Reversible Data Hiding for Encrypted Image with Privacy Protection for Image Content

Prof. Manjusha M. Patil
Department of Electronics & Telecommunication
MGI-COET, Shegaon, India
mmpatil208@gmail.com

Prof. Sagar R. Deshmukh
Department of Computer Science & Engineering
MGI-COET, Shegaon, India
sagardeshmukh04@gmail.com

Prof. Ashwini G. Sharma
Department of Computer Science & Engineering
MGI-COET, Shegaon, India
ashwini.unnatti@gmail.com

Prof. Parag K. Shelke
Department of Computer Science & Engineering
MGI-COET, Shegaon, India
pkshelke21.engg@gmail.com

***Abstract*—** In this paper, a method for the scheme reversible data hiding where recovery of the cover image and hidden data can be done in the receiver is proposed. Owner encrypts the original image with the encryption key for the protection of the privacy of the contents of an image. Each block of the encrypted image is added to little secret by the hider data using the key-data hiding. Data hiding process causes only slight modifications to each partial block flipping pixels, which improves the visual quality of the decoded image. The image can be easily decrypted on the receiver using the key encryption key data hiding a feature adaptive assessment of softness characteristic along the isophote direction, the secret data can be extracted from the decoded image, and recovery of the original image can be recovered more successfully.

.***Keywords-*** *Reversible data hiding Privacy protection Image encryption Data embedding Image decryption Data extraction Image recovery Isophote direction*

*****

I. INTRODUCTION

Data hiding has another name as concealment of information. This type of technique that go unnoticed can embed secret information cover image, for example, videos, audios and images [1]. There are two ways to hide data (1) that reached the various functionalities for data protection coverage through the integration of data, i.e. watermark, in different ways[2];(2) conducting secret communication (steganography) for maximum payload incorporation of secret data [3]. In recent years, experiments have been conducted to study how the complete recovery of data coverage. After removing the hidden data, known as reversible data hiding (RDH) [4-7].

Previous work on RDH focused on two basic principles, the first is the difference expansion (DE) [4] and the other is the shift of the histogram (SA) [5,6]. In the RDH-DE [4] based method, cover image is divided into a number of non-overlapping, pairs of neighboring pixels, and the difference of each pair of pixels is calculated and doubled. Then, the difference duplicate of each pair of pixels or remains reserved or modified by one to match the parity of each bit secret to hide. The processed difference was re-assigned to two pixels in each pair, and the stego pixels occurred carrying secret data. Therefore, the payload maximum opacity of this approximate scheme 0.5 bits per pixel (bpp).

On the receiving side, hidden secrets bits can be easily removed from the least significant bit (LSB) of the distinction of re-calculated in stego pairs of pixels. The original values of pairs of pixels cover can also be retrieved through the inverse transformation for distinction. However, the problems of underflow and overflow can occur for some pixels due to the operation of, therefore, for additional information inappropriate pixel location map is RDH required. A scheme proposed moving the histogram cover image in 2006 [5]. In this scheme, the maximum point and the point cover image histogram zero were chosen first, and then the intervals of the histogram within the range of the right one of the peak points left one zero point were all shifted to the right by one. Therefore, it has created a vacant bin histogram direct the peak. During insertion, the pixel values corresponding to the peak point or remain unchanged were or incremented by one according to the secret bits. Obviously, the payload total concealment of secret bits depended on the number of pixels of the peak point in the histogram.

The receiver can easily extract the hidden bits through the histogram stego image, and further moved rearwardly moved containers for image retrieval. However, the peak point information, zero point must be transmitted to the receiver side as ancillary data.

In order to further improve the performance of hiding the capacity and quality of the stego image for traditional schemes based-DE and based in SA recently, so many researchers have attempted to introduce the mechanism of prediction RDH [8-18]. Instead of directly using the original

image as presentation data, prediction based schemes used the relative data of the original image, i.e. the prediction error (PE) as coverage data for embedding purpose, and PE may be obtained by difference between the original image and the prediction image [8]. PE has been enhanced to carry secret bits and added back to the prediction image to produce the final stego image. On the receiving side, the same prediction image must be generated and then the modified PE containing the hidden bits can also be obtained, ensuring the accuracy of some secret extraction and recovery of original image. Therefore, the two foci of the RDH predictions based studies are: (1) how to acquire appropriate PE of the original image through predictor; (2) how to operate the EP obtained for reversible data embedding.

A class of typical RDH predictors based on the causal context of the current pixel to the prediction, that is, the neighboring pixels on the left and upper region of the current pixel [8-12]. This type of causality based predictors for RDH context often keeps the pixels of one / two top most rows and one / two wing left column of the original image unchanged and performs progressive pixel prediction remaining in the order of raster. Schemes in [10, 11] adopted the mean value of causal context as the current pixel value predicted. Schemes in [8, 9] used the median predictors of detection edges (MED) which exploits the value ratio between the three pixels in the causal context. Prediction Gradient adjusted (GAP) used in [12] first calculates the edge characteristics with respect to direction and intensity of the current pixel through seven pixels in its causal context, and then generates the corresponding predicted value in accordance with estimated edge features. Another class of typical RDH predictors is based on image interpolation mechanism [13-17]. Such predictors based interpolation RDH often indicates a part of original image pixels scattered with different patterns as reference pixels, which are then used to help forecast remaining pixels by interpolation techniques different images. Hong Chen and present an adaptive mechanism for the distribution of pixel reference [13], which can reach a satisfactory compromise for prediction accuracy and the ability to hide. In their method, more reference pixels are in the region of complex instead of smooth region, and according to the reference pixels, the techniques bilinear bi-cubic interpolation and tested to calculate the predicted values for remaining pixels. Qin et al. improved the mechanism of choice for reference pixels in [14] and an RBI diffusion curvature (CDD) based on the inpainting method with a third-order equation partial differential (PDE) for interpolation was introduced, which can get results predicted more accurate. Schemes in [15,16] borrowed the idea of local edge detection image zoom in image processing and CFA adopted refined local reference patterns for the prediction. The weighting factors and thresholds for improved interpolation respectively in these two schemes to achieve better performance.

