EUSIPCO 2013 1569746443

A SEPARABLE LOSSLESS DATA EMBEDDING SCHEME IN ENCRYPTED IMAGES CONSIDERING HIERARCHICAL PRIVILEGE

Masaaki FUJIYOSHI

Department of Information and Communication Systems, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan

ABSTRACT

This paper proposes a new scheme of separable lossless data embedding for encrypted images in which hidden data can be extracted from an image with embedded data even the image is encrypted. The proposed scheme firstly encrypts an image and simultaneously prepares room for lossless data embedding. Data are, then, concealed in the encrypted image by a lossless data embedding method based on histogram shifting, and the encrypted image carrying hidden data is sent to a receiver. According to key sets which the receiver has, he/she is allowed to take seven different actions based on hierarchy, whereas the conventional separable scheme offers only three actions. This feature of the proposed scheme extends applicable scenarios. Moreover, the proposed scheme always restore the original image, whereas the conventional scheme sometimes fails to do. Experimental results show the effectiveness of the proposed scheme.

***Index Terms*—** Encryption, Scramble, Access control, Digital watermarking, Annotation

1. INTRODUCTION

Data embedding technology has been diligently studied [1–3], for not only security-related problems [4, 5], in particular, intellectual property rights protection of digital content [6], but also non security-oriented issues [4, 7] such as broadcast monitoring [8]. A data embedding scheme inserts data referred to as a *payload* to a target signal that is called as the *original* signal. It, then, generates a slightly distorted signal conveying the payload where the signal is referred to as a *stego* signal.

Many of data embedding schemes extract the embedded payload from the stego signal but schemes leave the stego signal as it is. In military and medical applications, recovering the original signal as well as hidden payload extraction are desired [9], so *lossless* data embedding (LDE) schemes which recover the original signal have been proposed [9–13]. This paper focuses on LDE.

Aside from data embedding, encryption is well-known for protecting signals. Except for naïve encryption [14] where a signal is encrypted without taking the signal's medium into account, media-aware encryption such as image scrambling [15] becomes popular. An image encryption technique once severely distorts or scrambles an image to protect the image visually, and the distorted image is referred to as an *encrypted* image. It generally decrypts the original image from the encrypted image without any error.

In some applications, both data embedding and image scrambling are desired. Even some studies encrypt an image by data embedding [16], applying two technologies to an image in series is the simplest solution. In this approach, however, image decryption is required to extract the embedded payload or vice versa according to the applying order [17–19], and this approach is referred to as non-separable [20].

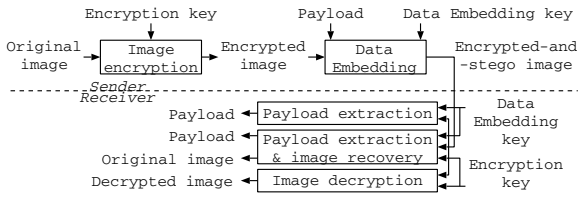


Fig. 1. The conventional scheme of separable lossless data embedding in encrypted images [20].

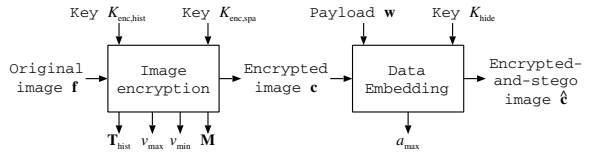
This paper proposes a scheme of LDE in encrypted images where either payload extraction or image decryption is applicable to an encrypted-and-stego image, i.e., the proposed scheme is *separable* [20]. The proposed scheme allows a receiver of the image 1) to extract the embedded payload, 2) to get a partially decrypted image, 3) to obtain a decrypted image, 4) to recover its original image, 5) both 1 and 2, 6) both 1 and 3, and 7) both 1 and 4, according to the receiver's rights, whereas the conventional scheme offers 1), 3), and 7) [20], viz., the proposed scheme takes hierarchical privilege into account. Moreover, the proposed scheme always restore the original image, while the conventional scheme sometimes fails to do.

