A Collaborative Scheme for Lossless Data Hiding and Image Scrambling

Shenchuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino-shi, Tokyo 191–0065, Japan
E-mail: liu-shenchuan@sd.tmu.ac.jp, mfujiyoshi@ieee.org, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes a scheme in which lossless data hiding and image scrambling do not interfere each other. The proposed scheme offers a flexibility in processing order of two technologies, namely lossless data hiding and scrambling. In other words, the proposed scheme can either extract embedding data from a scrambled stego image first or descramble the scrambled stego first, without considering the process orders of how the scrambled stego image is produced. The conventional schemes having the same features only serve lossy data hiding and are dedicated only to compressed images. In contrast, the proposed scheme works in the spatial domain and serves lossless data hiding.**

I. Introduction

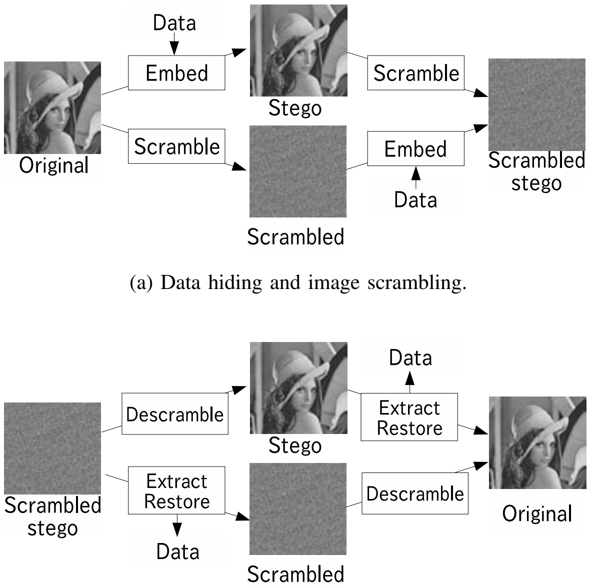
Data hiding technology has been diligently studied, for not only security-related problems [1], [2] but also non security-oriented issues [1], [3]. A data hiding technique embeds data into a target signal that is called as the *original* signal. It, then, generates a slightly distorted signal carrying the data, and this distorted signal is referred to as a *stego* signal.

Though many of data hiding techniques extract hidden data but leave a stego signal as it is [4], restoration of the original image as well as extraction the hidden data are desired [5]–[7] in military and medical applications. So *lossless* data hiding schemes that restore the original image from a stego image have been proposed [5]–[15].

On the other hand, image scrambling technology that distorts an image to generate a visually protected image has been also actively studied for secure image database [16], access control to images [17], privacy protection [18], waking an observer of a video surveillance system [18], and so on.

In some secure applications, both data hiding and image scrambling are desired. Applying two technologies to an image in series is the simplest solution, this cascading, however, requires the corresponding inverse operations; a flow in which scrambling image firstly and then hiding data to the scrambled image requires hidden data extraction and image recovery to descramble the image. It reduces the combination efficiency and raise the security risk as well.

To solve this inconvenience, collaborative schemes offering a flexible processing order have been proposed [19], [20]. These schemes can either extract hidden data from or descramble a scrambled stego image regardless of the processing order between data hiding and scrambling. These schemes, however, are dedicated to compressed images and serve only lossy data hiding in which the original image cannot be recovered.



(a) Data hiding and image scrambling.

(b) Data extraction and image descrambling.

Fig. 1. A collaborative scheme for data hiding and image scrambling.

This paper proposes a spatial domain-based collaborative scheme that serves lossless data hiding. The proposed scheme hides data to an image and scrambles the image in non-overlapping blocks in which a block consists of two parts; for data hiding and scrambling. By using a common parameter, the proposed scheme identifies the watermarked blocks even after the image is scrambled.

II. Conventional Schemes

The concept of a collaborative scheme is shown in Fig. 1 in which the scheme offers a flexible processing flow. A collaborative scheme can extract the watermark from scrambled stego image without descrambling it or descramble the scrambled stego without extracting the hidden data.

The conventional schemes use quantized DCT coefficients in a compression encoding for data hiding and image scrambling [19], [20]. In one conventional method [19], the quantized DCT coefficients are divided into those positive and negative sign components and amplitude components, the sign is used for image scrambling while the amplitude is used for data hiding as shown in Fig. 2.