Once the predicted result for an original image was obtained PE also can be easily calculated. The advantages of using PE which refer to data that were PE often had more concentrated than the original image because the prediction accuracy histogram and histogram more concentrated PE can lead to increased hiding power and minor distortions embedding. Similar to the RDH based-HS for data cover the original image, some schemes reported select one or two highest containers histogram of PE obtained and carried out operations SA in PE for reversible data incorporation of [9,13]. Lee et al. expanded PE within a range of smaller values and shifted the PE largest remaining to avoid overlap [10]. The expanded PE can be used to carry reversible secret bits. Actually, the gear shift operation to the histogram of PE can be considered as a special case of PE expansion. Different conventional methods that evenly embedded in each expanded bit PE, Li et al. He proposed a strategy for incorporating adaptation that can embed more bits in the smallest PE situated in the smooth regions, improving the capacity limit of conventional [12] methods. Due to the popularity of cloud computing in recent years, a lot of personal data may be stored and processed with various Internet features to reduce the burden on the client computing user [19]. But in order to protect user privacy, user data must be encrypted before being processed on the Internet. Therefore, research on data processing in the encrypted domain are needed. As for the processing of RDH in encrypted images, here, give us a scenario of application, for example, in a hospital with cloud server for storage and data management, medical (content owner) obviously has the right to know and access the contents of the medical image of his / her patient during diagnosis; after the doctor finishes the current diagnosis, he / she will send the medical imaging center cloud storage hospital, ie database of medical imaging center built by the cloud server, for data management and the backup. However, in order to protect the privacy of the patient, the doctor must first encrypt patient medical image and then send center manager of the database of medical images. Although the administrator (ocultador data) does not know the content of the received image, he / she can incorporate some dialing information, such as the doctor's name, identification number, department and date of diagnosis, which can effectively facilitate management image and can be used for future retrieval.

Recently, there has been some work on RDH in encrypted images [20-26]. Generally speaking, there are three main categories of methods for RDH encrypted images, ie, methods of vacating the room-occultation data after encryption of images [20 to 23], methods of booking the room-hiding encrypting data before images [24,25], and based on homomorphic encryption properties [26] method. Compared to the last two categories, the first category of methods to vacate room-occultation data after encryption, are more applicable in

practice because the original image, it is only necessary for encryption with low complexity encryption flow before embedding data. However, such methods may suffer from low visual quality of the marked images, decrypted and extracted bits errors and recovered images. Other systems concealment of relevant data in the encrypted domain were reported in [27-31]. Schemes [27to29].The embedded data in encrypted images while schemes [30, 31] considered embed data encrypted videos. In addition, schemes [27,28,30] are reversible and diagrams [29,31] are irreversible.

II PREVIOUS WORKS

The scheme [20] proposed by Zhang employee for the first time stream cipher to encrypt all bits of the original image. So he room-occultation data can be overridden by turning the three least significant bits of half pixel, and one bit of secret can be embedded into each divided the encrypted image block. Once decoded, the receiver can extract the embedded bits and recover the original image with the Help spatial correlation. Hong et al. improved method Zhang fully exploiting the pixels in softness evaluation for each and considering correlations block of pixels on the border of the neighboring based on the side-match between the recovered blocks blocks and unrecovered blocks, which can reduce the error rate extracted bits smaller block [21]. Zhang extended his previous work [20] in a separable scheme [22], wherein the least significant bits of the encrypted image is compressed to create a little space housing embedding bits. On the receiving side, this scheme can perform operations independent data extraction and image decryption individually.

Unlike schemes [20 to 23] vacated the room data hidden behind image encryption, Ma et al. proposal to reserve room occultation data before encryption of images [24]. In their scheme, before encryption, original image is divided into two partitions and the LSB of a partition is embedded in the other partition using an algorithm traditional RDH. Thus, the least significant bits of the first partition. They were reserved and used for embedding data with a simple LSB replacement after encryption. Following the idea of reserving room before encryption, the regime [25] estimated first some chosen pixels of the original image, and then changed the estimation and encrypted errors, which may be used additionally for RDH, incorporated with the remaining pixels encrypted to produce the final encrypted image. Since the data hiding process of this scheme It is essentially based on the displacement for the histogram PE, data extraction and image retrieval were free of errors.

Chen et al. RDH he proposed a scheme based encoded signals the system of public key encryption and homomorphic encryption, and digital images applied as an example for the description [26]. In this scheme during encryption of images, each pixel value is segmented into two parts, i.e. seven most significant bits (MSB) and LSB, and these two parts are encrypted respectively. Then two LSB encrypted encryption of each pair of pixels are modified to reversibly embed a secret bit according to the properties of homomorphism. The receiver can easily extract the embedded bits and recover the original image judging by the ratio of the decrypted two least significant bits in each pair of pixels.

