedding steganographic method

The RS-diagram of our method in Fig.5 indicates that the stego images seemingly do not contain any embedded data in their LSBs because the relative values of percentages Rm and Sm are invariant with the increase of the embedding capacity. This proves that our steganographic method is secure from the viewpoint of the dual statistics method.

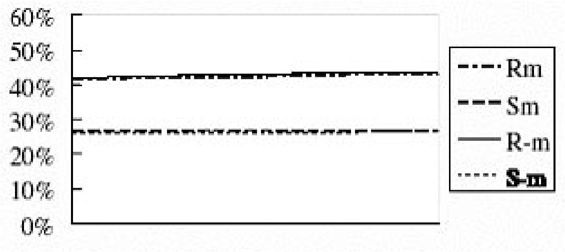


Fig.5. RS-diagrams produced by our method

3.2.2. Jeremiah J. Harmsena's Histogram Attack

A new steganalytic method has been proposed by Jeremiah J. Harmsena[8] in 2003. Harmsen based his attack on the fact that noise adding in the spatial domain corresponds to low-pass filtering of the histogram. Thus, the histogram of stego images has less power in high frequencies than the same histogram for cover images. The attack starts with calculating the histogram of images standing for the number of pixels with the pixel value . Then, h is transformed using the Fourier transform to obtain . Finally, he calculates the center of gravity of and uses this quantity as the distinguishing statistics to differentiate between cover and stego images.

To test our method, 100 images captured from Kodak digital camera DC290 are used. These images are 8 bit, 720*480 pixels, lossless grey images stored in TIFF format. For each image the center of gravity of is computed for the original image as well as the stego image produced by our method. To compare our algorithm with ordinary DCT-based algorithm, Alturki's DCT-based steganographic method [7] has been also tested. The results were shown in Fig.6 and Fig.8 respectively. As for ordinary DCT-based method, we can see that Harmsena's attack can effectively distinguish stego images from original images. But as is shown in Fig.7, Harmsena's method could not distinguish between original and stego images produced by our method. This proves that our steganographic method is secure from the viewpoint of Harmsena's method.

4. CONCLUSIONS AND FUTURE WORKS

In this paper, we proposed a novel secure DCT-based steganographic method, based on the analysis of typical steganalytic algorithms and statistical distributions of DCT coefficients. Extensive experimental results demonstrate that the method not only can preserve good image quality, but also can resist some typical statistical attacks. We are focusing our future research on applying the ideas of the proposed method for JPEG images.

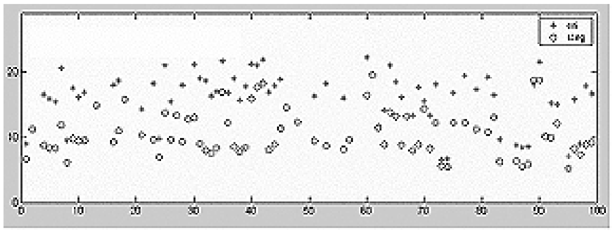


Fig.6. Results of Alturki's DCT-based method

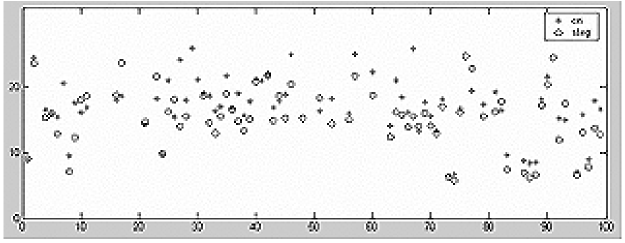


Fig.7. Results of our method

5. REFERENCES

[1] Steganographic software: http://www.jjtc.com/Steganography/toolmatrix.htm

[2] Eiji Kawaguchi, and Richard O.Eason, "Principle and Applications of Bpcs-Steganography", *SPIE's International Symposium on Voice, Video, and Data Communications*, Nov. 1998

[3] Yeuan-Kuen Lee and Ling-Hwei Chen, "An Adaptive Image Steganographic Model Based on Minimum-Error Lsb Replacement", *Ninth National Conference on Information Security*, Taichung, Taiwan. May 14-15, 1999. page(s): 8-15

[4] Jiri Fridrich, R. Du and M.Goljan, "Detecting LSB Steganography in Color and Grey-Scale Images", *Magazine of IEEE Multimedia Special Issue on Security*, Oct. 2001, page(s):22-28.

[5] Jiri Fridrich, R. Du and M. Long, "Steganalysis of LSB Encoding in Color Image", *Proceeding of IEEE International Conference on Multimedia and Expo*, Piscataway, 2000

[6] Lisa M. Marvel, Charles T.Retter, and Charles G.Boncelet, "Hidding Information in Images", *International Conference on Image Processing*, 1998, Vol.2: 396-398

[7] Faisal Alturki, and Russell Mersereau, "A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications", *International Conference on Information Technology: Coding and Computing,* 2001. page(s):228-233.

[8] J.J. Harmsen and W. A. Pearlman, " Steganalysis of Additive Noise Modelable Information Hiding", *Proc. SPIE Electronic Imaging*, Santa Clara, January 21–24, 2003