Signal Processing 104 (2014) 387–400

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

High-capacity reversible data hiding in encrypted images by prediction error

Xiaotian Wu [a], Wei Sun [b,c,*]

[a] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
[b] School of Software, Sun Yat-sen University, Guangzhou 510006, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 30 December 2013
Received in revised form
25 April 2014
Accepted 29 April 2014
Available online 9 May 2014

Keywords:
Privacy preserving
Reversible data hiding
Image encryption
Prediction error

ABSTRACT

In recent years, signal processing in encrypted images received much attention from academia due to the privacy preserving property. Reversible data hiding in encrypted images is a technique that embedded additional data into an encrypted image without accessing the content of the original image, the embedded data can be extracted and the encrypted image can be recovered to the original one. In this paper, two reversible data hiding methods in encrypted images, namely a joint method and a separable method, are introduced by adopting prediction error. In the joint method, data extraction and image reconstruction are performed at the same time. The reversibility, number of incorrect extracted bits are significantly improved while maintaining good visual quality of recovered image, especially when embedding rate is high. In the separable method, data extraction and image recovery are separated. The separable method also provides improved reversibility and good visual quality of recovered image for high payload embedding.

© 2014 Published by Elsevier B.V.

1. Introduction

Reversible data hiding in images is a methodology that embeds additional messages into some distortion-unacceptable covers, such as medical, military or law forensic images, with a reversible manner that the original covers can be losslessly recovered after the embedded messages are extracted. In recent years, many reversible data hiding approaches have been proposed. Tian [1] introduced a difference expansion method, where two pixels are used as a group and a bit is embedded into each group by expanding the pixel difference. Ni et al. [2] exploited the image histogram and concealed the secret data by shifting the histogram. Tai et al. [3] proposed an efficient reversible data hiding method by shifting the histogram with the assistance of a binary tree. More investigations on reversible data hiding can be found in [4–11].

Signal processing in encrypted domain has attracted considerable research interest. With regard to providing confidentiality for images, encryption is an effective and popular means for a content owner to convert the original and meaningful content to incomprehensible one. However, in some scenarios a content owner does not trust the processing service provider, and does not want the service provider to access the content of the original image. The content owner may encrypt the image before transmission. The service provider would embed some additional messages within the encrypted image for other purposes such as image notation or authentication.

Recently, some methods on reversible data hiding in encrypted images have been proposed. Those proposed methods can be classified into two categories: joint methods

[*] Corresponding author at: School of Software, Sun Yat-sen University, Guangzhou 510006, China.
E-mail addresses: wxt.sysu@gmail.com (X. Wu), sunwei@sysu.edu.cn (W. Sun).

http://dx.doi.org/10.1016/j.sigpro.2014.04.032
0165-1684/© 2014 Published by Elsevier B.V.

and separable methods. For those joint methods, data extraction and image recovery are performed jointly. In [12], one additional bit is embedded into an associated block of cipher-text image encrypted by AES algorithm. Data extraction and image recovery are performed based on the analysis of local standard deviation of the marked encrypted image. But the embedding payload is low, and the image decrypted directly from the marked encrypted image is seriously degraded. Later, Zhang [13] introduced a method of reversible data hiding in encrypted images by modifying the least significant bits (LSBs) of the encrypted image. More exactly, a content owner encrypts the original image using XOR operation, and then a service provider partitions the encrypted image into blocks of the same size. Each block is separated into two disjoint sets. According to the embedded data, the 3 LSBs of one set are flipped. A receiver decrypts the image by using XOR operation, and uses the block smoothness to extract the embedded bits and to recover the original block. The embedding payload increases and the high fidelity of directly decrypted image is preserved. However, the probability of correctly retrieving the embedded bits and recovering the image significantly decreases when high embedding payload is adopted. Hong et al. [14] improved Zhang's method by using side match technique and a better metric for measuring the block smoothness. The capability of extracting correct embedded data and reconstructing the image is further enhanced. Another improved joint method [15] is proposed by adopting a pseudo-random sequence modulation mechanism. The additional bits are embedded by modifying the LSBs of some encrypted pixels which are determined by the pseudo-random sequences. Main advantage of this method is that the reversibility for obtaining correct extracted bits and recovering the original image is improved, when a small number of bits are embedded. In all, those reported joint methods are not capable of obtaining error-free extracted bits when high payload embedding is used.

For the second type of methods, data extraction and image decryption are separable so that perfectly extracting the embedded bits is guaranteed. Zhang [16] proposed a separable method, where some encrypted data are firstly compressed, and space for data embedding is emptied out. A receiver having the data hiding key can extract the additional data with any error, while a receiver having the encryption key can decrypt received data to obtain an image similar to the original one. If both the data hiding and encryption keys are available, the receiver can retrieve the additional data and recover the original image. Zhang's method [16] guarantees an error-free data extraction, but it is not suitable for high payload embedding. For providing better rate-distortion performance, an efficient method using low-density parity-check codes and side information is given in [17]. To obtain an error-free recovered image, Ma et al. [18] introduced a reversible data hiding methodology for encrypted images by reserving room before encryption with a conventional reversible data hiding algorithm, where the reserved room is used to accommodate the additional data. In their method, data extraction and image reconstruction are free of any error. Zhang et al. [19] proposed a reversibility improved method. Prior to encrypting the image, room for data embedding is vacated by shifting the histogram of estimating errors of some pixels. Data retrieving and image recovery in their method are error-free. Although these two methods improve the embedding capacity and the reversibility significantly, empty out room for data embedding by the content owner might be impossible, because reversible data hiding in encrypted image always requires the content owner to do nothing except image encryption, and data embedding is supposed to be accomplished by the service provider. Qian et al. [20] introduced a separable reversible data hiding approach for encrypted images using a histogram modification and n-nary data hiding method. Reserving room is no longer required at the content owner's side, and an error-free recovered image is obtained by their method.

For the mentioned methods such as [13,14,16], the reversibility, number of incorrect extracted bits and visual quality of lossy recovered image are not satisfactory when high payload embedding is carried out. In this paper, two reversible data hiding methods for encrypted images based on prediction error are introduced to improve the mentioned problems. Both the methods can provide improved reversibility and better visual quality of lossy recovered image. Further, the number of incorrect extracted bits is significantly reduced by the proposed joint method.

The remaining part of this paper is organized as follows. The joint method of reversible data hiding in encrypted images is described in Section 2. Section 3 introduces the separable method. Experimental results and discussions are provided in Section 4. Section 5 gives some concluding remarks and future work.

2. The joint method

The first method consists of three phases: image encryption phase, data hiding phase and joint data extraction and image reconstruction phase, as depicted in Fig. 1. In image encryption phase, a content owner encrypts an original uncompressed image by using an encryption key, and produces an encrypted version of the original image. In data hiding phase, a service provider (also called data-hider) embeds some additional data within the encrypted image by utilizing a data hiding key. Note that, the service provider does not know any information about the original image. In joint data extraction and image reconstruction phase, a receiver can decrypt the marked encrypted image by the encryption key, and obtain a directly decrypted image which is similar to the original one. Further, the receiver can convert the directly decrypted image to the original version and extract the embedded data with the aid of data hiding key.

