A Secure Steganographic Method on Wavelet Domain of Palette-Based Images[⋆]

Wei Ding, Xiang-Wei Kong, Xin-Gang You, and Zi-Ren Wang

School of Electronic and Information Engineering,
Dalian University of Technology, China
weiding_dlut@hotmail.com, {kongxw,youxg}@dlut.edu.cn

Abstract. This article presents a novel secure steganographic method on wavelet domain of GIF images. Secret information is usually embedded in palettes or indices of GIF images directly by formerly presented steganographic methods. These methods may introduce visible noise and detectable changes of parameters in images. The new method based on integer wavelet transform dispels noise introduced by data-hidding into adjacent pixels. Matrix encoding is also applied in embedding. Both scattering noise and matrix encoding improve the quality of the stego-images and the security of secret communication. Experimental results show the fine security of the proposed method in resisting attacks by χ^2 detecting method and Fridrich's detecting method.

Keywords: Steganography; GIF image; integer wavelet; matrix encoding; security

1 Introduction

GIF images are popular carriers used in steganography because of its widely use on Internet. Although steganographic algorithms on GIF images appeared early, there are not so many secure methods at present for many detecting methods were also presented. GIF format contains a palette and image indices pointing to the corresponding colors in the palette. There are 256 kinds of colors at most in the palette. Most of current steganographic methods embed secret information directly in palettes or indices of GIF Images. There are mainly three classes of approaches. Gif-shuffle [1] uses different combinations of colors to embed secret message, leading to a limited capacity of 210 bytes. Artifacts are easy to be detected by χ^2 steganalysis method [2] in stego-images created with softwares such as S-Tools [3] or Hide&Seek [4] which change the palette and image indices simultaneously. Schemes changing indices directly such as EZ Stego [5] and methods presented by Fridrich [6,7,8] may introduce visible noise which deteriorates the quality of images. And EZ Stego can not counteract the steganalysis methods presented by Fridrich [9].

[⋆] This paper is supported by the project of National Nature Science Foundational of China (Grant No. 60372083).

K. Aizawa, Y. Nakamura, and S. Satoh (Eds.): PCM 2004, LNCS 3333, pp. 426–432, 2004.

In this article, a novel secure steganographic algorithm is presented which embeds secret information in the high frequency coefficients of the wavelet domain. Thus, noise generated by embedding message is scattered into adjacent pixels. We implement matrix encoding in the process of embedding which also improves the security of the algorithm. The principle of the new approach is introduced in section 2. Section 3 lists experimental results that show the security of the algorithm in defending χ^2 detecting method and steganalysis method presented by Fridrich.

2 Method Description

2.1 Integer Wavelet Transform

In GIF images, image indices are stored as integer and its scale is 0∼255 when there are 256 kinds of colors in the palette. If transform in common use such as DCT or DWT is used in steganography [10] on GIF images, the overflow in spacial domain is hard to control. So we should adopt the integer wavelet transform. S transform presented by Swelden [11] is adopted in this paper. It is the Harr integer wavelet transform mapping integers to integers. The overflow can be controlled by preprocessing that we will present in section 2.3. The S transform is:

$$l = \left\lfloor \frac{x+y}{2} \right\rfloor, \quad h = y - x \tag{1}$$

The inverse transform is:

$$x = l - \left\lfloor \frac{h}{2} \right\rfloor, \quad y = l + \left\lfloor \frac{h+1}{2} \right\rfloor \tag{2}$$

When we apply these formulas to images, x and y denote the adjacent pixels values in a row or a volume of the image. l and h are the low frequency and high frequency part respectively. "$\lfloor\rfloor$" means "the greatest integer less than or equal to".

