ROBUST LOSSLESS DATA HIDING BASED ON BLOCK GRAVITY CENTER FOR SELECTIVE AUTHENTICATION

Kyung-Su Kim[a], Min-Jeong Lee[a], Young-Ho Suh[b], and Heung-Kyu Lee[a]

[a]School of EECS, Division of CS, KAIST, Guseong-dong, Yuseong-gu, Daejeon, South Korea
[b]Digital Content Research Division, ETRI, Gajeong-dong,Yuseong-gu, Daejeon, South Korea

ABSTRACT

Reversible or lossless data hiding enables host media to be restored from marked media without any loss of host information. However, since most of existing lossless data hiding methods are fragile, hidden data cannot be extracted after marked media goes through alteration such as JPEG compression. In this paper, we present a robust (referred to as semi-fragile) lossless data hiding method that utilizes sub-sampling and block gravity center. Gravity center of sub-sampled part of each block is insensitive to alteration, so it achieves robustness. This technique can be applied to selective authentication for images. That is, if a marked image does not change at all, the hidden data is correctly extracted and at the same time an original image is recovered. After compression, the hidden data is still extracted without error. Experimental results prove that the presented scheme achieves both reversibility and robustness against the predefined distortion.

Index Terms— Content authentication, gravity center, semi-fragile lossless data hiding, reversible watermarking.

1. INTRODUCTION

Lossless data hiding, or so-called reversible data hiding, enables exact recovery of an original image from a marked image after a hidden message removal for content authentication and tamper proofing. It is applied in applications where the recovery of the original image is desired. In quality-sensitive applications such as military imaging and remote sensing where a slight modification can lead to significant difference in final decision making process, the original image without any modification is required during image analysis. Recently, there are different ways to embed message for reversibility in literature. In [1, 2], they losslessly compressed a selected feature from an image to obtain enough space, which is then filled up with a message to be hidden. In [3, 4], they embedded a message in transform domain such as discrete cosine transform (DCT) or discrete wavelet transform (DWT) by modifying corresponding coefficients. Some employed a difference expansion technique where message bits were embedded by expanding the differences of pixel pairs [5, 6]. Histogram modification techniques were proposed by [7, 8]. However, since most of them were fragile, the hidden message cannot be extracted after the marked image goes through alteration such as compression. Two lossless data hiding techniques robust against compression were proposed so far. These techniques are more useful and more practical than fragile schemes because they allow incidental modification for selective authentication in the real situations. When no alteration occurred during transmission, the original image was recovered after removing hidden data. If the marked image changed by alteration, hidden data is still extracted without error. In [9], pixels were divided into two pseudo-random sets and the message was embedded by rotating the center of the circular histogram of each set. However, since modulo-256 addition was employed to achieve reversibility, the marked image suffered from salt-and-pepper visual artifacts. Ni *et al.* [10] used the difference values of two randomly chosen pixels in each image block as a robust parameter. This method did not generate salt-and-pepper noise but embedding capacity and extraction performance depended on the used error correction code (ECC).

In this paper, we propose a novel robust lossless data hiding method that modifies a gravity center of two sub-sampled parts in blocks. This gravity center provides both lossless data hiding for exact authentication and robustness for selective authentication. This paper is organized as follows. Sec. 2 presents our robust lossless data embedding and extraction algorithm including the selected robust quantity. Experimental results are shown in Sec. 3 and Sec. 4 concludes.

2. THE PROPOSED ROBUST LOSSLESS DATA HIDING ALGORITHM

This section presents a gravity center based lossless data hiding algorithm for images in spatial domain. Fig. 1 describes an overall flowchart of the proposed scheme, which is composed of data embedding, extraction, and recovery procedures.

Email: kskim@mmc.kaist.ac.kr

978-1-4244-4291-1/09/$25.00 ©2009 IEEE

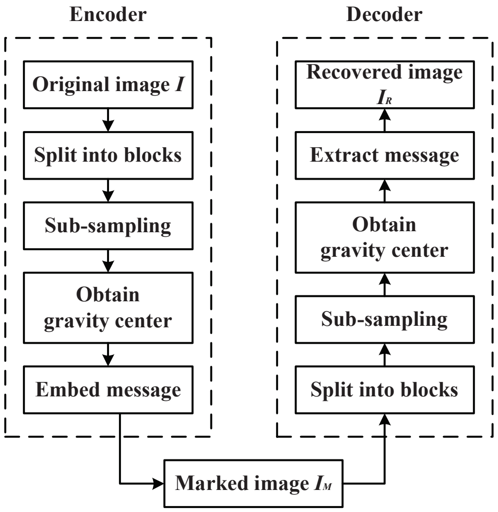


Fig. 1. Flowchart of the proposed lossless data hiding.