2.1. Image encryption phase

The original uncompressed image C with $M \times N$ pixels is assumed to be gray level, and each gray level is denoted by 8 bits. Let (i,j) be the pixel location, and let $C(i,j)$ be the associated gray value, where $C(i,j) \in [0,255]$, $1 \le i \le M$, $1 \le j \le N$. The original image C is decomposed into 8 bit

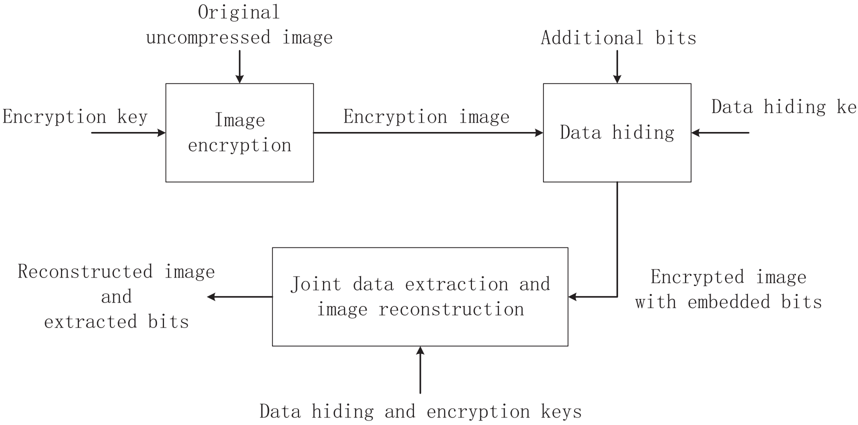
Original uncompressed image
Encryption key
Image encryption
Encryption image
Additional bits
Data hiding
Data hiding key
Reconstructed image and extracted bits
Joint data extraction and image reconstruction
Encrypted image with embedded bits
Data hiding and encryption keys

Fig. 1. Diagram of the proposed joint method.

planes, as represented by

$$b_k(i,j) = \lfloor C(i,j)/2^{(k-1)} \rfloor \bmod 2 \tag{1}$$

where $1 \le k \le 8$ and procedure $\lfloor \cdot \rfloor$ is a floor function that maps a real number to the largest previous integer.

A content owner generates $8MN$ pseudo-random bits $r_k(i,j)$ by an encryption key using a standard stream cipher. The generated pseudo-random bits are used to encrypt the original image by

$$e_k(i,j) = b_k(i,j) \oplus r_k(i,j) \tag{2}$$

where symbol $\oplus$ represents the XOR operation, and $e_k(i,j)$ is the associated encrypted bit. By orderly composing the encrypted bits, an encrypted version of the original image is achieved, as denoted by

$$E(i,j) = \sum_{k=1}^{8} e_k(i,j) \times 2^{(k-1)}. \tag{3}$$

2.2. Data hiding phase

In the data hiding phase, the service provider embeds additional bits within the encrypted image though he cannot access the original content. A collection of locations in the encrypted image is pseudo-randomly chosen according to the data hiding key. Let Γ_{Qual} and Γ_{Forb} be the qualified and forbidden sets of locations in the encrypted image, respectively. Precisely, pixels on locations in Γ_{Qual} are used to carry the additional data while pixels on locations in Γ_{Forb} are not. Γ_{Qual} and Γ_{Forb} satisfy $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. Initially, let $\Gamma_{Qual} = \emptyset$ and $\Gamma_{Forb} = \{(i,j)| i=1 \bigvee j=1 \bigvee i=M \bigvee j=N\}$. The border locations of the encrypted image are chosen to form initial Γ_{Forb}. For each time, randomly select a location (i,j) based on the data hiding key. If $(i,j) \notin \Gamma_{Forb}$, then put (i,j) into Γ_{Qual} and put $(i+1,j),(i-1,j),(i,j+1),(i,j-1)$ into Γ_{Forb}. If $(i,j) \in \Gamma_{Forb}$, the selection algorithm goes to the next round. When the number of locations in Γ_{Qual} exceeds a predefined threshold α_{TH}, the selection algorithm terminates. Pixels on the α_{TH} selected locations are used for data embedding. Note that, for each location in Γ_{Qual}, pixels on the four neighboring locations are prohibited from modification.

Pixels on the α_{TH} selected locations in Γ_{Qual} are divided into L group, and each group contains n pixels, where $n = \lfloor \alpha_{TH}/L \rfloor$. Denote the n pixels of the dth group as $B(1,d), B(2,d), \ldots, B(n,d)$. Let $S(1), S(2), \ldots, S(L)$ be the L bits to be embedded. When $S(d)=1$, the tth $(1 \le t \le 6)$ bits of the n pixels in the dth group are flipped. When $S(d)=0$, the tth bits of the n pixels in the dth group remain the same. When all the bits are embedded, a marked encrypted image is constructed.

2.3. Joint data extraction and image reconstruction phase

In this phase, we consider that a receiver has both the data hiding and encryption keys. When a receiver obtains a marked encrypted image, he firstly generates $8MN$ pseudo-random bits $r_k(i,j)$ by the encryption key. The $8MN$ bits are applied to the encrypted image to calculate the XOR result. And a directly decrypted image, which is similar to the original one, is obtained. Note that, only the tth bits of some selected pixels in the directly decrypted image differ from those in the original image.

Next, the receiver uses the data hiding key to retrieve α_{TH} pixels in the directly decrypted image. The α_{TH} pixels are divided into L groups, and each group contains n pixels, as denoted by $D(1,d), D(2,d), \ldots, D(n,d)$. For each pixel $D(u,d), 1 \le u \le n$, we obtain the corresponding four decrypted neighboring pixels t_1, t_2, t_3, t_4. The location relationship between pixel $D(u,d)$ and the four neighboring pixels is depicted in Fig. 2.

Herein, we introduce an improved context adaptive interpolation algorithm to estimate the actual value of $D(u,d)$. Conventional context adaptive interpolation can refer to [21] for details. The to-be-estimated pixels are categorized into eight types based on the characteristics of their neighboring pixels. The characteristic of the four neighboring pixels is evaluated by slope, as calculated by

$$SL = |t_1 - t_2| - |t_3 - t_4|. \tag{4}$$

The classification of slope is illustrated in Table 1. According to Table 1, the to-be-estimated pixel is predicted by

$$D_{est}(u,d) = \gamma_1 t_1 + \gamma_2 t_3 + \gamma_3 t_2 + \gamma_4 t_4 \tag{5}$$

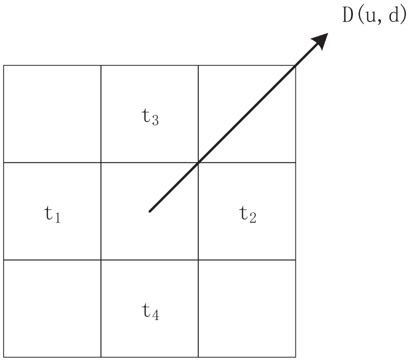

Fig. 2. The location relationship between pixel $D(u,d)$ and the four neighboring pixels.

Table 1
Classification of slopes.

Slope SL	Description	Type
$SL \geq 40$	Sharp edge in horizontal direction	1
$40 > SL \geq 20$	Edge in horizontal direction	2
$20 > SL \geq 8$	Weak edge in horizontal direction	3
$8 > SL \geq 0$	No edge	4
$0 > SL \geq -8$	No edge	5
$-8 > SL \geq -20$	Weak edge in vertical direction	6
$-40 > SL \geq -20$	Edge in vertical direction	7
$SL \geq -40$	Sharp edge in vertical direction	8

where $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ are four prediction coefficients which correspond to the eight types of slopes given in Table 2.

