Formation technique of code for the information hiding

Kazushi Kikuta[a,*], Yudai Sugimoto[b], Zhang Lifeng[a]

[a]1-1sensui-cho Tobataku, Kitaktushu city, Fukuoka Japan 804-8550
Kyushu Institute of Technology

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

Abstract

Code, cipher and steganography exist in methods for preventing the contents of information from being known to third parties. Ciphers are now widely used as keys can be easily created. Cipher has the drawbacks of decryption with Brute-force attack, safety drop due to unexpected solution and The existence of possibility that the existence of confidential information may be noticed by a third party. In this research, we make code from images used for steganography. In this research, we propose a method to generate codes from images used for steganography. By combining steganography and code consisting of images, we eliminate the drawbacks of cipher and make it easy to create and manage keys. The alphabet or symbol is converted into a code by using the pixel value of the image data to be embedded. Also, depending on the amount of change in the pixel value of the image before and after embedding, it is verified whether it is possible to judge whether information is embedded in the image after embedding.

Keywords: codebook, code, steganography.

1. Introduction

1.1 encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. 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 practice of concealing a file, message, image, or video within another file, message, image, or video. The data embedded with information by steganography and the original data are very similar, so it can not be determined by the human eye. By embedding secret information in images, it is impossible for others to judge the existence of information. However, when the embedded data is retrieved, the information is read.

(b) Code

Code is words or phrase are converted into something else. There are things that replace only specific words that you want to keep confidential and those that replace them using replacement dictionaries called code books. Those that replace only certain can easily create encryption text, but they are easily deciphered. On the other hand, substitution by a code book is not easily deciphered, but since a code book is a huge key, 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, there is a possibility that it can be easily deciphered if unexpected decoding methods are found or the performance of the computer is increased

1.2 Purpose

Ciphers are now widely use. It has the possibility of being easily deciphered for the above reason. In this research, we are trying not to notice the existence of personal information to other person, aim to not read information even if it is known, to make it easier to manage keys and eliminate management errors. Use steganography using images to make it impossible to recognize the existence of personal information.

2. Principle

The code is composed of the code of the initial position and the code of 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 experiment, an image of 256 × 256 24 bit color is used for the input image.

2.1 Creating a Three dimensions matrix

Erase 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 a certain component of image data 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 number

R:(01001) G:(11100) B:(00110)

Arrange these number

(010011110000110)

Cut out the created 15-bit number in bit units and store it in each channel. Values for each channel are shown in Table 1. Perform these operations with all the components of the image.

Table 1. Value for each channel.

n	0	1	2	3	4
Value of n channel	0	1	0	0	1
n	5	6	7	8	9
Value of n channel	1	1	1	0	0
n	10	11	12	13	14
Value of n channel	0	0	1	1	0

2.2 Creating initial position code

The values of i, j, 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, represent i, j, n in binary numbers and arrange new numbers to 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 1 of the least significant bit of the character code.

Figure 1 shows a part of the three-dimensional matrix created in 2.1. i = 189 j = 20 When n = 4 it is equal to the least significant bit of the character code of a. When i, j, n are represented by binary numbers respectively, i = (10111101) j = (00010100) n = (0100), the code of the initial position is (10111101000101000100).

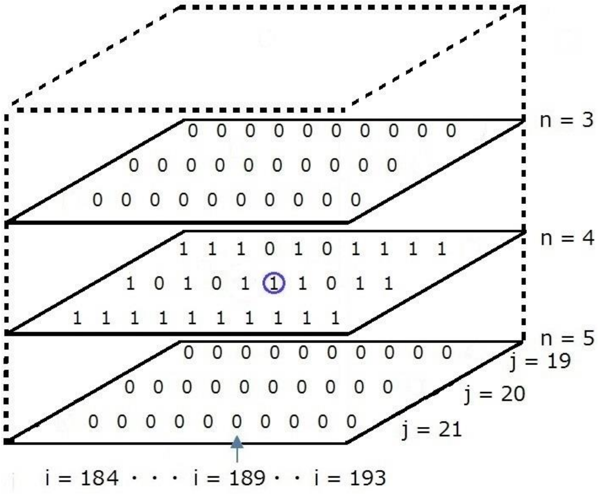

Figure 1. A part of a matrix.

2.3 Creating movement direction code

Define the moving direction as shown in Table 2.

