SPECIAL SECTION ON LATEST ADVANCES AND EMERGING APPLICATIONS OF DATA HIDING

Received May 1, 2016, accepted May 8, 2016, date of publication May 26, 2016, date of current version July 7, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2573308

INVITED PAPER

Reversible Data Hiding: Advances in the Past Two Decades

YUN-QING SHI[1], (Fellow, IEEE), XIAOLONG LI[2], XINPENG ZHANG[3], (Member, IEEE), HAO-TIAN WU[4], (Senior Member, IEEE), AND BIN MA[5]

[1]Electrical and Computer Engineering Department, New Jersey Institute of Technology, Newark, NJ 07102, USA
[2]Institute of Computer Science and Technology, Peking University, Beijing 100871, China
[3]School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China
[4]School of Digital Media, Jiangnan University, Wuxi 214122, China
[5]School of Information Science, Qilu University of Technology, Jinan 250353, China

Corresponding author: Y.-Q. Shi (shi@njit.edu)

ABSTRACT In the past two decades, reversible data hiding (RDH), also referred to as lossless or invertible data hiding, has gradually become a very active research area in the field of data hiding. This has been verified by more and more papers on increasingly wide-spread subjects in the field of RDH research that have been published these days. In this paper, the various RDH algorithms and researches have been classified into the following six categories: 1) RDH into image spatial domain; 2) RDH into image compressed domain (e.g., JPEG); 3) RDH suitable for image semi-fragile authentication; 4) RDH with image contrast enhancement; 5) RDH into encrypted images, which is expected to have wide application in the cloud computation; and 6) RDH into video and into audio. For each of these six categories, the history of technical developments, the current state of the arts, and the possible future researches are presented and discussed. It is expected that the RDH technology and its applications in the real word will continue to move ahead.

INDEX TERMS Reversible data hiding, lossless data hiding, invertible data hiding, histogram shifting, difference expansion, prediction-error, sorting, robust reversible data hiding, video reversible data hiding, audio reversible data hiding.

I. INTRODUCTION

Data hiding has received much attention from the research community in the past more than two decades [1], [2]. By this technique, it can embed secret data into a cover medium, and later enable the intended user to extract the embedded data from the marked medium for various purposes. However, for most data hiding methods, the cover medium has been distorted during the data embedding operation and hence cannot be restored into its original form after data extraction. In some sensitive scenarios, such permanent distortion is strictly forbidden and the exact recovery of the original cover medium is required. To solved this issue, reversible data hiding (RDH), also called lossless or invertible data hiding, is proposed to losslessly recover both the embedded data and the cover medium [3]–[5]. That is, with the RDH, besides the embedded data, the cover medium can be exactly recovered from the marked data as well. The first RDH algorithm is the one proposed by Barton in a US patent in 1997 [6]. He proposed to embed the authentication information into a digital medium, and enable legitimate users to extract the embedded authentication information for verifying the authenticity of the received data. So far, there is a rapid increase of applications that utilize RDH, and several examples have been reported in the literature including image authentication [6], [7], medical image processing [8], [9], video error-concealment coding [10], stereo image coding [11], [12], vector map recovery in CAD (computer-aided design) engineering graphics [13], [14], and data coloring in the cloud [15], etc.

As a special type of data hiding, the RDH has its own advantages and disadvantages compared with conventional data hiding techniques such as digital watermarking and steganography. For digital watermarking, its main concern lies in how to reliably extract the embedded data from a possibly degraded marked medium. It considers the robustness as top priority, but rarely cares about the cover medium recovery. Whereas, steganography conceals data into a cover medium in a way that the embedded data is undetectable. It focuses on imperceptivity of both the hidden data and the act of data embedding, i.e., the embedded data is not only imperceptible to human eyes but also to potential analyzers. Compared with these two data hiding techniques, the specific property of RDH is the perfect recovery of both of the cover medium and the embedded secret data. In general, RDH is a fragile technique and it poses no robustness against possible attacks.

