*International Journal of Internet, Broadcasting and Communication Vol.13 No.3 50-55 (2021)*
*http://dx.doi.org/10.7236/IJIBC.2021.13.3.50*

**IJIBC 21-3-7**

# Data hiding technique using image pixel value and spatial encryption technique

Soo-Mok Jung

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

***Abstract***

*In this paper, we proposed a technique for hiding the double-encrypted confidential data in the image using the pixel value of the image and the spatial encryption technique. The proposed technique inserts encrypted confidential data into the LSB of an image pixel in order to maintain high image quality. The stego-image generated by hiding the encrypted confidential data has very good quality and is visually indistinguishable from the original cover image, so that it is impossible to recognize whether the confidential data is hidden in the stego-image. It is possible to extract the original confidential data from the stego-image without loss. By conducting an experiment on the proposed technique, it was confirmed that the proposed technique is an effective technique for the practical application of data hiding. The proposed technique can be used in applications such as military and intellectual property protection that require high security.*

***Keywords:*** *Confidential data, Encryption, Cover image, Stego-image, Hiding*

## 1. Introduction

Data hiding techniques are used to hide confidential data such as intellectual property information in images. An image created by hiding confidential data in a cover image is called a stego-image. In data hiding technique, the quality of the stego-image must be excellent so that the cover image and the stego-image cannot be visually distinguished. Therefore, imperceptibility is very important in data hiding techniques. [1][2] It should also be possible to extract the original confidential data from the stego-image without loss.

A technique for hiding confidential data in the LSB has been proposed. [3]-[6] If confidential data bits are hidden in the LSB of each pixel of an image, the image quality of the stego-image is excellent, thereby the imperceptibility is satisfied. However, since confidential data can be easily extracted from the stego-image, there is a problem in that the security of the confidential data is weakened. To solve the weak security problem in the technique of hiding confidential data in the LSB of the image pixel, this research team has proposed data hiding techniques that enhance the security of confidential data. [7]-[9]

In this paper, a technique of double-encrypting the confidential data and hiding it in the LSB of the cover image pixel is proposed. In order to double-encrypt confidential data in the proposed technique, we applied a method of first encrypting confidential data using pixel values and then spatially encrypting it. The proposed

Manuscript Received: June. 3, 2021 / Revised: June. 8, 2021 / Accepted: June. 11, 2021
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Science and Engineering, Sahmyook University, Korea

technique is an improvement of the existing scheme. [9] The proposed technique is a secure confidential data hiding technique that maintains the security of confidential data very high. The structure of this paper is as follows. The technique of hiding the confidential data bit in the LSB of an image pixel is briefly described in Chapter 2, and the proposed technique is described in detail in Chapter 3. The experimental results for various images are described in Chapter 4, and the conclusion is described in Chapter 5.

## 2. Technique for hiding confidential data in the LSB of image pixel

Each pixel of a color image has R, G, and B component values. And since the R, G, and B component values are each expressed as 1 Byte, they have a value between 0 and 255. For example, in a red pixel, the R, G, and B component values have values of 255, 0, and 0, respectively. When data is hidden in each pixel of an image, a technique of inserting confidential data bits into the LSB of each R, G, and B components is used. Since each component is represented by 8 bits, the weight of the MSB is 128 and the weight of the LSB is 1, so the data is hidden in the LSB of the pixel in order to hide the data while minimizing the change of each component value. Therefore, in the case of hiding confidential data bit in the LSB of each pixel in the color image, it is possible to hide up to 3 bits per pixel.

The R, G, and B values of the white pixel are 255, 255, and 255, respectively. If confidential data bits 1, 1, and 1 are hidden in each of the R, G, and B components in this pixel, all 1s are inserted into each LSB of the R, G, and B components, so the values of R, G, and B are all 255. If confidential data 0, 0, and 0 are hidden in R, G, and B components, respectively, 0 is inserted into each LSB of R, G, and B components, so the values of R, G, and B are all 254. Therefore, when the confidential data bits are hidden in the R, G, and B components, the difference from the value of the original component becomes 0 or 1, and has an average difference of 0.5.

