International Journal of Internet, Broadcasting and Communication Vol.16 No.1 132-139 (2024)
http://dx.doi.org/10.7236/IJIBC.2024.16.1.132

IJIBC 24-1-16

An Improved Reversible Data Hiding Technique using Histogram Characteristics and Double Encryption Technique

Soo-Mok Jung

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

Abstract

In this paper, we proposed an effective technique that uses location-based encryption technique and spatial encryption technique to improve security vulnerabilities in previous reversible data hiding technique that can hide twice as much confidential data as the NSAS technique. If the proposed technique is applied to hide confidential data in an image, the same amount of confidential data can be hidden compared to the previous technique, but the security of confidential data is greatly enhanced. By hiding confidential data in an image using the proposed technique, high-quality stego-image can be generated, making it impossible to visually distinguish whether confidential data is hidden in the image. Additionally, confidential data can be restored from stego-image without loss, and the original cover image can also be restored without loss. Through experiments, it was confirmed that when confidential data is hidden by applying the proposed technique, the quality of the stego-image is maintained up to 39.73dB, and the security of the stego-image is greatly strengthened.

Keywords: *Reversible Data Hiding, Cover Image, Stego-image, NSAS, Encryption*

1. Introduction

Data hiding techniques have been used to hide confidential data requiring security in images. In the data hiding technique, confidential data is hidden in a cover image to create a stego-image in which the confidential data is hidden. People should not be able to visually detect whether confidential data is hidden in the stego-image. In order to satisfy these conditions, the quality of the stego-image must be very excellent [1][2].

In data hiding techniques, confidential data can be extracted from stego-images without loss. In particular, in the reversible data hiding technique, not only confidential data but also the original cover image can be extracted from the stego-image without loss. In these data hiding techniques, it is necessary to prevent malicious users from accessing confidential data, and even if they do, they cannot decrypt confidential data. Therefore, the image quality of the stego-image must be excellent and confidential data must be encrypted and hidden.

Manuscript Received: December. 24, 2023 / Revised: January. 13, 2024 / Accepted: January. 24, 2024
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Engineering, Sahmyook University, Korea

Most data hiding techniques proposed to improve the quality of stego-images are irreversible data hiding techniques. In other words, confidential data can be extracted from a stego-image without loss, but loss occurs when extracting the original cover image from the stego-image, so the restored cover image is not the same as the original cover image [3]. Reversible data hiding techniques, which can not only extract confidential data from stego-images without loss but also extract the original cover image without loss, are important in application fields such as military and medicine [4].

The NSAS technique, a reversible data hiding technique that hides confidential data by moving the histogram of the image, was proposed [2]. In the NSAS technique, peak point 1 and peak point 2 are examined in the histogram of the cover image. Additionally, the zero point 1 and zero point 2 closest to each peak point are examined and the pixel between the peak point and the zero point is moved by 1. Afterwards, confidential data is hidden in the pixel positions corresponding to peak point 1 and peak point 2. Therefore, the maximum number of bits of confidential data to be hidden is equal to the sum of the number of pixels at peak point 1 and peak point 2 of the cover image histogram.

The Adjacent Pixel Difference (APD) technique, which is an improved version of the NSAS technique, has been proposed [3]. In the APD technique, a pixel value difference sequence consisting of pixel value differences between adjacent pixels is generated from a cover image. Afterwards, the histogram for the pixel value difference sequence is obtained and then the confidential data is hidden similar to the NSAS technique.

A technique to hide encrypted confidential data using the bit plane swapping technique was proposed [4], and a technique of moving the histogram by modifying the improved multilevel histogram for pixel difference was used to hide confidential data. A technique for hiding has been proposed [5].

Our research team published papers [6-8] and submitted patents [9, 10] on techniques to improve the performance of the APD technique by using the characteristics of adjacent pixels, locality existing in adjacent pixels, and encryption techniques. A new reversible data hiding technique of prediction-error expansion based on a multilayer perceptron was proposed [11].

Additionally, our research team proposed a technique that can hide twice the amount of confidential data hidden in the NSAS technique [12].

In this paper, in order to improve the low security of the previous technique, we proposed a technique to enhance security by applying histogram characteristics and double encryption techniques to hiding confidential data. If confidential data is hidden using the proposed technique, the image quality of the stego-image is very good, and confidential data and the original cover image can be extracted from the stego-image without loss.