When the estimated pixel $D_{est}(u,d)$ is calculated, the prediction error and the flipped prediction error are computed. The prediction error is obtained by

$$ER(u,d) = |D_{est}(u,d) - D(u,d)|. \tag{6}$$

The flipped prediction error is computed by

$$ER_f(u,d) = |D_{est}(u,d) - D_f(u,d)| \tag{7}$$

where $D_f(u,d)$ is the pixel $D(u,d)$ with the tth bit flipped. For each group pixels $D(1,d), D(2,d), \ldots, D(n,d)$, the total prediction error and the total flipped prediction error are calculated by

$$ER(d) = \sum_{u=1}^{n} ER(u,d) \tag{8}$$

and

$$ER_f(d) = \sum_{u=1}^{n} ER_f(u,d), \tag{9}$$

respectively. The corresponding embedded bit is extracted by

$$S(d) = \begin{cases} 0 & \text{if } ER(d) \leq ER_f(d) \\ 1 & \text{if } ER(d) > ER_f(d). \end{cases} \tag{10}$$

If the extracted bit $S(d)$ is 0, the original n pixels are $D(1,d), D(2,d), \ldots, D(n,d)$. If the extracted bit $S(d)$ is 1, the original n pixels are $D_f(1,d), D_f(2,d), \ldots, D_f(n,d)$. When all the bits are extracted, the directly decrypted image is recovered to the original one.

Table 2
Prediction coefficients of the eight types of slopes.

Type	γ_1	γ_2	γ_3	γ_4
1	0.35	0.15	0.35	0.15
2	0.22	0.28	0.22	0.28
3	0.30	0.20	0.30	0.20
4	0.124	0.317	0.232	0.326
5	0.19	0.31	0.19	0.31
6	0.23	0.27	0.23	0.27
7	0.172	0.305	0.218	0.303
8	0.22	0.28	0.22	0.28

3. The separable method

In the joint method, data extraction and image recovery are highly connected. If someone has the data hiding key but not the encryption key, he cannot extract embedded bits from the marked encrypted image.

In this section, we introduce a separable reversible data hiding method in encrypted images, where data extraction and image recovery are separable. Four phases are contained: image encryption phase, data hiding phase, data extraction phase and image recovery phase. Diagram of the proposed separable method is demonstrated in Fig. 3. In the separable method, a content owner encrypts an original image by an encryption key and the service provider embeds additional data into the encrypted image using a data hiding key. If the receiver only has the encryption key, he can obtain a filtered decrypted image which looks like the original one. But the embedded bits cannot be extracted from the filtered decrypted image even though he has a data hiding key. If the receiver has the data hiding key, he can extract the embedded data from the encrypted image. Further, when both the encryption and data hiding keys are obtained, the receiver can extract the additional data and reconstruct the original image. Herein, data extraction must be carried out before image decryption.

3.1. Image encryption and data hiding phases

In the image encryption phase, a content owner uses an encryption key to encrypt the original uncompressed image, and obtains an encrypted image. The encryption algorithm is the same as that in the joint method.

In data hiding phase, a service provider embeds additional data into the encrypted image. First of all, the service provider pseudo-randomly selects L pixels in the encrypted image according to a data hiding key. The selection algorithm is the same as that in the data hiding phase of the joint method. For each selected pixel, the four neighboring pixels are guaranteed not to be modified. In the separable method, L is the length of the to-be-embedded bits $S(1), S(2), \ldots, S(L)$.

Let $B(1), B(2), \ldots, B(L)$ be the L selected pixels in the encrypted image. The additional bits are embedded into the tth bits of the corresponding selected pixels, as denoted by

$$B'(d) = B(d) - b \times 2^{(t-1)} + S(d) \times 2^{(t-1)} \tag{11}$$

where $B'(d)$ is the marked encrypted pixels and b is calculated by

$$b = \lfloor B(d)/2^{(t-1)} \rfloor \bmod 2. \tag{12}$$

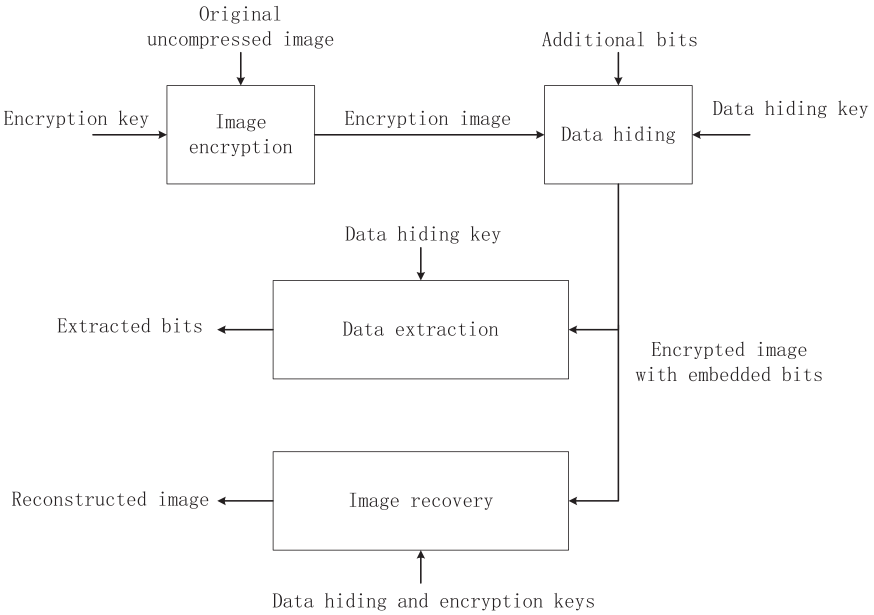

Fig. 3. Diagram of the proposed separable method.

In this method, $t \geq 7$. The additional bits are hidden in the most significant bits or the second most significant bits, since the two most significant bits in image are almost predictable when sufficient side information are given.

3.2. Data extraction phase

In this phase, we consider that the receiver only has the data hiding key. The L pixels in the encrypted image are obtained according to the data hiding key. Let $B'(1), B'(2), \ldots, B'(L)$ be the retrieved pixels, the L embedded bits are achieved by

$$S(d) = \lfloor B'(d)/2^{(t-1)} \rfloor \bmod 2, \quad 1 \leq d \leq L. \tag{13}$$

3.3. Image recovery phase

In image recovery phase, two cases are considered: (1) the receiver only has the encryption key, and (2) the receiver has the data hiding and encryption keys.

When the receiver only has the encryption key, he generates $8MN$ pseudo-random bits $r_k(i,j)$ by the encryption key, and uses the generated bits to decrypt the encrypted image. Then, a median filtering is applied to the decrypted image, and a filtered decrypted image is obtained.