Table 2 Definition of movement direction

direction of movement	i→i + 1	i→i - 1	j→j + 1
	1	2	3
direction of movement	j→j + 1	k→k - 1	k→k - 1
	4	5	6

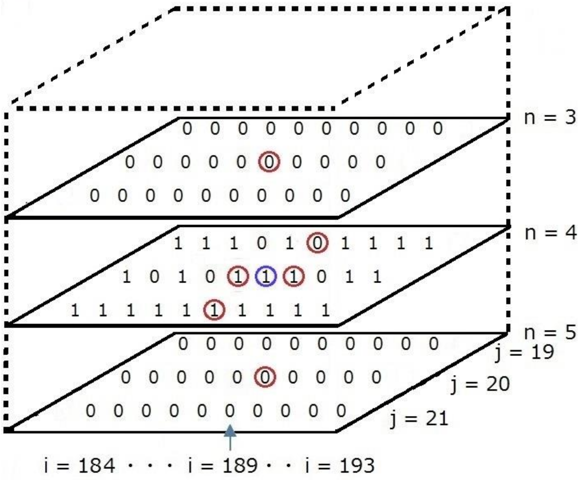

Figure 2. Determination of movement direction.

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.

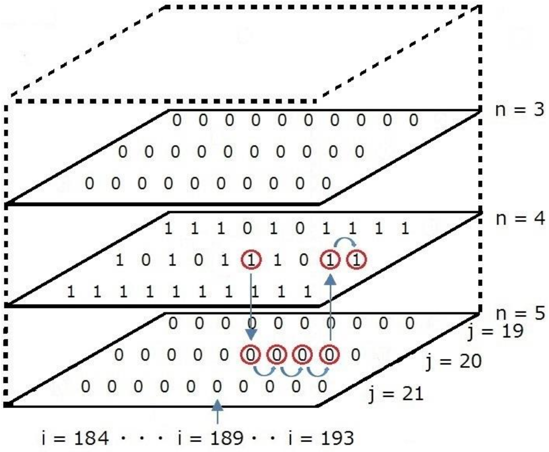

Figure 3. Movement direction.

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). When 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. (011, 001, 001, 001, 001, 110, 001) when the code in the moving direction is (011001001001110001), it is (3, 1, 1, 1, 6, 1) when it is represented by a decimal number. 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

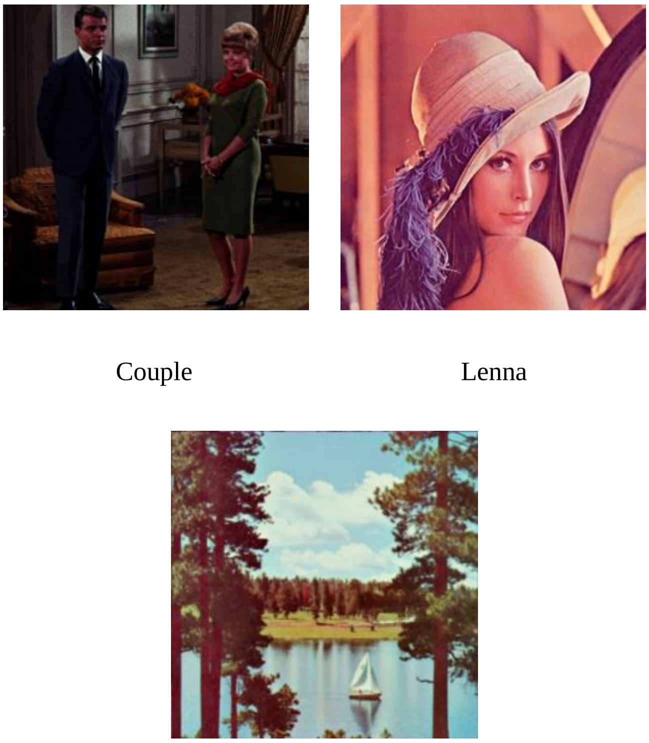

Figure 4. Stego-object.

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 the image embedded with the code and the original image of the image with Gaussian noise added.

4. Results

Histograms on amount of change are as shown in the figure below.

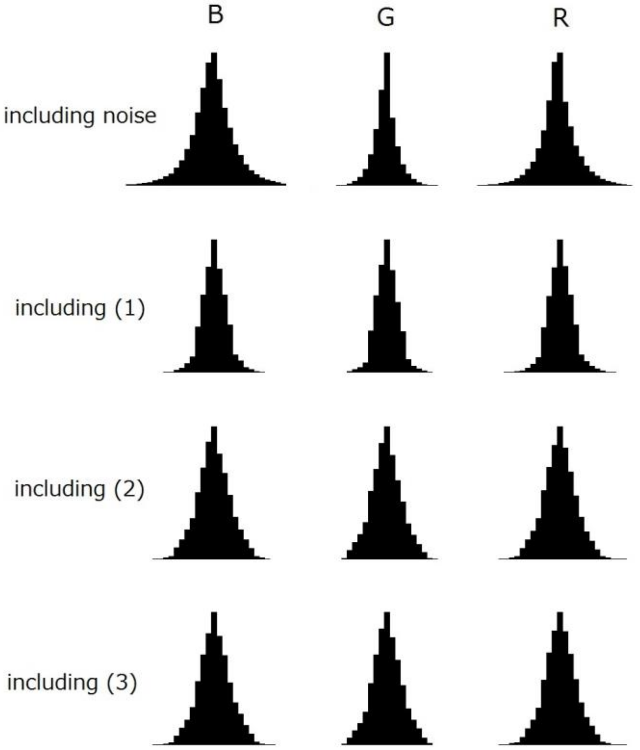

Figure 5. Couple Histograms.