The structure of this paper is as follows. Chapter 2 describes related research. Chapter 3 explains the proposed technique. The experimental results are described in Chapter 4, and the conclusion is described in Chapter 5

2. Related Works

In the NSAS technique, which hides confidential data in a cover image by shifting the histogram, a histogram of the cover image is created in the first step to hide confidential data in the cover image.

In the second step, the left and right pixel values of the two-pixel values corresponding to the two highest frequencies in the histogram are determined as Peak Point Left (PP_L) and Peak Point Right (PP_R) respectively. The first pixel value with a frequency of 0 towards the left from the PP_L is determined as Closest Zero Point

Left (CZP_L), and the first pixel value with a frequency of 0 towards the right from the PP_R is determined as Closest Zero Point Right (CZP_R).

In the third step, pixel values that are greater than CZP_L and less than PP_L are increased by -1, and pixel values that are greater than PP_R and less than CZP_R are increased by +1.

In the fourth step, confidential data is hidden in the pixels of the cover image with pixel values of PP_L and PP_R. If the confidential data to be hidden is 0, the PP_L and PP_R values do not change. That is, it increases by -0, +0. If the confidential data to be hidden is 1, the PP_L and PP_R values are increased by -1 and +1. In the NSAS technique, the histogram is shifted like this to create a stego-image in which confidential data is hidden.

The procedure for restoring confidential data and cover images from stego-images in the NSAS technique is as follows. If the pixel value of the stego-image is greater than or equal to CZP_L and less than or equal to PP_L-2, the pixel value is increased by +1. If the pixel value of the stego-image is greater than or equal to PP_R+2 and less than or equal to CZP_R, the pixel value is increased by -1. If the pixel value of the stego-image is PP_L-1, confidential data 1 is extracted and the pixel value is increased by +1. If the pixel value of the stego-image is PP_L, confidential data 0 is extracted and the pixel value is increased by +0. If the pixel value of the stego-image is PP_R+1, confidential data 1 is extracted and the pixel value is increased by -1. If the pixel value of the stego-image is PP_R, confidential data 0 is extracted and the pixel value is increased by -0. In this way, confidential data and the original cover image can be extracted from the stego-image without loss.

The procedure of the previous technique, which hides twice the amount of confidential data hidden in the NSAS technique, is as follows. In the first step, a histogram for the cover image that hides confidential data is created.

In the second step, find PP_L, PP_R, CZP_{L0}, CZP_{L1}, CZP_{L2}, CZP_{R0}, CZP_{R1}, and CZP_{R2} in the histogram. Here, CZP_{L0} and CZP_{R0} are the same as CZP_L and CZP_R of the NSAS technique. In the histogram, the first pixel value with a frequency of 0 to the left of CZP_{L0} is set to CZP_{L1}, and the second pixel value with a frequency of 0 is set to CZP_{L2}. And in the histogram, the first pixel value with a frequency of 0 to the right of CZP_{R0} is set to CZP_{R1}, and the second pixel value with a frequency of 0 is set to CZP_{R2}. In this technique, there must be three consecutive pixel values with a frequency of 0 to the left of the PP_L, including CZP_{L0}, in the histogram of the cover image. Additionally, there must be three consecutive pixel values with a frequency of 0 to the right of the PP_R, including CZP_{R0}.

In the third step, if the pixel value of the cover image is greater than or equal to CZP_{L0}+1 and at the same time less than or equal to PP_L-1, the pixel value is increased by -3. Likewise, if the pixel value of the cover image is greater than or equal to PP_R+1 and at the same time less than or equal to CZP_{R0}-1, the pixel value is increased by +3.

In the fourth step, confidential data is hidden in the pixels of the cover image with pixel values of PP_L and PP_R. If the confidential data to be hidden is 00, the PP_L or PP_R value is not increased. That is, it is increased by -0 or +0. If the confidential data to be hidden is 01, the PP_L or PP_R value is increased by -1 or +1. If the confidential data to be hidden is 10, the PP_L or PP_R value is increased by -2 or +2. If the confidential data to be hidden is 11, the PP_L or PP_R value is increased by -3 or +3. In this way, the histogram of the cover image is shifted to create a stego-image, which is an image in which confidential data is hidden in the cover image. In this technique, the procedure for restoring confidential data and cover image from stego-image is as follows. If the pixel value of the stego-image is greater than or equal to CZP_{L2} and at the same time less than or equal to PP_L-4, the pixel value is increased by +3. If the pixel value of the stego-image is greater than or equal to PP_R+4 and at the same time less than or equal to CZP_{R2}, the pixel value is increased by -3.