2. CONVENTIONAL SEPARABLE LOSSLESS DATA EMBEDDING SCHEME IN ENCRYPTED IMAGES

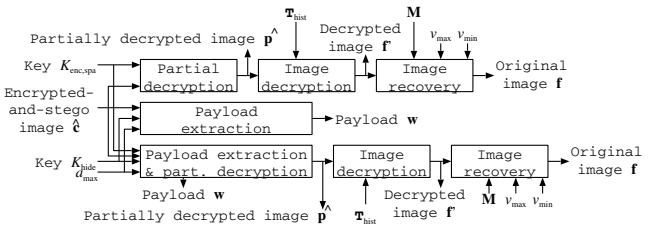
This section reviews the conventional scheme of separable LDE in encrypted images [20] shown in Fig. 1 to clarify the problem focused in this paper.

This scheme [20] firstly applies a bitwise exclusive-or operation to an original image and pseudo random bits, in a bit-by-bit of pixel-by-pixel manner, where pseudo random bits are generated by a standard stream cipher using an encryption key. A pixel permutation is further applied to the encrypted image, and then, several pixels are pseudo-randomly selected with a data embedding key. Parameters for data embedding are placed over the least significant bit of selected pixels. The original state of the above mentioned bits and a payload are placed over less significant bits of remaining pixels.

With the key for data embedding, a receiver can extract parameters and the embedded payload from the encrypted-and-stego image. A receiver having the encryption key can apply the bitwise exclusive-or operation to the image and pseudo random bits, and pixels of the image are correctly decrypted except for less significant bits in pixels conveying the payload and overhead information; he/she gets a decrypted image which differs from the original image. A receiver who has both keys can extract the payload and recover the



(a) Encryption and data embedding.



(b) Decryption, data extraction, and original image recovery.

Fig. 2. Proposed scheme.

original image. This scheme, however, estimates, instead of recovers, the original state of bits which are lost by embedding the payload and overhead information. It results in that this scheme sometimes fails to restore the original image.

Two major problems of this conventional scheme are following. 1) It is assumed that the receiver who needs the payload alone needs the original image, even access control with multiple levels [21, 22] based on the hierarchy is desired in organizations. 2) The original image is not always recovered. It is dysfunctional in applications in which LDE and encryption are desired.

To overcome these two disadvantages of the conventional scheme, the next section proposes a new scheme of separable LDE in encrypted images. The proposed scheme offers receivers seven different actions based on their rights and it always restores the original image.

3. PROPOSED SCHEME

This section proposes a new scheme for separable LDE in encrypted images which is shown in Fig. 2. Four algorithms of the proposed scheme are described in the subsequent sections, and the features of the proposed scheme are summarized.

It is assumed hereafter that Q-bit quantized $X \times Y$-sized image $\mathbf{f} = \{f(x,y)\}$ is an original image, where $x = 0,1,\ldots,X-1$, $y = 0,1,\ldots,Y$, and $f(x,y) \in \{0,1,\ldots,2^Q-1\}$.

3.1. Image Encryption

This algorithm has two aims; One is image encryption and the other is preparing room for subsequent data embedding. Original image $\mathbf{f}$ and keys $K_{\text{enc,hist}}$ and $K_{\text{enc,spa}}$ are fed to this algorithm, and the algorithm outputs Q-bit quantized $X \times Y$-sized encrypted image $\mathbf{c}$, pixel values $v_{\max}$ and $v_{\min}$, histogram permutation table $\mathbf{T}_{\text{hist}}$, and a location map as follows.

Step 1. Obtain tonal distribution $\mathbf{h} = \{h(v)\}$ from original image $\mathbf{f}$, where $h(v)$ represents the number of pixels with pixel value v and $v = 0,1,\ldots,2^Q-1$. Find two pixel values $v_{\max}$ and $v_{\min}$, where

$$v_{\max} = \arg\max_v h(v), \tag{1}$$

$$v_{\min} = \arg\min_v h(v), \tag{2}$$

respectively.

Step 2. Location map $\mathbf{M}$ which indicates the spatial position of pixels with pixel value $v_{\min}$ is generated. In addition, Q-bit quantized $X \times Y$-sized nonlinear quantized image $\mathbf{f}' = \{f'(x,y)\}$ is generated, to zero the number of pixels with pixel value $v_{\min}$ and simultaneously to increase the number of pixels with pixel value $v_{\max}$, as

$$f'(x,y) = \begin{cases} v_{\max}, & f(x,y) = v_{\min} \\ f(x,y), & \text{otherwise} \end{cases}, \tag{3}$$

where $f'(x,y) \in \{0,1,\ldots,2^Q-1\}$.