In the rest of this paper, the following six subjects on RDH are presented. In Section II, the longest section in this paper, the various RDH schemes in image spatial domain are presented. Two major approaches: difference expansion (DE) and histogram shift (HS) together with some effective procedures including prediction-error and sorting are described. Some effective algorithms are presented. Section III is about RDH for JPEG compressed images, which are actually widely utilized in reality. Section IV presents the so-called robust RDH, meaning that if an image with reversible data hiding has been lossily compressed, while the original image will not be able to recover exactly, but the hidden message can still be recovered if the compression is not very severe. In Section V, instead of the PSNR (peak-signal-noise-ratio), which is widely used in the image RDH, some other image quality measure is considered to be utilized. Section VI addresses the RDH for encrypted images, which is expected to be very useful for cloud computation. In Section VII, the RDH for video and RDH for audio are presented. Surprisingly, the number of the published papers on RDH for video and audio is relatively much smaller, indicating that more research works are called for. Finally, a summary is made at the end of the paper.

II. REVERSIBLE DATA HIDING FOR UNCOMPRESSED IMAGES

As the most investigated subject of RDH, the RDH in image spatial domain is reviewed at first in this section. The cover data considered here is uncompressed grayscale image in bitmap format.

The feasibility of image RDH is due to the lossless compressibility of natural images since redundancy (e.g., interpixel correlation) exists in natural images. The difficulty in redundancy utilization leads researchers to pay attention to the principles of RDH. Usually, two criterions are adopted to measure the embedding performance of RDH: the PSNR and the embedding capacity (EC). By comparing the marked image with the original one, the first criterion measures the modification due to data embedding in terms of mean square error (MSE). A high PSNR means better imperceptivity, i.e., the marked image is perceived more similar to the original one. On the other hand, EC accounts for the number of data bits embedded into the cover image. Since the two criterions are conflicting, i.e., the higher EC the lower PSNR, a trade-off between them is usually sought in RDH to fulfill a specific application.

In the rest of this section, some early stage RDH schemes are first introduced in Section II-A. Then two most popularly utilized RDH technologies, DE and HS, are presented together with some commonly used schemes such as prediction-error expansion (PEE) and some recent developments in Section II-B and Section II-C, respectively. Next, a new reversible embedding technique based on code division multiplexing (CDM) and some works emphasising the theoretical aspect of RDH are introduced in Section II-D and Section II-E, respectively. Finally, a brief summary is given in Section II-F.

A. EARLY WORKS ON RDH

The first several RDH schemes developed at the early stage were designed for the purpose of fragile authentication. As a representative of this type of methods, we now describe Honsinger *et al.*'s method [7]. In this method, the marked image is obtained by first adding the secret data with the original image, and then taking the resulted value modulo 256. Its data embedding can be formulated as $J = (I + M)$ *mod* 256, where I, M, and J are respectively the cover image, the payload derived from the hash function of the cover image, and the marked image. In the authentication side, the payload M can be reconstructed from the marked image, then subtract the payload from the marked image to losslessly recover the original image. The modulo-256 operation can prevent the overflow/underflow problem in data embedding, i.e., a pixel value either exceeds the upper or the lower bound, thus guaranteeing the reversibility of data hiding. However, a drawback of this method is that the marked image may suffer a salt-and-pepper noise when the cover image contains some boundary pixels with the value of 255 or 0. Moreover, since fragile authentication does not need much data to be embedded into a cover medium, the capacity of this type of methods is not large.

