International Journal of Internet, Broadcasting and Communication Vol.15 No.1 63-69 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.1.63

IJIBC 23-1-8

An Improved Reversible Data Hiding Technique using Histogram Characteristics of Image

Soo-Mok Jung

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

Abstract

In this paper, we propose an effective reversible data hiding technique that increases the confidential data hiding amount of the NSAS technique itself by utilizing the characteristics of image. The proposed technique shifts the histogram using multiple zeros of the histogram and hides 2 bits of confidential data at each peak point. Using the proposed technique, the amount of confidential data that can be hidden is doubled compared to the existing technique, and high-quality stego-image can be created. Confidential data can be restored without loss from the stego- image, and the original cover image can be restored without loss. Through experiments, it was confirmed that the proposed technique can hide twice as much confidential data than the existing technique, and the image quality of the stego-image is very good with a maximum of 39.75dB.

Keywords: *cover image, stego-image, data hiding, NSAS, reversible data hiding*

1. Introduction

Data hiding techniques for embedding confidential data in cover media such as images and videos have been developed. In data hiding techniques, a stego-image is created by hiding confidential data in a cover image. And confidential data can be extracted from the stego-image without loss. In the data hiding technique, the quality of the stego-image in which confidential data is hidden must be so good that people cannot visually recognize whether confidential data is hidden in the stego-image [1][2].

Most of the data hiding techniques proposed to improve the quality of stego-images are irreversible data hiding techniques. That is, the restored cover image obtained after extracting confidential data from the stego-image is distorted and does not match the original cover image [3].

A reversible data hiding technique in which the restored cover image obtained after extracting secret data from the stego-image completely mat3ches the original cover image is very important in applications such as medicine, military, and digital libraries [4].

Ni et al. proposed a reversible data hiding technique (NSAS) that uses image histograms [2]. The NSAS technique examines the peak point and zero-point pair in the histogram of the cover image and shifts the pixels between (peak point, zero-point). Then, confidential data is embedded at the pixel location corresponding to the peak point. Therefore, the maximum number of bits hided is limited to the number of pixels at the peak

Manuscript Received: January. 25, 2023 / Revised: February. 2, 2023 / Accepted: February. 4, 2023
Corresponding Author: jungsm@syu.ac.kr
Tel: +82-2-3399-1786, Fax: +82-2-3399-1791
Professor, Division of Computer Engineering, Sahmyook University, Korea

point of the histogram of the cover image.

Li et al. proposed an Adjacent Pixel Difference (APD) technique that improved the NSAS technique. [3] In the APD technique, a pixel value difference sequence composed of differences in pixel values between adjacent pixels is generated from a cover image. Then, after obtaining the histogram of the pixel value difference sequence, confidential data is embedded like the NSAS technique. And various techniques that improved the APD technique were proposed by our research team. [4]-[8]

In this paper, we proposed a technique to improve the amount of confidential data hidden in the NSAS technique itself by utilizing the characteristics of image.

The organization of this paper is as follows. In Section 2, NSAS technique is described. In Section 3, the proposed technique is described. The experimental results are described in Section 4. In Section 5, the conclusion is described.

2. NSAS Technique

Ni et al. proposed a data hiding technique (NSAS) using histogram shift. In this technique, the histogram of the original cover video is first obtained. In the acquired histogram, among the first and second most frequent pixel values, the left value is determined as PP_L (peak point left) and the right value as PP_R (peak point right).

The closest pixel value having a value of 0 at the left side of the PP_L is determined as CZP_L (closest zero point right). The closest pixel value having a value of 0 at the right side of the PP_R is determined as CZP_R (closest zero point right).

While scanning the image from left to right and top to bottom, if the pixel value has a value between CZP_L and PP_L, the pixel value is decreased by 1 (the histogram is moved to the left by 1). If the pixel value is between PP_R and CZP_R, the pixel value is increased by 1 (the histogram is moved to the right by 1). After that, if the pixel value is PP_L or PP_R, confidential data is hidden in the corresponding pixel as follows. When confidential data 0 is hidden in a pixel whose pixel value is PP_L, the pixel value is not changed, and when secret data 1 is hidden, the pixel value is decreased by 1. Similarly, when secret data 0 is hidden in a pixel having a PP_R pixel value, the pixel value is not changed, and when secret data 1 is hidden, the pixel value is increased by 1.

The pixel values created in this way become the pixel values of the stego-image. Therefore, the maximum number of confidential data bits hidden in the stego-image is limited to the sum of the number of pixels having PP_L and PP_R values in the cover image. The data hiding procedure of the NSAS technique consists of four steps as follows.

Step 1. Create a histogram of the cover image.