If the pixel value of the stego-image is PP_L or PP_R, confidential data 00 is extracted and the pixel value is increased by +0 or -0. If the pixel value of the stego-image is PP_L-1 or PP_R+1, confidential data 01 is extracted and the pixel value is increased by +1 or -1. If the pixel value of the stego-image is PP_L-2 or PP_R+2, confidential data 10 is extracted and the pixel value is increased by +2 or -2. If the pixel value of the stego-image is PP_L-3 or PP_R+3, confidential data 11 is extracted and the pixel value is increased by +3 or -3. In this way, confidential data and the original cover image can be extracted from the stego-image without loss. This technique can hide twice the amount of confidential data hidden in the NSAS technique, but because confidential data can be easily extracted from stego-image, this technique is vulnerable to security.

3. Proposed Technique

In this paper, to solve the low security problem of previous technique, we proposed a technique to hide confidential data using the characteristics of the histogram and double encryption technique. The procedure of the proposed technique is as follows.

Step 1: Create a histogram for the cover image that will hide confidential data.

Step 2: Find PP_L, PP_R, CZP_{L0}, CZP_{L1}, CZP_{L2}, CZP_{R0}, CZP_{R1}, CZP_{R2} in the histogram. Here, PP_L, PP_R, CZP_{L0}, CZP_{L1}, CZP_{L2}, CZP_{R0}, CZP_{R1}, and CZP_{R2} are the same as the values in the NSAS technique

Step 3: Apply equations (1) to (3) to each pixel of the cover image to generate a histogram shifted image (HSI). P used in equations (1) to (3) represents the cover image pixel. Histogram shifted Image Pixel (HSIP) represents the pixel of the resulting image (HSI) created by shifting the histogram of the cover image.

$$\text{if } (CZP_{L0}+1 \le P \le PP_L-1) \text{ HSIP=P-3} \tag{1}$$

$$\text{else if } ((PP_R+1 \le P \le CZP_{R0}-1)) \text{ HSIP=P+3} \tag{2}$$

$$\text{else HSIP=P} \tag{3}$$

Step 4.1: Determine the pattern for spatially encrypting confidential data. In the process of hiding confidential data in the cover image, the confidential data is spatially encrypted and hidden according to a defined spatial encryption pattern. Figure 1 shows spatial encryption patterns can be defined and used in various ways. The value representing the spatial encryption pattern is used as the encryption key k.

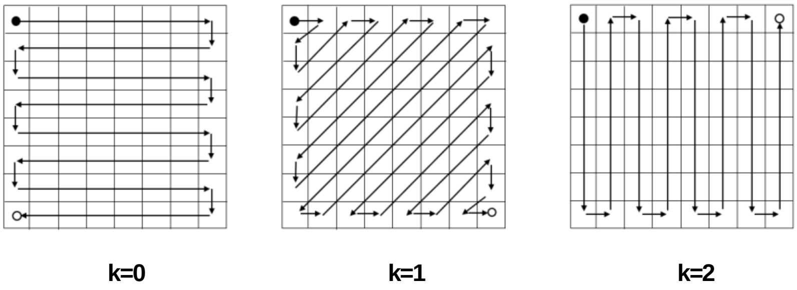


Figure 1. Examples of patterns for spatial encryption

Step 4.2: The HSI is sequentially scanned according to a pattern for spatially encrypting and hiding confidential data. The coordinates (X, Y) of the scanned pixel and the encryption keys m and n are applied to Equation

(4) to generate i. i is used to encrypt confidential data. In equation (4), mod represents the remainder operation, and the bar represents the absolute value operation symbol. After that, Equations (5) to (12) are sequentially executed. CD used in the equation represents 2-bit confidential data, and SIP represents the pixel of the stego-image. XOR used in equations (5)-(18) represents exclusive OR operation.