ISBN: 978-602-8944-11-3

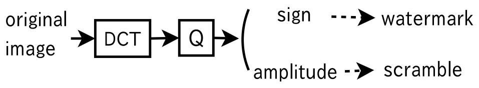


Fig. 2. Conventional method [19].

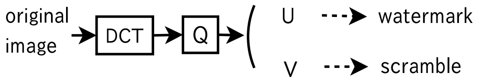


Fig. 3. Conventional method [20].

Similarly, the quantized DCT coefficients are randomly divided into two non-overlapped groups in the other scheme [20]; here groups are represented by $\mathbb{U}$ and $\mathbb{V}$. In this scheme, group $\mathbb{U}$ is used for image scrambling and group $\mathbb{V}$ is used for data hiding as shown in Fig. 3.

Due to using quantized transformed coefficients, neither watermark extraction nor image descrambling works properly for decoded images in the conventional schemes. Moreover, because the conventional schemes are based on quantized DCT coefficients, the schemes cannot recover the original image or extract any hiding data from a watermarked image.

In the next section, a novel collaborative scheme for lossless data hiding and image scrambling is proposed which is based on the spatial domain.

III. Proposed Scheme

This section proposes a spatial domain-based collaborative scheme for lossless data hiding and image scrambling. The proposed scheme hides data to and scrambles an image in non-overlapping blocks in which a block is further divided to two parts; for data hiding and for scrambling. The proposed scheme uses a common parameter for two technologies so that it is a collaborative scheme.

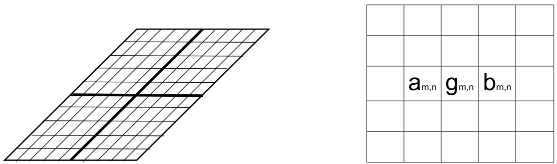
A. System Overview

The proposed scheme embeds data and scrambles an image in spatial domain. $X \times Y$-sized gray scale image $\mathbf{f}$ in which each pixel is represented by K bits, i.e., $\mathbf{f} = \{f(x,y) | 0 \leq f(x,y) \leq 2^K - 1, 0 \leq x \leq X-1, 0 \leq y \leq Y-1\}$, is assumed to be an original image.

The proposed scheme divides $\mathbf{f}$ to $M \times N$ of $X_B \times Y_B$-sized non-overlapped blocks, $\mathbf{B}_{m,n}$ ($m = 0, 1, \ldots, M-1$ and $n = 0, 1, \ldots, N-1$), as shown in Fig. 4 (a) where $X_B = Y_B = 5$. E pixels in $\mathbf{B}_{m,n}$ are used for data hiding as shown in Fig. 4 (b) where $E = 3$ and pixels used for data hiding are represented by $a_{m,n}$, $g_{m,n}$, and $b_{m,n}$. Hereafter, $X_B = Y_B = 5$ and $E = 3$ as shown in Fig. 4.

The proposed scheme embeds L-length binary sequence $\mathbf{w} = \{w_l | w_l \in \{0,1\}, l = 0, 1, \ldots, L-1\}$ into the image. If block $\mathbf{B}_{m,n}$ is usable that a usable block satisfies the criteria for lossless data hiding, one bit data w_l is hidden in pixel $g_{m,n}$. It is noted that $a_{m,n}$ and $b_{m,n}$ are unchanged.

In all blocks, the rest $X_B Y_B - E$ pixels in the block are scrambled by using $X_B \times Y_B$-sized scramble matrices $\mathbf{R}_1$ and $\mathbf{R}_2$. In unwatermarked blocks, E pixels for data hiding are further scrambled using $M \times N$-sized scramble matrix $\mathbf{Q}$.



(a) Image $\mathbf{f}$ is divided to $M \times N$ of $X_B \times Y_B$-sized blocks ($X_B = Y_B = 5$).

(b) Block $\mathbf{B}_{m,n}$ consists of E pixels for data hiding and $X_B Y_B - E$ pixels for image scrambling ($E = 3$).

Fig. 4. Block division and part division in a block.

B. Algorithms

Five algorithms are described in the following sections, namely deriving a parameter which is common for data hiding and scrambling, data hiding, data extraction and image recovery, image scrambling, and descrambling.

1) Parameter Derivation: The algorithm to derive parameter p from original image $\mathbf{f}$ as follows.

