TELKOMNIKA, Vol. 11, No. 5, May 2013, pp. 2822 ~ 2829
ISSN: 2302-4046

Edge Steganography for Binary Image

Hongxia Wang*[1], Gouxi Chen[2], Meng Zhang[2]
Shanxi Water Technical Professional College, Taiyuan, 030024, China
School of Computer Science and Technology, North University of China, Taiyuan 030051, China
*Corresponding author, e-mail: wanghxsxty@163.com, chengouxicgx@163.com, zhanlangx0@gmail.com

Abstract

In order to improve the steganographic robustness of the algorithm in binary images, suppose an new steganographic method which deals with the edge of the binary image using mathematical morphology and combines F5 encoding method to embedded information. Marginalization and reconstruction on binary image by dilation and erosion operations, and tag blocks that can embed information to. Finally embed secret information using F5 algorithm. Through experiments and analysis it comes out the steganographic robustness of the algorithm can be enhanced, and have a small changes on the carrier image quality after embedding information, and also has a good embedding capacity.

Keywords*: steganography, mathematical morphology, binary image, F5 algorithm*

1. Introduction

Essentially the binary image is black-and-white image which each pixel only one bit, and it has simple storage and compact structure. It is widely used in the field of information hiding. Precent Steganographic algorithm based on binary image can be summarized as block embedding method, modified tours embedded method, boundary modified method, the half-tone image method, character displacement method and frequency domain embedding method [1-3].

Document [4] divide text steganography to semantic steganography and format steganography, further more, it divide text steganography to semanteme, syntax and space. Document [5-8] proposed a series of algorithms for text format moving mainly include line shift and character shift. According to the image connectivity and smoothness requirements, document [9] embedded secret into block. The security of the above methods are not good and anti-poor offensive.

This paper propose a new steganography algorithm that combines the mathematical morphology with boundary modifications, and use F5 coding algorithm. Through experimental demonstration, this algorithm has strong robustness, highly steganographic safety.

This paper is organized as follows. In section 2, preprocess cover images using mathematical morphology and block labeling. Section 3 describes the embedding course. Section 4 is the implement of this algorithm. Section 5 is the analysis of the experiment results. Finally is the conclusion.

2. Pretreatment of The Carrier Image

2.1. The Basic Principle of Mathematical Morphology

Mathematical morphology produced in 1964, was proposed by Dr. J. Serra and teacher Mather Wing of Paris School of Mines. Mathematical morphology based on the rigorous mathematical theory and geometry, focuses on the geometry and relationship of the image .From the perspective of set theory, mathematical morphology contains the computational methods that change from one aggregate to another. The purpose of the change is to find the specific geometry of original aggregate, and the aggregate being changed contain the information. The change is achieved by a feature assemble named structural elements. The basic idea is that use a structural element to explore an image, find out the appropriate site to put structural element, and mark the sites, to obtain the information of the image.

Received January 12, 2013; Revised March 21, 2013; Accepted March 30, 2013

Suppose *X* is image aggregate, *B* is structural elements aggregate, mathematical morphology means *B* do the corresponding operations to *X*. In fact, structural element is also a image aggregate. Design a origin for every structural element, it is the reference point of the structural element and mathematical morphology. Here are several basic operations of mathematical morphology.

- dilation—the operator of dilation is $\oplus$,*X* is dilated by *B* is $X \oplus B$, it is defined as:

$$X \oplus B=\left\{ x\left|[(\hat{B})_X \cap A] \neq \Phi \right.\right\} \quad (1)$$

In formula (1): $\hat{B}$ is the mapping of *B*, it is defined as:

$$\hat{B} = \left\{ x\left| x = -b, b \in B \right.\right\} \quad (2)$$

$(\hat{B})_X$ means shift mapping of *B* for *x* bits, it is defined as:

$$(M)_X = \left\{ y\left| y = a + x, a \in M \right.\right\} \quad (3)$$

In formula (3): the process of the dilation that *B* to *X* is that: map the center pixel of *B* at first, then shift the mapping of *B* for *x*, the intersection of *X* and *B* is not empty set. In other words, the aggregate of the dilation of *B* to *X* is that, the aggregate of the site of the center pixel of *B*, when there is at least one nonzero elements intersect between the mapping of *B* and *X*. That is, formula (1) can be written as:

$$X \oplus B = \left\{ x\left|[(\hat{B})_X \cap X \subseteq X] \right.\right\} \quad (4)$$

Formula (4) can help us to understand the dilation operations by the concept of convolution. If as *B* the template of convolution, dilation means do the mapping of *B* about the center pixel, and then move the mapping continuously on *X*.