Step 3. Derive 2^Q-length histogram permutation table $\mathbf{T}_{\text{hist}} = \{t_{\text{hist}}(v)\}$ by giving key $K_{\text{enc,hist}}$ to a restricted pseudo random number generator (PRNG) where $t_{\text{hist}}(v) \in \{0,1,\ldots,2^Q-1\}$ and $t_{\text{hist}}(v_{\min})$ is restricted to as

$$t_{\text{hist}}(v_{\min}) = t_{\text{hist}}(v_{\max}) - 1. \tag{4}$$

Generate Q-bit quantized $X \times Y$-sized histogram permuted image $\mathbf{p} = \{p(x,y)\}$ as

$$p(x,y) = t_{\text{hist}}\left(f'(x,y)\right), \tag{5}$$

where $p(x,y) \in \{0,1,\ldots,2^Q-1\}$.

Step 4. Get $X \times Y$-sized spatial permutation table $\mathbf{T}_{\text{spa}} = \{\mathbf{t}_{\text{spa}}(x,y)\}$ by feeding key $K_{\text{enc,spa}}$ to a pseudo random matrix generator where $\mathbf{t}_{\text{spa}}(x,y) = \{(m,n)\}$. Create encrypted image $\mathbf{c} = \{c(m,n)\}$ by

$$c(m,n) = p(x,y), \tag{6}$$

where

$$(m,n) = \mathbf{t}_{\text{spa}}(x,y), \tag{7}$$

$m = 0,1,\ldots,X-1$, $n = 0,1,\ldots,Y-1$, and $c(m,n) \in \{0,1,\ldots,2^Q-1\}$.

Here, encrypted image $\mathbf{c}$ which is given to the data embedding algorithm described in the next section is generated.

Figure 3 shows an example where 3-bit quantized 5×4-sized images are used, i.e., $X = 5$, $Y = 4$, and $Q = 3$. Figure 3 (f) shows zero histogram bin is next to the largest histogram bin, where the histogram permutation with Eq. (5) achieves it as shown in Fig. 3 (f). It is noted that the zero histogram bin is not next to the largest histogram bin in image $\mathbf{f}'$ quantized by Eq. (3) as shown in Fig. 3 (d). It is confirmed that the contour still remains after the histogram permutation, c.f., Figs. 3 (c) and (e), the spatial permutation does not change the histogram, c.f., Figs. 3 (f) and (h).

3.2. Data Embedding

This algorithm hides L-length binary payload $\mathbf{w} = \{w(l)\}$ into encrypted image $\mathbf{c}$ based on a LDE method [10] where $L \le h(v_{\max}) + h(v_{\min})$, $l = 0,1,\ldots,L-1$, and $w(l) \in \{0,1\}$. The algorithm takes $\mathbf{c}$ and key K_{hide}, and it outputs image $\hat{\mathbf{c}} = \{\hat{c}(x,y)\}$ and pixel value $a_{\max}$ where $\hat{\mathbf{c}}$ is the encrypted-and-stego image.

(a) Original image **f**. (b) Original histogram **h**.

(c) Quantized image $\mathbf{f}'$. (d) Quantized histogram.

(e) Histogram permuted image **p**. (f) Histogram permuted histogram.

(g) Encrypted image **c**. (h) Encrypted histogram.

Fig. 3. An example of image encryption in the proposed scheme for a 3-bit quantized 5×4-sized image ($X = 5$, $Y = 4$, $Q = 3$, $v_{\max} = 4$, $v_{\min} = 0$, $t_{\text{hist}}(v_{\min}) = 5$, and $t_{\text{hist}}(v_{\max}) = 6$). The histogram permuted image (e) is drastically changed from its original image (a), but the contour still remains. The spatial permuted image (g) is different from the histogram permuted image, but those histogram are the same, c.f., (f) and (h).