1. $m := 0$.
2. $n := 0$.
3. For two pixels $a_{m,n}$ and $b_{m,n}$, average $\bar{g}_{m,n}$ and absolute difference $d_{m,n}$ are obtained by

$$\bar{g}_{m,n} = \left\lfloor \frac{a_{m,n} + b_{m,n}}{2} \right\rfloor, \tag{1}$$

$$d_{m,n} = |a_{m,n} - b_{m,n}|, \tag{2}$$

respectively, where $\lfloor t \rfloor$ rounds the real-value t to the nearest integer towards negative infinity.
4. Intermediate parameter $s_{m,n}$ is obtained by

$$s_{m,n} = \begin{cases} d_{m,n}, & \tilde{g}_{m,n} < 0 \text{ or } \tilde{g}_{m,n} > 2^K - 2 \\ \infty, & \text{others} \end{cases}, \tag{3}$$

where

$$\tilde{g}_{m,n} = 2g_{m,n} - \bar{g}_{m,n}. \tag{4}$$

5. $n := n + 1$. Continue to Step 3 unless $n = N$.
6. $m := m + 1$. Continue to Step 2 unless $m = M$.
7. The minimum value of $s_{m,n}$'s and the maximun of $d_{m,n}$'s become S and D, respectively.

$$S = \min_{m,n} s_{m,n}, \tag{5}$$

$$D = \max_{m,n} d_{m,n}. \tag{6}$$

8. Finally, parameter p is derived by

$$p = \min\left(2^K - 1 - D, S\right). \tag{7}$$

This derived parameter p is commonly used for data hiding and image scrambling. That is, the above mentioned algorithm takes account into collaboration of lossless data hiding and image scrambling.

2) Data Hiding: The proposed scheme hides one bit data w_l to usable block $\mathbf{B}_{m,n}$ by the following algorithm.

1. $m := 0$ and $l := 0$.
2. $n := 0$.
3. Absolute difference between $a_{m,n}$ and $b_{m,n}$, i.e., $d_{m,n}$, is obtained by Eq. (2).
4. Stego pixel $\hat{g}_{m,n}$ is derived by
$$\hat{g}_{m,n} = \begin{cases} \tilde{g}_{m,n} + w_l, & d_{m,n} < p \\ g_{m,n}, & \text{others} \end{cases}, \tag{8}$$
where $\tilde{g}_{m,n}$ is given by Eq. (4).
5. If $\mathbf{B}_{m,n}$ is usable that $\mathbf{B}_{m,n}$ satisfies $d_{m,n} < p$, $l := l+1$.
6. $n := n+1$. Continue to Step 3 until $n = N$.
7. $m := m+1$. Continue to Step 2 until $m = M$.
8. Stego image $\hat{\mathbf{f}}$ is generated.

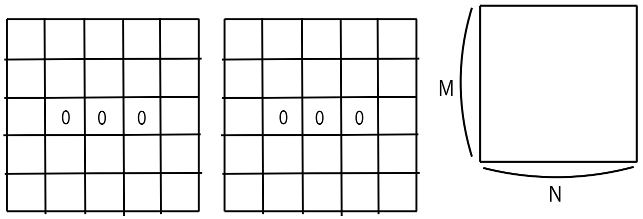
3) Hidden Data Extraction and Image Restoration: The following algorithm is applied to stego image $\hat{\mathbf{f}}$ to extract embedded data $\mathbf{w}$ and restore original image $\mathbf{f}$.

1. $m := 0$ and $l := 0$.
2. $n := 0$.
3. Absolute difference $d_{m,n}$ is obtained by Eq. (2).
4. One bit data w_l is extracted from watermarked block by the following equation, if $d_{m,n} < p$.
$$w_l = (\hat{g}_{m,n} + \bar{g}_{m,n}) \bmod 2. \tag{9}$$
5. Original pixel $g_{m,n}$ is restored by
$$g_{m,n} = \begin{cases} \frac{\hat{g}_{m,n} + \bar{g}_{m,n} - w_l}{2}, & d_{m,n} < p \\ \hat{g}_{m,n}, & \text{others} \end{cases}. \tag{10}$$
6. If $d_{m,n} < p$, $l := l+1$.
7. $n := n+1$. Continue to Step 3 unless $n = N$.
8. $m := m+1$. Continue to Step 2 unless $m = M$.
9. L-bit binary data sequence $\mathbf{w}$ and original image $\mathbf{f}$ are obtained.