When the receiver has the data hiding and encryption keys, he can extract the embedded bits and resort the encrypted image to the original version. Pixels with embedded bits are chosen by the data hiding key, and each embedded bit is extracted by fetching the tth bit of the associated selected pixel. According to the encryption key, $8MN$ pseudo-random bits $r_k(i,j)$ can be obtained. These bits are utilized to decrypt the encrypted image. In the directly decrypted image, only the tth bits of the L specific pixels may differ from the original. Let $D(1), D(2), \ldots, D(L)$ be the L pixels in the directly decrypted image. Herein, we adopt the improved context adaptive interpolation algorithm (described in the joint data extraction and image reconstruction phase of the joint method) to estimate the values of $D(1), D(2), \ldots, D(L)$.

Denote the estimated value of $D(d), 1 \leq d \leq L$ as $D_{est}(d)$, $1 \leq d \leq L$. Two possible values of $D(d)$ are achieved by setting the tth bit as 0 and 1 as represented by

$$D_0(d) = D(d) - b \times 2^{(t-1)} + 1 \times 2^{(t-1)} \tag{14}$$

and

$$D_1(d) = D(d) - b \times 2^{(t-1)} \tag{15}$$

where

$$b = \lfloor D(d)/2^{(t-1)} \rfloor \bmod 2. \tag{16}$$

Two prediction errors $ER_0(d)$ and $ER_1(d)$ are calculated by

$$ER_0(d) = |D_0(d) - D_{est}(d)| \tag{17}$$

and

$$ER_1(d) = |D_1(d) - D_{est}(d)|. \tag{18}$$

The output original pixel $D_{out}(d)$ is determined by the minimal prediction error, as represented by

$$D_{out}(d) \begin{cases} D_0(d) & \text{if } ER_0(d) \leq ER_1(d), \\ D_1(d) & \text{if } ER_0(d) > ER_1(d). \end{cases} \tag{19}$$

When the L output original pixel $D_{out}(1), D_{out}(2), \ldots, D_{out}(L)$ are obtained, the original uncompressed image is achieved.

In the separable method, a median filter is used when a receiver only has the encryption key. In this case, the secret image is approximately reconstructed, and some embedded bits are corrupted due to the filtering. Actually, the main purpose of a receiver with an encryption key is to obtain the contents of the image but not the embedded data. Whether the embedded bits are destroyed or not is not significant for the receiver. When a receiver only has the data hiding key, he can extract the embedded bits from the encrypted cover. In the proposed separable method, embedded data must be retrieved from the encrypted image but not the directly/filtered decrypted image. When a receiver has both the encryption and data hiding keys, he can retrieve the bits and reconstruct the image. Herein, data extraction must be done before image recovery. Since some most significant bits or second most significant bits are modified in the separable method, it introduces salt-and-pepper noise on the directly decrypted image. The median filtering is used to suppress the noise.

4. Experimental results and discussions

4.1. Performance measurements

For reversible data hiding methods in encrypted images, we are concerned about the following performances: reversibility, embedding rate, number of incorrect extracted bits, the visual quality of directly decrypted image and the visual quality of recovered image after data extraction. Reversibility indicates the capacity of the algorithm to losslessly recover the original image without any error. For the mentioned methods [13,14,16] and the proposed methods, perfectly reconstructing the original image is not always guaranteed. As a result, we adopt the probability of lossless recovery to evaluate the reversibility. Higher probability represents better reversibility.

The embedding rate is computed by

$$\text{Embedding rate} = \frac{\text{Total embedded bits}}{\text{Total pixels of the image}}. \tag{20}$$

The embedding rate (bit per pixel, bpp) is expected to be as large as possible so that more information can be concealed.

Since some reversible data hiding methods [13,14] in encrypted images are not separable, extracted bits may be incorrect. The number of incorrect extracted bits is used for performance measurement as well, and it is expected to be small.

Peak signal-to-noise ratio (PSNR) is adopted to evaluate the visual quality, as calculated by

$$PSNR = 10\,\log_{10}\frac{255^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(O_{i,j}-M_{i,j})^2} \tag{21}$$

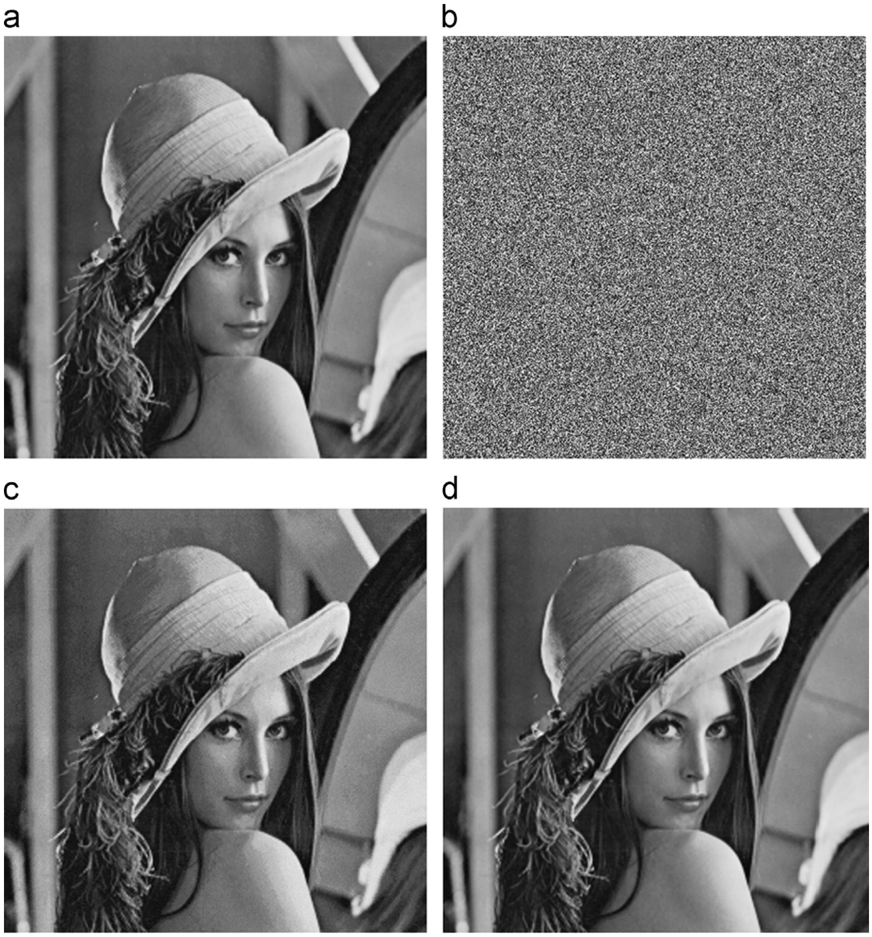

Fig. 4. Experiment by the joint method with 16,384 bits embedded, embedding rate=0.0625 bpp, incorrect extracted bit rate=0. (a) Original image Lena, (b) encrypted image with embedded bits, (c) directly decrypted image, PSNR=33.06 dB, (d) recovered image after data extraction, PSNR=+∞ dB.

where $O_{i,j}$ and $M_{i,j}$ are the original pixel value and the modified pixel value, respectively.

4.2. Experiments of the two methods

The test image Lena which consists of 512 × 512 pixels is adopted for the experiment by the joint method. The experiment is shown in Fig. 4, where 16,384 bits are embedded, and the associated embedding rate and number of incorrect extracted bits are 0.0625 bpp and 0, respectively. The parameters n and t used in this experiment are 4 and 5, respectively. That means each group contains $n=4$ pixels, and the 5th bit of each selected pixel may be flipped. The original uncompressed image is shown in Fig. 4(a), the encrypted image with embedded bits is illustrated in Fig. 4(b). The receiver decrypts the encrypted image by the encryption key, and obtains a directly decrypted image with PSNR of 33.06 dB, as shown in Fig. 4(c). Embedded bits are extracted by the data hiding key and the original image is recovered without any error, as indicated by PSNR of $+\infty$ dB.

