Lossless Data Hiding Based on Histogram Modification of Difference Images*

Sang-Kwang Lee[1], Young-Ho Suh[1], and Yo-Sung Ho[2]

[1] Electronics and Telecommunications Research Institute (ETRI)
161 Gajeong-dong, Yuseong-gu, Deajeon, 305-350, Korea
{sklee,syh}@etri.re.kr
[2] Gwangju Institute of Science and Technology (GIST)
1 Oryong-dong, Buk-gu, Gwangju, 500-712, Korea
hoyo@gist.ac.kr

Abstract. In this paper, we propose a new lossless data hiding method where distortion due to data embedding can be completely removed from the watermarked image after the watermark has been extracted. In the proposed method, we utilize characteristics of the difference image and modify pixel values slightly to embed the data. We show that the lower bound of the PSNR (peak-signal-to-noise-ratio) values for typical images are about 51.14 dB. Moreover, the proposed method is quite simple and fast. Experimental results demonstrate that the proposed scheme can embed a large amount of data while keeping high visual quality of test images.

Keywords: Lossless data hiding, watermarking, histogram modification

1 Introduction

Digital representation of multimedia content offers various advantages, such as easy and wide distribution of multiple and perfect replications of the original content. However, the fact that an unlimited number of perfect copies can be illegally produced is a serious threat to the right of content owners. In order to protect the intellectual property rights, we can apply information hiding techniques in various application areas, such as broadcast monitoring, proof of ownership, content authentication, copy control, and transaction tracking [1].

In most data hiding techniques, the original image is inevitably distorted due to data embedding itself. Typically, this distortion cannot be removed completely due to quantization, bit replacement, or truncation at the gray level 0 and 255. Although the distortion is often quite small, it may be unacceptable for medical or legal imagery or images with a high strategic importance in certain military

* This work was supported in part by Gwangju Institute of Science and Technology (GIST), in part by the Ministry of Information and Communication (MIC) through the Realistic Broadcasting Research Center (RBRC) at GIST, and in part by the Ministry of Education (MOE) through the Brain Korea 21 (BK21) project.

K. Aizawa, Y. Nakamura, and S. Satoh (Eds.): PCM 2004, LNCS 3333, pp. 340–347, 2004.

applications [2]. Thus, it is desired to reverse the watermarked image back to the original image after the embedded data are extracted. Data embedding satisfying this requirement, is referred to as lossless data hiding.

In recent years, several lossless data hiding techniques have been proposed for images. Lossless data embedding can take place in the spatial domain [2,3,4], or in the transform domain [5,6]. Ni et al. [4] proposed a lossless data embedding technique, which utilizes the zero or the minimum point of the image histogram. It can embed a large amount of data and the PSNR values of watermarked images are always higher than 48 dB. However, gray level values of the zero point and the peak point should be transmitted to the receiving side for data retrieval.

In this paper, we propose a new lossless data hiding method where we exploit the difference image histogram to embed more data than other lossless data hiding schemes. The proposed scheme gives about 3 dB improvement in PSNR for typical images as compared to Ni's scheme [4]. Moreover, there is no need to transmit any side information to the receiving side for data retrieval.

This paper is organized as follows. In Section 2, we describe details of the proposed lossless data hiding method using the histogram modification of the difference image. After experimental results are presented in Section 3, we conclude this paper in Section 4.

2 Proposed Lossless Data Hiding Scheme

2.1 Watermark Embedding

Figure 1 shows the watermark embedding procedure of the proposed scheme, which consists of watermark generation, creating the difference image, histogram shifting, and histogram modification.