1. Derive tonal distribution $\mathbf{d} = \{d(a)\}$ from encrypted image **c**, where $d(a)$ represents the number of pixels with pixel value a and $a = 0, 1, \ldots, 2^Q - 1$. Find pixel value $a_{\max}$ where

$$a_{\max} = \arg\max_a d(a), \tag{8}$$

$$d_{\max} = \max d(a) = d(a_{\max}). \tag{9}$$

2. Generate $d_{\max}$-length pixel permutation table $\mathbf{T}_{\text{hide}} = \{t_{\text{hide}}(\delta)\}$ by giving key K_{hide} to a PRNG, where $\delta = 0, 1, \ldots, d_{\max} - 1$ and $t_{\text{hide}}(\delta) \in \{0, 1, \ldots, d_{\max} - 1\}$.
3. Payload **w** is embedded in **c** by

$$\hat{c}(m,n) = \begin{cases} a_{\max} - 1, & c(m,n) = a_{\max} \text{ and } w(l) = 0 \\ a_{\max}, & c(m,n) = a_{\max} \text{ and } w(l) = 1 \\ c(m,n), & \text{otherwise} \end{cases}, \tag{10}$$

where $\hat{c}(x,y) \in \{0, 1, \ldots, 2^Q - 1\}$. It is noted that l-th payload bit $w(l)$ is hidden to the $t_{\text{hide}}(l)$-th $c(m,n)$ with pixel value $a_{\max}$ in left-to-right and top-to-bottom scanning order.

Now, image $\hat{\mathbf{c}}$, the encrypted-and-stego image, is ready to be transmitted to a receiver. It is noted that $d(a_{\max}) = d(t_{\text{hist}}(v_{\max})) = h(v_{\max})$.

An example of data embedding for the image shown in Fig. 3 (g) is shown in Fig. 4. According to pixel permutation table $\mathbf{T}_{\text{hide}}$, two pixels of four pixels with pixel value $a_{\max}$ become $(a_{\max} - 1)$ to carry payload bit '0,' c.f., Eq. (10).

(a) Encrypted-and-stego image $\hat{\mathbf{c}}$. (b) Encrypted-and-stego histogram.

Fig. 4. An example of data embedding for the image shown in Fig. 3 (g). Payload '0110' is pseudo randomly hidden over four pixels with pixel value '6,' and two of four pixels become '5,' according to pixel permutation table $\mathbf{T}_{\text{hide}}$ ($a_{\max} = 6$ and $d(a_{\max}) = d_{\max} = 4$).

Through algorithms described in Sect. 3.1 and 3.2, several keys are used and several parameters are output. Here, they are summarized as key sets; key set for partial decryption $\mathbf{K}_{\text{pd}}$ consists of key $K_{\text{enc,spa}}$, i.e., $\mathbf{K}_{\text{pd}} = \{K_{\text{enc,spa}}\}$, key set for decryption $\mathbf{K}_{\text{dec}}$ is comprised of histogram permutation table $\mathbf{T}_{\text{hist}}$, that is, $\mathbf{K}_{\text{dec}} = \{\mathbf{T}_{\text{hist}}\}$, and key set for original image recovery $\mathbf{K}_{\text{rec}}$ includes pixel values $v_{\max}$ and $v_{\min}$ and location map $\mathbf{M}$ ($\mathbf{K}_{\text{rec}} = \{v_{\max}, v_{\min}, \mathbf{M}\}$), whereas key set for payload extraction $\mathbf{K}_{\text{ext}}$ has pixel value $a_{\max}$ and key K_{hide}, viz., $\mathbf{K}_{\text{ext}} = \{a_{\max}, K_{\text{hide}}\}$. It is assumed that these key sets are transmitted from a sender to a receiver through a secure communication channel.

3.3. Embedded Payload Extraction

If a receiver getting $\hat{\mathbf{c}}$ also receives key set $\mathbf{K}_{\text{ext}}$, the receiver can take out embedded payload **w** from $\hat{\mathbf{c}}$.

1. Generate pixel permutation table $\mathbf{T}_{\text{hide}}$ by giving key K_{hide} to the PRNG which is identical to that used in the previous section.
2. According to $\mathbf{T}_{\text{hide}}$, extract concealed payload **w** from $\hat{\mathbf{c}}$ as

$$w(l) = \begin{cases} 0, & \hat{c}(m,n) = a_{\max} - 1 \\ 1, & \hat{c}(m,n) = a_{\max} \end{cases}, \tag{11}$$

where $w(l)$ is extracted from the $t_{\text{hide}}(l)$-th $\hat{c}(m,n)$ with pixel value $a_{\max}$ in left-to-right and top-to-bottom scanning order.