As shown in Equations (4) to (12), confidential data is encrypted. Afterwards, the encrypted confidential data is spatially encrypted according to the pattern corresponding to the encryption key k value in step 4.1 to generate a stego-image consisting of the final HSIP. Therefore, the security of the proposed technique is greatly improved over the previous technique.

$$i= (|X-m|+|Y-n|) \bmod 4 \tag{4}$$

$$\text{if} ((HSIP==PP_L) \text{ AND } ((CD \text{ XOR } i)==00)) \ HSIP=HSIP \tag{5}$$

$$\text{else if} ((HSIP==PP_L) \text{ AND } ((CD \text{ XOR } i)==01)) \ HSIP=HSIP-1 \tag{6}$$

$$\text{else if} ((HSIP==PP_L) \text{ AND } ((CD \text{ XOR } i)==10)) \ HSIP=HSIP-2 \tag{7}$$

$$\text{else if} ((HSIP==PP_L) \text{ AND } ((CD \text{ XOR } i)==11)) \ HSIP=HSIP-3 \tag{8}$$

$$\text{else if} ((HSIP==PP_R) \text{ AND } ((CD \text{ XNOR } i)==00)) \ HSIP=HSIP \tag{9}$$

$$\text{else if} ((HSIP==PP_R) \text{ AND } ((CD \text{ XNOR } i)==01)) \ HSIP=HSIP+1 \tag{10}$$

$$\text{else if} ((HSIP==PP_R) \text{ AND } ((CD \text{ XNOR } i)==10)) \ HSIP=HSIP+2 \tag{11}$$

$$\text{else if} ((HSIP==PP_R) \text{ AND } ((CD \text{ XNOR } i)==11)) \ HSIP=HSIP+3 \tag{12}$$

The procedure for extracting confidential data and the original cover image from the stego-image in the proposed technique is as follows.

$$\text{if} (CZP_{L2} \leq P < PP_L-3) \ P=HSIP+3; \text{ else if} ((PP_R+3 < P \leq CZP_{R2}) \ P=HSIP-3 \tag{13}$$

$$\text{else } P=HSIP; \ \ i= (|X-m|+|Y-n|) \bmod 4 \tag{14}$$

$$\text{if} (HSIP==PP_L) \ \{CD=00 \text{ XOR } i, P=HSIP\}; \text{ else if} (HSIP==PP_L-1) \ \{CD=01 \text{ XOR } i, P=HSIP+1\} \tag{15}$$

$$\text{else if} (HSIP==PP_L-2) \ \{CD=10 \text{ XOR } i, P=HSIP+2\}; \text{ else if} (HSIP==PP_L-3) \ \{CD=11 \text{ XOR } i, P=HSIP+3\} \tag{16}$$

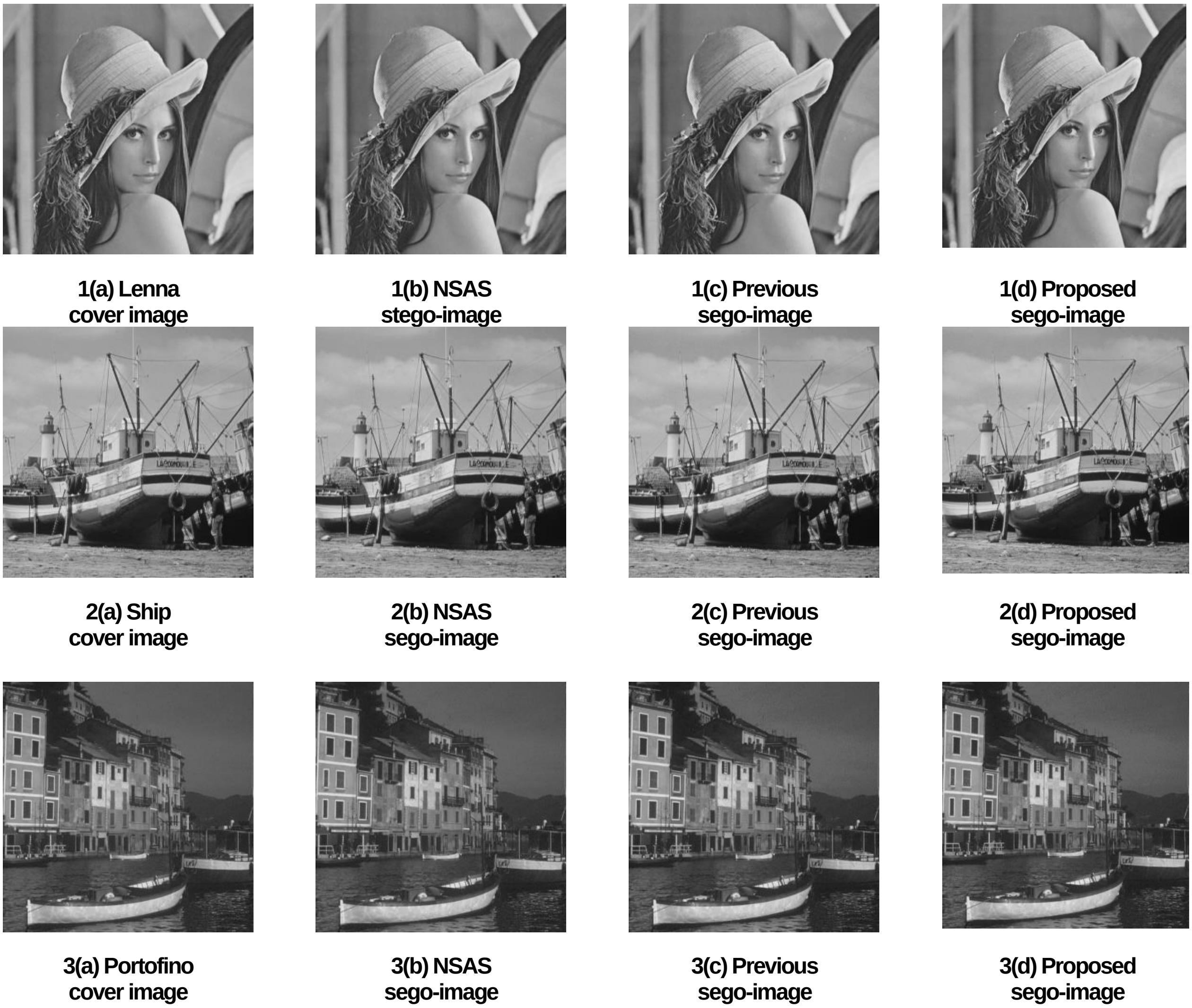
$$\text{else if} (HSIP==PP_R) \ \{CD=00 \text{ XNOR } i, P=HSIP\}; \text{ else if} (HSIP==PP_R+1) \ \{CD=01 \text{ XNOR } i, P=HSIP-1\} \tag{17}$$