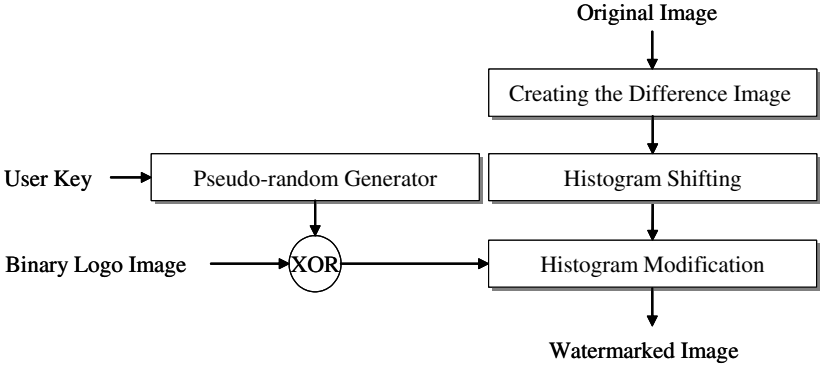


Fig. 1. Proposed watermark embedding

In order to generate a binary watermark sequence $W(m,n)$ of size $P \times Q$, we combine a binary random sequence generated by the user key, $A(l)$ of length $P \times Q$ with a binary logo sequence $B(m,n)$ of size $P \times Q$ pixels using the bit-wise XOR operation.

$$W(m,n) = A(l) \oplus B(m,n), \quad 0 \le l \le P \times Q - 1, \\ 0 \le m \le P-1,\ 0 \le n \le Q-1 \tag{1}$$

For a grayscale image $I(i,j)$ of size $M \times N$ pixels, we form the difference image $D(i,j)$ of size $M \times N/2$ from the original image.

$$D(i,j) = I(i,2j+1) - I(i,2j),\ 0 \le i \le M-1,\ 0 \le j \le \frac{N}{2} - 1 \tag{2}$$

where $I(i,2j+1)$ and $I(i,2j)$ are the odd-line field and the even-line field, respectively. For watermark embedding, we empty the histogram bins of -2 and 2 by shifting some pixel values in the difference image. If the difference value is greater than or equal to 2, we add one to the odd-line pixel. If the difference value is less than or equal to -2, we subtract one from the the odd-line pixel. Then, the modified difference image $\widetilde{D}(i,j)$ can be represented as

$$\widetilde{D}(i,j) = \widetilde{I}(i,2j+1) - I(i,2j) \tag{3}$$

where

$$\widetilde{I}(i,2j+1) = \begin{cases} I(i,2j+1)+1 & \text{if } D(i,j) \ge 2 \\ I(i,2j+1)-1 & \text{if } D(i,j) \le -2 \\ I(i,2j+1) & \text{otherwise} \end{cases} \tag{4}$$

In the histogram modification process, the watermark $W(m,n)$ is embedded into the modified difference image $\widetilde{D}(i,j)$. The modified difference image is scanned. Once a pixel with the difference value of -1 or 1 is encountered, we check the watermark to be embedded. If the bit to be embedded is 1, we move the difference value of -1 to -2 by subtracting one from the odd-line pixel or 1 to 2 by adding one to the odd-line pixel. If the bit to be embedded is 0, we skip the pixel of the difference image until a pixel with the difference value -1 or 1 is encountered. In this case, there is no change in the histogram. Therefore, the watermarked fields $I_w(i,2j+1)$ and $I_w(i,2j)$ are obtained by

$$I_w(i,2j+1) = \begin{cases} \widetilde{I}(i,2j+1)+1 & \text{if } \widetilde{D}(i,j) = 1 \text{ and } W(m,n) = 1 \\ \widetilde{I}(i,2j+1)-1 & \text{if } \widetilde{D}(i,j) = -1 \text{ and } W(m,n) = 1 \\ \widetilde{I}(i,2j+1) & \text{otherwise} \end{cases} \tag{5}$$

and

$$I_w(i,2j) = I(i,2j) \tag{6}$$

2.2 Watermark Extraction and Recovery

Figure 2 depicts the watermark extraction and recovery procedure. In this process, we extract the binary logo image and reverse the watermarked image to the original image.

