International Journal of Internet, Broadcasting and Communication Vol.14 No.1 116-121 (2022)
http://dx.doi.org/10.7236/IJIBC.2022.14.1.116

IJIBC 22-1-14

Multi-encryption Watermarking Technique using Color Image Pixels

Soo-Mok Jung

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

Abstract

In this paper, we propose a highly secure watermarking technique in which the watermark is multi-encrypted using the R, G, and B component pixels of color image, and then the multi-encrypted watermark is hidden in the LSB of the color image pixel. According to the technique proposed in this paper, the quality of the stego-image created by hiding the multi-encrypted watermark in the LSB of the color image is so excellent that the difference from the cover image cannot be recognized. Also, it is possible to extract the original watermark from the stego-image without loss. If the watermark is hidden in the image using the proposed technique, the security of the watermark is maintained very well because the watermark hidden in the stego-image is multi-encrypted. The proposed watermarking technique can be used in the applications such as military and intellectual property protection requiring high security.

Keywords: *Watermarking, Multi-encrypted watermark, Color image, Cover image, Stego-image*

1. Introduction

Techniques have been used to hide a watermark, which is intellectual property information such as ownership information, in a color image. The visual quality of the stego-image generated by hiding the watermark in the image should be excellent enough to be indistinguishable from the original cover image. And it should be possible to extract the original watermark from the stego-image without loss. Therefore, in the watermarking technique, the imperceptibility of not knowing whether the watermark is hidden in the Stego image is very important.[1][2] If the image quality of the stego-image is maintained well, the difference between the stego-image and the original cover image cannot be visually recognized. Therefore, it is not possible to recognize whether the watermark is hidden in the stego-image, so the imperceptibility is satisfied.

In the technique of hiding the watermark in image, it is important to maintain the image quality so high that the image quality of the stego-image has little visual difference from the original cover image. Techniques for hiding the watermark in the LSB of the image pixel have been proposed. [3]-[6] When the data bit of the watermark is hidden in the LSB of each pixel of the image, the image quality of the stego-image is excellent, which satisfies the imperceptibility. However, there is a problem in that the security of the watermark is weakened because the watermark data bits can be easily extracted from the stego-image.

Manuscript Received: November. 28, 2021 / Revised: December. 3, 2021 / Accepted: December. 8, 2021
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Science & Engineering, Sahmyook University, Korea)

In this paper, to solve the security problem in the technique of hiding the watermark data bit in the LSB of the color image, the watermark is multi-encrypted by using the R, G, and B component pixels of the image. Thereafter, the multi-encrypted watermark is hidden in the LSB of the color image so that the security of the watermark is maintained very high. The proposed technique is a technique that improves the performance of the existing techniques proposed by this research team.[7]-[10]

The structure of this paper is as follows. Chapter 2 describes the existing technique for hiding watermark data bits in the LSB of image pixels, and Chapter 3 describes the proposed technique. The experimental results are described in Chapter 4, and the conclusion is described in Chapter 5.

2. Technique for hiding the watermark in the LSB of the image pixel

Each pixel of a color image consists of R, G, and B components. R, G, and B components are each expressed as 1 byte, so each component has a value between 0 and 255, and 1 pixel consists of 3 bytes. Watermark data bits are hidden in the LSB of the R, G, and B components. If watermark data bits 0, 0, 1 are hidden in the LSBs of R, G, and B components of white (R: 255, G: 255, B: 255) pixel, the values of R, G, and B components change slightly. That is, the values of the R, G, and B components become 254, 255, and 254, respectively. In each of R, G, and B components, the average of the values that are slightly changed by hiding the watermark data bit is 0.5. The color change of pixels caused by subtle differences in each of R, G, and B components cannot be visually discerned. Therefore, it is impossible to visually distinguish the original image from the stego-image with the hidden watermark. When the watermark data is hidden in the LSB of each pixel of the color image, it is possible to hide up to 3 bits per pixel.

Although this technique is simple and can be implemented simply, the watermark data is hidden in the LSB of the pixel and the original watermark data can be simply extracted from the generated stego-image, so the security of the watermark is weak.