2.1. Sub-sampling

Sampling is the process of selecting units (*e.g.,* pixels, coefficients) from an image. We introduce a lossless data hiding algorithm that utilizes sub-sampled images obtained by sub-sampling. For the $N_1 \times N_2$ image $I(i,j)$, where $i = 1,\ldots,N_1, j = 1,\ldots,N_2$, then four sub-sampled images are obtained as below [8]

$$\begin{aligned}&S_1(x,y) = I(2i,2j), \quad S_2(x,y) = I(2i,2j+1),\\ &S_3(x,y) = I(2i+1,2j),\\ &S_4(x,y) = I(2i+1,2j+1)\end{aligned} \tag{1}$$

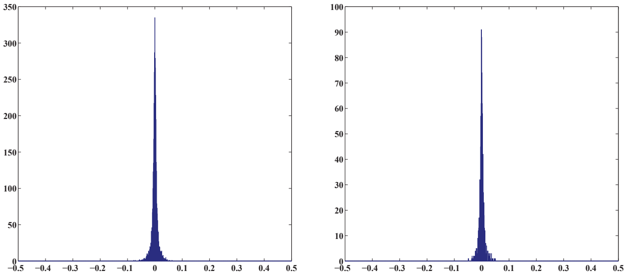
where $x = 1,\ldots,N_1/2$ and $y = 1,\ldots,N_2/2$. Since the sub-sampled images are strongly correlated and have highly spatial redundancy, we utilize this characteristic and achieve the robustness for selective authentication.

2.2. Robust Quantity

Since the obtained 4 sub-sampled images are close to each other, the gravity centers in each sub-sampled image are also close to each other. In order to be robust against incidental alteration such as compression and noise addition, we select this gravity center as the robust parameter. To enhance robustness, two averaged sub-sampled images are employed instead of all sub-sampled images. For example, $A_1(x,y) = \lfloor(S_1(x,y) + S_4(x,y))/2\rfloor$ and $A_2(x,y) = \lfloor(S_2(x,y) + S_3(x,y))/2\rfloor$ can be obtained. Then, the gravity center (G_{x_1}, G_{y_1}) of A_1 is defined as following.

$$\begin{aligned}G_{x_1} &= \frac{\sum_{x=1}^{N_1/2}\sum_{y=1}^{N_2/2}(x \cdot A_1(x,y))}{\sum_{x=1}^{N_1/2}\sum_{y=1}^{N_2/2} A_1(x,y)}\\ G_{y_1} &= \frac{\sum_{x=1}^{N_1/2}\sum_{y=1}^{N_2/2}(y \cdot A_1(x,y))}{\sum_{x=1}^{N_1/2}\sum_{y=1}^{N_2/2} A_1(x,y)}\end{aligned} \tag{2}$$

In the proposed method, we first split I into $M \times N$ image blocks. After that, sub-sampling is applied to each block and then gravity centers are calculated. For a given image block, we expect that the difference value between two gravity centers in A_1 and A_2 is very close to zero. Fig. 2 depicts the distribution of the difference values of G_x between A_1 and A_2 in *Lena* image when both M and N are equal to 8 and 16, respectively. Note that most difference values are very close to zero and thus this result supports our observation. This difference value is chosen as our robust quantity to embed message.

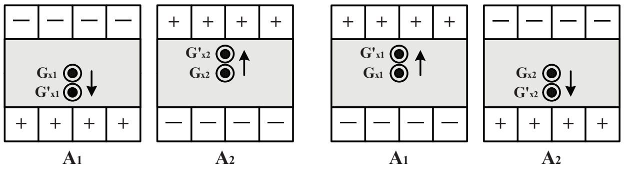


(a) $\mu = -1.6 \times 10^{-4}$,$\sigma = 0.01$ (b) $\mu = 7.8 \times 10^{-5}$,$\sigma = 0.009$

Fig. 2. Distribution of difference values of G_x when block sizes are (a) 8×8 and (b) 16×16, repectively. The mean and deviation values of two cases are almost zero.