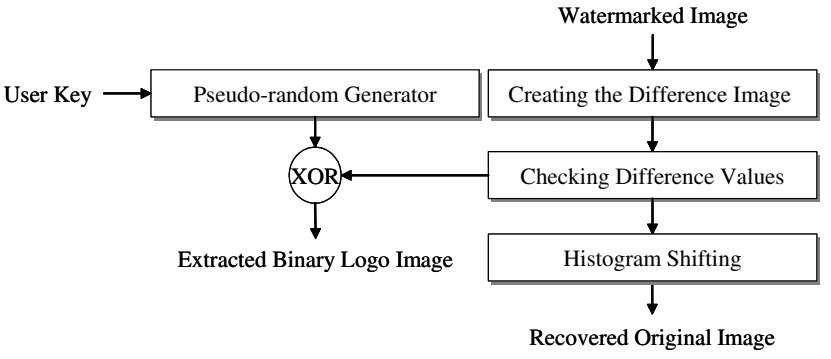


Fig. 2. Proposed watermark extraction and recovery

We calculate the difference image $D_e(i,j)$ from the received watermarked image $I_e(i,j)$. The whole difference image is scanned. If the pixel with the difference value of -1 or 1 is encountered, the bit 0 is retrieved. If the pixel with the difference value of -2 or 2 is encountered, the bit 1 is retrieved. In this way, the embedded watermark $W_e(m,n)$ can be extracted.

$$W_e(m,n) = \begin{cases} 0 & \text{if } D_e(i,j) = -1 \text{ or } 1 \\ 1 & \text{if } D_e(i,j) = -2 \text{ or } 2 \end{cases} \tag{7}$$

In order to reconstruct the binary logo image $B_e(m,n)$, we perform the bitwise XOR operation between the binary random sequence generated by the user key, $A_e(l)$ and the detected binary watermark sequence $W_e(m,n)$.

$$B_e(m,n) = A_e(l) \oplus W_e(m,n) \tag{8}$$

Finally, we reverse the watermarked image back to the original image by shifting some pixel values in the difference image. The whole difference image is scanned once again. If the difference value is less than or equal to -2, we add one to the odd-line pixel. If the difference value is greater than or equal to 2, we subtract one from the odd-line pixel. The recovered odd-line field $I_r(i,2j+1)$ can be expressed as

$$I_r(i,2j+1) = \begin{cases} I_e(i,2j+1) - 1 & \text{if } D_e(i,j) \geq 2 \\ I_e(i,2j+1) + 1 & \text{if } D_e(i,j) \leq -2 \\ I_e(i,2j+1) & \text{otherwise} \end{cases} \tag{9}$$

Since we manipulate pixel values of only the odd-line field in the watermark embedding process, the recovered even-line field $I_r(i,2j)$ is

$$I_r(i,2j) = I_e(i,2j) \tag{10}$$

2.3 Lossless Image Recovery

The proposed scheme cannot be completely reversed because the loss of information occurs during addition and subtraction at the boundaries of the grayscale range (at the gray level 0 and 255). In order to prevent this problem, we adopt modulo arithmetic for watermark addition and subtraction. For the odd-line field $I(i, 2j+1)$, we define the addition modulo c as

$$I(i, 2j+1) +_c 1 = (I(i, 2j+1) + 1) \bmod c \tag{11}$$

where c is the cycle length. The subtraction modulo c is defined as

$$I(i, 2j+1) -_c 1 = (I(i, 2j+1) - 1) \bmod c \tag{12}$$

The reversibility problem arises from pixels with truncated due to overflow or underflow. Therefore, we use $+_c$ and $-_c$ instead of + and - only when truncation due to overflow or underflow occurs. In other words, we have only to consider $255 +_c 1$ and $0 -_c 1$.

In the receiving side, it is necessary to distinguish between the cases when, for example, $I_e(i, 2j+1) = 255$ was obtained as $I(i, 2j+1)+1$ and $I(i, 2j+1) -_{256} 1$. We assume that no abrupt change between two adjacent pixels occurs. If there is a significant difference between $I_e(i, 2j+1)$ and $I_e(i, 2j)$, we estimate that $I(i, 2j+1)$ was manipulated by modulo arithmetic.