The second experiment by the separable method is shown in Fig. 5, where totally 40,960 bits are embedded, the embedding rate is 0.1563 bpp, and the number of incorrect extracted bits is 0. In this experiment, the parameter n is 8 which means that the most significant bits are emptied out for storing the additional data. The original image Airplane is demonstrated in Fig. 5(a), and the marked encrypted image is shown in Fig. 5(b). If the receiver only has the data hiding key, he can extract the bits from the encrypted image. If the receiver only has the encryption key, he can get a filtered decrypted image which looks like the original one with PSNR of 32.38 dB, as illustrated in Fig. 5(c). When the receiver has both the data hiding and the encryption key, he can extract the embedded bits and resort the encrypted image to the original one without any error.

4.3. Performance analysis

We further analyze the two proposed methods using different parameters and different test images. Herein, five different test images are adopted, as indicated in Fig. 6.

Comprehensive experiments using some possible pairs of t and n values by the proposed joint method are shown in Table 3, where 4096 bits are embedded. Since the modified pixels in the encrypted image are determined by the data hiding key, we repeat the experiment with the same configuration but different data hiding keys for 100

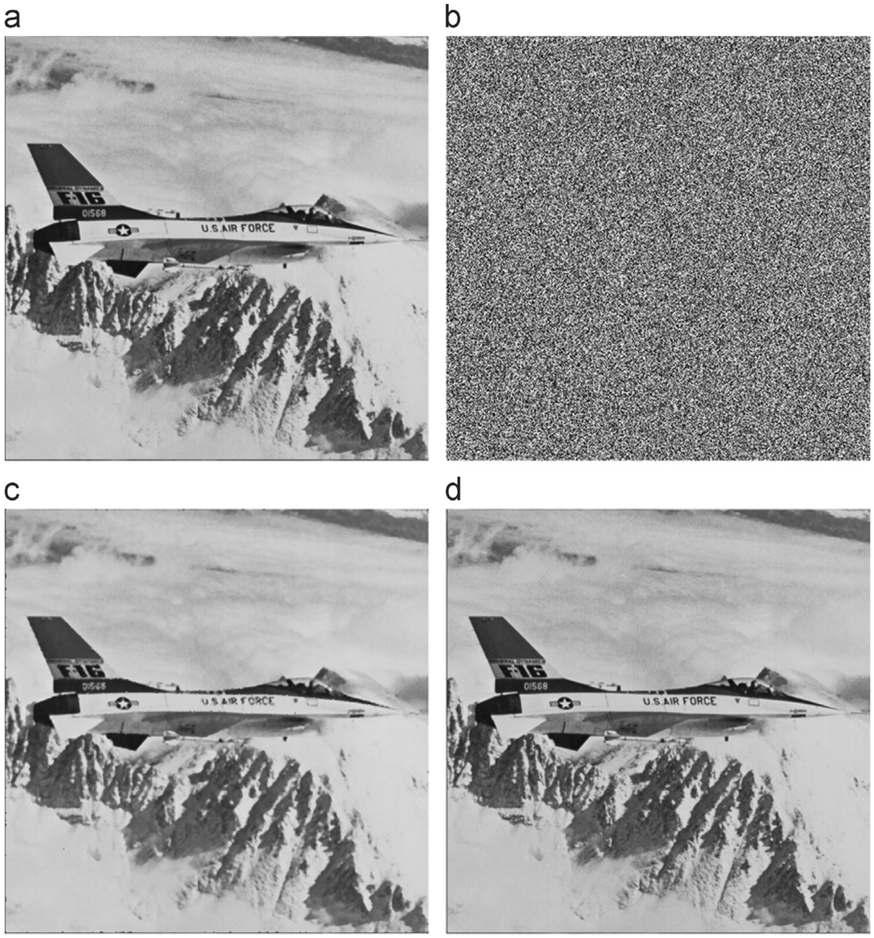

Fig. 5. Experiment by the separable method with 40,960 bits embedded, embedding rate=0.1563 bpp, incorrect extracted bit rate=0. (a) Original image Airplane, (b) encrypted image with embedded bits, (c) filtered decrypted image, PSNR=32.38 dB, (d) recovered image after data extraction, PSNR=$+\infty$ dB.

Fig. 6. Test images used in the experiments. (a) Lena, (b) Baboon, (c) Airplane, (d) Lake, and (e) Cartoon.

Table 3
Performance analysis of the joint method with different t and n for test image Lena, where 4096 bits are embedded.

n	t	Average incorrect extracted bits	Directly decrypted image	Recovered image	
				Prob for lossless recovery	Lossy recovered image
1	1	1319.1	69.21	0	71.15
5	1	794.94	62.21	0	66.32
10	1	527.34	59.21	0	65.09
1	2	927.81	63.18	0	66.62
5	2	255.2	56.18	0	65.24
10	2	59.46	53.16	0	68.58
1	3	426.51	57.17	0	63.97
5	3	35.25	50.17	0	67.88
10	3	1.52	47.17	0.23	78.05
1	4	178.8	51.15	0	61.75
5	4	1.96	44.16	0.12	74.38
10	4	0.03	41.14	0.97	74.25
1	5	53.13	45.12	0	61.02
5	5	0	38.14	1	–
10	5	0	35.10	1	–
1	6	3.56	39.11	0.03	67.27
5	6	0	32.10	1	–
10	6	0	29.09	1	–

times, and calculate the average values. According to Table 3, when t and n are bigger than 3 and 4, respectively, the number of incorrect extracted bits is small and it is possible to recover the original image without any error. As a result, it is suggested to use $t \geq 4$ and $n \geq 5$ for the proposed joint method.

Performance analysis of the joint method for different test images is given in Tables 4–8, where different parameters are utilized. For the recovered image after data extraction, it is expected to convert to original without any error. And we calculate the probability of lossless recovery, as indicated in the second column to the right. We also calculate the average PSNR of those lossy recovered image, as demonstrated in the first column to the right.