- Erode-- the operator of erode is Θ , *X* is eroded by *B* is $X \Theta B$, it is defined as:

$$X \Theta B = \left\{ x\left|(\hat{B})_x \subseteq X \right.\right\} \quad (5)$$

Formula (5) explain that the result of *B* erode *X* is the aggregate of all the *x*, in which the *B* that translation *x* is still in *X* .In other words, the aggregate that *B* erode *X* is the aggregate of the original position of *B* when *B* is completely included in *X*.

2.2. Choice of Structural Elements

The treatment that mathematical morphology to image is based on the concept that fill place the structural elements, choose of structural elements and the information of the image has close relationship, we can complete different image analysis through construction different structural complete, and obtain different experimental results.

Translation the structural elements *S* for *x* get S_x ,if S_x and *X* intersect is not empty ,we record the point *x*, the aggregate that being composed by *x* that meet the above conditions is called the result that *S* dilate *X*. The formula is :

$$X \oplus S=\left\{ x\left| S_x \cup x \neq \varnothing \right.\right\} \quad (6)$$

The result of dilation is to larger the target, as figure 1 shows:

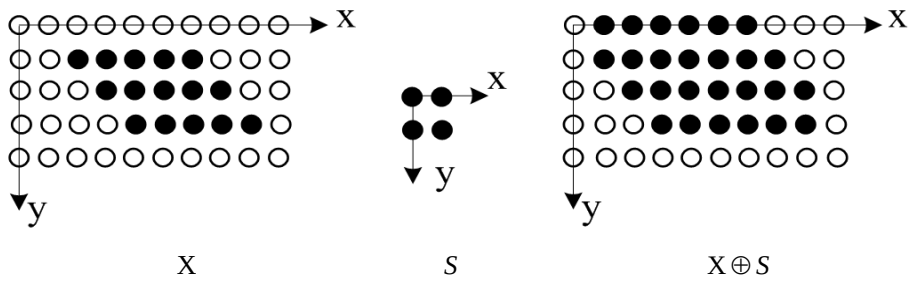


Figure 1. Dilation example

The method of the dilation is that, compare the original point of *S* and the point of *X* one by one, if one point of *S* fall within the scope of *X*, then the point that corresponding to the original point of *S* being the image; image to the right is the result of being dilated. It can be seen, it contain all the range of *X*, like *X* being dilated a lap. And if the original point of the structural elements different, the results of the dilation are different.

2.3. To Achieve the Mathematical Morphology Algorithm

We can see from the above description, if dilated by the structural elements, the object image will dilate a lap .Then if we let the image that being dilated minus the original image, can get the edge of the image. In binary image, the edge of the object appear as the form of mutation of gray value. When the structural elements at flat areas (the same gray value), because the difference of the value is big, the value of output image that being changed is lower than the original image. So if we let the dilated image minus the original image, can get the edge of the original image [10].

Expressed the thought by morphological operations is that:

$$(X \oplus B) - X = X \bigcap (X \oplus B)^C \tag{7}$$

This article chooses 3×3 structural elements for the experimental.

Figure 2 is the result of binary image being simulation in mathematical morphology. In which, the original image Figure 2(a) is the image that owned by the sender and receiver ,being used to compare the images when got by the receiver Being dilated with 3×3 structural elements, and being misused, we can get the edge image Figure 2(c) that can be used in steganographic research.

(a) Original binary image (b) Image being dilated (c) Edge image

Figure 2. Extract edge based on binary image

2.4. Restore Cover by Image Partition And Identifying

After extract the edge of the original image, we should also treat it through the method of image partition and identifying .Divide the edge image figure 2(c) into 3×3 image module, $F_1, F_2, ..., F_{2t}$ a total of 2t.

Provide F_i (i=1,3,5…2t-1) is the identification module, then F_j is the aggregate of module that the information can be embedded.

In F_i, provide the module that average pixel is between 0.3 and 0.7 is F_u ($F_u \subset F_i$) ,then the module that F_u corresponding F_u+1($F_{u+1} \subset F_j$) is the image module that can be embedded into information. Compose the module that can be embedded into new image *T*, *T* is the real image that can be embedded information.

