International Journal of Advanced Smart Convergence Vol.11 No.4 163-169 (2022)
http://dx.doi.org/10.7236/IJASC.2022.11.4.163

IJASC 22-4-18

Data Hiding Technique using the Characteristics of Neighboring Pixels and Encryption Techniques

Soo-Mok Jung

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

Abstract

In this paper, we propose a data hiding technique that effectively hides confidential data in the LSB of an image pixel by using the characteristics of the neighboring pixels of the image and the encryption techniques. In the proposed technique, the boundary surface of the image and the flat surface with little change in pixel values are investigated. At the boundary surface of the image, 1 bit of confidential data is encrypted and hidden in the LSB of the boundary pixel to preserve the characteristics of the boundary surface. In the pixels of the plane where the change in pixel value is small, 2 bits secret data is encrypted and hidden in the lower 2 bits of the corresponding pixel. In this way, when confidential data is hidden in an image, the amount of confidential data hidden in the image is greatly increased while maintaining excellent image quality. In addition, the security of hidden confidential data is strongly maintained. When confidential data is hidden by applying the proposed technique, the amount of confidential data concealed increases by up to 92.2% compared to the existing LSB method. The proposed technique can be effectively used to hide copyright information in commercial images.

Keywords: *Data embedding technique, Adjacent pixel value, LSB, confidential data, Cover image, Stego-image*

1. Introduction

Data hiding is a technology that hides confidential digital data such as text, pictures, and symbols in digital images so that people cannot recognize them. An image in which confidential data is hidden is called a stego image. In the data hiding technique, confidential data must be extracted without loss from the stego image in which confidential data is hidden. In addition, imperceptibility, which is a property that cannot recognize that confidential data is hidden in a stego image, must be satisfied. [1][2] Imperceptibility is satisfied when the quality of the stego image is so good that it is impossible to distinguish between the stego image and the original cover image.

Data hiding techniques have been developed that hide confidential data bits in the LSB of image pixels. [3]-[6] This technique has the advantage that the secret data hiding procedure is very simple and easy to implement. However, as many confidential data bits as the total number of pixels constituting an image can be hidden.

Manuscript Received: November. 5, 2022 / Revised: November. 8, 2022 / Accepted: November. 10, 2022
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Engineering, Sahmyook University, Korea

Therefore, this technique has a disadvantage in that a large amount of confidential data cannot be concealed.

Recently, the research team proposed image hiding techniques that enhances the security of confidential data. [7]-[9] In this paper, we propose a technique that effectively hides confidential data by applying the characteristics of neighboring pixels and applying encryption techniques using neighboring pixels, which are improved techniques from the technique previously proposed by this research team. When confidential data is hidden in an image using the proposed technique, the amount of confidential data hidden in the image is greatly increased and the security of the hidden confidential data is greatly strengthened.

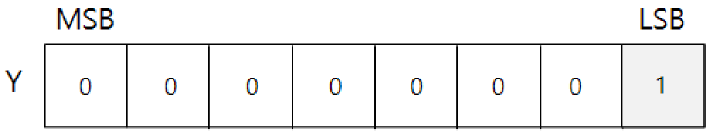
The organization of this paper is as follows. In Section 2, a technique for hiding the confidential data bits in the LSBs of image pixels is described. In Section 3, we describe a proposed technique that can increase the number of confidential data bits hidden in an image by using the characteristics of neighboring pixels and an encryption technique using neighboring pixels. The experimental results are described in Section 4, and the conclusion is described in Section 5.

2. The technique for hiding confidential data in the LSB of a pixel

Each pixel of a gray scale image is represented by 1 byte. Therefore, each pixel value has a value between 0 and 255. The technique of hiding confidential data in the LSB of pixel values is shown in Figure 1. As shown in Figure 1, one bit of confidential data is hidden in the LSB among the 8 bits representing the pixel value. Therefore, hiding the confidential data bit '1' in the LSB of a pixel with pixel value 255 (completely white) turns pixel value 255 into 254. Therefore, if we hide confidential data in the LSB of a pixel, the average of the pixel value difference is 0.5.