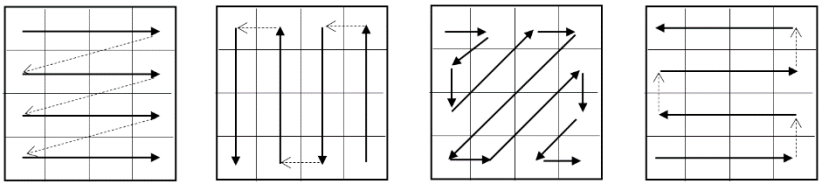
Since this difference cannot be recognized by the human eye, it is impossible to visually distinguish the stego-image with confidential data bits inserted from the original cover image. However, if the confidential data is hidden in the LSB, the security of the confidential data is weakened because the confidential data can be simply extracted from the stego-image.

## 3. Proposed technique using double encryption

When confidential data is hidden in the LSB of the image pixel, there is a problem in that the security of the confidential data is lowered because it is vulnerable to external attacks. In order to overcome this problem, this paper proposes a technique that strengthens the security of confidential data. In order to enhance the security of confidential data, the confidential data bits are encrypted as in Equation (1) using the pixel value of the cover image.

$$EnB_i = EnB_{i-1} \text{ XOR } B_i \quad (1)$$

In Equation (1), $B_i$ represents the (i)th bit in confidential data bit. $EnB_i$ represents the encrypted i-th confidential data bit. i has a value from 1 to w·h-1. In this case, w and h represent the number of horizontal pixels of the image and the number of vertical pixels of the image, respectively. In Equation (1), $EnB_0$ indicates that the LSB value of the 0-th pixel of the cover image is used as $EnB_0$. The encrypted confidential data bits generated by Equation (1) are encrypted confidential data to be hidden in the LSB of each pixel of the image using a spatial encryption technique. For secondary encryption, spatial encryption is performed. In order to perform spatial encryption, confidential data is hidden by defining various types of encryption order as shown in Figure 1. Figure 1 shows a spatial encryption pattern according to a spatial encryption key (SEK). Figure 1 shows four cases, but various other spatial encryption patterns can be defined.



(a) SEK=0 (b) SEK=1 (c) SEK=2 (d) SEK=3

**Figure 1. Spatial encryption pattern**

Figure 2 shows the cover image, the sego image, and the procedure for hiding confidential data in the cover image when the key value is SEK=0 in the proposed technique. (a) shows the cover image, and (b) shows the generated stego-image. (c) shows the procedure for generating a stego-image by hiding confidential data bits in the cover image. $C_i$(Pixel value of cover image) represents pixel value of the cover image scanned according to SEK=0. $LSB_i$(LSB of pixel value of cover image) indicates the LSB of each pixel value of $C_i$. It is assumed that confidential data bits($B_i$) hidden in the cover image are 010011000111000. $EnB_i$(Encrypted $B_i$) is the result of encryption of confidential data bits according to Equation (1), and this result becomes the LSB value of each corresponding pixel of the stego-image. $S_i$(Pixel value of stego-image) is a result of combining $EnB_i$ with the LSB of each $C_i$, which becomes the pixel values of the stego-image. Finally, if the stego-image is constructed according to the spatial encryption pattern using $S_i$, it becomes as shown in Figure (b). As shown in Figure 2, no encrypted secret data bit is hidden in the first pixel of the spatial encryption pattern. Therefore, one less encrypted confidential data bit than the total number of pixels of the cover image are hidden. And the generated stego-image is almost identical to the cover image, so that the difference from the cover image cannot be visually recognized. Therefore, the imperceptibility is satisfied.

| | | | | |
|---|---|---|---|---|
| 120 | 125 | 123 | 121 |
| 124 | 125 | 128 | 130 |
| 130 | 129 | 131 | 135 |
| 137 | 139 | 140 | 143 |

(a) Cover image

| | | | |
|---|---|---|---|
| 120 | 124 | 123 | 121 |
| 125 | 124 | 129 | 131 |
| 131 | 129 | 130 | 135 |
| 136 | 138 | 140 | 142 |

(b) Stego-image

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_i$(Pixel value of cover image) | 120 | 125 | 123 | 121 | 124 | 125 | 128 | 130 | 130 | 129 | 131 | 135 | 137 | 139 | 140 | 143 |
| $LSB_i$(LSB of pixel value of cover image) | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| $B_i$(Confidential data bits) | ↓ | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓↗ | ↓ |
| $EnB_i$(Encryped $B_i$) | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| $S_i$(Pixel value of stego-image) | 120 | 124 | 123 | 121 | 125 | 124 | 129 | 131 | 131 | 129 | 130 | 135 | 136 | 138 | 140 | 142 |