For test image *Lena*, when the embedding rate is 0.0156 bpp, it is possible to achieve complete reversibility (i.e., probability for lossless recovery is 1) by increasing the parameters n and t, such as $(n=11, t=4)$, $(n=7, t=5)$ and $(n=3, t=6)$. When the embedding rate increases (e.g., 0.0625 bpp and 0.0938 bpp), it is also possible for the proposed joint method to achieve high reversibility. Further, the number of average incorrect extracted bits is relatively low. Less than one bit is incorrectly extracted on average, as demonstrated in Table 4. But the performance of test image *Baboon* is different, as illustrated in Table 5. The number of average incorrect extracted bits is much higher than that of *Lena*, since Baboon contains a lot of details and precise prediction on the pixels is difficult. But the errors can be significantly reduced by increasing n and t. More experimental data are concluded in Tables 6, 7 and 14, where test images *Airplane*, *Lake* and *Cartoon* are used. A smaller number of average incorrect extracted bits,

Table 4
Performance analysis of the joint method with different parameters for test image Lena.

n	t	Embedded rate	Total embedded bits	Average incorrect extracted bits	Directly decrypted image	Recovered image	
						Prob for lossless recovery	Lossy recovered image
7	4	0.0156	4096	0.27	42.69	0.76	75.43
11	4	0.0156	4096	0	40.73	1	–
3	5	0.0156	4096	0.69	40.35	0.56	71.99
5	5	0.0156	4096	0.01	38.14	0.99	71.24
7	5	0.0156	4096	0	36.68	1	–
3	6	0.0156	4096	0	34.33	1	–
3	6	0.0625	16,384	0	28.29	1	–
4	6	0.0625	16,384	0	27.12	1	–
2	6	0.0938	24,576	0.2	28.31	0.83	68.74

Table 5
Performance analysis of the joint method with different parameters for test image Baboon.

n	t	Embedded rate	Total embedded bits	Average incorrect extracted bits	Directly decrypted image	Recovered image	
						Prob for lossless recovery	Lossy recovered image
3	5	0.0156	4096	590.89	40.36	0	45.75
5	5	0.0156	4096	373.97	38.13	0	45.52
7	5	0.0156	4096	238.85	36.67	0	46.01
3	6	0.0156	4096	188.04	34.33	0	44.71
7	6	0.0156	4096	24.26	30.64	0	50.01
11	6	0.0156	4096	3.76	28.69	0.02	56.50
15	6	0.0156	4096	0.47	27.34	0.63	59.67
4	6	0.0625	16,384	470.70	27.06	0	39.47

Table 6
Performance analysis of the joint method with different parameters for test image Airplane.

n	t	Embedded rate	Total embedded bits	Average incorrect extracted bits	Directly decrypted image	Recovered image	
						Prob for lossless recovery	Lossy recovered image
7	4	0.0156	4096	10.03	42.70	0	66.01
11	4	0.0156	4096	0.92	40.73	0.4	72.32
3	5	0.0156	4096	19.42	40.35	0	60.72
5	5	0.0156	4096	2.1	38.13	0.08	68.31
7	5	0.0156	4096	0.24	36.67	0.78	69.51
11	5	0.0156	4096	0.01	34.69	0.99	67.81
3	6	0.0156	4096	0.6	34.34	0.54	66.61
7	6	0.0156	4096	0	30.66	1	–
3	6	0.0625	16,384	2.46	28.31	0.06	63.87
4	6	0.0625	16,384	0.42	27.06	0.73	65.78
2	6	0.0938	24,576	49.83	28.31	0	52.26

better reversibility and better lossy recovered image quality are achieved for test image *Airplane*, since it is smooth. But reversibility of test image *Cartoon* is different, it is significantly enhanced by larger n. Moreover, the number of average incorrect extracted bits and reversibility can be greatly improved by increasing the parameters n and t.

Extensive experiments are conducted to evaluate the performance of the separable method, as illustrated in Table 9. In the separable method, all the embedded bits are extracted without any error. As a result, the average number of incorrect extracted bits is 0, and it is not mentioned in Table 9. For test image *Lena*, the original image can be losslessly recovered for all the embedding rates demonstrated. For other test images such as *Airplane* and *Lake*, the reversibility (i.e., the probabilities for lossless recovery are 0.99 and 0.73, respectively) is high when the embedding rate is 0.0156 bpp and t is 8. When the embedding rate increases to 0.0625, the probabilities decrease to 0.93 and 0.26. Further, when high embedding rate (0.1563 bpp) is used, the probabilities for *Airplane* and *Lake* decrease to 0.74 and 0.04, respectively. When $t=8$ and the embedding rate is 0.0156 bpp, the probability for lossless recovery is 0.29 for test image *Cartoon*. In conclusion, reversibility by the separable method for test image

Table 7
Performance analysis of the joint method with different parameters for test image Lake.

n	*t*	Embedded rate	Total embedded bits	Average incorrect extracted bits	Directly decrypted image	Recovered image	
						Prob for lossless recovery	Lossy recovered image
7	4	0.0156	4096	252.31	42.69	0	51.79
11	4	0.0156	4096	107.40	40.73	0	53.54
3	5	0.0156	4096	139.04	40.34	0	52.04
5	5	0.0156	4096	42.27	38.12	0	55.04
7	5	0.0156	4096	12.86	36.67	0	58.86
11	5	0.0156	4096	1.40	34.70	0.25	65.78
3	6	0.0156	4096	5.06	34.31	0	60.72
7	6	0.0156	4096	0.01	30.64	0.99	63.76
3	6	0.0625	16,384	22.57	28.31	0	54.01
4	6	0.0625	16,384	5.21	27.06	0	59.57
2	6	0.0938	24,576	190.43	28.31	0	46.41

Table 8
Performance analysis of the joint method with different parameters for test image Cartoon.

n	*t*	Embedded rate	Total embedded bits	Average incorrect extracted bits	Directly decrypted image	Recovered image	
						Prob for lossless recovery	Lossy recovered image
3	5	0.0156	4096	7.45	40.35	0	65.05
5	5	0.0156	4096	0.51	38.13	0.64	70.21
7	5	0.0156	4096	0.04	36.67	0.96	69.78
3	6	0.0156	4096	1.86	34.33	0.17	64.56
7	6	0.0156	4096	0	30.65	1	–
3	6	0.0625	16,384	6.06	28.31	0	60.07
4	6	0.0625	16,384	1.9	27.06	0.2	62.96
2	6	0.0938	24,576	150.63	28.31	0	47.43

Airplane is high. For the test images *Baboon* and *Cartoon*, no matter which embedding rate is used, the probabilities are relative low.

For those lossy reconstruction of the original image, PSNRs for test image *Baboon* are 51.01 dB, 44.69 dB and 40.57 dB when $t=8$ and the embedding rates are 0.0156 bpp, 0.0625 bpp and 0.1563 bpp, respectively. When $t=8$, the visual quality of lossy recovered image is about 60 dB for test image *Airplane*. And it is above 54 dB and 48 dB for test images *Lake* and *Cartoon*, respectively.

4.4. Comparisons and discussions

Comparisons among the proposed methods and state-of-the-art works are provided in this subsection. For joint reversible data hiding methods in encryption images, we are concerned about the reversibility, embedding rate, number of incorrect extracted bits and visual quality of the recovered image. Performance comparisons among the proposed joint method and two related approaches [13,14] are demonstrated in Tables 10–14. Default parameters used in the proposed joint method are $n=5, t=5$ and $n=7, t=6$ when embedding rate is 0.0156 bpp. Parameters are $n=3, t=6$ and $n=4, t=6$ when embedding rate is 0.0625 bpp.

For test image *Lena*, almost complete reversibility is achieved by the proposed joint method when embedding rates are 0.0156 bpp and 0.0625 bpp. While the reversibility is not provided by Zhang's method [13] and Hong et al.'s method [14]. The numbers of incorrect bits in these two methods are relatively high when embedding rate is 0.0625 bpp.