Eq. (8) preserves $a_{m,n}$ and $b_{m,n}$, so $d_{m,n} = |a_{m,n} - b_{m,n}| < p$ can tell watermarked blocks in this algorithm.

4) Image Scrambling: The following scrambling algorithm is applied to an image to obtain a scrambled image.

1. $m := 0$.
2. $n := 0$.
3. Block $\mathbf{B}_{m,n}$ is scrambled by
$$\mathbf{B}'_{m,n} = (\mathbf{B}_{m,n} + m\mathbf{R}_1 + n\mathbf{R}_2) \bmod 2^K, \tag{11}$$
where $\mathbf{R}_1$ and $\mathbf{R}_2$ are $X_B \times Y_B$-sized matrices consisting of random integers between 0 and $2^K - 1$. As shown in Figs. 5 (a) and (b), elements corresponding to E pixels for data hiding are zeros in $\mathbf{R}_1$ and $\mathbf{R}_2$.
4. Absolute difference $d_{m,n}$ is obtained by Eq. (2).
5. If $\mathbf{B}_{m,n}$ is unwatermarked that $d_{m,n} > p$ holds in $\mathbf{B}_{m,n}$, E pixels for data hiding are further scrambled as
$$a'_{m,n} = (a_{m,n} + mQ(m,n)) \bmod 2^K, \tag{12}$$
$$b'_{m,n} = (b_{m,n} + mQ(m,n)) \bmod 2^K, \tag{13}$$
$$g'_{m,n} = (g_{m,n} + nQ(m,n)) \bmod 2^K, \tag{14}$$
where $\mathbf{Q}$ is a $M \times N$-sized matrix consisting of random integers between 0 and $2^K - 1$ as shown in Fig. 5 (c).
6. $n := n+1$. Continue to Step 3 until $n = N$.
7. $m := m+1$. Continue to Step 2 until $m = M$.
8. Scrambled image $\mathbf{f}'$ is obtained.



(a) Matrix $\mathbf{R}_1$. (b) Matrix $\mathbf{R}_2$. (c) Matrix $\mathbf{Q}$.

Fig. 5. Matrices for image scrambling. $\mathbf{R}_1$ and $\mathbf{R}_2$ are $X_B \times Y_B$-sized matrices of random integers between 0 and $2^K - 1$ for all blocks and $\mathbf{Q}$ is $M \times N$-sized matrix of random integers between 0 and $2^K - 1$ for unwatermarked blocks, where $X_B = Y_B = 5$. Elements corresponding to E pixels for data hiding are zeros in $\mathbf{R}_1$ and $\mathbf{R}_2$, where $E = 3$.

Scrambling using matrices $\mathbf{R}_1$ and $\mathbf{R}_2$ does not change E pixels for data hiding for watermarked blocks, whereas E pixels are further scrambled by $\mathbf{Q}$ in unwatermarked blocks.

5) Descrambling: The following algorithm descrambles scrambled images even the scrambled image conveys hidden data.

1. $m := 0$.
2. $n := 0$.
3. Scrambled block $\mathbf{B}'_{m,n}$ is descrambled by
$$\mathbf{B}_{m,n} = \left(\mathbf{B}'{}_{m,n} - m\mathbf{R}_1 - n\mathbf{R}_2\right) \bmod 2^K. \tag{15}$$
4. Absolute difference $d_{m,n}$ is obtained by Eq. (2).
5. In block $\mathbf{B}_{m,n}$ in which $d_{m,n} > p$, E pixels are also descrambled as
$$a_{m,n} = \left(a'_{m,n} - mQ(m,n)\right) \bmod 2^K, \tag{16}$$
$$b_{m,n} = \left(b'_{m,n} - mQ(m,n)\right) \bmod 2^K, \tag{17}$$
$$g_{m,n} = \left(g'_{m,n} - nQ(m,n)\right) \bmod 2^K. \tag{18}$$
6. $n := n+1$. Continue to Step 3 until $n = N$.
7. $m := m+1$. Continue to Step 2 until $m = M$.
8. Descrambled image $\mathbf{f}$ is obtained.

C. Features

This section summarizes the three main features of the proposed scheme, namely collaborative for data hiding and image scrambling, spatial domain processing, and lossless data hiding.