III PROPOSE WORK

In the proposed scheme, there are three types of functions, that is, the content owner, hider data, and receiver. Using an encryption key the content owner encrypts his / her original image and then subjected the image data encrypted to hider. The data hider embeds the secret to the image encrypted by a key-message data hiding. Note that the data hider has no idea about the original content the picture. Marked encrypted image is transmitted to the receiver via a public channel. The receiver can use the encryption key authorized by the content owner for decoded image that is visually similar to the original image and then can use the data concealment-key authorized byhider technique to extract further and retrieve the secret message the original image. The flowchart of the proposed system is illustrated in Fig. 1.

A. *Image encryption*

Suppose that the size of original image I is M x N, and the gray value I(i, j) of each pixel in I can be represented by 8 bits, i.e., $b_{i,j,0}$, - $b_{i,j,1,}$. . . ,$b_{i,j,7}$, see Eqs. (1) and (2).

$$b_{i,j,k} = \left\lfloor \frac{I(i,j)}{2^k} \right\rfloor \bmod 2, \quad k = 0,1,\ldots,7, \tag{1}$$

$$I(i,j) = \sum_{k=0}^{7} (2^k \times b_{i,j,k}), \tag{2}$$

Where the integers i and j denote the pixel coordinates belonging to [1,M] and [1,N], respectively. Before submitting the image to the data hider, in order to protect privacy, the content owner encrypts the image content using a stream cipher way. Different with the
schemes in [20,21], in our scheme, eight different random binary matrices all sized M _ N, i.e., $E^{(k)}$ = {ei,j $^{(k)}$}M_N, k = 0,1, . . . ,7, are generated according to the encryption key of the content owner, and are used for image encryption by following Eqs. 3–5 orderly.

$$b'_{i,j,k} = b_{i,j,k} \quad k = 0,1,\ldots,7, \tag{3}$$

$$b'_{i,j,3} = b_{i,j,3} \oplus e^{(3)}_{i,j}, \tag{4}$$

$$b'_{i,j,k} = b'_{i,j,k} \oplus e^{(k)}_{i,j}, \quad k = 0,1,\ldots,7, \tag{5}$$

Where the symbol denotes the exclusive-or operation and b' i,j,k is the encrypted version of bi,j,k except for the case k = 3. In other words, except for the fourth LSB layer, all the other seven bit layers of the original image I are encrypted by the random binary matrices. Then, all b' $_{i,j,k}$ are collected to produce the final encrypted image i.e:

$$I_e(i,j) = \sum_{k=0}^{7} (2^k \times b'_{i,j,k}), \quad (6)$$

where i.e. (i, j) represents the pixel value at the coordinate (i, j) of the encrypted image i.e.

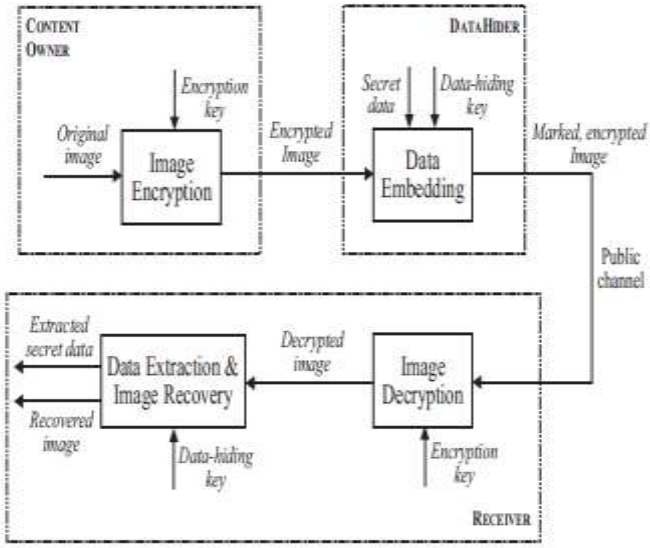

Fig.1. Flowchart of the proposed scheme.

It should be noted that in the image encryption procedure our scheme, according to a number of observations, the encoded LSB fourth layer not disclose the contents of original image because the fourth LSB layer is usually almost random and It reflects very few image content. This fourth unencrypted LSB layer data will help further embedding procedure by flipping the lower layers LSB. However, if the bit layer is higher than the fourth is chosen as the best picture unencrypted recovery performance can be obtained, but the visual quality of decrypted image becomes worse and content of the original, the image will be released after the attack of substitution (seven encrypted layers are set at a constant value) as slightly higher layers are more relevant to the content of images. Therefore, it is recommended the fourth LSB layer is unencrypted and used to help for data embedding.

After image encryption, Ie presents the data hider data embedding. Note that potential attackers, including data hider can not access the main contents of the image without encryption key content owner.

B. Data embedding

After receiving the marking image Iew encrypted, the receiver first decodes the received image and then extracts the embedded pieces and the original image is recovered. Note that the receiver has the encryption key content owner and key-hiding data hider data**.** By the encryption key, the receiver generates eight random binary matrices that are same with those of the content owner, i.e.