(c) the procedure for hiding confidential data in the cover image when the key value is SEK=0

**Figure. 2. Hiding confidential data in the proposed technique**

In the proposed technique, Equation (2) is used to extract the original confidential data bit from the stego-image.

$$Ex\_B_i = Ex\_EnB_{i-1} \text{ XOR } Ex\_EnB_i \quad (2)$$

The procedure for extracting the original confidential data bits from the stego-image using Equation (2) is shown in Figure 3. $S_i$(pixel value of stego-image) is a result of scanning the stego-image according to a pattern corresponding to a spatial encryption key value (SEK=0). Each LSB of $S_i$ becomes $Ex\_EnB_i$(Extracted $EnB_i$). $Ex\_B_i$(Extracted $B_i$) can be extracted from the $Ex\_EnB_i$ using Equation (2). As shown in Figure 3, confidential data bits($B_i$) hidden in the stego-image can be extracted without loss.

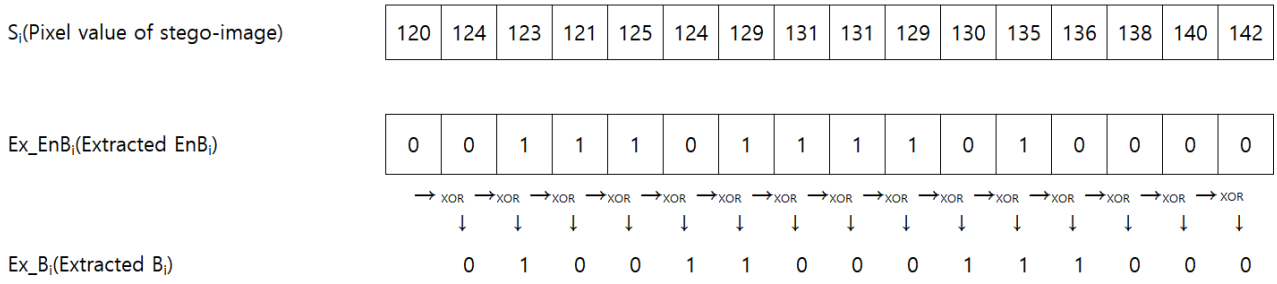



**Figure 3. The procedure for extracting confidential data bits from the stego-image**

## 4. Experimental results

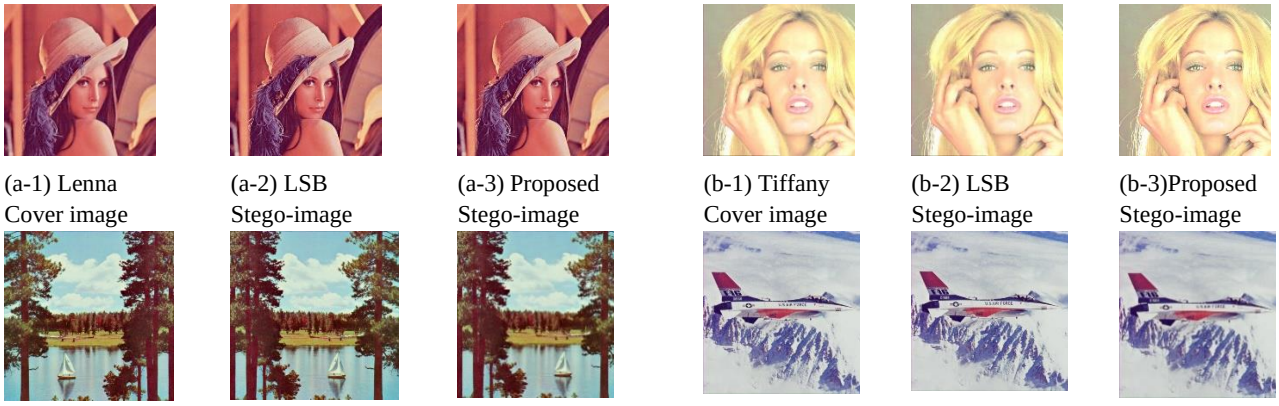
To test the effectiveness of the technique proposed in this paper, an experiment was performed using Lenna, Tiffany, sail-boat, and airplane of 512x512 size as cover images. The converted English abstract of this paper into binary was used as confidential data, and the confidential data was repeatedly hidden in the cover image. Confidential data was hidden in the R, G, and B planes of each cover image using Equation 1 and the spatial encryption key value SEK=0 in Figure 1.