3. Proposed technique

When the watermark is hidden in the LSB of the color image, since it is easy to extract the watermark from the stego-image, the security of the watermark is weak. In order to overcome the security vulnerability of the watermark, the watermark data bit is encrypted using pixel information as in Equation (1). In Equation (1), i has a value from 0 to W·H-1. W and H represent the width of the image and the height of the image, respectively. $E_F(x)_i$ in Equation (1) indicates the first encrypted watermark data bit before being hidden in the i-th pixel of R(x=0), G(x=1), B(x=2) components.

In Equation (1), x may have 0, 1, or 2 values, and each value represents a component of R(x=0), G(x=1), and B(x=2). In Equation (1), k and m must be values that satisfy the conditions of Equation (1). $D(x)_i$ represents the original watermark data bits to be hidden in the LSB of the i-th pixel of the R(x=0), G(x=1), and B(x=2) components. The symbol (⊕) used in Equation (1) is a logical operation symbol representing Exclusive-OR operation.

If x=0, k=7, m=6, $P(x)_{i\_K}=P(0)_{i\_7}$ indicates the MSB of the i-th pixel of the R component. $P(x)_{i\_k-m}=P(0)_{i\_1}$ indicates the left first bit of the LSB of the i-th pixel of the R component. As shown in Equation (1), since $1 \le k-m \le 7$ is satisfied, k-m can represent the position from the MSB of the i-th pixel of the corresponding component to the first bit left of the LSB. The watermark data bits encrypted by Equation (1) are re-encrypted using the pixel values of other components as in Equation (2). The value of n in Equation (2) must be a value that satisfies the condition of Equation (2). If x=2, k=7, n=0, $P((x+1) \bmod 3)_{i\_k+n}=P(0)_{i\_7}$ represents the MSB of the i-th pixel of the R component. After multi-encrypting the watermark data bits using Equations (1) to (2), it is hidden

in the LSB of the corresponding component pixel of the color image. k, m, n used in Equations (1) and (2) become encryption keys. As such, the multi-encrypted watermark data bit has very high security.

An example in which the multi-encrypted watermark data bits are hidden in the LSB of the R, G, and B component is as follows. It is assumed that the pixel values of the cover image R plane are 44, 198, 209, and 187, and the watermark data bit to be hidden is 0000. It is assumed that the pixel values of the G-plane are 227, 201, 62, and 148, and the watermark data bits to be hidden are 1111. It is assumed that the pixel values of the B-plane are 177, 87, 5, and 30 and the watermark data bit is 0011. And it is assumed that the encryption keys are k=4, m=3, and n=2, respectively. If the watermark data 0000 to be hidden in the R component is encrypted using Equation (1), the encrypted watermark data bits become 0110. These results can be obtained as follows. $E_{F(0)0}=P_{(0)0\_4} \oplus P_{(0)0\_1} \oplus D_{(0)0}=0 \oplus 0 \oplus 0=0$, $E_{F(0)1}=P_{(0)1\_4} \oplus P_{(0)1\_1} \oplus D_{(0)1}=0 \oplus 1 \oplus 0=1$, $E_{F(0)2}=P_{(0)2\_4} \oplus P_{(0)2\_1} \oplus D_{(0)2}=1 \oplus 0 \oplus 0=1$, $E_{F(0)3}=P_{(0)3\_4} \oplus P_{(0)3\_1} \oplus D_{(0)3}=1 \oplus 1 \oplus 0=0$.