Since human vision is inaccurate, even if the value of a pixel having a value between 0 (black) and 255 (white) is changed by a maximum of 1, a person cannot perceive the changed difference. Therefore, it is impossible to visually distinguish the original cover image in which confidential data is not hidden in the LSB of pixels and the stego image in which confidential data is hidden in the LSB of pixels.

In the technique of hiding confidential data in the LSB of a pixel, since 1 bit of confidential data can be hidden per pixel, the maximum number of confidential data bits hidden in an image is the width (W) x height (H) bits of the image. Therefore, the technique of hiding confidential data in the LSB of pixels is simple and easy to implement, but has a disadvantage in that the number of confidential data bits is limited to the number of pixels in the image. In addition, since confidential data hidden in stego image can be easily extracted, there is a critical weakness in security.



	MSB							LSB
Y	0	0	0	0	0	0	0	1

Figure 1. Confidential data embedding in LSB of a pixel

3. Proposed technique

In this paper, we propose a technique to effectively hide confidential data in the LSB of a pixel by using neighboring pixels and an encryption technique. The procedure of the proposed technique for generating a stego image by hiding confidential data in a cover image is shown in Equations (1) to (6).

```
$b_0=(CD_i \oplus (MSB_{-1} \text{ of } R_1) \oplus (MSB_{-1} \text{ of } R_2) \oplus (MSB_{-1} \text{ of } R_3)) \odot KEY_i$   (1)
$diff_k = |T - R_k|$ where k=1 to 12   (2)
if (any one of $diff_k$ is greater than threshold)   (3)
{   // the location is on the boundary surface
     SI(y, x)=T & 0XFE | (Encrypted confidential data 1-bit $b_0$)   // generate stego image pixel   (4)
}
else
{   // the location where the pixel value changes smoothly
    $b_1=(CD_i \oplus (MSB \text{ of } R_1) \oplus (MSB \text{ of } R_2) \oplus (MSB \text{ of } R_3)) \odot KEY_i$   (5)
    SI(y, x)=T & 0XFC | (Encrypted confidential data 2-bit $b_1$, $b_0$) // generate stego image pixel   (6)
}
```

In the proposed technique, confidential data is hidden in inverse s-order as shown in Figure 2. In an image, a boundary surface has important information of the image. These boundary surfaces are generated by adjacent regions having heterogeneous distributions of pixel values. When the pixel values on the boundary surface change, the contour characteristics of the image change. Therefore, in the proposed technique, 1 bit of confidential data is encrypted and hidden in the LSB of each pixel of the boundary surface. In the area outside the boundary surface, the characteristics of the area are investigated to select a location to hide 2 bits of confidential data, and then 2 bits of confidential data are encrypted and hidden in each pixel of the found location.

First, 1 bit of confidential data to be hidden in the LSB of a pixel is encrypted as shown in Equation (1). In Equation (1), CD_i and KEY_i represent the i-th bit of confidential data and the i-th bit of KEY respectively. The initial value of i is 0. The value of i increases by 1 after encryption is performed. If the value of i increases and becomes greater than the position of the last bit, the value of i becomes 0. The symbol $\oplus$ represents exclusive-OR and the symbol $\odot$ represents exclusive-NOR. MSB_{-1} in Equation (1) means the right bit of the MSB. In Equation (1), when a pixel does not exist, the corresponding pixel value is set to 0.

