International Journal of Internet, Broadcasting and Communication Vol.13 No.1 187-193 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.1.187

IJIBC 21-1-22

Watermarking Technique using Image Characteristics

Soo-Mok Jung

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

Abstract

In this paper, we propose an image watermarking technique that effectively hides confidential data in the LSB of image pixels by utilizing the characteristics of the image. In the proposed technique, the image is precisely divided into boundary surface and normal region other than the boundary surface and performs different processing. The boundary surface existing in the image is created by meeting different regions and contains important information of the image. One bit of confidential data is concealed in the LSB of the pixel at the boundary surface to preserve the characteristics of the boundary surface. In normal region other than the boundary surface, the pixel values are similar, and the change with the adjacent pixel values is smooth. Based on this property, even if the 2 bits of confidential data are hidden in the lower 2 bits of the pixel in the normal region, the difference cannot be visually distinguished. When confidential data is concealed in an image as described above, the amount of confidential data concealed in an image can be increased while maintaining excellent image quality. Concealing confidential data by applying the proposed method increases the amount of confidential data concealed by up to 84.6% compared to the existing method. The proposed technique can be effectively used for commercial image watermarking that hides copyright information.

Keywords: *Watermarking, Adjacent pixel, LSB, confidential data, Cover image, Stego-image*

1. Introduction

Image watermarking is a technique of concealing digital watermark such as text, picture, and symbol, which are confidential data related to ownership, in images so that humans cannot recognize them. In image watermarking technique, a watermark must be extracted without loss from an image in which the watermark is hidden. In addition, it is necessary to satisfy imperceptibility in which humans cannot recognize whether a watermark is hidden in an image. [1][2] In order to satisfy the imperceptibility, the image quality of the watermark-hidden image should be very good, so that the watermark-hidden image and the original image cannot be visually distinguished.

Image watermarking techniques for concealing watermark data bits in LSBs of pixels in an image have been developed. [3]-[6] The technique of concealing watermark data bits in the LSBs of image pixels has an advantage of being easy to implement due to a simple procedure, but it has a disadvantage that the number of

Manuscript Received: January. 4, 2021 / Revised: January. 10, 2021 / Accepted: January. 17, 2021
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Engineering, Sahmyook University, Korea

confidential data bits that can be concealed is limited to the number of pixels of the image.

Recently, this research team proposed an image watermarking technique that enhances the security of confidential data, but the maximum watermark data bit that can be hidden in an image is limited by the number of pixels in the image. [7]-[8] In order to improve the disadvantage of the existing techniques in which the number of bits of confidential data to be hidden is limited by the number of image pixels, in this paper, a watermarking technique using image characteristics is proposed. Using the proposed technique, the number of bits of confidential data that can be hidden in an image can be increased.

The structure of this paper is as follows. In Chapter 2, a technique for concealing the watermark data bits in the LSBs of image pixels is described. In Chapter 3, we describe a proposed technique that can increase the number of confidential data bits hidden in an image by using the characteristics of the image. The experimental results are described in Chapter 4, and the conclusion is described in Chapter 5. Finally, in Chapter 6, future studies are described.

2. The technique for concealing the watermark in the LSB of the pixel value

Each pixel of a color image is composed of R, G, and B component values. R, G, and B components are each represented by 1 byte, so each has a value between 0 and 255, and 1 pixel consists of 3 bytes. When the watermark is concealed in the LSB, bits of watermark data are inserted into the LSB of each component of R, G, and B. Figure 1 shows a case where bit “010” of watermark data, which is confidential data, is hidden in white (R: 255, G:255, B:255) pixel.

As the bits of the watermark data are inserted into the LSB of the R, G, and B components, the values of the R, G, and B components are slightly changed. In Figure 1, you can see that the values of the R, G, and B components became 255, 254, and 255 respectively. For each component, this small difference is 0.5 on average. The color change of the pixel that occurs due to the very small difference in each component becomes impossible to visually recognize. Therefore, it is impossible to visually distinguish the original image from the image in which the watermark is hidden. When watermark data is concealed in the LSB of each pixel of a color image, as shown in Figure 1, a maximum of 3 bits per pixel can be concealed. Because this technique is simple, implementation is simple. However, when the watermark data is concealed in the LSB, the number of concealed watermark data bits is limited to the number of pixels in the image.

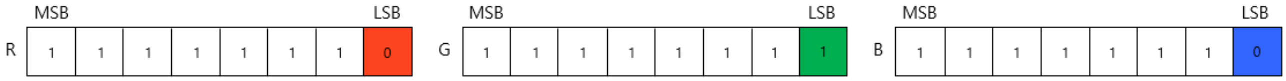


Figure 1. Sample Confidential data embedding in LSBs of R, G, B components of a pixel

3. Proposed technique

In order to hide confidential data in the LSB of a pixel by utilizing the characteristics of the image, the proposed technique investigates the characteristics of the image. The boundary surface existing in the image is created by meeting different regions and includes important information of the image. When the values of the pixels at the boundary surface change, the characteristics of the outline of the image change. When confidential data is concealed in the LSB of a pixel by utilizing the characteristics of an image in order to increase the confidential data to be concealed, the processing of the pixel at the boundary surface of the image and the pixel in the normal region are different.

