Formation technique of code using pixel value for the information hiding

Kazushi Kikuta^{a,*}, Yudai Sugimoto^b, Qingqing Hong^a, Zhang Lifeng^a

^a1-1sensui-cho Tobataku, Kitaktushu city, Fukuoka Japan 804-8550
Kyushu Institute of Technology

*Corresponding Author: kikuta.kazushi305@mail.kyutech.jp

Abstract

Information hiding algorithm such as code, cipher and steganography are used for protecting the secret information from third parties. Ciphers are now widely used as keys can be easily created. Cipher have drawbacks of decryption with Brute-force attack, safety drop due to unexpected solution and the the existence of confidential information may be noticed by a third party. This research propose a new approach to make code from images used for steganography. The codes are generated from the carry images used for transmission. By adapted the proposed code consisting algorithm to carry images, we eliminate the drawbacks of cipher and make it easy to create and manage keys. Also, by inspect the distribution of changes in the pixel value before and after embedding, it is possible to judge whether information embedding itself can be awarded.

Keywords: codebook, code, steganography.

1. Introduction

1.1 Encryption

Encryption is method for confidential information is not read in by a third parties. In cryptography, a key is a piece of information that determines the functional output of a cryptographic algorithm. Steganography, code, and cipher are the main methods of encryption.

(a) Steganography

Steganography is the method of concealing a file, message, image, or video within another. The data is embedded with image by steganography and the original

image is very similar, so it cannot be determined by the human eye. Embedding secret information in images make it impossible to others to judge the existence of information. However, if the embedded data in image is retrieved, the secret information is read.

(b) Code

Code is words or phrase converted into something else. Code is that replace only specific word that you want to keep confidential or replace all words using replacement dictionaries called code books. That replace only certain word can easily create encryption text, but they are easily deciphered. On the other hand, it is difficult for us to decipher code made by code book. But, code book is a huge key. Therefore it takes much time to create a key and key management is difficult.

(c) Cipher

Cipher is a transposition or substitution of information characters and character codes according to a specific algorithm. Because the key is short, the cipher is able to easily generate a new key even if the key is stolen. However, code has possibility that it can be easily deciphered if unexpected decoding methods are found or the performance of the computer is increased

1.2 Purpose

Now, Ciphers use widely. It has the possibility of being easily deciphered for the above reason. In this Study, It aims to propose new approach to make code from images used for steganography therefore it can be tried not to notice the existence of personal information to other person and make it easier to manage keys and eliminate management errors.

2. Principle

The code is composed of the initial position and the movement direction. After creating the codes of ASCII character codes 10 and 13 and 32 to 126, the code is determined from the character code corresponding to each character of information. In this Study, an image of 256×256 24 bit color is used for the input image.

2.1 Creating a Three dimensions matrix

Input image is deleted the lower 3 bits of the R, G, B pixel values of the input image and create a new 15 bit number. As an example, when the pixel value of component is R: 147 G: 230 B: 52, they are expressed as binary numbers as follows R:(01001011) G:(11100110) B:(00110100) When you delete the lower 3 bits of each pixel value R:(01001) G:(11100) B:(00110) these numbers are arranged (010011110000110) 15 bit number is cut out and stored it in each channel. Values for each channel are shown in Table 1. Three dimensions matrix is created by being performed with all the components of the image.

2.2 Creating initial position code

The values of i , j and n are determined by random numbers, and the value of the (i, j) - component n channel of the created three dimensional matrix is compared with the least significant bit of the character code. When it is different, we again decide the values of i , j , n . If it is equal, arrange each numbers in binary numbers make it the code of the initial position. The character code 97 is taken as an example. When 97 is represented by a binary number, it is 1100001. Compare the value of the (i, j) - component n channel of the three dimensional matrix with the least significant bit of the character code. Figure 1 shows a part of the three-dimensional matrix created in 2.1. When $i = 189$ $j = 20$ $n = 4$, it is equal to the least significant bit of the character code. i , j and n are represented by binary numbers respectively, $i = (10111101)$ $j = (00010100)$ $n = (0100)$, the code of the initial position is (10111101000101000100).