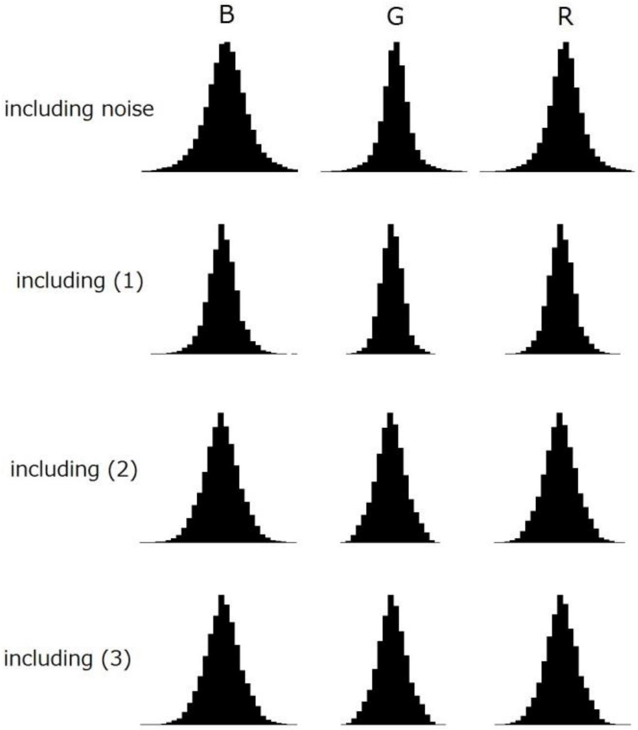

Figure 6. Lenna Histograms.

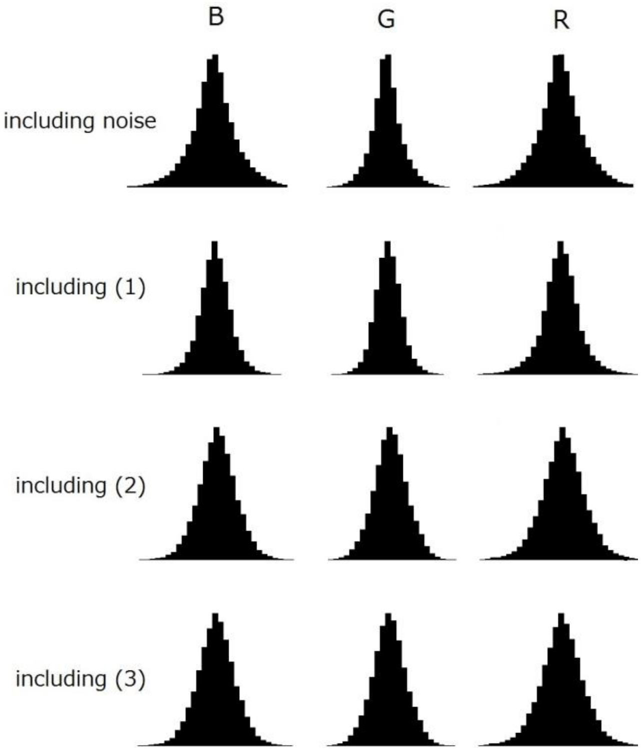

Figure 7. Sailboat Histograms.

When comparing include noise and the others histogram, distributions was similar.

5. Conclusions

From experimentation, assess existence of confidential information is difficult 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) Lewis Carroll, Alice's Adventures in Wonderland : Down the Rabbit-Hole http://etc.usf.edu/lit2go/1/alices-adventures-in-wonderland/1/chapter-i-down-the-rabbit-hole/(1865)

(2) Lewis Carroll, Alice's Adventures in Wonderland : The Rabbit Sends in a Little Bill http://etc.usf.edu/lit2go/1/alices-adventures-in-wonderland/7/chapter-iv-the-rabbit-sends-in-a-little-bill/(1865)

(3) Lewis Carroll, Alice's Adventures in Wonderland : The Queen’s Croquet-Ground http://etc.usf.edu/lit2go/1/alices-adventures-in-wonderland/18/chapter-viii-the-queens-croquet-ground/(1865)