Step 2. Determine the PP_L, CZP_L, PP_R, and CZP_R.

Step 3. While scanning the cover image from left to right and from top to bottom, Equations (1) to (3) are applied to each pixel of the cover image to generate a histogram-shifted image. Here, CP represents the pixel value of the cover image, and HP represents the pixel value of the histogram-shifted image.

$$\text{if } (CZP_L<CP<PP_L) \; HP=CP-1 \quad \ldots\ldots (1)$$

$$\text{else if } (PP_R<CP<CZP_R) \; HP=CP+1 \quad \ldots\ldots (2)$$

$$\text{else } HP=CP \quad \ldots\ldots (3)$$

Step 4. While scanning the histogram-shifted image, which is the result of step 3, from left to right and top to bottom, secret data is hidden in pixels having PPL and PPR values as shown in Equations (4) to (8) to create a stego-image. Here, SP represents the pixel value of the stego-image.

if ((HP==PP_L) AND (confidential data==0)) SP=HP…………………..............(4)

else if ((HP==PP_L) AND (confidential data==1)) SP=HP-1……………….... (5)

else if ((HP==PP_R) AND (confidential data==0)) SP=HP…………………....(6)

else if ((HP==PP_R) AND (confidential data==1)) SP=HP+1………………....(7)

else SP=HP………………………………………………………………(8)

Equations (9) to (15) are used to extract confidential data from the stego-image and restore the original cover image. While scanning the stego-image from left to right and top to bottom, Equations (9) to (15) are applied to each pixel of the stego-image to extract confidential data and restore the original cover image.

if (CZP_L<=SP<PP_L -1) CP=SP+1……………………………………………..(9)

else if (SP==PP_L -1) {CP=SP+1, confidential data=1}…...………………....(10)

else if (SP==PP_L) {CP=SP, confidential data=0} …………………………..(11)

else if (SP==PP_R) {CP=SP, confidential data=0} …………..………………(12)

else if (SP==PP_R +1) {CP=SP-1, confidential data=1} ……..………………(13)

else if (PP_R+1<SP<=CZP_R) CP=SP-1………………………………………(14)

else CP=SP……………………………………………………………..(15)

3. Proposed Technique

In the proposed technique, the following procedure is performed to hide twice as much confidential data than the conventional technique by shifting the histogram using the characteristics of the image.

Step 1. Create a histogram of the cover image.

Step 2. Determine PP_L, PP_R, CZP_{L1}, CZP_{L2}, CZP_{L3}, CZP_{R1}, CZP_{R2}, CZP_{R3}.
Here, CZP_{L1} and CZP_{R1} are the same as CZP_L and CZP_R in the NSAS technique. In the histogram, the first 0 value on the left of CZP_{L1} is determined as CZP_{L2}, and the second 0 value is determined as CZP_{L3}. Similarly, in the histogram, the first 0 value on the right side of CZP_{R1} is determined as CZP_{R2}, and the second 0 value is determined as CZP_{R3}. In the proposed technique, there must be three consecutive 0s to the left of CZP_{Li}, including CZP_{Li}, and three consecutive 0s to the right of CZP_{Ri}, including CZP_{Ri}, in the histogram of the cover image. For convenience, it is assumed that this condition is satisfied when i = 3.

Step 3. While scanning the cover image from left to right and top to bottom, Equations (16) to (18) are applied to each pixel of the cover image to create an image with histogram shifted.

if ((CZP_{L3}<CP<CZP_{L2}) OR (CZP_{L2}<CP<CZP_{L1}) OR (CZP_{L1}<CP<PP_L)) HP=CP-3…………...(16)

else if ((PP_R<CP<CZP_{R1}) OR (CZP_{R1}<CP<CZP_{R2}) OR (CZP_{R2}<CP<CZP_{R3})) HP=CP+3……..(17)

else HP=CP………………………………………………………………………..….(18)

Step 4. While scanning the histogram-shifted image from left to right and top to bottom, a stego-image is created by hiding 2 bits of confidential data in each pixel having PP_L and PP_R values using Equations (19) to (27).

if ((HP==PP_L) AND (confidential data==00)) SP=HP……(19)

else if ((HP== PP_L) AND (confidential data==01)) SP=HP-1……(20)

else if ((HP==PP_L) AND (confidential data==10)) SP=HP-2……(21)

else if ((HP==PP_L) AND (confidential data==11)) SP=HP-3……(22)

else if ((HP==PP_R) AND (confidential data==00)) SP=HP……(23)

else if ((HP==PP_R) AND (confidential data==01)) SP=HP+1……(24)

else if ((HP==PP_R) AND (confidential data==10)) SP=HP+2……(25)

else if ((HP==PP_R) AND (confidential data==11)) SP=HP+3……(26)

else SP=HP……(27)

As shown in equations (19) to (27), since the proposed technique hides 2 bits of confidential data in each pixel having PP_L and PP_R values, it can hide twice as much confidential data as the existing NSAS technique.