If encryption is performed once again using Equation (2), the multi-encrypted watermark data bits become 1010. These results can be obtained as follows. $E_{S(0)0}=E_{F(0)0} \oplus P_{(1)0\_6}=0 \oplus 1=1$, $E_{S(0)1}=E_{F(0)1} \oplus P_{(1)1\_6}=1 \oplus 1=0$, $E_{S(0)2}=E_{F(0)2} \oplus P_{(1)2\_6}=1 \oplus 0=1$, $E_{S(X)3}=E_{F(0)3} \oplus P_{(1)3\_6}=0 \oplus 0=0$. Therefore, if the multi-encrypted watermark data 1010 is hidden in the LSB of the R component pixel, the pixel values of the R component of the stego-image are 45, 198, 209, and 186. In the same way, the multi-encrypted watermark data hidden in the G component becomes 0010, and the G component pixel values of the stego-image become 226, 200, 63, and 148. The multi-encrypted watermark data hidden in the B component is 1101, and the B component pixel values of the stego-image are 177, 87, 4,31.

The original watermark data can be extracted without loss by using Equations (3) to (4) from the stego-image in which the multi-encrypted watermark data is hidden. The pixel values of the R component of the stego-image in which the multi-encrypted watermark is hidden are 45, 198, 209, and 186. The pixel values of the G component of the stego-image are 226, 200, 63, and 148. The pixel values of the B component of the stego-image are 177, 87, 4, and 31. When Equations (3) to (4) are applied to extract the original watermark data bits from the stego-image, the watermark data extracted from the R, G, and B components become 0000, 1111, and 0011. If the multi-encrypted watermark data is hidden in the cover image using the proposed method, very high security is maintained and the original watermark data can be extracted without loss.

$$E_{F(X)i}=P_{(X)i\_k} \oplus P_{(X)i\_k+m} \oplus D_{(X)i} \quad \text{where } 1 \leq k \leq 7,\ 0 \leq m \leq 6,\ 1 \leq k-m \leq 7 \tag{1}$$

$$E_{S(X)i}=E_{F(X)i} \oplus P_{((X+1) \bmod 3)i\_k+n} \quad \text{where } 0 \leq n \leq 6,\ 1 \leq k+n \leq 7 \tag{2}$$

$$E_{F(X)i}=E_{S(X)i} \oplus P_{((X+1) \bmod 3)i\_k+n} \tag{3}$$

$$D_{(X)i}=E_{F(X)i} \oplus P_{(X)i\_k} \oplus P_{(X)i\_k+m} \tag{4}$$

4. Experimental results

To confirm the performance of the proposed technique, experiments were performed using 512x512 size Lenna, airplane, Tiffany, and sail-boat as cover images. The encryption key values of Equations (1) to (2) used for watermark multiple encryption were k=4, m=3, n=2. The English abstract of this paper was used as confidential data, watermark data. After converting the watermark data into binary, Equations (1) to (2) were applied to generate multi-encrypted watermark data bits. Multi-encrypted watermark data bits were repeatedly hidden in the order of R, G, and B planes. Figure 1 shows the experimental result image. Figures a-1, b-1, c-1, and d-1 are each cover image used in the experiment. Figures a-2, b-2, c-2, and d-2 are stego-images generated by applying the conventional technique of sequentially hiding pure watermark data bits in the pixel's LSB. Figures a-3, b-3, c-3, and d-3 show the stego-image generated by multi-encrypting the watermark by applying

Equations (1) to (2) of the proposed technique.

As shown in Figure 1, the cover image and the stego-image cannot be visually distinguished because the quality of the stego-image in which the multi-encrypted watermark data is hidden using the proposed technique is very good. Even if a multi-encrypted watermark is extracted from a stego image for malicious purposes, the security of the watermark is maintained very high because the watermark is multi-encrypted.

Table 1 is the experimental result data in which the watermark is hidden in each cover image by the proposed technique. As shown in Table 1, when the proposed technique is used, the maximum number of hidden watermark data bits is 786,432 bits corresponding to (W·H)·3. Although the number of bits of watermark data hidden in the proposed method is the same as that of the existing LSB method, the security of the watermark is greatly improved in the proposed method because the watermark data is multi-encrypted and hidden in the cover image.