In an image, a pixel value at boundary surface has a large difference from a pixel value in the adjacent normal region other than the boundary surface. Since the boundary surface contains important information of the image, in order to minimize the change of the pixel value at the boundary surface, 1 bit of confidential data is hidden in the LSB of the pixel to maintain the sharpness of the boundary surface. Since the normal region other than the boundary surface is an area in which pixel values change smoothly, in the normal region, 2 bits of confidential data are hidden in the lower bits of the pixel. In this way, the amount of confidential data hidden in the image can be increased while maintaining excellent image quality.

Figure 2 shows the locations of adjacent pixels used to determine whether an arbitrary location (y, x) is a location at the boundary surface while scanning the cover image from left to right and top to bottom. In Figure 2, the coordinate axis represents the case of applying the screen coordinate system. In Figure 2, the pixel value at the (y, x) position is A. That is, P(y, x) = A. A´ in Figure 2 is a value calculated by Equation (1). That is, the value with the lower 2 bits of A as 0 is expressed as A'. If P(y, x)=A=255, then A' becomes 252. In Equation (1), & is a symbol for bitwise AND operation, and 0X is a symbol for hexadecimal. B', C', D', and E' represent the values in which the lower 2 bits of the pixel value at the corresponding position are 0.

$$A' = A \ \& \ 0XFC \tag{1}$$

The absolute value of the difference between the value A' at the position (y, x) and the values at the adjacent position is obtained using equations (2) to (5). Equation (6) is an equation that calculates the sum of the values obtained in Equations (2) to (5). Equation (7) is an equation for determining whether the position (y, x) is a position at the boundary surface. If diff_Sum is greater than T1 or any one of diff1~diff4 is greater than T2, the corresponding position is determined to be a position at the boundary surface. That is, if the condition of the if statement of Equation (3) is satisfied, the corresponding position is determined to be a position at the boundary surface, and 1 bit of confidential data is hidden in the LSB of the pixel as shown in Equation (4). Since 1 bit of confidential data is hidden in the LSB of the pixel at the boundary surface, most important information on the boundary surface is maintained, making it impossible to visually feel that the boundary surface has changed.

If the condition of the if statement in Equation (3) is not satisfied, it is determined that the location is not a location at the boundary surface but is included in the normal region. Thereafter, 2 bits of confidential data are hidden in the lower 2 bits of the pixel as shown in Equation (5). In the case of a normal region, the pixel values are similar, and since the change with the adjacent pixel value is gentle, even if 2 bits are hidden in the lower 2 bits of the pixel value, the difference cannot be visually distinguished. S(y, x) in Equations (8) and (9) represents the pixel value at the (y, x) position on the stego-image, which is the resulting image in which confidential data is hidden. CD(n) in Equations (8) and (9) represents n-bit confidential data. Therefore, the CD(1) represents 1-bit confidential data and may have a value of 0 or 1. The CD(2) represents 2-bit confidential data and may have a value of 00, 01, 10, and 11. That is, when P(y, x) is 255 and CD(2) is 10(2), the value of S(y, x) calculated according to Equation (9) is 254.

When confidential data is concealed according to the proposed technique, Equations (2) to (7) cannot be applied to pixels in the top row, left column, and right column of the cover image. Therefore, in this case, 1 bit of confidential data is hidden in the LSB of the pixel as shown in Equation (8). When watermarking is performed according to this procedure, the boundary surface characteristics of the stego-image are excellent, so that the visual quality of the stego-image is excellent, and the number of bits of confidential data to be hidden increases.

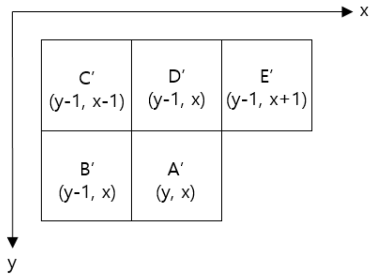


Figure 2. Adjacent pixels used to investigate the characteristics of an image

```
diff1 = abs(A´-B´)                                                          (2)
diff2 = abs(A´-C´)                                                          (3)
diff3 = abs(A´-D´)                                                          (4)
diff4 = abs(A´-E´)                                                          (5)
diff_Sum=diff1+ diff2+ diff3+ diff4                                         (6)
if(diff_Sum>=T1 || (diff1>=T2 || diff2>=T2 || diff3>=T2 || diff4>=T2))      (7)
{   / / (y, x) is the position at the boundary surface
    S(y, x)=P(y, x) & 0XFE + CD(1);                                          (8)
}
else
{   // (y, x) is the position in the normal region
    S(y, x)=P(y, x) & 0XFC + CD(2);                                          (9)
}
```