In order to extract confidential data from the stego-image and restore the original cover image, Equations (28) to (38) are applied to each pixel of the stego-image while scanning the stego-image from left to right and top to bottom. Applying Equations (28) to (38) to the stego-image, the confidential data is fully extracted and the cover image is restored without distortion.

if ((CZP_{L3}-3<SP<CZP_{L2}-3) OR (CZP_{L2}-3<CP<CZP_{L1}-3) OR (CZP_{L1}-3<CP< PP_L-3)) CP=SP+3……(28)

else if (SP==PP_L -3) {CP=SP+3, confidential data=11} ……(29)

else if (SP==PP_L -2) {CP=SP+2, confidential data=10} ……(30)

else if (SP==PP_L -1) {CP=SP+1, confidential data=01} ……(31)

else if (SP==PP_L) {CP=SP, confidential data=00} ……(32)

else if (SP==PP_R) {CP=SP, confidential data=00} ……(33)

else if (SP==PP_R +1) {CP=SP-1, confidential data=01} ……(34)

else if (SP==PP_R +2) {CP=SP-2, confidential data=10} ……(35)

else if (SP==PP_R +3) {CP=SP-3, confidential data=11} ……(36)

else if ((PP_R+3<SP<CZP_{R1}+3) OR (CZP_{R1}+3<CP<CZP_{R2}+3) OR (CZP_{R2}+3<CP< CZP_{R3}+3)) CP=SP-3...(37)

else CP=SP……(38)

The proposed technique is valid only when there are three consecutive 0s on the left side, including CZP_{Li}, and three consecutive zeros on the right side, including CZP_{Ri}, in the histogram of the cover image.