For test image *Baboon*, the number of incorrect extracted bits is significantly reduced by the proposed joint method, as depicted in Table 11. When embedding rate is 0.0156 bpp, PSNRs of lossy recovered images by the proposed method are higher than those by the two methods [13,14]. When embedding rate is 0.0625 bpp, PSNRs of lossy recovered images by the proposed method are approximately the same as those by the two methods. For test images *Airplane*, *Lake* and *Cartoon*, the reversibility by the proposed joint method is better than the two related methods. High probability for losslessly recovering the original image is guaranteed by large *n* and *t*. Further, the number of incorrect extracted bits is significantly reduced, and high visual quality of lossy recovered image is obtained by the proposed joint method as well. One concern in the proposed joint method is that the visual quality of directly decrypted image is not satisfactory. But for low embedding rate (e.g., 0.0156 bpp) and small *n* and *t*, higher PSNR is achieved.

For the separable method, since data extraction and image recovery are separated, extracted bits are completely correct. As a result, only the reversibility, embedding rate and visual quality of the recovered image are concerned for the performance. Performance comparison between the

Table 9
Performance analysis of the separable method with different parameters for different test images.

Test images	t	Embedded rate	Total embedded bits	Filtered decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Lena	7	0.0156	4096	41.07	1	–
	7	0.0625	16,384	40.18	1	–
	8	0.0156	4096	41.01	1	–
	8	0.0625	16,384	39.86	1	–
	8	0.1563	40,960	37.62	1	–
Baboon	7	0.0156	4096	23.72	0	46.59
	7	0.0625	16,384	23.66	0	40.66
	8	0.0156	4096	23.68	0	51.01
	8	0.0625	16,384	23.49	0	44.69
	8	0.1563	40,960	23.08	0	40.57
Airplane	7	0.0156	4096	34.69	0	56.25
	7	0.0625	16,384	34.39	0	49.85
	8	0.0156	4096	34.62	0.99	60.17
	8	0.0625	16,384	34.01	0.93	60.17
	8	0.1563	40,960	32.47	0.74	60.17
Lake	7	0.0156	4096	30.93	0.01	60.34
	7	0.0625	16,384	30.77	0	53.91
	8	0.0156	4096	30.89	0.73	59.39
	8	0.0625	16,384	30.56	0.26	58.32
	8	0.1563	40,960	29.76	0.04	54.84
Cartoon	7	0.0156	4096	39.95	0	53.59
	7	0.0625	16,384	38.97	0	47.60
	8	0.0156	4096	39.73	0.29	57.95
	8	0.0625	16,384	38.15	0	53.31
	8	0.1563	40,960	35.43	0	48.96

Table 10
Performance comparison among the proposed joint method and related methods for test image Lena.

Methods	Embedding rate	Total embedded bits	Incorrect extracted bits	Directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Our $n=5, t=5$	0.0156	4096	0.01	38.14	0.99	71.24
Our $n=7, t=6$			0	30.53	1	–
Zhang [13]			59	37.90	0	55.69
Hong et al. [14]			3	37.89	0	68.19
Our $n=3, t=6$	0.0625	16,384	0	28.29	1	–
Our $n=4, t=6$			0	27.12	1	–
Zhang [13]			2218	37.90	0	44.80
Hong et al. [14]			410	37.89	0	52.37

proposed separable method and Zhang's method [16] is demonstrated in Table 15. In Zhang's method [16], different parameters (L, M, S) introduce different performance data. Herein, parameters $(L=64, M=1, S=1)$, $(L=64, M=3, S=4)$ and $(L=32, M=3, S=5)$ are used when embedding rates are 0.0156 bpp, 0.0625 bpp and 0.1563 bpp, respectively. The parameter n used in the proposed separable method is 8.

For test image *Lena*, complete reversibility (i.e., probability for lossless recovery is 1) is provided by the proposed method. For test images *Airplane*, *Lake* and *Cartoon*, reversibility is provided by the proposed method, and the probabilities for *Airplane* are high. But for test image *Baboon*, the probability for lossless recovery is 0. However, all the test images cannot be recovered to the original ones (i.e., probability for lossless recovery is 0) by Zhang's method [16] for the demonstrated embedding rates. The proposed separable method obtains improved reversibility when high embedding rates are used.

Moreover, higher PSNRs of lossy recovered image are provided by the proposed separable method. Difference of PSNR between the proposed method and Zhang's method [16] becomes significant when the embedding rate increases. Better visual quality of lossy reconstructed image is provided by the proposed method. However, the visual quality of filtered decrypted image by the proposed

Table 11
Performance comparison among the proposed joint method and related methods for test image Baboon.

Methods	Embedding rate	Total embedded bits	Incorrect extracted bits	Directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Our $n=5, t=5$	0.0156	4096	373.97	38.13	0	45.52
Our $n=7, t=6$			24.26	30.64	0	50.01
Zhang [13]			643	37.90	0	42.99
Hong et al. [14]			403	37.91	0	45.05
Our $n=3, t=6$	0.0625	16,384	760.09	28.30	0	38.63
Our $n=4, t=6$			470.70	27.06	0	39.47
Zhang [13]			5571	37.93	0	39.65
Hong et al. [14]			3482	37.93	0	41.72

Table 12
Performance comparison among the proposed joint method and related methods for test image Airplane.

Methods	Embedding rate	Total embedded bits	Incorrect extracted bits	Directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Our $n=5, t=5$	0.0156	4096	2.1	38.13	0.08	68.31
Our $n=7, t=6$			0	30.66	1	–
Zhang [13]			181	38.00	0	51.07
Hong et al. [14]			6	37.99	0	66.26
Our $n=3, t=6$	0.0625	16,384	2.46	28.31	0.06	63.87
Our $n=4, t=6$			0.42	27.07	0.73	65.78
Zhang [13]			3054	38.00	0	43.18
Hong et al. [14]			763	37.99	0	49.97

Table 13
Performance comparison among the proposed joint method and related methods for test image Lake.

Methods	Embedding rate	Total embedded bits	Incorrect extracted bits	Directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Our $n=5, t=5$	0.0156	4096	42.27	38.12	0	55.04
Our $n=7, t=6$			0.01	30.64	0.99	63.76
Zhang [13]			223	37.92	0	47.73
Hong et al. [14]			56	37.90	0	53.67
Our $n=3, t=6$	0.0625	16,384	22.57	28.31	0	54.01
Our $n=4, t=6$			5.21	27.06	0	59.57
Zhang [13]			4398	37.90	0	40.80
Hong et al. [14]			1726	37.90	0	44.97

method is lower than that by Zhang's method [16]. But the visual quality of filtered (directly) decrypted image is much less important. In all, the main advantages of the two proposed methods are that the embedding capacity is increased while low number of incorrect extracted bits, high reversibility and better visual quality of recovered image are maintained as well.

4.5. *Feature comparison*

Feature comparison of different methods is provided in Table 16. Features of the proposed joint method are the same as Zhang's method [13] and Hong et al.'s method [14]. Completely error-free extracted bits and completely error-free recovered image cannot be obtained. For the

Table 14
Performance comparison among the proposed joint method and related methods for test image Cartoon.

Methods	Embedding rate	Total embedded bits	Incorrect extracted bits	Directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Our $n=5, t=5$	0.0156	4096	0.51	38.13	0.64	70.21
Our $n=7, t=6$			0	30.65	1	–
Zhang [13]			951	37.94	0	41.75
Hong et al. [14]			71	37.93	0	49.98
Our $n=3, t=6$	0.0625	16,384	6.06	28.31	0	60.07
Our $n=4, t=6$			1.9	27.06	0.2	62.96
Zhang [13]			6283	37.93	0	39.39
Hong et al. [14]			3626	37.92	0	40.75

Table 15
Performance comparison between the proposed separable method and Zhang's method [16].