The procedure for extracting confidential data from a stego-image in which confidential data is hidden is as follows. While scanning the stego-image from left to right and top to bottom, use equations (2) to (7) at an arbitrary position (y, x) to determine whether the position is on the boundary surface. If it is a position at the boundary surface, 1 bit of hidden confidential data is extracted using Equation (10). In other words, if S(y, x) in Equation (10) is 254, CD(1) has a value of 0, and the extracted 1-bit confidential data is 0. If it is not a position at the boundary surface, then 2 bits of hidden confidential data are extracted using Equation (11). In equation (11), if S(y,x) is 254, the extracted CD(2) becomes 2, and the 2-bit confidential data becomes 10. Since 1-bit confidential data is hidden in the LSB in the highest row, left column, and right column of the stego-image, 1-bit confidential data is extracted using Equation (10).

```
CD(1)=S(y, x) & 0X01;                                                       (10)
CD(2)=S(y, x) & 0X03;                                                       (11)
```

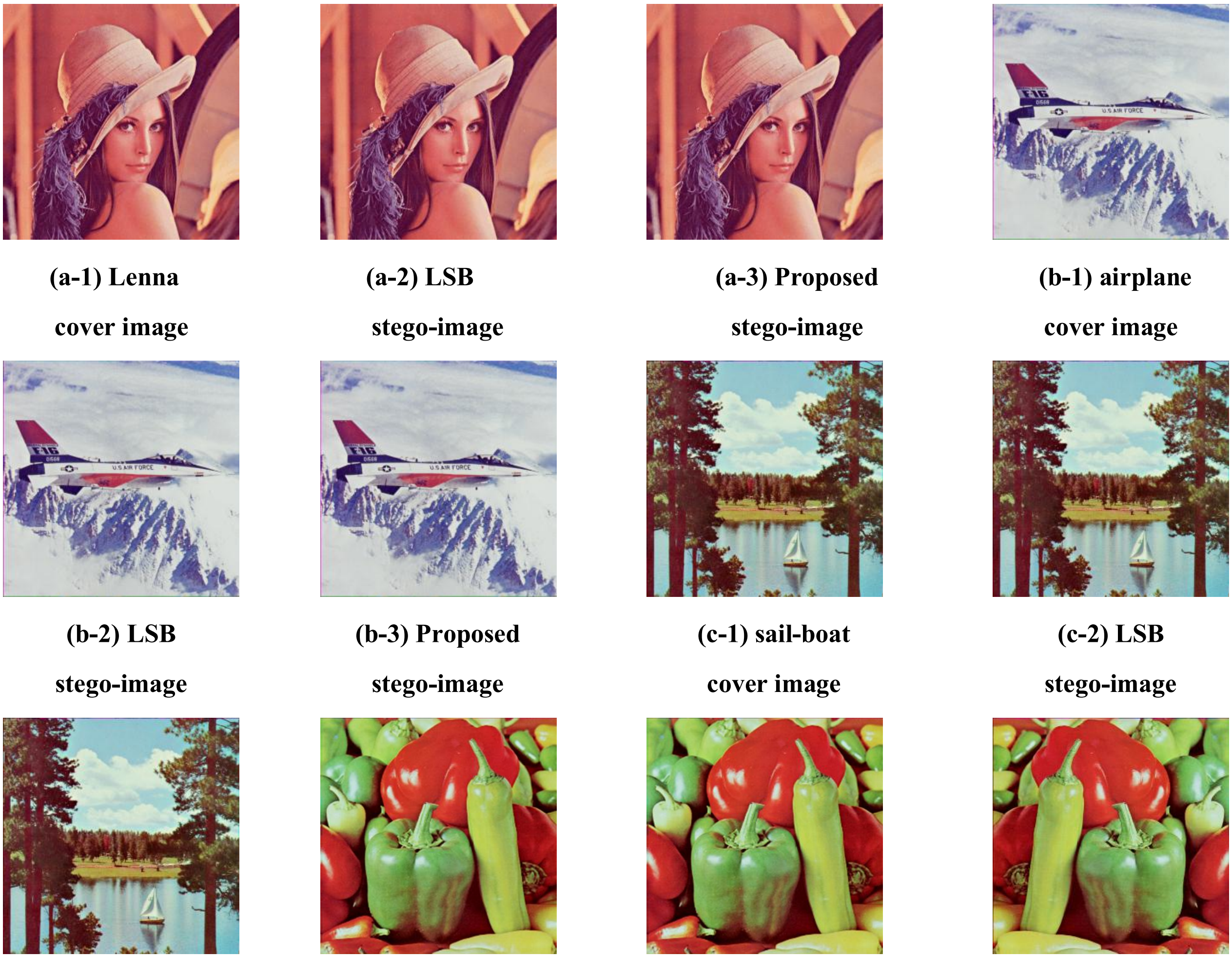
Using the proposed technique, it is possible to conceal a lot of confidential data while maintaining excellent visual quality of the stego-image. In addition, confidential data can be extracted from the Stego image without loss, and the difference between the stego-image and the original cover image cannot be visually distinguished because the image quality of the stego-image is excellent.

