International Journal of Advanced Culture Technology Vol.7 No.4 242-245 (2019)
DOI 10.17703/IJACT.2019.7.4.242

IJACT 19-12-28

Watermarking Algorithm using LSB for Color Image with Spatial Encryption

Soo-Mok Jung

Professor, Division of Computer Science & Engineering, Sahmyook University, Seoul, Korea
jungsm@syu.ac.kr

Abstract

In this paper, watermark embedding technique was proposed to securely conceal the watermark in color cover image by applying the spatial encryption technique. The embedded watermak can be extracted from stego-image without loss. The quality of the stego-image is very good. So it is not possible to visually distinguish the difference between the original cover image and the stego-image. The validity of the proposed technique was verified by mathematical analysis. The proposed watermark embedding technique can be used for intellectual property protection, military, and medical applications that require high security.

Keywords: *water mark embedding, stego-image, spatial encryption, color image*

1. INTRODUCTION

Watermark embedding technique is used to hide intellectual property information in image. The image where the intellectual property information is hidden is a stego-image. It is possible to extract intellectual property information from the stego-image without loss. Imperceptibility requirement is important in water mark embedding technique to make it impossible for humans to know whether watermark is hidden in stego-images. [1][2]

In the watermark embedding technique, the watermark data embedded in the stego-image should not be perceivable by human. Therefore, imperceptibility is very important in data hiding [1] [2]. It is possible to satisfy the imperceptibility by making the quality of the generated stego-image excellent after hiding watermark data in the cover image and making it impossible to recognize the difference between the cover image and the stego-image. Therefore, it is important that the stego-image is created so that there is little difference from the original cover image.

A technique for watermark data hiding at LSB has been proposed. [3] If watermark data is embedded in LSB, watermark data can be easily extracted from the stego-image. Therefore, the safety of the watermark is significantly lowered. Many techniques for embedding watermark data using LSB have been developed[4]-[6], but this paper proposes a technique for embedding watermark data in LSB using spatial encryption.

2. TECHNIQUE FOR HIDING WATERMARK DATA IN LSB

Each component of the color image is composed of 8 bits and has a value between 0 and 255. Figure 1 shows the data structure of each component.

Manuscript received: October 02, 2019 / revised: October 18, 2019 / Accepted: November 05, 2019
Corresponding Author jungsm@syu.ac.kr
Author's affiliation :
Professor, Division of Computer Science & Engineering, Sahmyook University, Seoul, Korea

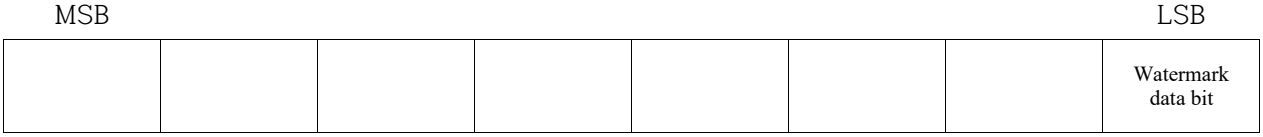


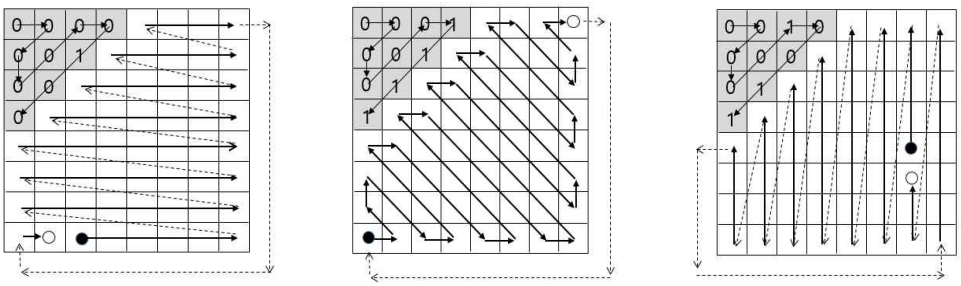
Figure 1. **Data structure of each component where watermark data bit is concealed.**

The value of each component is stored in 8 bits, and the watermark data bit is stored in the LSB having the lowest weight. Since the value of the LSB has been replaced with a watermark data bit, a value difference occurs by an average of 0.5. Since it is a color component represented by 0 to 255, when there is a difference of 0.5, it cannot be visually distinguished. Therefore, this technique can conceal the watermark data bits very simply, and the image quality of the stego image generated by concealing the watermark data is very good. However, since watermark data can be easily extracted using LSBs of each component, it is very vulnerable to security.

3. PROPOSED ALGORITHM

Color image has R, G, and B components. So, it is possible to construct R, G, and B planes by separating RGB component from color image. For each plane, watermark data bits are embedded in the LSBs of each pixel as shown in Figure 2. In Figure 2, in the R, G, and B planes, the left gray pixels are the area that store the information of spatial encryption. The information of spatial encryption is 10 bits and it consists of three fields.