2.2 Matrix Encoding

Matrix encoding[12,13] is used to improve the security of the algorithm. When the length of secret message is less than the maximum capacity of the cover image, the number of changes due to message embedding can be decreased by adopting matrix encoding. When a secret message x with k bits is going to be hidden in a code a which contains n modifiable positions, we can find a proper code a' using matrix encoding for code a. Let f be a hash function that extracts k bits from code a. The hash function $f(a)$ can be determined by the followed equation:

$$f(a) = \bigoplus_{i=1}^{n} a_i * i \tag{3}$$

where $\oplus$ represents the operation of exclusive or and a_i is the ith modifiable position in the code a. The code a' is the modified code a which is generated by the f function and message x with $x = f(a')$. The Hamming distance $d(a, a')$ follows:

$$d\left(a, a'\right) \leq d_{\max} \tag{4}$$

In the formula $d_{\max}$ represents the maximum of changed indices without matrix encoding when message is embedded under the same condition. Thus we use $(d_{\max}, n, k)$ to represent this matrix encoding. The discussion presented by Westfield[13] shows that the embedding efficiency using matrix encoding is higher than that without matrix encoding.

2.3 Algorithm of the New Method

The indices scale is 0∼255 for GIF images with 256 colors. Embedding data in coefficients obtained from integer wavelet transform directly may overflow the range of image index value. The overflow will result in the failure of extracting information. The preprocessing adopted by this method to overcome this difficulty is described as follows.

Preprocessing. Let x' , y' be the indices of the stego-image and x, y are the indices of the corresponding pixel in the cover image (0≤x≤255,0≤y≤255). Δx, Δy are the values of the modification in spatial domain, thus:

$$x' = x + \Delta x, \quad y' = y + \Delta y \tag{5}$$

Let Δh be the value of the modification of the high frequency coefficients after embedding, then from (2):

$$x' = l - \left\lfloor \frac{h + \Delta h}{2} \right\rfloor, \quad y' = l + \left\lfloor \frac{h + 1 + \Delta h}{2} \right\rfloor \tag{6}$$

From (5) and (6) we can obtain the following:

$$\Delta x = \left\lfloor \frac{h}{2} \right\rfloor - \left\lfloor \frac{h + \Delta h}{2} \right\rfloor, \quad \Delta y = \left\lfloor \frac{h + 1 + \Delta h}{2} \right\rfloor - \left\lfloor \frac{h + 1}{2} \right\rfloor \tag{7}$$

According to the deduction above we can find the changing direction of the scale. Δh may be equal to –1, 0 or 1 during embedding. The changed value of the index may be –1, 0 or 1 after inverse transform according to (7). Then the range of indices changes from (0∼255) to (-1∼256). So the scale of indices in the cover should be adjusted to (1,254) in preprocessor in order to keep the indices of the stego image in the normal range. The process is presented as follows:

1. Let $f(c_i)$ be the appearance frequency of color c_i; Let A and B be the two indices of colors which have the least appearance frequency in the palette:

$$\begin{aligned} f(A) &= \min f(c_i)\ (i = 0, 1, \cdots, 255) \\ f(B) &= \min f(c_i)\ (i = 0, 1, \cdots, 255, i \neq A) \end{aligned} \tag{8}$$

2. C and D are the closest color indices to A and B respectively according to Euclidean norm distance in the palette (C≠A≠B, D≠A≠B).
3. Let *width* and *height* be the width and height of the image respectively. Let $index_j$ be the index of the jth pixel in the image. Replace A, B with C,D respectively in image indices:

$$index_j = \begin{cases} C \quad if \quad index_j = A \\ D \quad if \; index_j = B \quad 0 \le j < width * height \\ index_j \quad otherwise \end{cases} \tag{9}$$

4. Replace 254, 255 with A and B, respectively in the original palette. Indices should be adjusted again because of the change of the palette:

$$index_j = \begin{cases} A \quad if \quad index_j = 254 \\ B \quad if \; index_j = 255 \quad 0 \le j < width * height \\ index_j \quad otherwise \end{cases} \tag{10}$$

At last preprocessor is finished.

