International Journal of Internet, Broadcasting and Communication Vol.11 No.1 85-88 (2019)
http://dx.doi.org/10.7236/IJIBC.2019.11.1.85

IJIBC 19-1-11

A Study on Confidential Data Hiding Technique with Spatial Encryption for Color Image

Soo-Mok Jung*

Division of Computer Science & Engineering, Sahmyook University, Korea
E-mail: jungsm@syu.ac.kr

Abstract

In this paper, we propose a technique for spatially encrypting confidential data into R, G, B planes of color image and extracting spatially encrypted confidential data. The effectiveness of the proposed technique is verified by mathematically analyzing the quality of the stego-image generated using the proposed technique. The proposed technique can hide confidential data securely into cover image by spatially encrypting the confidential data, and can extract confidential data from the stego-image. The quality of the stego-image created by applying the proposed technique is very good. The average value of the quality of the stego-image is 51.14 dB. Therefore, it is not visually recognizable whether the confidential data is hidden in the stego-image. The proposed technique can be widely used for military and intellectual property protection.

Keywords: *Data Hiding, Cover Image, Stego-image, Confidential Data, Confidential Data Extraction*

1. Introduction

Data hiding techniques are used to hide confidential data into cover images. Confidential data can be extracted from the stego-image which is generated by inserting confidential data into a cover image.

In the data hiding technique, the confidential data hidden in the stego-image should not be recognized by the human. Therefore, imperceptibility is very important in data hiding.[1] [2] It is possible to satisfy the non-recognition property by making the quality of the generated stego-image excellent by hiding confidential data in the cover image, so that the difference between the cover image and the stego-image can not be recognized. Therefore, it is important that the stego-image must be generated almost the same as the original cover image. A technique for hiding confidential data at the LSB has been proposed.[3] If confidential data is hidden in the LSB, confidential data can be easily extracted from the stego-image. Various data hiding techniques have been proposed. [4] - [9] In this paper, we propose a technique to hide confidential data in LSB and to confidentially encrypt confidential data to solve problems that occur when confidential data is

Manuscript Received: Jan. 19, 2019 / Revised: Jan. 25, 2019 / Accepted: Feb. 1, 2019

Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Division of Computer Science & Engineering, Sahmyook University, Korea

hidden in LSB. The composition of this paper is as follows. In Section 2, we describe the technique of data hiding in LSB. In Chapter 3, we describe the proposed method for spatially encrypted confidential data hiding. In Section 4, we describe the mathematical analysis of the quality of the stego-image. Finally, we conclude in Chapter 5.

2. LSB Technique

The pixel value has a value between 0~255 since the pixel is represented by 8 bits. The technique of hiding confidential data in the LSB hides the confidential data in the least weighted LSB among 8 bits representing the pixel value as shown in Fig. 1. When 1 bit of confidential data is hidden in the LSB, the pixel value is increased or decreased by one at most. Therefore, the value between 0~255 is changed by 1 at most. Since human vision can not detect such a small change, it is impossible to recognize whether the confidential data is hidden in the pixel. This method has a disadvantage in that the original pixel data is changed, but there are advantages in that the confidential data can be simply hidden in the pixel data and the confidential data can be easily extracted.

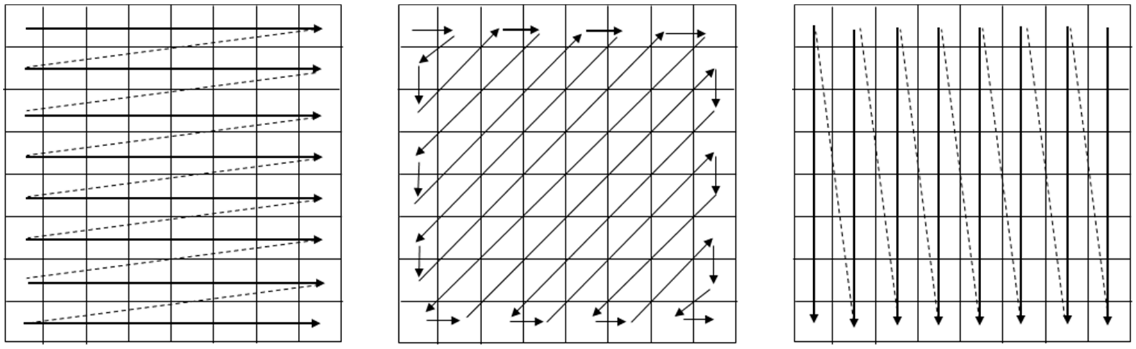
MSB							LSB
							confidential data

Figure 1. Confidential data hiding in LSB

3. Proposed Technique

If confidential data is concealed in the LSB, everyone can easily extract confidential data. In order to solve this problem, this paper propose a method to encrypt spatially confidential data in color image.

The color image has R, G, and B components. It is possible to construct the R plane by separating only the R component from the color image, form the G plane by separating only the G component, and form the B plane by separating only the B component. Confidential data is concealed in the LSB of each pixel for each of the R, G, and B planes as shown in Fig. 2.