3. Information Hiding Algorithm Based on Mathematical Morphology

3.1. Introduce the Embedding Algorithm

In this paper, the embedding information is the matrix coding technology. Matrix coding technology was proposed by Ron Crandall in 1998. The embedding rate improved greatly since F5 steganography introduce the technology.

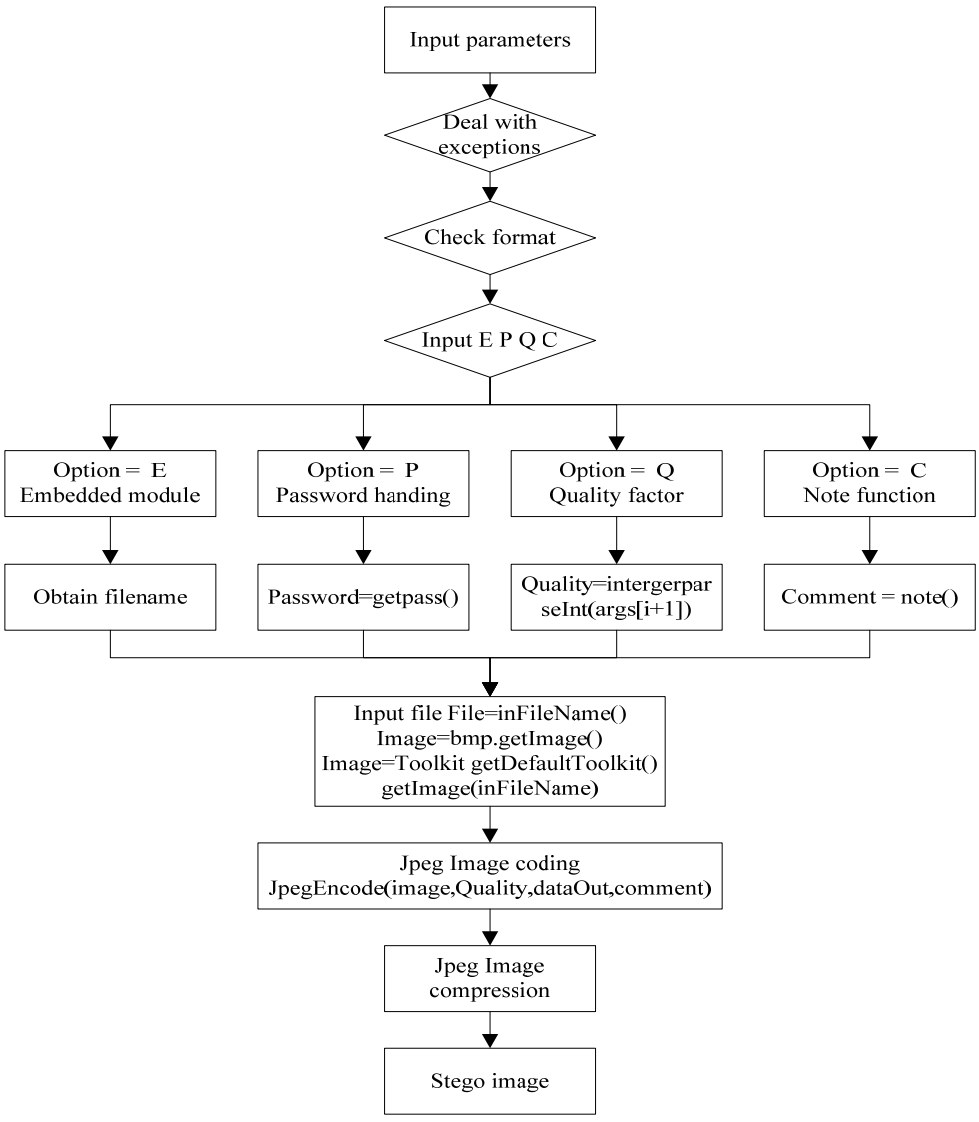


Figure 3. Embedding module that F5 hidden information

Embedding efficiency is the bits that each image can be improved for the secret information. In the usual LSB steganography, the average rate that change LSB when embedded 1 bit information is 1/2.That is, every changing can only embed 2 bit information. But in the F3 steganography and F4 steganography, because it may appear invalid embedded, the rate of the embedding might be low. The purpose of the matrix coding is to embed more secret information when improve less bits.