$$\text{else if} (HSIP==PP_R+2) \ \{CD=10 \text{ XNOR } i, P=HSIP-2\}; \text{ else if} (HSIP==PP_R+3) \ \{CD=11 \text{ XNOR } i, P=HSIP-3\} \tag{18}$$

4. Experimental Results

The performance of the technique proposed in this paper was evaluated using 512x512 gray scale images Lena, ship, and Portofino as cover images. The cover images used are the same as the cover images used to evaluate the performance of previous technique. The confidential data used in the experiment was the result of converting the abstract of this paper into binary, and this was repeatedly hidden in the cover image to create a stego-image. The encryption keys used in the experiment are as follows. k=0, m=1, n=2.

Figure 2 shows the cover image and experiment result images. In Figure 2, the first images(1(a), 2(a), 3(a)) are the cover images, and the second images(1(b), 2(b), 3(b)) are stego-images created by applying the NSAS technique to hide confidential data in the cover image. The third images(1(c), 2(c), 3(c)) are stego-images created by hiding confidential data in the cover image using previous technique. The fourth images(1(d), 2(d), 3(d)) are stego-images created by hiding confidential data in the cover image using the proposed technique. As shown in Figure 2, the visual quality of the stego-image generated by hiding confidential data in the cover image using the technique proposed in this paper is so excellent that the cover image and the stego-image cannot be visually distinguished. Therefore, it is almost impossible to recognize whether confidential data is hidden in a stego-image.



1(a) Lenna cover image

1(b) NSAS stego-image

1(c) Previous sego-image

1(d) Proposed sego-image

2(a) Ship cover image

2(b) NSAS sego-image

2(c) Previous sego-image

2(d) Proposed sego-image

3(a) Portofino cover image

3(b) NSAS sego-image

3(c) Previous sego-image

3(d) Proposed sego-image

Figure 2. Cover images & stego-images

Using the confidential data extraction method of the proposed technique, the confidential data hidden in the stego-image can be completely extracted without loss, and the original cover image can also be restored from the stego-image without loss.

The image quality of the stego-image measured in experiments performed using each cover image and the number of confidential data bits hidden in the stego-image are shown in Table 1. As shown in <Table 1>, the number of hidden data bits in the proposed technique is the same as the previous technique. However, since confidential data is double encrypted and hidden in the cover image as in steps 3 and 4, so it has much higher security than previous technique. Additionally, the minimum PSNR value of the stego-image is 38.65dB and the maximum PSNR value is 39.73dB. Therefore, the difference between the cover image and the stego-image cannot be visually recognized.