In order to find a location that is far from the boundary surface and has a gradual change in pixel value, the value of Equation (2) is calculated using 12 neighboring pixels as shown in Figure 3. In Equation (2), *T* and *R_k* are values in which the lower 2 bits including LSB of the pixel values T and R_k are set to 0 and only the upper 6 bits are considered. In Figure 3, the coordinate axis is the case where the screen coordinate system is applied. If any one of the $diff_k$ values calculated in Equation (2) is greater than the threshold, the position is determined to be a position on the boundary surface. In this case, Equation (4) is used to hide encrypted 1-bit confidential data in the pixels at the boundary surface. For example, assume that the original pixel values without excluding the lower two bits are R_1 = 254, R_2 = 255, R_3 = 63, R_4~R_{12} = 255, T = 62, and CD = 01101001…..…, KEY = 10010110, i = 0 (CD_0=0, KEY_0=1). In this case, the value of encrypted confidential data bit b_0 to be hidden in the LSB of the pixel at the (y, x) position of the stego image is calculated as $0=(0\oplus1\oplus1\oplus0)\odot1$ according to Equation (1). Since at least one of $diff_k$ value calculated in Equation (2) is very large, the condition of Equation (3) is satisfied. So, Equation (4) is performed. As shown in Equation (4), the encrypted confidential data 0 is hidden in the LSB of the pixel having the value of 62(T=62), and the pixel value becomes 62. Therefore, the pixel value at the (y, x) position of the stego image is 62. That is, SI (y, x) = 62. In Equation (4), 0X is a symbol indicating that it is a hexadecimal number.

On the other hand, assume that the original pixel values without excluding the lower two bits are R_1 = 254, R_2 = 255, R_3 = 254, R_4~R_{12} = 255, T = 255, and CD = 01101001……., KEY = 10010110, i = 0 (CD_0=0, KEY_0=1). In this case, the value of encrypted confidential data bit b_0 to be hidden in the LSB of the pixel at the (y, x) position of the stego image is calculated as $1=(0\oplus1\oplus1\oplus1)\odot1$ according to Equation (1). Since the $diff_k$ value calculated in Equation (2) is very small, the condition of Equation (3) is not satisfied. So, Equation (5) and (6) are performed. The value of encrypted confidential data bit b_1 to be hidden in the left bit of LSB is calculated as $1=(1\oplus1\oplus1\oplus1)\odot0$ according to Equation (5). Since the value of i was increased by 1 after Equation (1) was performed, CD_1 and KEY_1 were used in Equation (5). As in Equation (6), when 1(b_1=1) is hidden in the left bit of the LSB of the pixel value 255 (T=255) and 1(b_0=1) is hidden in the LSB, the pixel value becomes 255. And this value becomes the pixel value of the (y, x) position of the stego image. That is, SI(y, x) = 255.

In the upper two rows and the left and right two columns, only 1-bit encrypted confidential data is hidden in each pixel. Therefore, 1-bit confidential data is encrypted as in Equation (1), and then the encrypted confidential data is hidden as in Equation (4) to generate a pixel value of a stego image. Therefore, Equations (2) and (3) are not performed for pixels in the top two rows, left two columns, and right two columns.

Since the visual quality of the stego image generated by the proposed technique is excellent, it is impossible to visually distinguish the stego image from the original cover image, so it is impossible to recognize whether confidential data is hidden in the stego image. In addition, even if encrypted confidential data is extracted from the stego image, the original confidential data cannot be decrypted from the encrypted confidential data, so the security of confidential data is greatly strengthened. Therefore, by using the proposed technique, the amount of hidden confidential data can be greatly increased while maintaining excellent visual quality of stego image, and the confidential data can be perfectly restored from the stego image if the encryption key is provided.

The process of extracting confidential data from the stego image is as shown in Equations (7) to (12). When Equations (8) and (12) are performed, the value of i increases by 1.

```
$b_0 = SI(y, x)\ \&\ 0X01$                                                              (7)
$CD_i = (b_0 \oplus (MSB_{-1} \text{ of } R_1) \oplus (MSB_{-1} \text{ of } R_2) \oplus (MSB_{-1} \text{ of } R_3)) \odot KEY_i$    (8)
$diff_k = |T - R_k|$ where k=1 to 12                                                   (9)
if (any one of $diff_k$ is less than or equal to threshold)                            (10)
{   // the location where the pixel value changes smoothly
    $b_1 = (SI(y, x)\ \&\ 0X02) >> 1$                                                  (11)
    $CD_i = (b_1 \oplus (MSB \text{ of } R_1) \oplus (MSB \text{ of } R_2) \oplus (MSB \text{ of } R_3)) \odot KEY_i$    (12)
}
```