The receiver can obtain **w** from $\hat{\mathbf{c}}$, but he/she cannot get either original image **f**, a decrypted image, or a partially decrypted image.

3.4. Decryption and Image Recovery

If one receiving $\hat{\mathbf{c}}$ has key set $\mathbf{K}_{\text{pd}}$, the receiver can obtain Q-bit quantized $X \times Y$-sized partially decrypted image $\hat{\mathbf{p}} = \{\hat{p}(x,y)\}$ where $\hat{p} \in \{0, 1, \ldots, 2^Q - 1\}$.

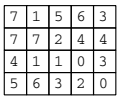
1. Generate spatial permutation table $\mathbf{T}_{\text{spa}}$ by giving key $K_{\text{enc,spa}}$ to the pseudo random matrix generator which is the identical to that used at Step 4 in Section 3.1. Inversely permute $\hat{\mathbf{c}}$ to obtain partially decrypted image $\hat{\mathbf{p}}$ as

$$\hat{p}(x,y) = \hat{c}(m,n), \tag{12}$$

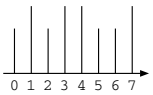
where

$$(m,n) = \mathbf{t}_{\text{spa}}(x,y). \tag{13}$$

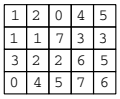
In addition, he/she has key set $\mathbf{K}_{\text{dec}}$, the receiver further obtain Q-bit quantized $X \times Y$-sized decrypted image $\hat{\mathbf{f}}' = \{\hat{f}'(x,y)\}$ where $\hat{f}'(x,y) \in \{0, 1, \ldots, 2^Q - 1\}$.



(a) Partially decrypted image $\hat{\mathbf{p}}$.



(b) Partially decrypted histogram.



(c) Decrypted image $\hat{\mathbf{f}}'$.

(d) Decrypted histogram.

Fig. 5. An example of decryption for the image shown in Fig. 4 (a). The contour lines of Fig. 3 (a) can be recognized in $\hat{\mathbf{p}}$ and $\hat{\mathbf{f}}'$ is still distorted by design to be different from the original image.

2. Inversely permute $\hat{\mathbf{p}}$ to obtain decrypted image $\hat{\mathbf{f}}'$ as

$$\hat{f}'(x,y) = t_{\text{hist}}^{-1}\left(\hat{p}(x,y)\right), \tag{14}$$

where t_{hist}^{-1} gives inverse permutation of t_{hist}.

Moreover, if the receiver also has key set $\mathbf{K}_{\text{rec}}$, he/she can recover original image $\mathbf{f}$.

3. Recover $\mathbf{f}'$ from $\hat{\mathbf{f}}'$ by

$$f'(x,y) = \begin{cases} v_{\max}, & \hat{f}'(x,y) = v_{\min} \\ \hat{f}'(x,y), & \text{otherwise} \end{cases}. \tag{15}$$

Finally, set the pixel value of pixels recorded in location map $\mathbf{M}$ to $v_{\min}$ to recover $\mathbf{f}$.

Partially decrypted image $\hat{\mathbf{p}}$, decrypted image $\hat{\mathbf{f}}'$, and original image $\mathbf{f}$ are recovered without extracting payload $\mathbf{w}$.

Figure 5 shows an example of decryption for the image shown in Fig. 4 (a). Partially decrypted image shown in Fig. 5 (a) is slightly distorted from the image shown in Fig. 3 (e) by data embedding, but the contour lines of the original image are recovered so that a receiver can get some information of content. The decrypted image shown in Fig. 5 (c) is still distorted by design to differ from the original image.

As described above, according to the receiver's rights, he/she can 1) extract embedded payload $\mathbf{w}$, 2) get partially decrypted image $\hat{\mathbf{p}}$, 3) obtain decrypted image $\hat{\mathbf{f}}'$, 4) recover original image $\mathbf{f}$, 5) both 1 and 2, 6) both 1 and 3, and 7) both 1 and 4, respectively, i.e., the receiver can take seven different actions for $\hat{\mathbf{c}}$.

3.5. Features

This section summarizes four features of the proposed scheme.

1) A receiver can take seven different actions according to his/her rights in the proposed scheme, whereas the conventional scheme allows the receiver to take three different actions [20]. This feature of the proposed scheme extends applicable scenarios.

2) The used LDE method [10] *is a complete LDE method.* Instead of estimating the original state in the conventional scheme, the proposed scheme employs a complete LDE method to always recover the original image.