Create the New Palette. The palette should be rearranged after the preprocessor. The arrangement algorithm is similar to traveling salesman problem. It is based on the principle that the sum of the Euclidean norm distance between rearranged adjacent colors is the least among all kinds of orders. So reordered neighboring color indices are close to each other. The process to create the new palette is described as Fig. 1. The first 254 colors rearranged. The indices range of those 254 colors in the new palette is assigned to (1,254). Then the first position in the new palette is filled with the second color and the last position is filled with its previous color. The original palette is also required to adjust to correspond the new palette. The procedure is described as follows:

OldPal[254]= NewPal[1] OldPal[255]= NewPal[254]

In the above description newPal[i] and oldPal[i] represent the ith position in the new palette and the original palette respectively.

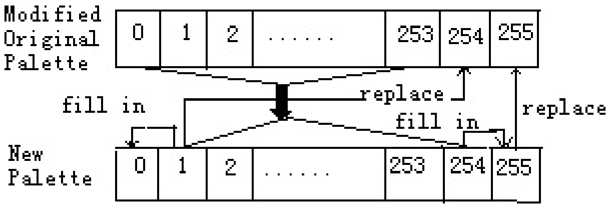

Fig. 1. producing the new palette

Procedure for Embedding. New image indices can be obtained when the new palette is created. Then embedding process with matrix encoding (1, n, k) is presented as following:

1. Let *maxcap* be the maximum of the embedding capacity of the image:

$$maxcap = width * height * 0.5 \tag{11}$$

2. Let *msglg* be the actual length of the secret message. Then proper n and k could be counted according to the formulas:

$$\begin{aligned} msglg > (maxcap * (k+1)/n - (maxcap * (k+1)/n\%n)) \\ msglg \leq (maxcap * k/n - maxcap * k/n\%n) \end{aligned} \tag{12}$$

   The operation '%' is to get the integral remainders.

3. Code a is composed by the LSBs of the n high frequency coefficients selected according to the order generated by a pseudo random seed. The hash function $f(a)$ can be determined by (3). When k bits message x is hidden in code a, the position s to be changed[13] is gained by:

$$s = x \oplus f(a) \tag{13}$$

   At last the modified code a' is obtained by:

$$a^{'} = \begin{cases} a, \quad if\ s = 0 (\Leftrightarrow s = f(a)) \\ (a_1, a_2, \cdots, \neg a_s, \cdots, a_n), \quad otherwise \end{cases} \tag{14}$$

   where ¬ is the bit-wise *not* operation.

4. Repeat step 3 to embed the next k bits until all message is embedded. Then apply inverse wavelet transform according (2).Store image data as GIF format.

Extract Secret information. Secret information could be extracted according to the inverse procedure of embedding.

3 Experimental Results and Discussion

Stego images created by the proposed method and EZ stego are called new-stego-images and EZ-stego-images respectively. Experimental results of PSNR shown in Table 1 indicate the good quality of new-stego-imges. In this section, χ^2 detecting[2] method and Fridrich's detecting method[9] are used to test the security of the new algorithm. The embedding capacity in experiments is 0.5bit/pixel. Experimental images are from different sources which contain 60 sheets of scanned images, 65 sheets of images from digital camera and 20 sheets of images from Fabien's standard image database on Internet[14]. As Table 1 shows new-stego-images counteract χ^2 steganalysis method for the detecting rate is

Table 1. Experimental Results of χ^2 steganalysis method and the average PSNR. The threshold is 60%; If the embedding probability counted from a image by χ^2 steganalysis method is above 60%, the image is considered as a stego-image

Image Class	Scanned Images	Digital Photos	Standard Images
Image Quantity	60 sheets	65 sheets	20 sheets
Detecting Rate	6.19%	4.16%	0%
Average PSNR	32.3098 dB	34.5622 dB	34.6144 dB