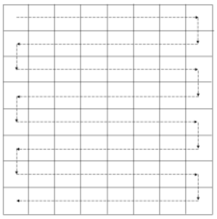


Figure 2. Order of hiding confidential data

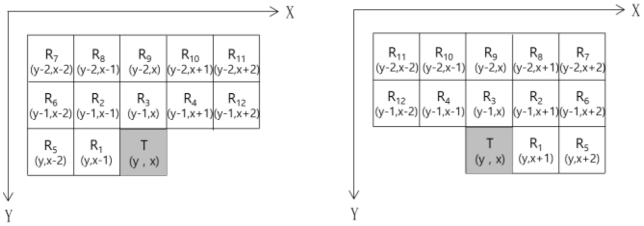


Figure 3. The Neighboring pixels used to find a location hiding 2 bits of confidential data when going in inverse s-order from left to right and right to left

4. Experimental results

To evaluate the performance of the proposed technique, experiments were performed using 512x512 gray scale images as cover images. The images used are Lenna, Splash, Pepper, and Blackb. The result of converting the abstract of this paper into binary was used as confidential data and repeatedly concealed in the cover image. The threshold of equation (3) was set to 31.

The images of the experimental results are shown in Figure 4. Figure 4(1) shows the cover images. Figure 4(2) shows stego images created with the technique of hiding confidential data in LSB. Figure 4(3) shows the stego images generated by the technique proposed in this paper. As shown in Figure 4, the visual quality of the stego image generated by hiding confidential data in the cover image with the proposed technique is very good. Therefore, it is not possible to recognize whether confidential data is hidden in the stego image because it is not visually distinguishable between the cover image and the stego image.

Using the proposed confidential data extraction technique, confidential data hidden in stego images can be extracted without loss. Also, since the proposed technique hides confidential data after encrypting it, even if confidential data is extracted from a stego image, it cannot be decrypted because the confidential data is encrypted. Therefore, using the proposed technique, the security of hidden confidential data is strongly maintained.

Table 1 shows the numerical data of the experimental results conducted using Lenna, Splash, Pepper, and Blackb as cover images. As shown in Table 1, when using the proposed technique, the number of hidden confidential data bits increased by up to 92.2% compared to the conventional LSB method. And the PSNR values of the stego images generated by concealing confidential data with the proposed technique were 50.49dB, 50.15dB, 50.45dB, and 50.53dB, respectively. In general, when the PSNR value is 40 dB or more, human eyes cannot distinguish the difference between the stego image and the original cover image.