3) Restricted histogram permutation is introduced to the encryption part in the proposed scheme so that the permutation partially encrypts an image (Eq. (5)) and simultaneously prepares room for LDE, c.f., Eq. (4).

Table 1. The embedding rate, L/XY [bits/pixel], and the averaged PSNRs of images where $L = h(v_{\max}) + h(v_{\min})$ [bits]. Prop.: the proposed scheme and Conv.: the conventional scheme [20].

Image	Embedding rate L/XY [bpp]	Averaged PSNR [dB]			
		Decrypted		Recovered	
		Prop.	Conv.	Prop.	Conv.
Baboon	0.012	31.28	51.14	∞	51.16
F-16	0.036	39.49	51.13	∞	51.30
Lena	0.012	33.34	51.13	∞	51.20
Peppers	0.012	31.81	51.14	∞	51.18
Sailboat	0.016	34.99	51.14	∞	51.18
Splash	0.027	28.05	51.15	∞	51.27
Tiffany	0.020	22.50	51.12	∞	51.23

4) Parameters are keys in the proposed scheme. Opposite to ordinary LDE schemes which try to become free from memorizing parameters [23,24], the proposed scheme utilizes parameters such as $a_{\max}$, $\mathbf{T}_{\text{hist}}$, $v_{\max}$, $v_{\min}$, and $\mathbf{M}$ for privilege control as well as keys $K_{\text{enc,spa}}$ and K_{hide}.

4. EXPERIMENTAL RESULTS

Seven 512×512-sized color images from database [25] are converted to 8-bit grayscale images for evaluation, i.e., $X = Y = 512$ and $Q = 8$. Mersenne twister [26] with 32-bit seed is used as the PRNG. Payload size L is set to capacity of the proposed scheme $h(v_{\max}) + h(v_{\min})$ and parameters of the conventional scheme [20] are chosen to maximize the peak signal-to-noise ratio (PSNR) of decrypted and recovered images.

Table 1 shows the embedding rate and the averaged PSNR for decrypted and recovered images of the proposed and conventional schemes. It is confirmed that the conventional scheme serves visually lossless decrypted images whereas the proposed scheme does remain noise to them. On the other hand, the proposed scheme perfectly recovers the original image from an encrypted-and-stego image, whereas the conventional scheme fails to do.

Figure 6 shows an example by the proposed scheme for image 'F-16,' and it is confirmed that the encrypted and encrypted-and-stego images are unintelligible enough. Even structural similarity (SSIM) [27] index for the partially decrypted image is low due to histogram permutation, the shape of content is recognizable for human visual system.

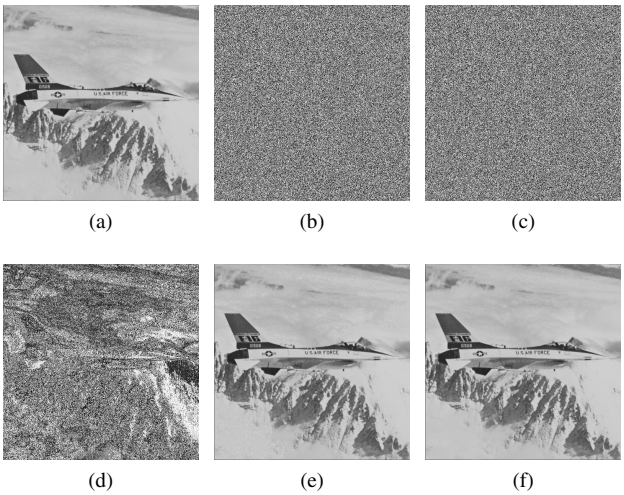
5. CONCLUSIONS

This paper has proposed a new scheme for separable LDE in encrypted images. The proposed scheme allows a receiver to take seven different actions which expands applicable scenarios, in particular, those with privilege hierarchies. In addition, this scheme always recovers the original image, whereas the conventional scheme sometimes fails to do.

Further works include making the proposed scheme commutative [28–30], detailed security analysis of the scheme, and extending the scheme to work in conjunction with image compression.

ACKNOWLEDGMENT

This work has been partly supported by the Grant-in-Aid for Young Scientists (B), No.20336522, from the Ministry of Education, Culture, Sports, Science and Technology of Japan and from the Japan Society for the Promotion of Science.