E(k) = {ei,j$^{(k)}$}$_{MxN}$, k = 0,1,. . . ,7. The five random binary matrices, i.e., E(k) (k = 3, 4, 5, 6, 7), are first utilized to decrypt the 5 MSB layers of the image Iew, see Eqs. 9–11.

$$b^*_{i,j,k} = b'_{i,j,k}, \quad k = 3,4,5,6,7, \quad (9)$$

$$b^*_{i,j3} = b'_{i,j3} \oplus e^{(3)}_{i,j}, \quad (10)$$

$$b^*_{i,j,k} = b^*_{i,j,k} \oplus e^{(k)}_{i,j}, \quad k = 3,4,5,6,7, \quad (11)$$

Where H(i, j) is a binary function, b' $_{i,j,3}$ denotes the fourth LSB of the pixel Ie (i, j) in Gs, and b0
;3 (l = 1,2,. . . ,v) denote the fourth LSBs of the v neighboring pixels within the block for Ie(i, j). Eqs. (7) and (8) imply that, when the v + 1 bits including b'$_{i,j,3}$ and b ;3
(l = 1,2,. . . ,v) are equal, i.e., H(i, j) = 0, no operations are conducted on the pixel Ie(i, j). On the other hand, when these v + 1 bits are not the same, i.e., H(i, j) = 1, the flipping operation should be conducted on the 3 LSBs of the pixel Ie(i, j). Thus, instead of flipping the 3 LSBs of all the pixels belonging to Gs that was applied in [20, 21], our scheme only chooses the partial pixels belonging to Gs to flip the 3 LSBs when embedding the secret bit s. It is because the flipping operation of 3 LSBs on those pixels Ie(i, j) that satisfy H(i, j) = 0 not only contributes nothing to the future secret extraction and image recovery, but also degrades the visual quality of decrypted image. Therefore, through elaborately choosing the pixels for flipping, the proposed scheme achieves the significant improvement for the visual quality of decrypted image, and also does not affect the accuracy of data extraction and image recovery. After all image blocks encrypted That is, they are crossed and held the above process, the data embedding procedure finishes and marking, the last encrypted image Iew occurs. The total number of embedded secret bits equals the number of block that is, M? N / z2, and the rate of incorporation of R is 1 / z2 bpp. In the next, the hider Iew data can be transmitted to the receiver via a public channel.

C. Image Decryption

After receiving the marking image Iew encrypted, the receiver first decodes the received image and then extracts the embedded pieces and the original image is recovered. Note that the receiver has the encryption key content owner and key-hiding data hider data**.** By the encryption key, the receiver generates eight random binary matrices that are same with those of the content owner, i.e.,

 ISSN: 2321-8169
427 - 435

E(k) = {ei, $j^{(k)}$}$_{MxN}$, k = 0,1,. . . ,7. The five random binary matrices, i.e., E(k) (k = 3, 4, 5, 6, 7), are first utilized to decrypt the 5 MSB layers of the image Iew, see Eqs. 9–11.

$$b^*_{i,j,k} = b'_{i,j,k}, \quad k = 3,4,5,6,7, \tag{9}$$

$$b^*_{i,j3} = b'_{i,j3} \oplus e^{(3)}_{i,j}, \tag{10}$$

$$b^*_{i,j,k} = b^*_{i,j,k} \oplus e^{(k)}_{i,j}, \quad k = 3,4,5,6,7, \tag{11}$$

Where the five bits b'$_{i,j,k}$ (k = 3, 4, 5, 6, 7) denote the 5 MSBs of the pixel at the coordinate (i, j) in Iew. Since the data embedding that is only conducted on the 3 LSB layers of the encrypted image does not modify its 5 MSB layers, thus, the decrypted value of Eq. (11), i.e., b* i,j,k, is exactly equal to the value bi,j,k of the original image I (k = 3, 4, 5, 6, 7). In other words, after the operations in Eqs. 9–11, the 5 MSB layers of Iew can be decrypted to their original versions. Next, the 3 LSB layers of Iew should be further decrypted. As stated in Section 3.2, during the data embedding, for each encrypted block to be embedded with secret bit s, the 3 LSBs of the z2/2 pixels in the block belonging to the group G1s are not modified; for the other z2/2 pixels in the block belonging to the group Gs, the 3 LSBs of some pixels are flipped, while the others are non-flipped. Therefore, similar with the decryption for the 5 MSB layers, for each block in Iew, through using E(k) (k = 0, 1, 2), the operation in Eq. (12) is conducted to decrypt the 3 LSB layers of Iew:

$$b^*_{i,j,k} = b'_{i,j,k} \oplus e^{(k)}_{i,j}, \quad k = 0,1,2. \tag{12}$$

Cleary, after the operation in Eq. (12), the 3 LSBs of the z2/2 pixels belonging to G1s and the pixels belonging to Gs with non-flipped 3 LSBs can be decrypted. In other words, besides the 3 LSBs of the z2/2 pixels belonging to G1 s, the 3 LSBs of the pixels belonging to Gs and satisfying H(i, j) = 0 are also decrypted to their original versions, i.e., bi,j,k (k = 0, 1, 2), see Eq. (13).

$$\begin{aligned} b^*_{i,j,k} &= b'_{i,j,k} \oplus e^{(k)}_{i,j} \\ &= (b_{i,j,k} \oplus e^{(k)}_{i,j}) \oplus e^{(k)}_{i,j} \quad \text{subject to } (i,j) \in G_{1-s}, \text{ or } (i,j) \in G_s \text{ and } \Theta(i,j) = 0, \\ &= b_{i,j,k}, \quad k = 0,1,2. \end{aligned} \tag{13}$$

But, after the operation in Eq. (12), the 3 LSBs of the pixels belonging to Gs and satisfying H(i, j) = 1 become the flipped versions of their original forms bi,j,k, see Eq. (14).

$$\begin{aligned} b^*_{i,j,k} &= b''_{i,j,k} \oplus e^{(k)}_{i,j} \\ &= (1 - b'_{i,j,k}) \oplus e^{(k)}_{i,j} \quad \text{subject to } (i,j) \in G_s \text{ and } \Theta(i,j) = 1, \; k = 0,1,2. \\ &= [1 - (b_{i,j,k} \oplus e^{(k)}_{i,j})] \oplus e^{(k)}_{i,j} \\ &= 1 - b_{i,j,k}. \end{aligned} \tag{14}$$