Test images	Methods	Embedded rate	Total embedded bits	Filtered/directly decrypted image	Recovered image	
					Prob for lossless recovery	Lossy recovered image
Lena	Our	0.0156	4096	41.01	1	–
	Zhang			54.18	0	65.89
	Our	0.0625	16,384	39.86	1	–
	Zhang			38.32	0	55.63
	Our	0.1563	40,960	37.62	1	–
	Zhang			38.01	0	44.65
Baboon	Our	0.0156	4096	23.68	0	51.01
	Zhang			54.15	0	55.14
	Our	0.0625	16,384	23.49	0	44.69
	Zhang			38.28	0	40.01
	Our	0.1563	40,960	23.08	0	40.57
	Zhang			37.92	0	38.79
Airplane	Our	0.0156	4096	34.62	0.99	60.17
	Zhang			54.36	0	60.14
	Our	0.0625	16,384	34.01	0.93	60.17
	Zhang			38.07	0	48.66
	Our	0.1563	40,960	32.47	0.74	60.17
	Zhang			38.21	0	42.08
Lake	Our	0.0156	4096	30.89	0.73	59.39
	Zhang			54.51	0	56.32
	Our	0.0625	16,384	30.56	0.26	58.32
	Zhang			38.19	0	42.63
	Our	0.1563	40,960	29.76	0.04	54.84
	Zhang			37.91	0	39.88
Cartoon	Our	0.0156	4096	39.73	0.29	57.95
	Zhang			54.26	0	58.78
	Our	0.0625	16,384	38.15	0	53.31
	Zhang			38.03	0	41.83
	Our	0.1563	40,960	35.43	0	48.96
	Zhang			38.01	0	40.83

proposed separable method, its features are the same as Zhang's separable method [16], where data extraction and image recovery are separable. Extracted bits in the separable method are always correct. For methods such as [18,19], significant improvements are achieved on obtaining error-free extracted bits and recovered image. But room for data embedding must be emptied out before image encryption by a content owner, which is somewhat impossible, since a content owner does nothing but encrypts his image for privacy consideration.

5. Conclusions and future work

This paper introduces two reversible data hiding approaches in encrypted images by using prediction error: a joint method and a separable method. For the first

Table 16
Feature comparison of related methods.

Methods	Features			
	Separable	Error in data extraction	Error in image recovery	Reserving room for data embedding
Proposed joint method	No	Yes	Yes	No
Proposed separable method	Yes	No	Yes	No
Zhang's method [13]	No	Yes	Yes	No
Hong et al.'s method [14]	No	Yes	Yes	No
Zhang's method [16]	Yes	No	Yes	No
Ma et al.'s method [18]	Yes	No	No	Yes
Zhang et al.'s method [19]	Yes	No	No	Yes

method, data extraction and image recovery algorithms are performed jointly. While comparing to related joint methods [13,14], improved reversibility, smaller number of incorrect extracted bits, better visual quality of lossy reconstructed image are obtained by the proposed method, especially when high embedding rate is used. For the second method, data extraction and image recovery algorithms are separable. Extracted bits are guaranteed to be correct. Further, the proposed separable method outperforms Zhang's method [16] in the reversibility and the visual quality of lossy recovered image for high payload embedding.

Future work on the proposed joint method is to improve both the data extraction and the image recovery for obtaining error-free extracted bits and recovered image. For the separable method, the media filter is used to improve the security in certain degree. When the filtering is not used, some embedded bits may be extracted even without the data hiding key. This is a major security concern in the separable method. In future work, data embedding for the separable method should be improved by changing the embedding intensity or introducing another data hiding strategy.

Acknowledgment

The authors wish to thank the anonymous reviewers for their insightful and invaluable suggestions and comments. This work was in part supported by China Postdoctoral Science Foundation (Grant no. 2014M552269), 973 Program (Grant no. 2011CB302400) and Natural Science Foundation of Guangdong Province, China (Grant no. S2013010013728).

References

[1] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol. 13 (8) (2003) 890–896.
[2] Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol. 16 (3) (2006) 354–362.
[3] W.-L. Tai, C.-M. Yeh, C.-C. Chang, Reversible data hiding based on histogram modification of pixel differences, IEEE Trans. Circuits Syst. Video Technol. 19 (6) (2009) 906–910.
[4] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, Lossless generalized-LSB data embedding, IEEE Trans. Image Process. 14 (2) (2005) 253–266.
[5] L. Kamstra, H.J. Heijmans, Reversible data embedding into images using wavelet techniques and sorting, IEEE Trans. Image Process. 14 (12) (2005) 2082–2090.
[6] C.-C. Chang, W.-L. Tai, C.-C. Lin, A reversible data hiding scheme based on side match vector quantization, IEEE Trans. Circuits Syst. Video Technol. 16 (10) (2006) 1301–1308.
[7] D.M. Thodi, J.J. Rodríguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process. 16 (3) (2007) 721–730.
[8] Y. Hu, H.-K. Lee, J. Li, DE-based reversible data hiding with improved overflow location map, IEEE Trans. Circuits Syst. Video Technol. 19 (2) (2009) 250–260.
[9] F. Peng, X. Li, B. Yang, Adaptive reversible data hiding scheme based on integer transform, Signal Process. 92 (1) (2012) 54–62.
[10] X. Li, J. Li, B. Li, B. Yang, High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion, Signal Process. 93 (1) (2013) 198–205.
[11] J. Li, X. Li, B. Yang, Reversible data hiding scheme for color image based on prediction-error expansion and cross-channel correlation, Signal Process. 93 (9) (2013) 2748–2758.
[12] W. Puech, M. Chaumont, O. Strauss, A reversible data hiding method for encrypted images, in: Electronic Imaging 2008, International Society for Optics and Photonics, 2008, pp. 68191E-1–68191E-9.
[13] X. Zhang, Reversible data hiding in encrypted image, IEEE Signal Process. Lett. 18 (4) (2011) 255–258.
[14] W. Hong, T.-S. Chen, H.-Y. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Process. Lett. 19 (4) (2012) 199–202.
[15] X. Zhang, C. Qin, G. Sun, Reversible data hiding in encrypted images using pseudorandom sequence modulation, in: Digital Forensics and Watermaking, Springer, Berlin, 2013, pp. 358–367.
[16] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 826–832.
[17] X. Zhang, Z. Qian, G. Feng, Y. Ren, Efficient reversible data hiding in encrypted images, J. Vis. Commun. Image Represent. 25 (2) (2014) 322–328.
[18] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inf. Forensics Secur. 8 (3) (2013) 553–562.
[19] W. Zhang, K. Ma, N. Yu, Reversibility improved data hiding in encrypted images, Signal Process. 94 (2014) 118–127.
[20] Z. Qian, X. Han, X. Zhang, Separable reversible data hiding in encrypted images by n-nary histogram modification, in: The Third International Conference on Multimedia Technology, Atlantis Press, Paris, 2013, pp. 869–876.
[21] W. Liu, W. Zeng, L. Dong, Q. Yao, Efficient compression of encrypted grayscale images, IEEE Trans. Image Process. 19 (4) (2010) 1097–1102.