The three fields are as follows: Data embedding pattern in R, G, and B planes are represented by 7 bits. The embedding order in the R, G, and B planes are represented by two bits. The embedding type in each plane of R, G and B is represented by 1 bit. 10 bits are stored in the LSBs of the upper left pixels. As shown in Figure 2, the order in which 10 bits are stored is in the order of zigzags.



(a) R plane (b) G plane (c) B plane

Figure 2. An example of embedding watermark data on each color plane

Since the data embedding pattern is represented by 7 bits, it is possible to designate a pattern spatially embedding watermark data in each plane as one of 128 types. Since the starting position for watermark data embedding is represented by 2 bits, the starting position can be set to a value between 0 and 3. 1 bit is used to specify the type of concealment of watermark data. So, it is possible to specify whether watermark data is to be concealed unchanged or inverted in each plane of RGB.

As shown in Figure 2 (a), the 10 bits of spatial encryption information of R plane are (0000000), (10), and (0). The data embedding patterns can be defined one of 128 types. For example, a pattern corresponding to (0000000) is as shown in Figure 2(a), a pattern corresponding to (0000001) is shown in Figure 2(b), and a pattern corresponding to (0000010) is shown in Figure 2(c).

Since the bits representing the embedding order are 2 bits, the order in which the corresponding plane is embedded can be specified. In Figure 2 (c), since the bits representing the embedding order are 01, B plane is embedded first. In Figure 2, the order of embedding the watermark data is B plane, R plane, G plane.

Since one bit is used to represent the embedding form, watermark data can be embedded in two forms. If the bit representing the embedding form is 0, the watermark data bit is embedded as it is without inversion, and if 1, the watermark data bit is embedded after being inverted. Therefore, the watermark data bits are concealed in the R plane of Figure 2 as it is. The G plane and the B plane are concealed after the watermark data bits are inverted. Since the sum of spatial encryption information of RGB plane is 30 bits, 1,073,741,824 different types of concealment are possible.

In Figure 2, the watermark data are embedded in the order of B(6,4), B(6,3), .. B(6,0), B(5,7), B(5,6), ... , B(0,4), B(7,7), ... , B(6,7), B(6,6), B(6,5), R(2,7), ... , R(7,0), R(0,7), R(1,7), G(0,7), ... , G(7,0). B(6,4) represents a location where the x coordinate is 6 and the y coordinate is 4 on the B plane.

If watermark data bits are concealed in a color image in this way, watermark data can be spatially encrypted and embedded. Therefore, the watermark data can be safely hidden in the cover image, and the watermark data can be perfectly extracted from the stego-image.

4. MATHEMATICAL ANALYSIS

The image quality of the stego-image in which watermark data are concealed can be measured as shown in equation (1) and (2).

$$PSNR = 10\log_{10}(255^2/MSE) \qquad (1)$$

$$MSE = (1/YX) \sum_{y=0}^{Y-1} \sum_{x=0}^{X-1} [C(y,x)-S(y,x)]^2 \qquad (2)$$

In Equation 2, C is the cover image and S is the stego-image. When watermark data is embedded in a 512x512 color image by applying the proposed algorithm, the image quality of a stego-image is calculated according to Equation (1) as follows: When the LSB value of each pixel of the R, G, and B planes is 50% identical to the watermark data and the spatial encryption information data, the MSE value is 0.5 in Equation (2). So the image quality of the stego-image is 51.14 dB. And watermark data to be embedded is 786,402 bits, and 1,073,741,824 different types of concealment are possible.

In the case where the fine change of the image is uniformly distributed throughout the image and the image quality is 40 dB or more, it is almost impossible to visually distinguish the difference between the original cover image and the stego-image. Therefore, if the watermark data is concealed in the color image by applying the proposed algorithm, the visual quality of the stego-image is very good and the embedded watermark data in the stego-image can be extracted without loss.

5. CONCLUSIONS

In this paper, an algorithm to hide watermark data in color image by applying spatial encryption was proposed. By concealing watermark data using the proposed algorithm, watermark data can be safely hidden and watermark data can be restored perfectly. The maximum number of bits that can be concealed is (width of image) ∗ (length of image) ∗ 3 − (10 ∗ 3) bits, 1,073,741,824 different types of concealment are possible, and the visual quality of the stego-image is an average of 51.14dB. The proposed algorithm can be applied to various fields such as military, copyright protection etc.

REFERENCES

[1] H. C. Huang, C. M. Chu, and J. S. Pan, “The optimized copyright protection system with genetic watermarking,” Soft Computing, Vol. 13, No. 4, pp. 333-343, Feb. 2009.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 3, pp. 354-362, March 2006.
[3] A.Z. Tirkel, G.A. Rankin, R.M. van Schyndel, W.J. Ho, N.R.A. Mee, and C.F. Osborne, "Electronic watermark", In Digital Image Computing, Technology and Applications, pp. 666-673, Macquarie University, Sidney, 1993.
[4] A. J. Zargar, "Digital Image Watermarking using LSB Technique," International Journal of Scientific & Engineering Research, Vol. 5, Issue 7, pp. 202-205, July, 2014
[5] P. Gaur, N. Manglani, "Image Watermarking Using LSB Technique," International Journal of Engineering Research and General Science, Vol. 3, Issue 3, pp. 1424-1433, May. 2015