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

Figure 2. Pixel order to hide confidential data by spatially encrypting in the R, G, and B plane

As shown in Fig. 2, confidential data is concealed in LSB of each pixel in the following order. R(0, 0), B(0, 7), G(0, 0), R(0, 1), B(1, 7), $\underline{G(0, 1)}$, R(0, 2), B(2, 7), $\underline{G(1, 0)}$, R(0, 3), B(3, 7), $\underline{G(2, 0)}$, ... R(7, 7), B(7, 0), $\underline{G(7, 7)}$. Here, R(0, 1) means a pixel where the value of the screen coordinate system in the R plane is y = 0 and x = 0. $\underline{G(0, 1)}$ represents a pixel where the value of the screen coordinate system in the G plane is y = 0, x = 1 and the confidential data is reversed to be hidden. If confidential data is concealed in a color image in this way, confidential data can be spatially encrypted and concealed, so confidential data can be safely hidden in a cover image. Confidential data hidden in the cover image can be safely and completely extracted in the same way as concealed.

Fig. 2 shows an example of hiding confidential data by spatially encrypting it, but various modified methods can be applied to this spatial encryption pattern.

4. Mathematical Analysis

By applying the proposed technique, the quality of the generated stego-image can be measured as shown in Equation (1). In Equation (2), C(i,j) means the pixel value at (i,j) in cover image, and S(i,j) means the pixel value at (i,j) in stego-image.

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

$$MSE=(1/XY)\sum_{i=0}^{X-1}\ \sum_{j=0}^{Y-1}[C(i,j)-S(i,j)]^2 \qquad (2)$$

When confidential data is hidden in 512x512 color image according to the proposed method, the quality of the stego-image is calculated according to Equation (1) as follows.

Case 1: When the value of LSB in each pixel of the R, G, B plane is completely opposite to the confidential data to be hidden, the value of MSE in Equation (2) becomes 1 and the quality of the stego-image becomes 48.13 dB. Here, $\underline{G}$ indicates that the value of each pixel in the G plane is subtracted from 255 to be inverted. That is, Equation (3) is applied to all the pixels in the G plane.

$$\underline{G}=255-G \qquad (3)$$

Case 2: When the LSB value of each pixel of the R, G, B plane completely coincides with the confidential data to be hidden, the quality of the stego-image becomes equal to the quality of the original cover image.

Case 3: When the LSB value of each pixel of the R, G, and B planes is 50% identical with the confidential data to be hidden, the quality of the stereo-image is 51.14 dB because the value of MSE is 0.5 in Equation (2).

Actually, the larger the size of the original cover image, the more convergent the quality of the stego-image becomes in Case 3. In the case where the fine change of the image is uniformly distributed throughout the image and the quality is 40 dB or more, the difference between the original cover image and the stego-image can not be distinguished by the naked eye. Therefore, when confidential data is concealed in color image by applying the proposed technique, the quality of the stego-image is maintained at 51.14 dB, and the visual quality of the stego-image is the same as that of the original cover image. And confidential data hidden in the stego-image can be extracted completely without loss.

5. Conclusions

In this paper, we propose a technique to encrypt confidential data spatially and hide it in color image. When confidential data is concealed by applying the proposed technique, confidential data can be spatially encrypted and securely concealed. The maximum number of bits that can be concealed is (image width) * (image height) * 3 bits, and concealed confidential data can be completely extracted. It is impossible to visually distinguish the difference between the stego-image and the original cover image because the quality of the stego-image generated by concealing confidential data on the color image as in the proposed technique is 51.14 dB. Therefore, it is impossible to recognize whether the confidential data is hidden in the stgo-image. The proposed technique can be applied to various fields such as military and copyright protection

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.

[2] 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] Y. C. Li, C. M. Yeh, and C. C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility," Digital Signal Processing, Vol. 20, No. 4, pp. 1116-1128, July 2010.

[5] C. L. Tsai, K. C. Fan, C. D. Chung, and T. C. Chuang, "Reversible and lossless data hiding with application in digital library," Proc. 38th Annual 2004 Int. Canahan Conf. on Security Technology, pp. 226-232, Albuquerque, New Mexico, USA, Oct. 2004.

[6] M. U. Celik, G. Sharma, A. M. Tekalp, E Saber, "Reversible data hiding," Proc. 2002 Intl. Conf. on Image Processing, Vol 3, pp. 157-160, Rochester, New York, USA, Sep. 2002.

[7] C. C. Chang, W. L. Tai, and C. C. Lin, "A reversible data hiding scheme based on side match vector quantization," IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 10, pp. 1301-1308, Oct. 2006.

[8] L. Kamstra, H.J.A.M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," IEEE Trans. on Image Process, Vol. 14, No. 12, pp. 2082-2090, Dec. 2005.

[9] G.S. Cho, "Data Hiding in NTFS Timestamps for Anti-Forensics," International Journal of Internet, Broadcasting and Communication, Vol. 8, No. 3, pp. 31-40, Aug. 2016.