$$\begin{cases} I(i, 2j+1) + 1 & \text{if } |I_e(i, 2j+1) - I_e(i, 2j)| \le \tau \\ I(i, 2j+1) -_{256} 1 & \text{otherwise} \end{cases} \tag{13}$$

where τ is a threshold value. Similarly, $I_e(i, 2j+1) = 0$ is estimated as

$$\begin{cases} I(i, 2j+1) - 1 & \text{if } |I_e(i, 2j+1) - I_e(i, 2j)| \le \tau \\ I(i, 2j+1) +_{256} 1 & \text{otherwise} \end{cases} \tag{14}$$

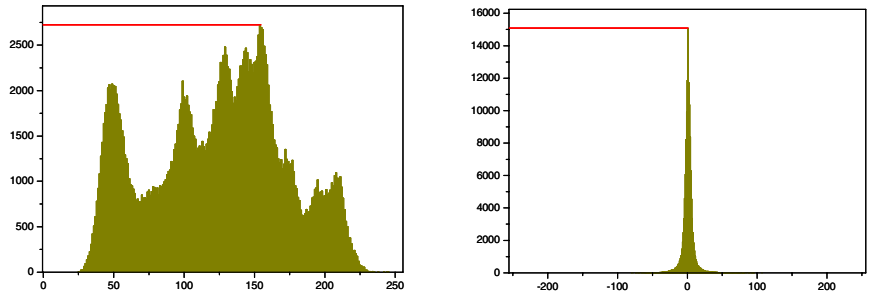
2.4 Lower Bound of PSNR and Embedding Capacity

Assume that there is no pixel with overflow and underflow in the original image. In the worst case, all pixels of the odd-line field will be added or subtracted by 1. The MSE (mean squared error) of this case is 1/2. Hence, the PSNR of the watermarked image can be calculated as

$$\text{PSNR(dB)} = 10 \log_{10}(255^2 \cdot 2) \approx 51.14 \tag{15}$$

In short, the lower bound of the PSNR of the watermarked image is about 51.14 dB. This result is much higher than other lossless data hiding techniques.

The embedding capacity of this scheme equals to the number of pixels with the difference values of -1 and 1 in the difference image. A large number of pixel values of the difference image have a tendency to be distributed around 0. Using this property of the difference image histogram, we can embed a large amount of



(a) Histogram of the original image (b) Histogram of the difference image

Fig. 3. Histogram Characteristics of Lena image

data as compared to the original image itself. Figure 3 shows this characteristic property of difference images. The number of pixels with the peak point in the histogram of the original Lena image is around 2,750. On the other hand, the number of pixels with the peak point in the histogram of the difference image is higher than 15,000.

3 Experimental Results and Analysis

In order to evaluate the performance of the proposed scheme, we perform computer simulations on many typical grayscale images of size 512×512 pixels. Figure 4 shows a watermark which is a binary logo image of size 128×56 pixels, equivalent to a binary sequence of 7,168 bits.

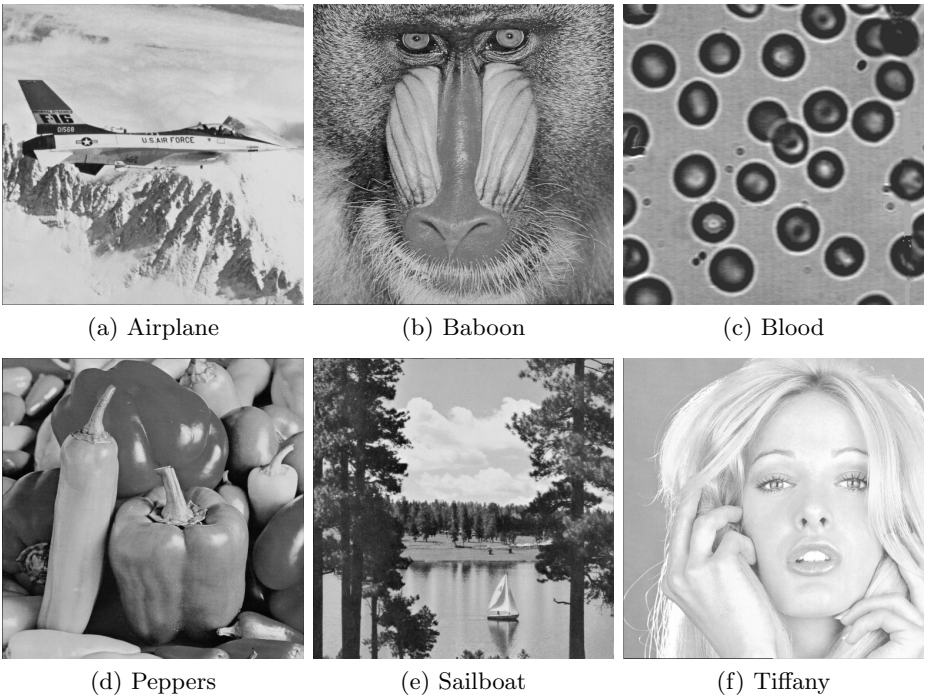
Fig. 4. Binary logo image of 128×56 pixels