In Eqs. 11–14, b′ i,j,k denotes the decrypted bit. Then, all M N bits of b′ i,j,k are collected to produce the decrypted image Id: Idði; jÞ ¼

$$I_d(i,j) = \sum_{k=0}^{7} (2^k \times b^*_{i,j,k}), \tag{15}$$

where Id(i, j) represents the pixel value at the coordinate (i, j) of the decrypted image Id sized M N. Therefore, after the exclusive-or operations based on the eight random binary matrices E(k) (k = 0,1,. . . , 7), except the 3 LSBs of the pixels belonging to Gs and satisfying H(i, j) = 1, the bits in Iew including the 5 MSB layers, the 3 LSBs of the z2/2 pixels belonging to G1s, and the 3 LSBs of the pixels belonging to Gs and satisfying H(i, j) = 0, can all be successfully decrypted, i.e., b* i,j,k = bi,j,k. Since only the 3 LSBs of the pixels belonging to Gs and satisfying H(i, j) = 1 are flipped in Id, the visual similarity between the decrypted image Id and the original image I is high. Note that, unlike schemes [20, 21] which You can only be decrypted 5 layers MSB and three least significant bits of the pixels belonging to G1? s, the proposed scheme can also decipher 3 LSB of the pixels belonging to Gs and satisfying H (i, j) = 0. For most natural images I, due to the characteristics of continuity and smoothness, there is a greater chance for a given pixel I (i, j) to satisfy the H (i, j) = 0, which can also be verified by a large number of experiments. Accordingly, the visual image decrypting quality of the proposed scheme is significantly better than those of schemes [20, 21]. As a scheme reversible data hiding, after the image decryption, the little secret embedded in each image block should be extracted and the decrypted image should fully recover to achieve reversibility.

D. Data extraction and image recovery

In fact, during the imaging procedure decryption, the receiver does not know the little secret embedded in each block s is 0 or 1. Therefore, the receiver does not also ensures the 3 LSBs layers which group, i.e., G0 or G1, for each block is given back, and he / she just\ know, for every little secret s integrated block e {0, 1}, 3 LSB of the pixels belonging to Gs and satisfying H (i, j) = 1 are turned around. In the methods of data extraction and image retrieval, the receiver must extract the bit s Secret embedded in each block judging by the pixels of which group, i.e., G0 or G1, turns around, and invest further flipped 3 LSBs of these pixels for image retrieval. Inspired by the schemes in [20,21], we also carry out trial each based on

the statistical characteristic of the image block. However, a different evaluation function used in our scheme to achieve increased accuracy of data extraction [20,21]. Detailed procedures data extraction and retrieval for identification are described as follows. For each current block B in Id, the receiver divides the z2 pixels of B into two groups, i.e., G0 and G1, using the same data-hiding key with the data hider, and first flips the 3 LSBs of the pixels in B belonging to G0 and satisfying H(i, j) = 1 to produce a new block B(0), see Eqs. (16) and (17).

$$b_{i,j,k}^{(0)} = b_{i,j,k}^{*}, \quad k = 0, 1, \ldots, 7, \tag{16}$$

$$b_{i,j,k}^{(0)} = 1 - b_{i,j,k}^{(0)} \quad \text{subject to } (i, j) \in \mathbf{G}_0 \text{ and } \Theta(i, j) = 1, \ k = 0, 1, 2, \tag{17}$$

where b(0) i,j,k denotes the kth LSB of the recovered pixel in B at the coordinate (i, j) after flipping the 3 LSBs of the pixels belonging to G0 and satisfying H(i, j) = 1. Then, after calculating the pixel values by b(0) i,j,k, the recovered block B(0) corresponding to the flipping operation on the 3 LSBs of the pixels belonging to G0 can be obtained. On the other hand, for each current block B in Id, the receiver then flips the 3 LSBs of the pixels in B belonging to G1 and satisfying H(i, j) = 1 to produce another new block B(1), see Eqs. (18) and (19).

$$b_{i,j,k}^{(1)} = b_{i,j,k}^{*}, \quad k = 0, 1, \ldots, 7, \tag{18}$$

$$b_{i,j,k}^{(1)} = 1 - b_{i,j,k}^{(1)} \quad \text{subject to } (i, j) \in \mathbf{G}_1 \text{ and } \Theta(i, j) = 1, \ k = 0, 1, 2, \tag{19}$$

where b(1) i,j,k denotes the kth LSB of the recovered pixel in B at the coordinate (i, j) after flipping the 3 LSBs of the pixels belonging to G1 and satisfying H(i, j) = 1. Then, after calculating the pixel values by b(1) i,j,k, the recovered block B(1) corresponding to the flipping operation on the 3 LSBs of the pixels belonging to G1 can be obtained. Through the above operations, for each block B in ID, the recipient can obtain two corresponding blocks, i.e., B (0) and B (1). Since the bit secret embedded in the current block B is assumed that s e {0, 1}, therefore, the B block (s) must be the correct result recovered, while block B (1? s) is the result of wrong 3 LSBs of some pixels compared with the original version of B. Then the receiver It should judge which, i.e., B (0) or B (1) is the correct recovered B as a result of the analysis through the softness of the two blocks. As we know, in general, neighboring pixels of natural origin image usually have superior spatial correlation. That is, the B successfully retrieved result (s) should have a relatively smooth distribution of pixel values that an erroneous result B (1? s). Thus, in the proposed scheme, an adaptive judging function W based on image contents is designed to evaluate the smoothness degree for B(0) and B(1) and assist for secret extraction and image recovery, see Eqs. (20)–(22).