1) Collaborative: The proposed scheme divides an image into two parts as well as the conventional schemes [19], [20]; A part is for data hiding and the other is for image scrambling. The proposed scheme, however, scrambles pixels for data hiding in unusable blocks that no data bit is hidden to unusable blocks. Parameter p that is commonly used for data hiding and image scrambling in the proposed scheme is derived with taking account into collaboration of data hiding and image scrambling.

Let

$$a_{m,n} + mQ(m,n) = \alpha_{m,n}2^K + a'_{m,n} \tag{19}$$

$$b_{m,n} + mQ(m,n) = \beta_{m,n}2^K + b'_{m,n} \tag{20}$$

from Eqs. (12) and (13) with non-negative integers $\alpha_{m,n}$ and $\beta_{m,n}$. When $a_{m,n} = b_{m,n}$,

$$\left|a'_{m,n} - b'_{m,n}\right| = |a_{m,n} - b_{m,n}| = d_{m,n} \geq p, \tag{21}$$

since Eqs. (12) and (13) adds same quantity $mQ(m,n)$. If $a_{m,n} \neq b_{m,n}$, it is summarized that

$$\left|a'_{m,n} - b'_{m,n}\right| = \left|(\alpha_{m,n} - \beta_{m,n})\,2^K - (a_{m,n} - b_{m,n})\right|. \tag{22}$$

Here,

$$\beta_{m,n} = \alpha_{m,n} + \left\lfloor \frac{a'_{m,n} - a_{m,n} + b_{m,n}}{2^K} \right\rfloor \tag{23}$$

is derived from Eqs. (19) and (20), and

$$-1 \leq \left\lfloor \frac{a'_{m,n} - a_{m,n} + b_{m,n}}{2^K} \right\rfloor < 2 \tag{24}$$

holds because $0 \leq a_{m,n}, b_{m,n}, a'_{m,n} < 2^K$. Thus,

$$0 \leq |\alpha_{m,n} - \beta_{m,n}| \leq 1 \tag{25}$$

is derived. When $a_{m,n} \neq b_{m,n}$ and $\alpha_{m,n} = \beta_{m,n}$, Eq. (22) results in

$$\left|a'_{m,n} - b'_{m,n}\right| = d_{m,n} \geq p. \tag{26}$$

For the condition that $a_{m,n} \neq b_{m,n}$ and $|\alpha_{m,n} - \beta_{m,n}| = 1$, when $\alpha_{m,n} \geq \beta_{m,n}$, $a_{m,n} \geq b_{m,n}$ holds, when $\alpha_{m,n} < \beta_{m,n}$, $a_{m,n} < b_{m,n}$ holds, Eq. (22) becomes

$$\left|a'_{m,n} - b'_{m,n}\right| = 2^K - d_{m,n}, \tag{27}$$

because $d_{m,n} < 2^K$. Since p is given by Eq. (7),

$$\left|a'_{m,n} - b'_{m,n}\right| = 2^K - d_{m,n} \geq p \tag{28}$$

holds. It is concluded that

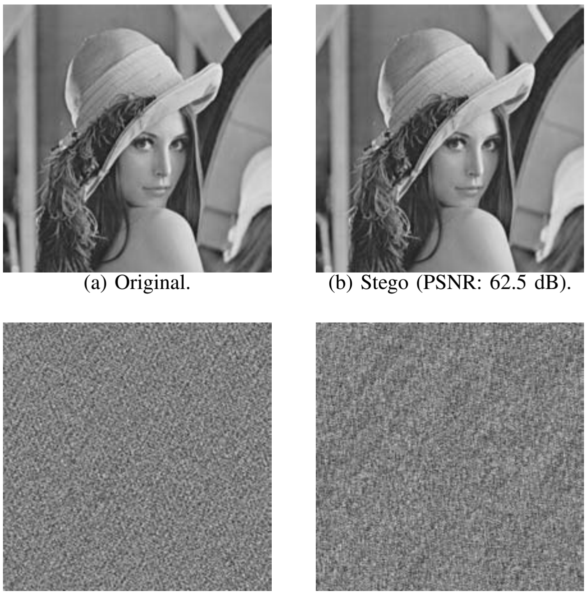
$$\left|a'_{m,n} - b'_{m,n}\right| \geq p \tag{29}$$

as well as

$$|a_{m,n} - b_{m,n}| \geq p. \tag{30}$$

So, the proposed scheme distingusishes usable blocks from the unusable, even the image is scrambled. Thus, the proposed scheme can extracts hidden data from a scrambled stego image as well as descrambles a scrambled stego image, as shown in Fig. 1.