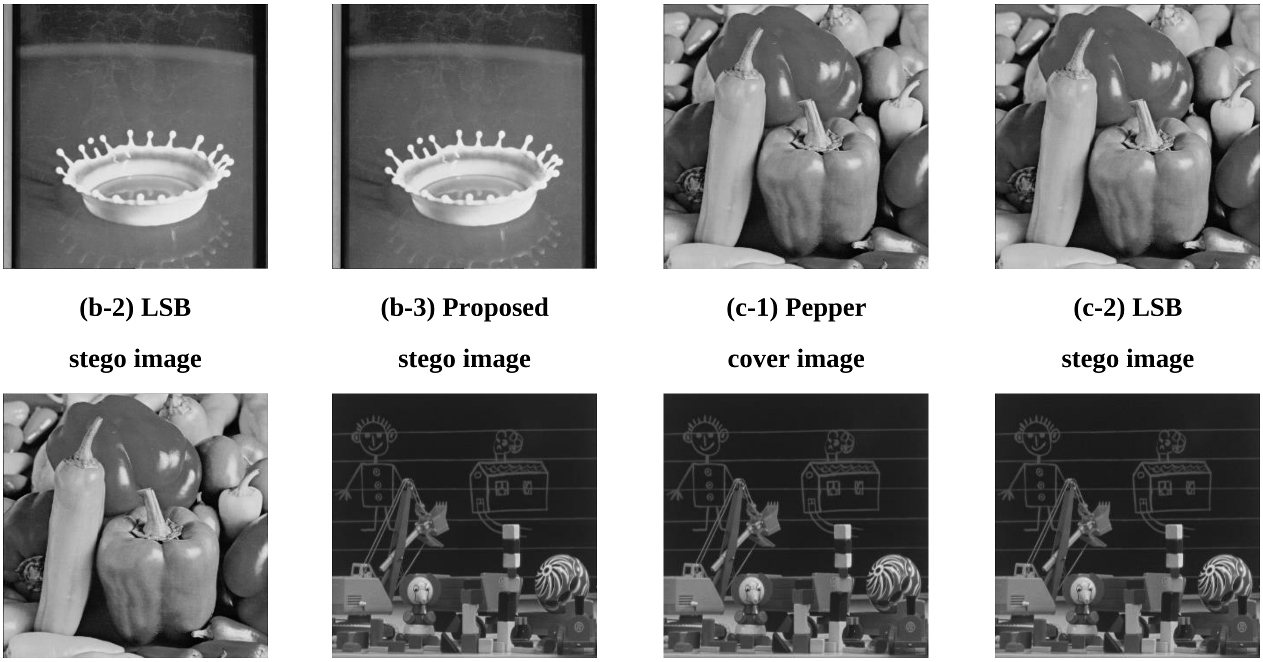
Therefore, the proposed technique generates stego images with very high visual quality, greatly increases the amount of confidential data hidden in images, and greatly improves the security vulnerabilities of the existing LSB techniques.

(a-1) Lenna cover image

(a-2) LSB stego image

(a-3) Proposed stego image

(b-1) Splash cover image



(b-2) LSB stego image

(b-3) Proposed stego image

(c-1) Pepper cover image

(c-2) LSB stego image

(c-3) Proposed stego image

(d-1) Blackb cover image

(d-2) LSB stego image

(d-3) Proposed stego image

Figure 4. Cover images & stego images

Table 1. Experimental results

Image	Technique	PSNR	Hidden bits	Hidden bit growth rate(%)
Lenna	LSB	55.91	262,144	
	Proposed	50.49	479,234	82.8
Splash	LSB	55.92	262,144	
	Proposed	50.15	503,811	92.2
pepper	LSB	55.92	262,144	
	Proposed	50.45	481,827	83.8
Blackb	LSB	55.92	262,144	
	Proposed	50.53	475,868	81.5

5. Conclusions

The proposed technique increases the secret data hidden in the pixel's LSB by up to 92.2% by using the characteristics of the image. The difference between the original cover image and the stego image cannot be visually distinguished because the PSNR value of the stego image generated using the proposed technique is over 50.15dB. Also, since the proposed technique encrypts and conceals confidential data, it greatly improves the security vulnerability of the existing techniques. Even if confidential data is extracted from a stego image, the confidential data is kept secure because it is encrypted. Using the proposed technique, confidential data can be extracted from stego images without loss.

Unlike medical images or military images, in the case of commercial cartoon images, it is not necessary to restore the original cover image from a stego image in which confidential data related to ownership is hidden, and the image quality of the stego image must be visually almost the same as that of the original cover image, the security of confidential data hidden in stego images must be kept very high. And confidential data must be safely extracted from the stego image. For these reasons, the proposed data hiding technique is an excellent technique that can be used very effectively to safely hide a large amount of confidential data in a general commercial image that does not require reversibility.

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

[9] S. M. Jung, “Watermarking Technique using Image Characteristics”, International Journal of Internet, Broadcasting and Communication, Vol. 13, No. 1, pp.187-193, February, 2021.
http://dx.doi.org/10.7236/IJIBC.2021.13.1.187