$$\Psi(\mathbf{B}^{(\alpha)}) = \sum_{x=1}^{z}\sum_{y=1}^{z}\left|\frac{\partial^2 B^{(\alpha)}(x,y)}{\partial \xi^2}\right|, \quad \alpha = 0 \text{ or } 1, \tag{20}$$

$$\begin{bmatrix}\xi \\ \eta\end{bmatrix} = \begin{bmatrix}-\sin\theta & \cos\theta \\ \cos\theta & \sin\theta\end{bmatrix} \times \begin{bmatrix}x \\ y\end{bmatrix}, \tag{21}$$

$$\theta = \arctan\left(\frac{\partial B^{(\alpha)}(x,y)}{\partial y} \Big/ \frac{\partial B^{(\alpha)}(x,y)}{\partial x}\right), \tag{22}$$

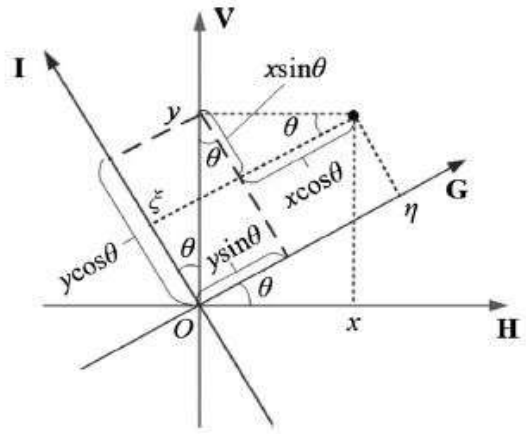

Fig. 2. An illustration for the relationship between the two coordinate systems O-$\xi\eta$ and O-xy.

where B(a)(x,y) denotes the pixel value at the coordinate (x,y) in the block B(a) sized z z, h is the angle of gradient direction at (x,y) in O-xy, and a is equal to 0 or 1.

IV EXPERIMENTAL RESULTS AND COMPARISONS

So as to verify the effectiveness of proposed system, experiments were conducted on a group of test images including four standard gray level images of size 512? 512, i.e. Lena, man, Lake, and baboon, as shown in Fig. 3 and the different images 1338 sized 512? 384 of the database uncompressed color images (UCID) [33]. For color images, the luminance components were used for the testing. All experiments were carried out on a computer with a 3.30 GHz Intel processor i3, 4.00 GB of memory and Windows 7 operating system and programming environment was Matlab 7.First, take the Lena image illustrated in Fig. 3 (a) as an example the proposed scheme. Once encrypted using the image of Lena the encryption key, encrypted eight bits of each pixel image

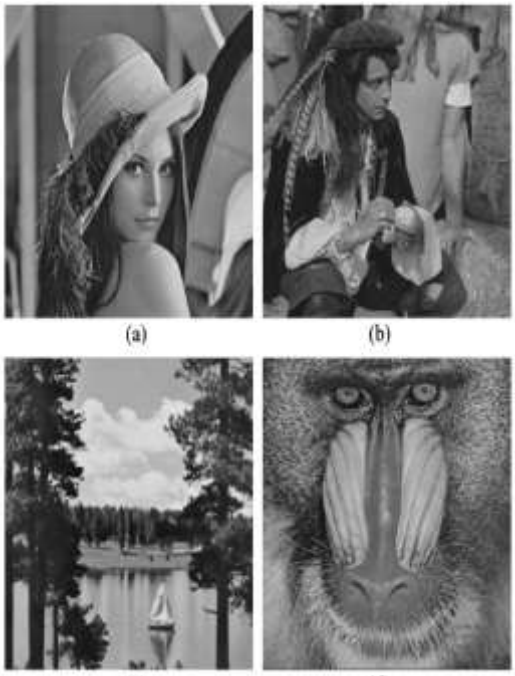

Fig.3. Four standard test images

were collected & converted into a gray value to produce the encrypted image, as shown in Fig. 4 (a). The size of the image blocks divided nonoverlapping was set as 16 16, ie, z = 16 pseudo-randomly generated secret bits 1024 and embedded in the image using the key-encrypted data hiding. Therefore, the rate of incorporation of R is 1024/5122 = 1/162 0.0039 bpp. The marked encrypted image shown in Fig. 4 (b). With the encryption key, marking, the image can be deciphered, see Fig. 4 (c), and the peak value signal to noise ratio (PSNR) of the decrypted image is 38.59 db. It can be seen that the decoded image is visually similar to the original image and the difference between them caused by embedding data is imperceptible. Then, with the key data hiding, all embedded secret bits can be successfully extracted from the decrypted image & the original image can be recovered more reversibly, see Fig. 4 (d). Due to the reversible recovery, the PSNR value of the image retrieved is positive infinity. In order to demonstrate the superiority of the proposed system, the proposed scheme with Zhang [20] and Hong et al compared scheme. Scheme [21] from two aspects, i.e., the visual quality of the decrypted image and the accuracy of the extracted bits and the recovered image. PSNR addition, structural similarity (SSIM) was also used to assess visual quality of the decoded image and the retrieved image. SSIM far developed on the basis of the characteristics of human visual system (HVS), which incorporate the structure information, luminance and contrast for the evaluation of image quality [34].