2) Spatial Domain Processing: The proposed scheme embeds data to an image and scrambles an image in the spatial domain, whereas the conventional schemes do in the transformed domain in a compression encoding of an image [19], [20]. That is, the conventional schemes are dedicated to compressed images, and these schemes neither extract hidden watermark nor descramble for decoded images. On the other hand, the proposed scheme works in the spatial domain, so it is applicable to any images.



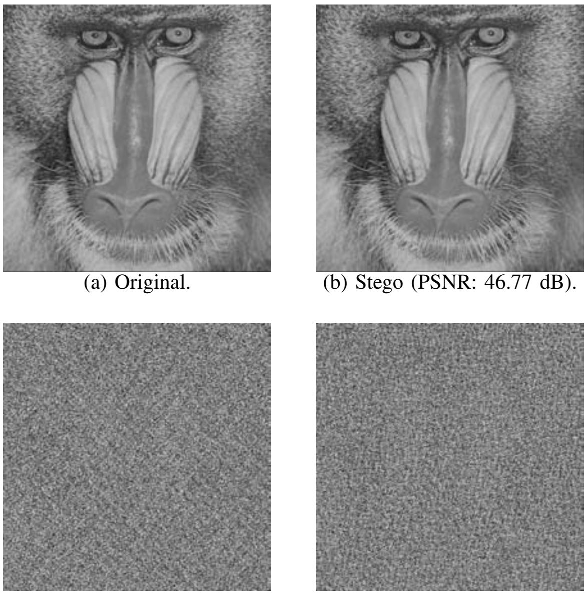
(a) Original.

(b) Stego (PSNR: 62.5 dB).

(c) Scrambled (PSNR: 9.609 dB).

(d) Scrambled stego (PSNR: 9.605 dB).

Fig. 6. Results for "lena." Stego images convey 633 bits hidden data in each, i.e., $L = 633$.



(a) Original.

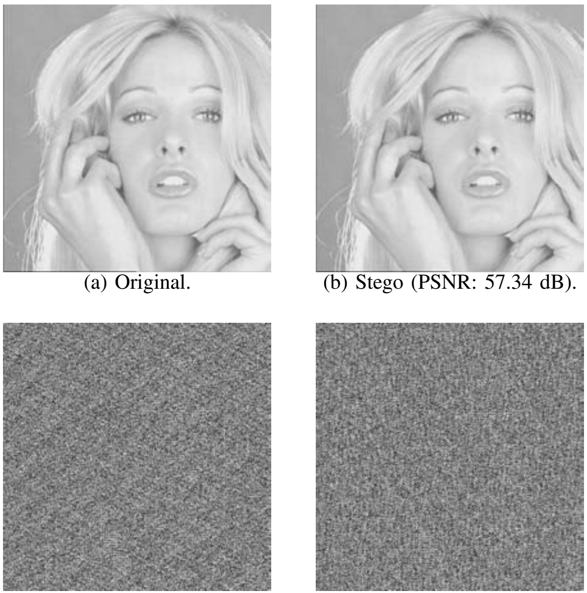
(b) Stego (PSNR: 46.77 dB).

(c) Scrambled (PSNR: 10.02 dB).

(d) Stego scrambled (PSNR: 10.01 dB).

Fig. 7. Results for "baboon." Stego images convey 4069 bits hidden data in each, i.e., $L = 4069$.

3) Lossless Data Hiding: By using parameter p that is obtained from the statistics of pixels neigbhoring to the pixel for watermarking, the usability is checked by comparing p and absolute difference $d_{m,n}$. The proposed scheme hides data only to usable blocks in which the operation for hidden data extraction based on arithmetic modulo 2 properly works.



(a) Original.

(b) Stego (PSNR: 57.34 dB).

(c) Scrambled (PSNR: 7.877 dB).

(d) Stego scrambled (PSNR: 7.884 dB).

Fig. 8. Results for “tiffany.” Stego images convey 2841 bits hidden data in each, i.e., $L = 2841$.