2.3. Data Embedding Algorithm

Let I be the original image to be transmitted and I_M be the marked image. First, we divide I into $M \times N$ blocks. For each block, we apply sub-sampling and obtain two gravity centers from two averaged sub-sampled parts explained in Sec. 2.1 and Sec. 2.2, respectively. Next, the difference value $D = G_{x_1} - G_{x_2}$ is calculated and it follows the distribution mentioned above. Let us assume that the embedded message $w(n)$ is a pseudo random binary sequence. For each block, if $w(n)$ is 1, we should make G_{x_1} larger than G_{x_2}. If $w(n)$ is 0, G_{x_2} has to be larger than G_{x_1}. To achieve this, a constant value (called an embedding level L) is added and subtracted



(a) Embed $w(n) = 1$ (b) Embed $w(n) = 0$

Fig. 3. Embedding method illustration ($M = N = 8$): the modified G'_{x_1} in A_1 is larger than the modified G'_{x_2} in A_2 to embed a bit '1' and is smaller than that to embed a bit '0'. The shade areas remain intact for visual quality.

as shown in Fig. 3. As a result of this, the original gravity center is moved and thus D is increased or decreased (*i.e.,* D is no longer centered on zero.). Finally, I_M is obtained through the inverse of the sub-sampling with the modified sub-sampled image blocks.

2.4. Data Extraction and Recovery Algorithm

Data extraction and recovery steps are the reverse process of data embedding steps. For the given marked image I_M, we first split I_M into blocks. For each block, sub-sampling is applied and two gravity centers are obtained. If G'_{x_1} is larger than G'_{x_2}, the embedded bit '1' is retrieved, otherwise '0' is retrieved. That is, the message is extracted using the following rule.

$$w(n) = \begin{cases} 1 & \text{if } D' = G'_{x_1} - G'_{x_2} \geq 0 \\ 0 & \text{if } D' = G'_{x_1} - G'_{x_2} < 0 \end{cases} \quad (3)$$

On the one hand, if the received marked image to be authentic does not change at all, the hidden message is correctly extracted by using Eq. (3) and at the same time the original image without any distortion is reconstructed by subtracting and adding L. On the other hand, if some alteration happens to the marked image, the hidden message is still extracted without error.

2.5. Low Bound of PSNR

PSNR is a well-known quantitative value to measure the distortion between the original image and the marked image. In the embedding procedure, the embedding level L is added or subtracted in only a half of the height. That is, the resultant mean square error (MSE) is $(0.5 \times L^2 \times N_1 \times N_2)/(N_1 \times N_2) = \frac{L^2}{2}$. The following equation represents theoretical low bound of PSNR value for different values of L.

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \approx 20 \times \log_{10}\left(\frac{360.62}{L}\right) \quad (4)$$

For example, if L is 4, the low bound of PSNR between the original image and the marked one is 39.10 dB.

3. SIMULATION RESULTS

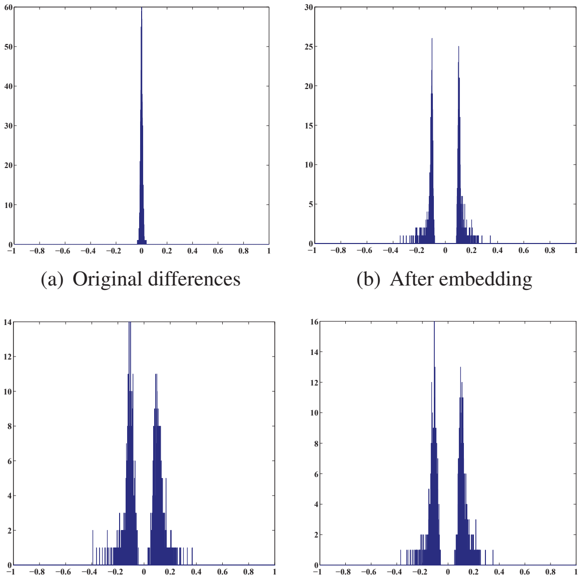
In all experiments, 2 commonly used grayscale images and 2 military images of size 512 × 512 are used as test images as depicted in Fig. 4. To embed the message bits, the block size $M(= N)$ is 16 the embedding level L are adjusted [4, 8]. Depending on the desired degree, the block size affects the embedding capacity and robustness. The embedding level affects the visual quality and robustness. For robustness test, we consider high-quality JPEG compression attack because quality-sensitive images should be compressed with low compression ratio ($Q \geq 85$). Noise addition attack also happens during transmission.

(a) Lena (b) Boat (c) Aerial (d) Tank

Fig. 4. Test images.

3.1. Performance of Selected Robust Quantity

In this section, we analyze the performance of selected robust quantity. The difference of two gravity centers is chosen as the robust parameter against alteration. Fig. 5 shows some results. In this case, the embedding capacity is 1024 bits and the PSNR value is 37.16 dB. As shown in the figure, it is proved that all embedded message bits are correctly extracted although the marked image goes through high-quality JPEG compression and noise addition.