F5 steganography system obtains embedding secret information module and extraction module, program flow chart shows as Figure 3 and Figure 4.

The proportion of F5 steganographic algorithm can achieve even more than 13% of the size of JPEG file. F5 steganography embed the information into whole image, and embed information not through LSB replacement algorithm but matrix coding, it can embed large number of information when change little bit. Compared with other steganographic system, it indeed has better robustness [11].

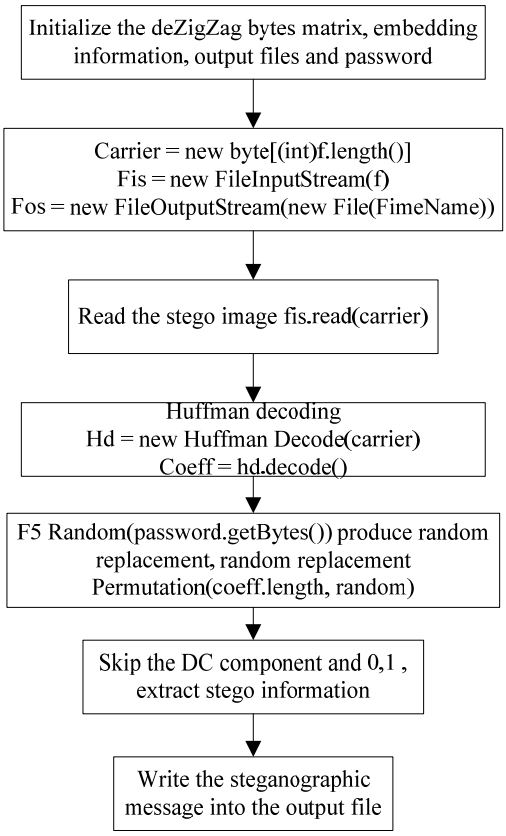
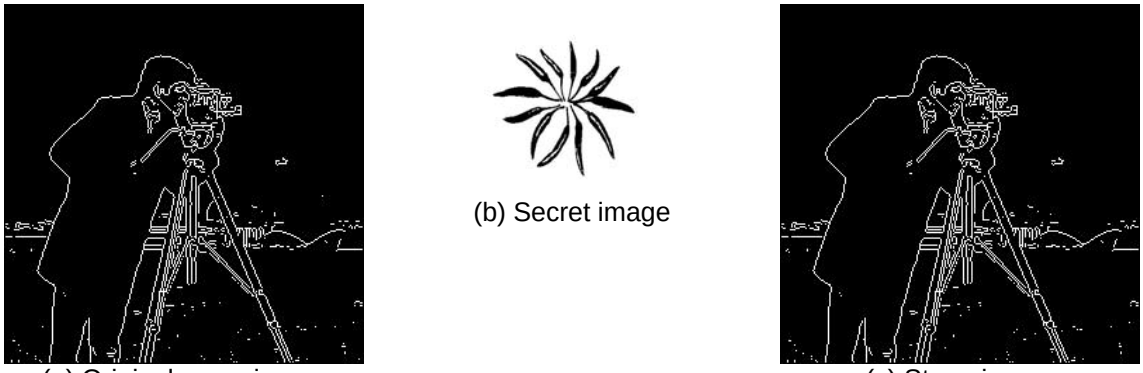


Figure 4. Hidden information by F5

4. Algorithm Implementation

4.1 Load Information

Let binary image figure 2(a) (256×256) that comes from the system as the example, embed which the binary image Figure 5(b)(50×50), transform Figure 2(a) into edge image Figure 2(c) through mathematical morphology and image partition and identifying, then embed the secret information Figure 5(b) into the edge image, complies the whole process in this algorithm, the result as Figure 5(c) shows:



(a) Original cover image (b) Secret image (c) Stego image

Figure 5. Embedding process

4.2. Restore the Stego Image

At first, treatment the binary image Figure 2 (a) in dilation, let the binary image that being dilated Figure 2 (b) munus the stego edgy image, then get the transmit stego image. As Figure 6 shows:

(a) the image that be dilate (b) stego edge image (c) stego original binary image

Figure 6. Process of the binary image restore

5. Analysis the experiment results

5.1. Analysis the Hiding Capacity

On the basis of the selection of the cover ,half of an image will be used to embed secret information ,but when embed secret information through F5 algorithm in binary image, in an image size $m \times n$, the upper limit of the bits that can hide when at most modify one pixel is $\log_2(mn+1)$ .Then, in this article, in the context of ensure the security increase by exponential ,if the size of the image is $M \times N$, steganographic capacity will be $\log_2(0.5MN+1)$.