As shown in Table 1, the PSNR values of the stego-image generated using the proposed technique are 51.157dB, 51.154dB, 51.074dB, and 51.152dB, respectively. In general, when the PSNR value is 40 dB or more, the human eye cannot distinguish the difference between the original cover image and the stego-image. Therefore, the proposed technique satisfies imperceptibility, and when the watermark is hidden with the proposed technique, the stego-image is visually no different from the original cover image, so whether the watermark is hidden in the stego-image cannot be recognized. Also, since the hidden watermark is double-encrypted, the security is maintained very high. In addition, the watermark, which is confidential data, can be extracted only by knowing the encryption key values from the stego-image. Therefore, the proposed technique is a very good watermarking technique.

(a-1) Lenna, Cover image

(a-2) LSB, stego—image

(a-3) Proposed, stego-image

(b-1) airplane, Cover image

(2) LSB, stego-image

(b-3) Proposed, stego-image

(c-1) Tiffany, cover image

(c-2) LSB, stego-image

(c-3) Proposed, stego-image

(c-1) sail-boat, cover image

(c-2) LSB, stego-image

(c-3) Proposed, stego-image

Figure 1. Cover image and stego-image

Table 1. Experimental results

Image	Technique	PSNR	Hidden bits
Lenna	LSB	51.176	786,432
	Proposed	51.157	786,432
airplane	LSB	51.147	786,432
	Proposed	51.154	786,432
Tiffany	LSB	51.081	786,432
	Proposed	51.074	786,432
sail-boat	LSB	51.153	786,432
	Proposed	51.152	786,432

5. Conclusions

In this paper, in order to solve the problem of weak security that occurs when the watermark is hidden in the LSB, we proposed a technique with excellent security in which the original watermark is encrypted multiple times and the multi-encrypted watermark is hidden in the LSB of each pixel of the R, G, and B planes of the color image. If the watermark is hidden in the color image by applying the proposed technique, the security of the watermark hidden in the stego image is maintained very high, and the original watermark can be extracted from the stego-image without loss. The maximum number of bits of watermark that can be hidden in the image is (W·H)x3 bits, and the PSNR value of the stego-image was at least 51.074dB. Therefore, it is impossible to identify whether the watermark is hidden in the stego-image with the human eye. The proposed technique is an effective watermarking technique that can be used for applications such as military and intellectual property protection that need to hide sensitive and confidential data.

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. DOI: https://doi.org/10.1007/s00500-008-0333-9

[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. DOI: https://doi.org/10.1109/TCSVT.2006.869964

[3] Z. Andrew, Tirkel, G. A. Rankin, G. Ron, V. Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne, "Electronic watermark", Digital Image Computing, Technology and Applications, pp. 666-673, Macquarie University, 1994.

[4] A. J. Zargar, "Digital Image Watermarking using LSB Technique", International Journal of Scientific & Engineering Research, Vol. 5, Issue 7, pp. 202-205, March, 2014.

[5] P. Gaur, and N. Manglani, "Image Watermarking Using LSB Technique", International Journal of Engineering Research and General Science, Vol. 3, Issue 3, pp. 1424-1433, June, 2015.

[6] B. Chitradevi, N. Thinaharan, M. Vasanthi, "Data Hiding Using Least Significant Bit Steganography in Digital Images", Stat. Approaches Multidiscip. Res. Vol. 1, pp. 143–150, January, 2017.

[7] S. M. Jung, "An Advanced Color Watermarking Technique using Various Spatial Encryption Techniques", The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 13, No. 3, pp.262-266, June, 2020. https://doi.org/10.17661/jkiiect.2020.13.3.262

[8] S. M. Jung, "Data hiding technique using image pixel value and spatial encryption technique", International Journal of Internet, Broadcasting, and Communication, Vol. 13, No. 3, pp.50-55, August, 2021. DOI: http://dx.doi.org/10.7236/IJIBC.2021.13.3.50

[9] S. M. Jung, "An Effective Technique to Conceal Confidential Data in the LSB of Image", Autumn Annual Conference of KIIECT, October, 2021.

[10] S. M. Jung, "Color Image Watermarking Technique using Adjacent Pixels and Spatial Encryption Technique", The Journal of the Convergence on Culture Technology, November, 2021.
DOI: https://dx.doi.org/10.17703/JCCT.2021.7.4.863