IV. Experimental Results

Figures 6, 7, and 8 show the results for 512×512-sized 8-bits grayscale images, “lena,” “baboon,” and “tiffnay,” respectively. That is, $X = Y = 512$ and $K = 8$.

It is found that the proposed scheme scrambles the images properly. It is confirmed that the scrambled and scrambled stego images are different by those PSNR values. Besides, it is confirmed the proposed scheme serves the flexibility in a processing flow as shown in Fig. 1.

V. Conclusions

This paper has proposed a collaborative scheme for lossless data hiding and image scrambling. Both the image scrambling and the data hiding are based on spatial domain which is differernt from the conventional schemes based on transformed domain. The proposed scheme serves lossless data hiding, whereas the conventional schemes only serve lossy data hiding, i.e., the original image cannot be recovered from the stego image.

Increasing the data hiding capacity is one of future works.

References

[1] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk, “Watermarking digital image and video data,” *IEEE Signal Process. Mag.*, vol.17, no.5, pp.20–46, Sep. 2000.

[2] M. Barni, “What is the future for watermarking? (Part I),” *IEEE Signal Process. Mag.*, vol.20, no.5, pp.55–59, Sep. 2003.

[3] M. Barni, “What is the future for watermarking? (Part II),” *IEEE Signal Process. Mag.*, vol.20, no.6, pp.53–59, Nov. 2003.

[4] M. Fujiyoshi, Y. Seki, H. Kobayashi, and H. Kiya, “Modulo arithmetic-based image watermarking and its theoretical analysis of image-quality,” in *Proc. IEEE ICIP*, 2005, pp.969–972.

[5] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, “Circular interpretation of bijective transformations in lossless watermarking for media asset management,” *IEEE Trans. Multimedia*, vol.5, pp.97–105, Mar. 2003.

[6] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” *IEEE Trans. Image Process.*, vol.14, pp.253–266, Feb. 2005.

[7] M. Fallahpour, D. Megias, and M. Ghanbari, “High capacity, reversible data hiding in medical images,” in *Proc. IEEE ICIP*, 2009, pp.4241–4244.

[8] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding — New paradigm in digital watermarking,” *EURASIP J. Applied Signal Process.*, vol.2002, pp.185–196, Feb. 2002.

[9] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol.13, pp.890–896, Aug. 2003.

[10] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol.16, pp.354–362, Mar. 2006.

[11] D. Coltuc, “Improved capacity reversible watermarking,” in *Proc. IEEE ICIP*, 2007, pp.249–252.

[12] P. Tsai, Y.-C. Hu, and H.-L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” *Signal Processing*, vol.89, pp.1129–1143, Jun. 2009.

[13] M. Fujiyoshi, S. Sato, H.L. Jin, and H. Kiya, “A location-map free reversible data hiding method using block-based single parameter,” in *Proc. IEEE ICIP*, 2007, pp.257–260.

[14] S. Han, M. Fujiyoshi, and H. Kiya, “A reversible image authentication method without memorization of hiding parameters,” *IEICE Trans. Fundamentals*, vol.E92-A, pp.2572–2579, Oct. 2009.

[15] R. Caldelli, F. Filippini, and R. Becarelli, “Reversible watermarking techniques: An overview and a classification,” *EURASIP J. Inf. Security*, vol.2010, 2010.

[16] I. Ito and H. Kiya, “Phase scrambling for blind image matching,” in *Proc. IEEE ICASSP*, 2009, pp.1521–1524.

[17] S. Imaizumi, M. Fujiyoshi, and H. Kiya, “Efficient collusion attack-free access control for multidimensionally hierarchical scalability content,” in *Proc. IEEE ISCAS*, 2009, pp.505–508.

[18] M. Fujiyoshi, K. Kuroiwa, and H. Kiya, “A Scrambling method for Motion JPEG videos enabling moving objects detection from scrambled videos,” in *Proc. IEEE ICIP*, 2008, pp.773–776.

[19] T. Abe, H. Fujii, K. Kushima, N. Sakurai, “Image distribution method with identifier embedding scheme for copyright protection,” *IEICE Trans. Fundamentals*, vol.J82-A, pp.1474–1482, Sept. 1999.

[20] H. Wakairo, S. Kang, Y. Sakamoto, “Digital watermarking technique to prevent from illegal reuse of the partial-scrambled video” in *Proc. IEICE MIH Workshop*, pp.53–58, Jun. 2010.