Figure 4 shows the experimental result images. Figures a-1, b-1, c-1, d-1 are the cover images of Lenna, Tiffany, sail-boat, and airplane, respectively. The stego-images generated by conventional techniques that hide confidential data in the LSB of each cover image pixel are shown in Figures a-2, b-2, c-2, and d-2. Figures a-3, b-3, c-3, and d-3 show the stego-images generated by hiding confidential data in the LSB of each cover image with the proposed technique. As shown in Figure 4, the visual quality of the stego-image generated by hiding confidential data in the cover image using the proposed technique is very good. It can be seen that the difference between the generated stego-image and the cover image cannot be visually distinguished, so that imperceptibility is satisfied. Therefore, humans can not recognize whether confidential data is hidden in the stego-image. And from the stego-image, the original confidential data can be extracted without loss.

Table 1 shows the experimental results data in which confidential data was hidden in the images of Lenna, Tiffany, sail-boat, and airplane using the proposed technique. As shown in Table 1, when confidential data is hidden in the cover image using the proposed technique, the number of hidden data bits is almost the same as compared to the conventional LSB technique. However, in the proposed technique, confidential data is double-encrypted using encryption keys and hidden in the cover image, so the security of confidential data is greatly improved. As shown in Table 1, the PSNR values of the stego-images generated using the proposed technique were 51.146dB, 51.148dB, 51.142dB, and 51.132dB, respectively. When confidential data is hidden in the LSB of an image pixel, the ratio between the LSB of the image pixel and the confidential data bit coincides with 50%, and the PSNR value converges to 54.1411dB. As shown in Table 1, it can be seen that the existing

and proposed technique for hiding confidential data in the LSB of an image pixel have a value close to 54.1411dB.

In general, when the PSNR value is 40 dB or more, the human eye cannot distinguish the difference between the stego-image and the original cover image. It can be seen that the imperceptibility is satisfied because the quality of the stego-image in which confidential data is hidden with the proposed technique is excellent. In the proposed technique, since the double-encrypted confidential data is hidden in the cover image, the secret data hidden in the stego-image can be extracted only by knowing the encryption keys. Therefore, the proposed technique is a confidential data hiding technique with excellent stego-image quality and excellent security of confidential data.



(a-1) Lenna Cover image | (a-2) LSB Stego-image | (a-3) Proposed Stego-image | (b-1) Tiffany 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) airplane 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 |
|---|---|---|---|
| **Lenna** | **LSB** | **51.177** | **786,432** |
| | **Proposed** | **51.146** | **786,429** |
| **Tiffany** | **LSB** | **51.074** | **786,432** |
| | **Proposed** | **51.148** | **786,429** |
| **sail-boat** | **LSB** | **51.159** | **786,432** |
| | **Proposed** | **51.142** | **786,429** |
| **airplane** | **LSB** | **51.141** | **786,432** |
| | **Proposed** | **51.132** | **786,429** |

## 5. Conclusions

In this paper, in order to solve the security problem that occurs when confidential data is hidden in the LSB, we proposed a technique of encrypting confidential data using image pixel value and then spatially encrypting it again to hide it in the LSB of each pixel of the cover image. When confidential data is hidden in the cover

image by applying the proposed technique, the confidential data hidden in stego-image remains highly secure because confidential data can only be extracted using encryption keys. According to the proposed technique, confidential data can be extracted from the stego-image without loss.

The maximum number of bits that can be hidden in the color cover image is (W·H-1)x3 bits, and the visual quality of the stego-image is greater than 51.132dB. So, the difference between the original cover image and the stego-image cannot be visually distinguished. Therefore, the human eye cannot identify whether confidential data is hidden in the stego-image. The proposed data hiding technique can be effectively used in military and intellectual property protection applications.

## Acknowledgement

This paper was supported by the Sahmyook University Research Fund in 2020.

## 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, "An Effective Technique to Conceal Confidential Data in the LSB of Image", 2021 KIIECT (Korea Institute of Information, Electronics, and Communication Technology) Spring Conference, May, 2021.