4. Experimental results

To confirm the performance of the proposed technique, an experiment was performed using 512x512 size Lenna, airplane, sail-boat, and pepper as cover images. Confidential data used in the experiment was repeatedly hidden in the cover image by converting the abstract of this paper into binary numbers. T1 and T2 used in Equation 7 were set to 50 and 20, respectively. Figure 3 (1) shows the cover images. Figure 3 (2) shows the stego images created by the existing technique of hiding confidential data in LSB. Figure 3 (3) shows the stego images created by performing watermarking with the proposed technique.

As shown in Figure 3, the visual quality of the stego-image created by concealing confidential data with the proposed technique is very good, so the cover image and the stego-image cannot be visually distinguished. Therefore, the user cannot recognize whether the watermark is hidden in the stego-image. In addition, the watermark hidden in the stego-image can be extracted without loss.

Table 1 shows the experimental results using Lenna, airplane, sail-boat, and pepper as cover images. As shown in Table 1, when the proposed method is used, the number of hidden confidential data bits is increased by up to 84.6% compared to the existing method. In addition, the PSNR values of the stego images generated using the proposed technique were 46.071dB, 44.704dB, 45.620dB, and 44.694dB, respectively. In general, if the PSNR value is more than 40dB, the difference from the original image cannot be distinguished by human vision. The proposed technique is an efficient technique that increases the amount of confidential data hidden in an image while maintaining a very high visual quality.



(a-1) Lenna cover image

(a-2) LSB stego-image

(a-3) Proposed stego-image

(b-1) airplane cover image

(b-2) LSB stego-image

(b-3) Proposed stego-image

(c-1) sail-boat cover image

(c-2) LSB stego-image

(c-3) Proposed stego-image

(d-1) pepper cover image

(d-2) LSB stego-image

(d-3) Proposed stego-image

Figure 3. Cover images & stego-images

Table 1. Experimental results

Image	Technique	PSNR	Hidden bits	Hidden bit growth rate(%)
Lenna	LSB	51.178	786,432	
	Proposed	46.071	1,412,193	79.6
airplane	LSB	51.141	786,432	
	Proposed	44.704	1,451,700	84.6
sail-boat	LSB	51.144	786,432	
	Proposed	45.620	1,291,984	64.3
pepper	LSB	51.161	786,432	
	Proposed	44.694	1,421,440	80.7

In the proposed technique, if T1 and T2 are set to 0, the condition of the if statement in Equation (7) is always true, so the proposed technique operates the same as the LSB technique.

5. Conclusions

The proposed technique is an effective technique that increases the confidential data that is concealed by using the characteristics of the image and maintains a very high visual quality of the stego-image where the confidential data is concealed. Using the proposed technique, it is possible to conceal confidential data, which is up to 84.6% higher than that of the conventional technique of concealing confidential data in the LSB of pixels. Due to the excellent quality of stego-image, the difference between the original cover image and the stego-image cannot be visually distinguished, and the confidential data is extracted from the stego-image without loss. The proposed image watermarking technique is an excellent technique that can be effectively used for general commercial image watermarking that does not require reversible characteristics. In general, if the PSNR value is more than 40dB, the difference from the original image cannot be distinguished by human vision. The proposed technique is an efficient technique that increases the amount of confidential data hidden in an image while maintaining a very high visual quality.

6. Future research

The proposed technique is a technique to increase the concealed confidential data by examining the characteristics of an image and then concealing the confidential data in the lower 1 bit or the lower 2 bits of the pixel according to the characteristics of the image. Since it is determined whether 1 bit or 2 bits are to be concealed according to T1 and T2, the security of the concealed confidential data is somewhat higher than the conventional method of concealing 1-bit confidential data in the LSB. In addition, 1-bit confidential data is hidden in the LSBs of the pixels in the top row, left column and right column of the cover image. Therefore, additional research is needed to strengthen the security of hidden confidential data. In future research, we intend to conduct research to strengthen the security of confidential data in the proposed technique.

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, "Image watermarking technique applying multiple encryption techniques", The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 13, No. 6, pp.503-510, December, 2020.
https://doi.org/10.17661/jkiiect.2020.13.6.503