(a) (b) (c)

(d) (e) (f)

Fig. 6. (a) Original F-16, (b) its encrypted version, (c) the encrypted-and-stego image with embedding rate 0.036 [bpp], (d) the partially decrypted image where the contour lines are visible (SSIM: 0.025), (e) the decrypted image which is distorted by design (PSNR: 39.49 dB), and (f) the recovered image which is identical to (a).

REFERENCES

[1] M. Wu and B. Liu, *Multimedia Data Hiding*. Springer-Verlag New York, 2003.

[2] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. San Francisco: Morgan Kaufmann Publishers, 2008.

[3] J. Fridrich, *Steganography in digital media*. Cambridge University Press, 2010.

[4] 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.

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

[6] C.-C.J. Kuo, T. Kalker, and W. Zhou, eds., "Digital rights management," *IEEE Signal Process. Mag.*, vol.21, no.2, pp.11–117, Mar. 2004.

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

[8] T. Tachibana, M. Fujiyoshi, and H. Kiya, "A removable watermarking scheme retaining the desired image quality," in *Proc. IEEE ISPACS*, 2003, pp.538–542.

[9] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," *EURASIP J. Inf. Security*, vol.2010, no.134546, 2010.

[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] C. Dragoi and D. Coltuc, "Improved Rhombus interpolation for reversible watermarking by difference expansion," in *Proc. EURASIP EUSIPCO*, 2012, pp.1688–1692.

[12] D. Coltuc and A. Tudoroiu, "Multibit versus multilevel embedding in high capacity difference expansion reversible watermarking," in *Proc. EURASIP EUSIPCO*, 2012, pp.1791–1795.

[13] M. Fujiyoshi and H. Kiya, "Generalized histogram shifting-based reversible data hiding with an adaptive binary-to-q-ary converter," in *Proc. APSIPA ASC*, 2012.

[14] B.B. Zhu, M.D. Swanson, and S. Li, "Encryption and authentication for scalable multimedia: Current state of the art and challenges," in *Proc. SPIE*, vol.5601, 2004, pp.157–170.

[15] H. Kiya and I. Ito, "Phase scrambling for image matching in the scrambled domain," in *Signal Processing*, S. Miron, Ed. InTech, 2010, pp.397–414.

[16] S. Ong, K. Wong, and K. Tanaka, "Reversible data embedding using reflective blocks with scalable visual quality degradation," in *Proc. IEEE IIH-MSP*, 2012, pp.363–366.

[17] A. Piva and S. Katzenbeisser, ed., "Special issue on signal processing in the encrypted domain," *EURASIP J. Inf. Security*, vol.2007, Jul. 2007.

[18] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol.18, pp.255–258, Apr. 2011.

[19] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol.19, pp.199–202, Apr. 2012.

[20] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol.7, pp.826–832, Apr. 2012.

[21] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-based access control models," *IEEE Computer*, vol.29, no.2, pp.38–47, Feb. 1996.

[22] M. Fujiyoshi, S. Han, and H. Kiya, "Reversible information hiding considering hierarchical access control," in *Proc. IEEE IAS*, 2009, pp.I-209–I-212.

[23] J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in *Proc. IWDW*, LNCS, vol.4283/2006, 2006, pp.348–361.

[24] M. Fujiyoshi and H. Kiya, "Reversible information hiding and its application to image authentication," in *Multimedia Information Hiding Technologies and Methodologies for Controlling Data*, K. Kondo, Ed. IGI Global, 2012, pp.238–257.

[25] "The USC-SIPI Image Database," Signal & Image Processing Institute, University of Southern California. [Online]. Available: http://sipi.usc.edu/database/

[26] M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Modeling and Computer Simulation*, vol.8, pp.3–30, Jan. 1998.

[27] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol.13, pp.600–612, Apr. 2004.

[28] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *SPIE Opt. Eng.*, vol.45, pp.080 510–1–080 510–3, Aug. 2006.

[29] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured haar transform domain," *Signal Process.: Image Commun.*, vol.26, pp.1–12, Jan. 2011.

[30] S. Liu, M. Fujiyoshi, and H. Kiya, "A collaborative scheme for lossless data hiding and image scrambling," in *Proc. IEICE/ITE/KSBE IWAIT*, 2011.