The original and watermarked Lena images are shown in Fig. 5. The Lena image does not contain pixels with truncated due to overflow or underflow. It is observed that there is no visible degradation due to embedding in the watermarked image. Figure 6 shows further six watermarked images.

Table 1 summarizes the experimental results. This table shows that the PSNR values of all watermarked images are above 51.14 dB, as we theoretically proved in Section 2.4. The capacity ranges from 8 kbits to 30 kbits for $512 \times 512 \times 8$ test grayscale images. This result shows that the proposed scheme offers adequate capacity to address most applications. It is also seen from Table 1 that an image like Baboon, which contains significant texture, has considerably lower capacity than simple images such as Airplane.

(a) Original image (b) Watermarked image

Fig. 5. Results with Lena image



(a) Airplane (b) Baboon (c) Blood

(d) Peppers (e) Sailboat (f) Tiffany

Fig. 6. Watermarked images

Table 1. Experimental results

Test images (512×512×8)	PSNR (dB)	Capacity (bits)	Overflow/underflow (No. of pixels)
Airplane	58.78	30,487	0
Baboon	51.49	7,383	0
Blood	55.59	22,009	20
Lena	57.63	23,579	0
Peppers	55.74	17,280	2
Sailboat	55.55	14,391	0
Tiffany	52.50	26,004	83

Some test images, such as Blood, Peppers, and Tiffany, contain pixels with overflow and underflow. However, the set of such pixels is relatively small and the artifacts due to overflow and underflow are not serious.

For simplicity, we used different values of -1 and 1 for watermark embedding. If we use the different value of 0 instead of -1 or 1, we can ensure larger capacity than that shown in the experiment.

4 Conclusions

We have proposed a lossless data hiding method based on difference image histogram. In order to solve the reversibility problem, we used the modulo arithmetic instead of the ordinary addition and subtraction. Experimental results showed that the proposed scheme provides high embedding capacity while keeping the embedding distortion as small as possible. Reversibility back to the original content is highly desired in sensitive imagery, such as military data and medical data. The proposed lossless data hiding technique can be deployed for such applications.

References

1. Lee, J., Hwang, S., Jeong, S., Yoon, K., Park, C., Ryou, J.: A DRM framework for distributing digital contents through the Internet. ETRI Journal (2003) 423–436
2. Fridrich, J., Goldjan, M., Du, R.: Invertible authentication. Proc. SPIE, Security and Watermarking of Multimedia Contents (2001) 197–208
3. Honsinger, C., Jone, P., Rabbani, M., Stoffel, J.: Lossless recovery of an original image containing embedded data. US Patent: 6,278,791 B1 (2001)
4. Ni, Z., Shi, Y., Ansari, N., Su, W.: Reversible data hiding. Proc. ISCAS (2003) 912–915
5. Goldjan, M., Fridrich, J., Du, R.: Distortion-free data embedding. Proc. 4th Information Hiding Workshop (2001) 27–41
6. Xuan, G., Zhu, J., Chen, J., Shi, Y., Ni, Z., Su, W.: Distortionless data hiding based on interger wavelet transform. IEE Electrionics Letters (2002) 1646–1648