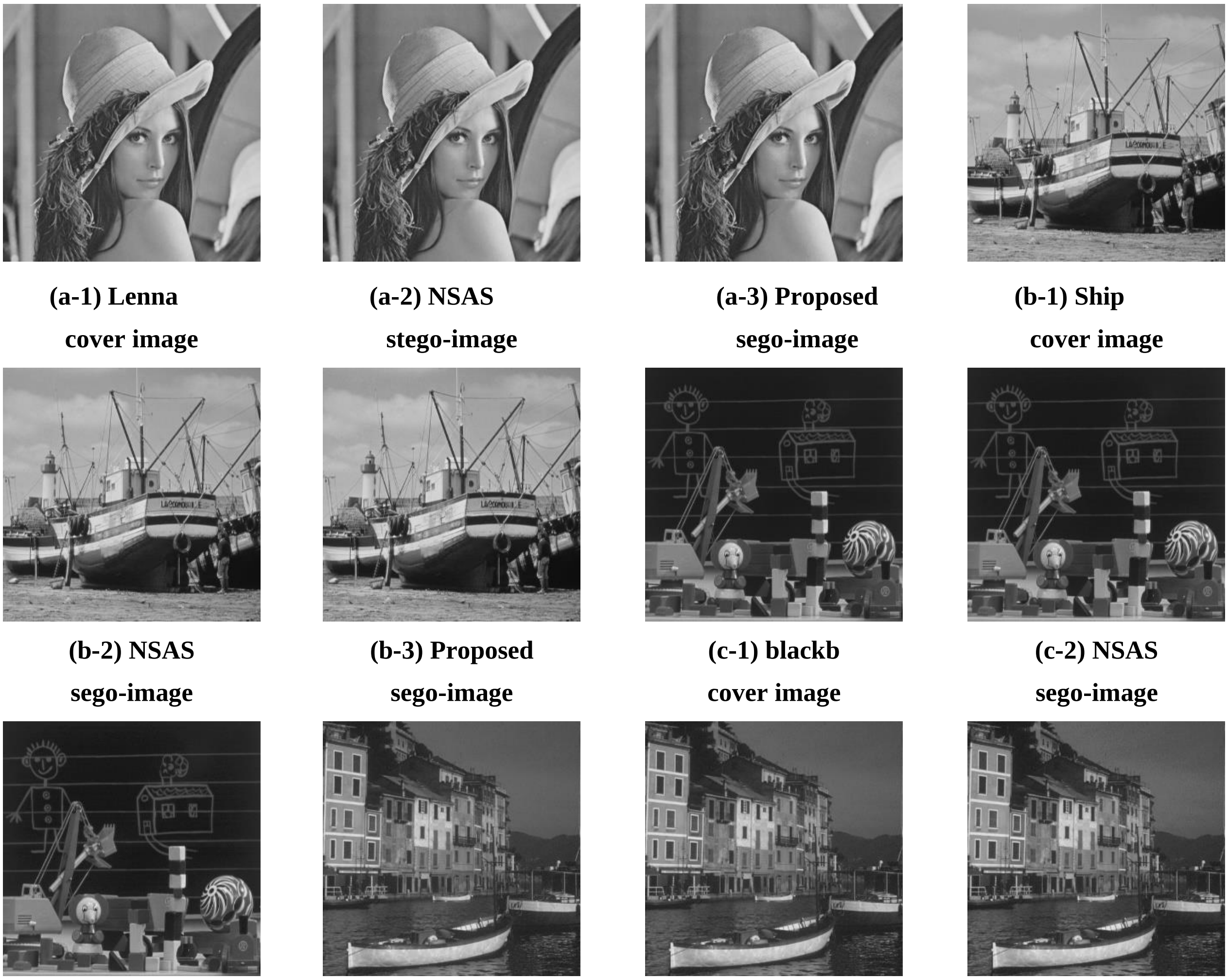
4. Experimental Results

To evaluate the performance of the technique proposed in this paper, experiments were performed using 512x512 gray scale images as cover images. Lena, ship, blackb, and Portofino images were used in the experiments. The result of converting the abstract of this paper into binary was used as confidential data, which was repeatedly concealed in the cover image to generate stego-image.

The images of the results of the experiments are shown in Figure 1. The cover images are shown in Figure 1(1). The stego-images generated by hiding confidential data in the cover images using the NSAS technique are shown in Figure 1(2). The stego-images generated by hiding confidential data in the cover images with the technique proposed in this paper are shown in Figure 1(3). As shown in Figure 1, it can be seen that the visual quality of the stego-images generated by hiding confidential data in the cover images using the proposed technique is very good. Therefore, since the human eye cannot visually distinguish between the cover images and the stego-images, it is impossible to recognize whether confidential data is hidden in the stego-images.

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

Table 1 is the numerical data of the experimental results performed with Lenna, ship, blackb, and Portofino as cover images. As shown in Table 1, the proposed technique can increase the confidential data hiding amount of the existing NSAS technique itself by 100%. And the PSNR values of the stego-images generated by concealing confidential data with the proposed technique were 38.66dB, 39.75dB, 39.01dB, and 38.70dB, respectively. Because the proposed technique generates the stego-images with very high visual quality, the human eye cannot recognize the difference between stego-images and original cover images.



(a-1) Lenna cover image

(a-2) NSAS stego-image

(a-3) Proposed sego-image

(b-1) Ship cover image

(b-2) NSAS sego-image

(b-3) Proposed sego-image

(c-1) blackb cover image

(c-2) NSAS sego-image

(c-3) Proposed sego-image

(d-1) Portofino cover image

(d-2) NSAS sego-image

(d-3) Proposed sego-image

Figure 1. Cover images & stego-images

Table 1. Experimental results

Image	Technique	PSNR	Hidden bits	Hidden bit growth rate(%)
Lenna	NSAS	48.18	5,701	
	Proposed	38.66	11,402	100%
ship	NSAS	49.33	10,546	
	Proposed	39.75	21,092	100%
blackb	NSAS	48.45	34,479	
	Proposed	39.01	68,958	100%
Portofino	NSAS	48.22	9,564	
	Proposed	38.70	19,128	100%

5. Conclusions

The proposed technique increases the confidential data hiding amount of the NSAS technique by 100% by moving the histogram using the characteristics of the image. The proposed technique shifts the histogram of cover image using multiple zeros of the histogram and hides 2-bits of confidential data at each peak point. As shown in Figure 1, it can be seen that the visual quality of the stego-images generated by hiding confidential data in the cover images using the proposed technique is very good. The PSNR value of the stego-image generated using the proposed technique is up to 39.75 dB, so the difference between the original cover image and the stego-image is visually indistinguishable.

Using the confidential data extraction scheme of the proposed technique, confidential data hidden in stego-image can be extracted without loss. Also, the original cover image can be restored without loss from the stego-image using the cover image recovering scheme of the proposed technique.

For this reason, the proposed reversible data hiding technique is an excellent technique for quickly and effectively concealing large amounts of confidential data in medical and military images requiring 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] Jung, S.M. “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

[5] S. M. Jung, 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

[6] Jung, S.M. Sahmyook University Industry-Academic Cooperation. 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.

[7] Jung, S.M.; On, B.W. Sahmyook University Industry-Academic Cooperation. 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.

[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