In the data embedding procedures of the schemes in [20,21], 3 LSBs of 50% pixels in each image block are flipped to embed secret data. For the proposed scheme, the 3 LSBs in only a portion of the 50% pixels satisfying the conditions in Eqs. (7), (8) are flipped. The detailed percentages of the flipped pixels for the schemes [20,21] and our scheme, in which the four test images of Fig. 3 and the images of UCID were used. The percentages for UCID are the average values for the 1338 images.

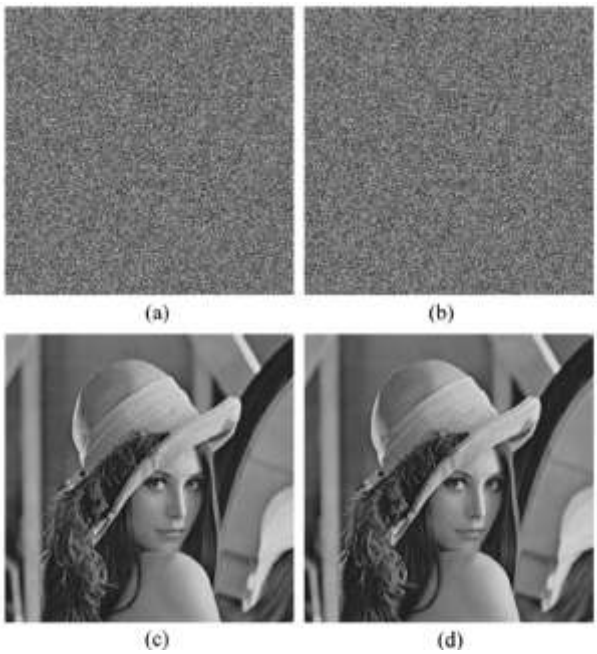

Fig.4. Encrypted image. (b) Marked, encrypted image. (c) Decrypted image containing embedded data. (d) Recovered image.

for each image, the flipped pixels of our scheme are obviously fewer than those of the schemes in [20,21]. It should be noted that, for these three compared schemes, the percentage of the flipped pixels in each image is statistically irrelevant to the size of divided blocks and the secret bits to be embedded. As stated in Section 3.2, the decrease of the flipped pixels can effectively improve the visual quality of decrypted images.

Besides reducing the number of pixels that have flipped contributions reversible embedding encrypted image, the proposed scheme also enter a judging adaptation function in the equation. (20) based on the characteristic distribution of local content to reduce errors in procedures secret bits extraction and image retrieval. FIG. 5 (a-e) show the results of comparing the error rates of the four images extracted test bit in Fig. 3 and the average error rate of the extracted bits 1338 UCID images under different block sizes z. We can find in Fig. 5 which, with the help of the evaluation function adaptation, the error rate of extracted bits of the proposed system is lower than the schemes in [20,21], and with increasing block size, the strongest softness in blocks also makes error rates fall rapidly to zero. Note that the error rate of extracted bits is closely related to the visual quality of the images recovered. In other words, for each image, the number of extracted bits incorrectly equals the number of blocks with operations moved from incorrect recovering flip the image. Obviously, the fewer bits are extracted incorrectly, the higher the image quality is recovered. The results of comparing the

corresponding visual quality, with respect to PSNR and SSIM, for different images retrieved, respectively. The symbol Inf in denotes the PSNR value corresponding image retrieved is positive infinity. It can be clearly seen that regardless of soft or complex images, the visual quality of the recovered images of our scheme outperforms the schemes in [20,21], which also means that our scheme can achieve fully recovery, ie, reversibility, with block sizes smaller than [20,21].

It should also be noted that although schemes [20-22] and our scheme of all room-end data hiding after image encryption, however, scheme [22] cannot be classified in same type together with [20,21] and our scheme because of its different mechanism design. In detail, in the scheme [22], if the receiver had both the key-data hiding and encryption key, he / she should only the first extract the data entered by the key-data hiding and then perform decryption for retrieve the image for the encryption key. In other words, the receiver can not decode the first image to obtain a sharp image and then extract the embedded data. Therefore, the regime [22] can not obtain the decrypted image containing embedded data, which is visually similar to the original image. However, for our system [20,21], the receiver can obtain the decrypted first image containing embedded data by the encryption key, and then perform data extraction and recovery of the image key-data hiding.

We also evaluated the time complexity of the proposed system was also evaluated. The execution time of the various images of the four main procedures of the proposed scheme, i.e. image encryption, data embedding, the image decoding, and the secret extraction recovery and image respectively (Z = 32). since the four procedures in our scheme can all be performed efficiently by calculations of lower complexity, execution time consumed by our scheme can satisfy the requirement of real-time applications.

CONCLUSION

In this paper, a set of effective reversible data hiding scheme with the ability of privacy protection for the image content is proposed. During embedding data, the data hider has no idea about the principle image content as the content owner encrypts the first original image with the encryption key before sending it to the hider data. The data hider only modifies the 3 layers of LSBsome elaborately selected pixels in the image encrypted by the secret to embed bits, and the number of modified pixels is less than half the total number of pixel images. Through the encryption key, the receiver can obtain the decryption, the image tag that is visually similar to the original image, and then, based on the image along the softness characteristics Isophote management, embedded secret bits can be correctly removed and the original image can be recovered reversibly by the key-data hiding. Therefore, the privacy of image content for the content owner is protected, and the operation of the reversible data hiding. You can also achieve. Experimental results show that, compared with reported schemes, our scheme has better visual the decrypted image quality and increased accuracy of secrecy extraction and image retrieval. At this stage, we only consider reversible data hiding for uncompressed images in the encrypted domain. In our future studies, so that our scheme more widely applicable, will carry out more studies on reversible data hiding compressed images such as JPEG and JPEG2000 images, in encrypted domain. Therefore, how to analyze the compressed sequence image and make the encoded bit stream have compatibility the original structure is important. Moreover, the proper way to exploit positions in the encoded bit stream JPEG / JPEG2000 for reversible data embedding deserves in-depth research.

REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding — a survey, Proc.IEEE 87 (7) (1999) 1062–1078.

[2] C.D. Vleeschouwer, J.F. Delaigle, B. Macq, Invisibility and application functionalities in perceptual watermarking: an overview, Proc. IEEE 90 (1) (2002) 64–77.

[3] X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Commun. Lett. 10 (113) (2006) 781–783.

[4] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circ. Syst. Video Technol. 13 (8) (2003) 890–896.

[5] Z.C. Ni, Y.Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans. Circ. Syst. Video Technol. 16 (3) (2006) 354–362.

[6] X.L. Li, B. Li, B. Yang, T.Y. Zeng, General framework to histogram-shifting-based reversible data hiding, IEEE Trans. Image Process. 22 (6) (2013) 2181–2191.

[7] X.P. Zhang, Reversible data hiding with optimal value transfer, IEEE Trans. Multimedia 15 (2) (2013) 316–325.

[8] D.M. Thodi, J.J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process. 16 (3) (2007) 721–730.

[9] W. Hong, T.S. Chen, C.W. Shiu, Reversible data hiding for high quality images using modification of prediction errors, J. Syst. Software 82 (11) (2009) 1833–1842.

[10] C.F. Lee, H.L. Chen, H.K. Tso, Embedding capacity raising in reversible data hiding based on prediction of difference expansion, J. Syst. Software 83 (10) (2010) 1864–1872.

[11] C. Qin, C.C. Chang, L.T. Liao, An adaptive prediction-error expansion oriented reversible information hiding scheme, Pattern Recogn. Lett. 33 (16) (2012) 2166–2172.

[12] X.L. Li, B. Yang, T.Y. Zeng, Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process. 20 (12) (2011) 3524–3533.

[13] W. Hong, T.S. Chen, Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism, J. Vis. Commun. Image Represent. 22 (2) (2011) 131–140.

 ISSN: 2321-8169
427 - 435

[14] C. Qin, C.C. Chang, Y.H. Huang, L.T. Liao, An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism, IEEE Trans. Circ. Syst. Video Technol. 23 (7) (2013) 1109–1118.

[15] G.R. Feng, L.Y. Fan, Reversible data hiding of high payload using local edge sensing prediction, J. Syst. Software 85 (2) (2012) 392–399.

[16] T.C. Lu, C.Y. Tseng, K.M. Deng, Reversible data hiding using local edge sensing prediction methods and adaptive thresholds, Signal Process. 104 (2014) 152– 166.

[17] X.L. 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.

[18] C.F. Lee, H.L. Chen, Adjustable prediction-based reversible data hiding, Digital Signal Process. 22 (6) (2012) 941–953.

[19] Z.H. Xia, X.H. Wang, X.M. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parall. Distr. Syst. (2015), http://dx.doi.org/10.1109/TPDS.2015.2401003.

[20] X.P. Zhang, Reversible data hiding in encrypted image, IEEE Signal Process. Lett. 18 (4) (2011) 255–258.

[21] 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.

[22] X.P. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inform. Forensics Secur. 7 (2) (2012) 526–532.

[23] X. Liao, C.W. Shu, Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels, J. Vis. Commun. Image Represent. 28 (2015) 21–27.

[24] K.D. Ma, W.M. Zhang, X.F. Zhao, N.H. Yu, F.H. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inform. Forensics Secur. 8 (3) (2013) 553–562.

[25] W.M. Zhang, K.D. Ma, N.H. Yu, Reversibility improved data hiding in encrypted images, Signal Process. 94 (2014) 118–127.

[26] Y.C. Chen, C.W. Shiu, G. Horng, Encrypted signal-based reversible data hiding with public key cryptosystem, J. Vis. Commun. Image Represent. 25 (5) (2014) 1164–1170.

[27] W. Puech, M. Chaumont, O. Strauss, A reversible data hiding method for encrypted images, Proc. SPIE 6819 (2008) 1–9.

[28] B. Yang, C. Busch, X. Niu, Joint reversible data hiding and image encryption, Proc. SPIE 7541 (2010) 1–10.

[29] R.M. Rad, K.S. Wong, J.M. Guo, A unified data embedding and scrambling method, IEEE Trans. Image Process. 23 (4) (2014) 1463–1475.

[30] D.W. Xu, R.D. Wang, Efficient reversible data hiding in encrypted H.264/AVC videos, J. Electron. Imag. 23 (5) (2014) 1–14.

[31] D.W. Xu, R.D. Wang, Y.Q. Shi, Data hiding in encrypted H.264/AVC video streams by codeword substitution, IEEE Trans. Inform. Forens. Secur. 9 (4) (2014) 596–606.

[32] M. Bertalmio, L. Vese, G. Sapiro, S. Osher, Simultaneous structure and texture image inpainting, IEEE Trans. Image Process. 12 (8) (2003) 882–889.

[33] G. Schaefer, M. Stich, UCID – an uncompressed color image database, in: Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multimedia, San Jose, USA, 2004, pp. 472–480.

[34] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Trans. Image Process. 13 (4)(2004) 600–612.