(a) Original differences (b) After embedding

(c) JPEG (Q=85) (d) noise addition ($\sigma^2 = 0.001$)

Fig. 5. Performance of our robust parameter for *Tank* image. M, N, and L are set to 16, 16, and 5, respectively.

3.2. Comparison with Other Algorithms

Table 1 summarizes comparison results with other existing algorithms, two fragile schemes [7, 8] and one semi-fragile scheme [9] for 4 test images: *Lena*, *Boat*, *Aerial*, and *Tank*. Since two fragile schemes are based on LSB modification, about 50% of the embedded bits were destroyed due to the attacks. [9] suffers from lack of embedding capacity since some probable blocks not to be reversible do not carry a message to be hidden. In the proposed method, the embedding capac-

Table 1. Comparison results in terms of the payload and the error rate for 4 test images. EC means the embedding capacity (bits). ER1 and ER2 mean the bit error rate (%) after JPEG compression (Q=85) and noise addition ($\sigma^2 = 0.001$), respectively. In [9], the block size and the level are set to 16 and 3, respectively. In the proposed method, $M = N = 16$ and $L = 5$ because they achieve better performance.

	Type	Lena			Boat			Aerial			Tank		
		EC	ER1	ER2	EC	ER1	ER2	EC	ER1	ER2	EC	ER1	ER2
Ni [7]	fragile	5412	50.8	49.2	10546	49.9	49.6	10128	49.7	50	16729	49.8	49.7
Kim [8]	fragile	18202	50.1	49.8	18384	49.7	49.9	15534	50	49.6	21831	49.7	50
Vleeschouwer [9]	s-fragile	1017	0	0	1016	0.1	0	955	0.6	3.7	994	0	0
Proposed	s-fragile	1024	0	0	1024	0	0	1024	0	0	1024	0	0

ity is 1024 bits and is completely extracted. Through the experiment, it is observed that larger block size and embedding level lead to stronger robustness. However, larger block size makes the embedding capacity lower and also larger embedding level makes the distortion higher. Thus, the block size and the embedding level should be adjusted depending on the requirement of the desired applications for selective authentication.

4. CONCLUSIONS

A block gravity center based robust (semi-fragile) lossless data hiding algorithm for selective authentication is proposed, where the difference between two gravity centers in the sub-sampled parts is modified to embed the message. We exploit the fact that difference values having small magnitudes occur frequently because two obtained gravity centers are very close. Under the given block size and the embedding level, the proposed algorithm shifts the distribution of differences by modifying pixel values. The proposed scheme does not use ECC and no overflow and underflow happens for the test images. Experimental results support that our algorithm achieves both lossless and robustness. This permits conveying the embedded message from lossless and lossy environments.

5. ACKNOWLEDGEMENT

This work was partially supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract, Ministry of Culture, Sports and Tourism(MCST) and Korea Culture Content Agency(KOCCA) in the Culture Technology(CT) Research & Developement Program 2009, and the IT R&D program of MKE/IITA. [2007-S017-01, Development of user-centric contents protection and distribution technology].

6. REFERENCES

[1] J. Fridrich, J. Goljan, and R. Du, “Invertible authenticaion,” in *Proc. SPIE, Security and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 2001, vol. 4314, pp. 197–208.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-lsb data embedding,” *IEEE Trans. Image Processing*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[3] B. Yang, M. Schmucker, C. Busch W. Funk, and S. Sun, “Integer dct-based reversible watermarking for images using companding technique,” in *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 2004, vol. 5306, pp. 405–415.

[4] G. Xuan, Y. Q. Shi, Q. Yao, Z. Ni, C. Yang, J. Gao, and P. Chai, “Lossless data hiding using histogram shifting method based on integer wavelets,” in *IWDW*, Jeju Island, Korea, Nov. 2006, LNCS, vol. 4283, pp. 323–332.

[5] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[6] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform,” *IEEE Trans. Image Processing*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[7] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Trans. Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[8] K.-S. Kim, M.-J. Lee, H.-K. Lee, and Y.-H. Suh, “Histogram-based reversible data hiding technique using subsampling,” in *The 10th Proc. ACM MMSEC*, Oxford, UK, Sep. 2008, pp. 69–74.

[9] C. De Bleeschouwer, J. F. Delaigle, and B. Macq, “Circular interpretation of bijective transformations in lossless watermarking for media asset management,” *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 97–105, Mar. 2003.

[10] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, “Robust lossless image data hiding,” in *Proc. IEEE ICME*, Taipei, Taiwan, June 2004, pp. 2199–2202.