Table 1. Experimental results

Image	Technique	PSNR	Hidden data bits	Security
Lenna	NSAS	48.18	5,701	Low
	Previous	38.66	11,402	Low
	Proposed	38.65	11,402	High
ship	NSAS	49.33	10,546	Low
	Previous	39.75	21,092	Low
	Proposed	39.73	21,092	High
Portofino	NSAS	48.22	9,564	Low
	Previous	38.70	19,128	Low
	Proposed	38.69	19,128	High

5. Conclusions

We proposed a technique to solve the weak security problem of previous techniques. The proposed technique encrypts the hidden confidential data and then spatially encrypts the encrypted confidential data when it is hidden in the cover image to generate a stego-image. As shown in Figure 2, if confidential data is double-encrypted and hidden in the cover image using the proposed technique to generate a stego-image, the PSNR value of the stego-image is up to 39.73dB, making it visually indistinguishable from the original cover image. Therefore, humans not only cannot recognize whether confidential data is hidden in a stego-image, but also cannot obtain double-encrypted confidential data from a stego-image. By applying the encryption key to the confidential data extraction and original cover image restoration method of the proposed technique, confidential data hidden in the stego-image can be extracted without loss and the original cover image can be restored from the stego-image without loss. Therefore, the proposed technique is an excellent technique that can effectively hide large amounts of confidential data in the cover image in medical and military fields that require high security and 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] 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.
DOI: https://doi.org/10.1016/j.dsp.2009.10.025

[4] S. Singh and S. Sharma, “Data Hiding using difference between adjacent pixels and bit plane swapping,” International Journal of Engineering and Computer Science, Vol. 3, Issue 6, pp. 6770-6778, June 2014. DOI: https://doi.org/10.18535/ijecs/v10i12.4640

[5] K. M. Hung, C. T. Hsieh, T. W. Chen, and L. M. Chen, “Reversible Data Hiding Based on Improved Multilevel Histogram Modification of Pixel Differences,” Journal of Applied Science and Engineering, Vol. 19, No. 4, pp. 489-495, 2016. DOI: https://doi.org/10.6180/jase.2016.19.4.12

[6] S. M. Jung, “An advanced reversible data hiding algorithm based on the similarity between neighboring pixels,” Journal of The Korea Society of Computer and Information, Vol. 21, No. 2, pp. 33–42, February 2016. DOI: https://doi.org/10.9708/jksci.2016.21.2.033

[7] S. M. Jung and B. W. On, “Reversible data hiding algorithm using spatial locality and the surface characteristics of image,” Journal of The Korea Society of Computer and Information, Vol. 21, No. 8, pp. 1-12, Aug. 2016. DOI: https://doi.org/10.9708/jksci.2016.21.8.001

[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. DOI: https://doi.org/10.17661/jkiiect.2020.13.6.503

[9] S. M. Jung, “A Method for Data Hiding Based on Pixel Value Predictions, a Method for Data Watermarking Using It, and an Apparatus for Data Hiding,” Korea Patent-Registration Number 1017645300000, 27 July 2017.
http://www.kipris.or.kr.

[10] S. M. Jung and B. W. On, “A Method for Reversible Data Hiding Based on Pixel Value Prediction According to Spatial Locality and Surface Characteristics, a Method for Reversible Watermarking Using It, and an Apparatus for Reversible Data Hiding, Reversible Watermarking,” Korea Patent-Registration Number 1018754010000, 02 July 2018.
http://www.kipris.or.kr.

[11] C. C. Hung, C. C. Lin, H. C. Wu, and C. W. Lin, “A Study on Reversible Data Hiding Technique Based on Three-Dimensional Prediction-Error Histogram Modification and a Multilayer Perceptron,” Applied Scences, Vol. 12, Issue 5, pp. 1~23, Dec. 2022. DOI: https://doi.org/10.3390/app12052502

[12] S. M. Jung, “An Improved Reversible Data Hiding Technique using Histogram Characteristics of Image,” International Journal of Internet, Broadcasting and Communication, Vol. 15, No. 1, pp.63-69, Feb. 2023. DOI: https://doi.org/10.7236/IJIBC.2023.15.1.63