Table 1. Value for each channel.

channel	Value	channel	Value
0	0	8	0
1	1	9	0
2	0	10	0
3	0	11	0
4	1	12	1
5	1	13	1
6	1	14	0

Figure 1. A part of a matrix.

2.3 Creating movement direction code

Define the moving direction as shown in Table 2.

Table 2 Definition of movement direction

direction of movement	definition name
$i \rightarrow i + 1$	1
$i \rightarrow i - 1$	2
$j \rightarrow j + 1$	3
$j \rightarrow j - 1$	4
$k \rightarrow k + 1$	5
$k \rightarrow k - 1$	6

Figure 2. Determination of movement direction.

Figure 3. Movement direction.

Next, it compares with the value after movement defined sequentially from the second bit to the most significant bit of the character code. If they are equal, it moves in that direction and the value defined in Table 2 is taken as the moving direction. If more than one exists, it is set to the minimum value. When they are all different, the code of the initial position is discarded and the initial position is determined again. In Figure 2, when comparing the value of the red circle with 0 of the second bit of 97, it becomes equal in the case of 3, 5 and 6 and the smallest number 3 becomes the initial moving direction. After determining the moving direction of six times, arrange the six defined numbers as binary numbers and use them as codes in the moving direction. In the case of the example, as shown in Figure 3, the code in the moving direction is (3, 1, 1, 1, 6, 1). Each number is expressed by 3 bit binary number, it becomes (011001001001110001).

2.4 Decryption

Separate the code of the initial position into 8 bits, 8 bits, 4 bits and let i, j, n from the left. Let the value of the (i, j) - component n channel of the three-dimensional matrix be the least significant bit of the character code. If the code at the initial position is (101111010101010), $i = 10111101$, $j = 00010100$, $n = 0100$, that is, the value of 1 in the value of the (189, 20) - component 4 channel in Figure 2.6 is the least significant bit of the character code. Next, the movement direction code is divided every 3 bits to determine the movement direction. When the code of the moving direction is (011001001001110001), it is (3, 1, 1, 1, 6, 1)

when it is expressed in decimal number after separating it by every 3 bits. After determining the moving direction, it moves in that direction, and the value at the place after moving is set as the next bit of the character code. This is done six times, it moves as shown in Figure 3 and becomes (1100001). When you return to decimal number you get character code 97.

3. Methodology

In this experiment, the image of Figure 4 and the sentences (1), (2) and (3) are used. Sentences (1), (2) and (3) are about 15,000 words. The sentences of (1), (2) and (3) change to code and embedded in the lower 3 bits of the image of Figure 4. Further, Gaussian noise is added to the image of Figure 4. We investigate the amount of change between original image and the image embedded with the code or the image with Gaussian noise added.

Couple

Lenna

Sailboat

Figure 4. Original image.

4. Results

The distribution of changes in the pixel value before and after embedding are as shown in the figure below.

Figure 5. Couple Histograms.

Figure 6. Lenna Histograms.

Figure 7. Sailboat Histograms.

Concerning Couple, Lenna and Sailboat, include noise's histogram, include (1)'s histogram, include (2)'s histogram, and include (3)'s histogram are Gauss distribution. Moreover, each histogram are similar. Therefore, it is difficult to assess existence of confidential information in the image from the amount of change.

5. Conclusions

In this Study, we make code from images used for steganography so that we can make it easy to create and manage keys. Moreover, by inspect the distribution of changes in the pixel value before and after embedding, it judged whether information embedding itself can be awarded. When comparing include noise and the others histogram, distributions was similar. Therefore, it is difficult to assess existence of confidential information in the image from the amount of change. But, I do not take account direction of movement biased and character usage frequency. Therefore, I must resolve them.

References

- (1) Stefan Katzenbeisser, Fabien A.P.Petitcolas "INFORMATION HIDIN", Norwood,Massachusetts :

ARTECH HOUSE, 1999

- (2) Takamatsu jun : Imaging process and image noise,
Information Processing Society of Japan, Vol. 2010-
CVIM-174, No.17, pp. 3, 2010
- (3) Niimi Michiharu, “Study about digital steganography ”
<http://hdl.handle.net/10228/1954>, 2013