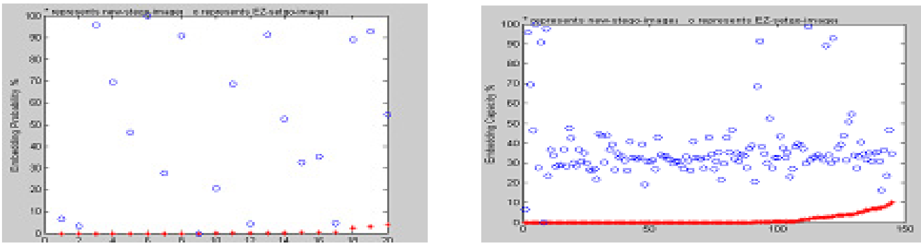

Fig. 2. Comparison of χ^2 detecting results on 20 sheets of images from Fabien's standard image database(the left) and camparison of Fridrich detecting results on 145 sheets of images(the right); 100% represents the embedding of capacity of 1bit/pixel; $*$ represents new-stego-image;

very low. Figure 2 show the comparison between new-stego-images and EZ-stego-images using χ^2 detecting method(the left) and Fridrich detecting method(the right). The comparisons indicate high security of the new algorithm. The security of new-stego-images is better than that of EZ-stego-images because that histogram of the image after embedding data by EZ Stego has many adjacent pairs but this phenomena in the new-stego-images is unconspicuous and noises in new-stego-images introduced by steganography is scattered into adjacent indices. All these experiments make it clear that the new method has fine performance.

4 Conclusion and Outlook

Experimental results show that new-stego-images produced by the new method has good quality and this method has high performance in defending χ^2 steganalysis method and steganalysis method presented by Fridrich. But artifacts might be visible in some GIF Images after embedding because they have small number of colors. So in futrue work, we should take more attention on the improvement of visual security in images with small number of colors.

References

1. Kwan, M.: Gifshuffle 2.0. Available from http://www.darkside.com.au/gifshuffle/ IEEE Trans. (2003)
2. A. Westfeld and A. Pfitzmann: Attacks on Steganographic Systems. Lecture Notes in Computer Science,vol.1768, Springer-Verlag, Berlin,(1999) pp. 61–76
3. Brown A.: S-Tools for Windows, Shareware. www.jjct.com/steganography/toolmatrix.htm (1994)
4. Colin Moroney : Available from www.jjct.com/steganography/toolmatrix.htm
5. Machado, R: EZ Stego, Stego Online, Stego. Available from http://www.stego.com (1997)
6. Fridrich, J.: Applications of data hiding in digital images. Tutorial for The ISSPA_99, Brisbane, Australia, (1999)
7. Fridrich, J.: A new steganographic method for palette-based images. IS&T PICS, Savannah, Georgia, 25-28 (1999) pp. 285–289
8. Fridrich, J., Du, J.: Secure steganographic methods for palette images. In: Proc. the Third Inform. Hiding Workshop LNCS, vol. 1768. Springer-Verlag, New York, pp. 47–60
9. Jessica Fridrich, Miroslav Goljan, David Soukal: Higher-order statistical steganalysis of palette images. In Proc. EI SPIE Santa Clara, CA, Jan (2003) pp. 178–190
10. Rufeng Chu, Xingang You, Xiangwei Kong, Xiaohui Ba: A DCT-based Image Steganographic Method Resisting Statistical Attacks. The 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing (IEEE ICASSP 2004)
11. Calderbank A R, Daubechies I, Sweldens W, et al: Wavelet transforms that map integers to integers[R]. Princeton, New Jersey, U.S.: Department of Mathematics, Princeton Universitv. (1996)
12. Ron Crandall: Some Notes on Steganography. Posted on Steganography Mailing List. http://os.inf.tu-dresden.de/.westfeld/crandall.pdf (1998)
13. Andreas Westfeld.: F5—A Steganographic Algorithm High Capacity Despite Better Stega nalysis. IH 2001, LNCS 2137, (2001) pp. 289–302
14. http://www.petitcolas.net/fabien/watermarking/image_database