5.2. Analysis the Visual Effects

The changing level of the cover image that embedded information expressed by PSNR [12], table1 shows the change of PSNR that same secret information embedded into different cover image, all the size of the covers are same .As we can seen from the table, the same secret information being embedded into different cover image that have same size, the PSNR was in the same magnitude, does not appear the situation that too high or too low. And, if PSNR more than 32, it will not caused by the human eye's attention.

Table 1. Embedded secrets in different covers

Cover image	PSNR	Cover image	PSNR
Cameraman.bmp	74.532	Papio.bmp	70.983
Lena.bmp	81.348	Vegetable.jpg	80.113
Elian.tiff	71.238	Donna.bmp	72.284

5.3. Analysis the Robustness

Steganography require the cover image not only visual effect is good, steganographic capacity are large, but also have good robustness, so it can resist the attack that intentionally or unintentionally. This article use several methods to test the robustness of the algorithm [13].

(a) Stego image (b) Stego image that be irregular cuted (c) Secret that extracted from stego image be irregular cuted

Figure 7. Irregular cut to the stego image

(a)original stego image (b) the stego image that added noise for 20% (c) the secret information

Figure 8. Add noise for 20% to the image

From the result figures we can see that, the algorithm has the anti-attack capability to irregular cut and noise.

5.4. Anti-Exhaustive

To the image that size m×n, the number of the methods that choose the structural elements when dilating is $\sum_{r=1}^{mn}(C_r^0+C_r^1+C_r^2+\cdots C_r^r)$,and the number of the methods that Image Partition and identifying is $(m-2)(n-2)$ .So, if the attacker does not know the key will not get the secret information by exhaustive.

6. Conclusion

This paper used mathematical morphology to preprocess binary image, and get the best suitable cover, then mark each block which can be embedded. The embedding process is F5 encode method. This method make the extract key more complication, the carrier image structure more closely, and also enhance resisting attack. Future will further improve the algorithm.

Acknowledgments

This work was supported by Forecasting Platform in Shanxi Province China (No: 20120311010-1, 20121133, 2130331-1).

References

[1] Cox IJ, Miller ML. The first 50 years of electronic watermarking. *Journal of Applied Signal Processing*. 2002; 2: 126~132.
[2] Rajlaxmi Chouhan, Agya Mishra, Pritee Khanna. Fingerprint Authentication by Wavelet-based Digital Watermarking. *International Journal of Electrical and Computer Engineering*. 2012; 2(4): 523-528.
[3] C Cachin. An Information-theoretic Model for Steganography. *Information Hiding 2nd International Workshop*. Portland, USA. 1998; (1525): 306-318.
[4] Gouxi Chen, Pengcheng Zhang, Meng Zhang et al. Batch zero-steganographic model for graph transformation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(4): 734-742.
[5] Tseng YC, Chen YY, Pan HK. A secure data hiding scheme for binary images. IEEE Transactions on Communications. 2002; 50(8): l227~123l.
[6] Anam Tariq, M Usman Akram. Personal Identification using Ear Recognition. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(2): 321-326.
[7] Low S, Maxemchukn F. Performance comparison of two text marking methods. *IEEE Journal on Selected Areas in Communications*. 1998; 16(4): 561-572.
[8] Low S, Lapone AM, Maxemchukn F. Document identification to discourage illicit. *IEEE Globe Communications*. 1995: 1203-1208.
[9] Wu M, Liu B. Data hiding in binary for authentication and annotation. *IEEE Transactions on Multimedia*. 2004. 6(4): 528-538.
[10] Hedieh S, Mansour J. Secure steganography based on embedding capacity. *International Journal of Information Security*. 2009; 8: 433-445.
[11] Luo XY, Liu FL, Yang CF, et al. On F5 Steganography in Images. *Computer Journal*. 2012; 55(4): 447-456.
[12] Li XL, Li J, Li B, et al. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. *Signal processing*. 2013; 93(1): 198-205.
[13] Bahi JM, Couchot JF, Guyeux C. A Class of Secure and Robust Algorithms. *Computer Journal.* 2012; 55(6): 653-666.