Some other initial RDH schemes, either for fragile authentication or high capacity, are based on lossless compression [16]–[24]. The idea behind these schemes is to release some space by losslessly compressing a subset S of the cover image, and utilize the saved space to embed data. The embedding is implemented by replacing S with its compressed form S_C and the message, so the maximum EC is the size of $S - S_C$. The performance of these methods is determined by the employed compression algorithm and the selected subset. In [16], Fridrich *et al.* made space by compressing a proper bit-plane of cover image. To embed a 128-bit hash value, a bit-plane is determined as the lowest one that provides just enough space for hash value embedding. Then, they concatenated the hash value with the compressed image data, and embedded them into the selected bit-plane by directly bits replacing. In [17], Goljan *et al.* proposed the so-called R-S scheme. In this method, the cover image is divided into blocks and a discrimination function capturing the smoothness of the blocks is used to classify them into three categories as Regular, Singular and Unusable. Then, a so-called RS-vector is formed by representing, say, an R-block by 1 and an S-block by 0 with the U-blocks skipped. After that, for each R- and S-block, according to the to-be-embedded bit, it is either unchanged or flipped to change its category (as S and R, respectively) using a flipping function. The actual embedded data consist of the pure payload and the overhead information, i.e., the compressed RS-vector. In [19], Xuan *et al.* proposed a high capacity RDH method based on integer wavelet transform (IWT). Their idea is to embed data into IWT coefficients of high frequency sub-bands. Specifically, they proposed to losslessly compress some selected middle bit-planes of IWT coefficients and make space for data embedding. Compared with [17], a higher capacity is achieved by [19] since a better bias is exploited by considering IWT. In [23], Celik *et al.* proposed a generalized least significant bit (G-LSB) compression method to improve the compression efficiency by using unaltered portions of cover data as side-information. Instead of modifying a bit-plane, the lowest levels of raw pixel values are determined by quantization and then used to accommodate the payload bits. By a prediction-error entropy coder, G-LSB can adjust the quantization step and overwrite the lowest levels of pixel values with the payload bits. This method is better than some previous lossless-compression-based works such as [16] and [18] due to its fine scalability along the capacity-distortion curve.

B. DIFFERENCE EXPANSION (DE)

In [25] and [26], Tian presented a promising high capacity RDH method based on DE. With DE, integer Haar wavelet transform is first applied to the cover image to derive difference values, and then these values are expanded to create vacancies for reversible data embedding. Here, we present the major step of Tian's DE method. For a pixel pair (x_0, x_1), define first their integer average and difference as $l = \lfloor (x_0 + x_1)/2 \rfloor$ and $h = x_1 - x_0$, respectively. In order to embed one bit $m \in \{0, 1\}$, the difference h is expanded to $h^* = 2h + m$ while the integer average l is kept unchanged. Then, the marked pixel pair is computed based on the new difference value h^* and the original integer average value l. That is to say, the marked pixel pair (y_0, y_1) is determined as

$$\begin{cases} y_0 = l - \lfloor h^*/2 \rfloor \\ y_1 = l + \lfloor (h^* + 1)/2 \rfloor. \end{cases} \tag{1}$$

By a simple reduction, one can get

$$\begin{cases} y_0 = 2x_0 - \lceil (x_0 + x_1)/2 \rceil \\ y_1 = 2x_1 - \lceil (x_0 + x_1)/2 \rceil + m. \end{cases} \tag{2}$$

In this form, the decoder can determine the embedded bit m as the LSB of $y_1 - y_0$, and recover the original pixel pair (x_0, x_1) as

$$\begin{cases} x_0 = l' - \lfloor h'/2 \rfloor \\ x_1 = l' + \lceil h'/2 \rceil \end{cases} \tag{3}$$

where $l' = \lfloor (y_0 + y_1)/2 \rfloor$ and $h' = \lfloor (y_1 - y_0)/2 \rfloor$ are computed from the marked pixel pair (y_0, y_1). By DE, one bit can possibly be embedded into a pixel pair and thus a large embedding rate up to 0.5 bit per pixel (bpp) can be achieved.

Compared with the previous lossless-compression-based schemes such as [18] and [21], the DE method performs better by providing a higher EC while keeping the distortion low. In particular, Tian employed a location map to record the selected expandable locations (i.e., the pixel pairs with small magnitude of differences), and afterwards, the technique of location map is widely adopted by many RDH algorithms mainly handling the oveflow/underflow problem. DE is a fundamental technique of RDH, and this technique has also been widely investigated and developed, mainly in the aspects of integer-to-integer transformation (IT), PEE, and adaptive embedding. We now give a brief presentation for these three type of extensions of DE as follows.

1) INTEGER-TO-INTEGER TRANSFORMATION (IT)

IT can be employed to design RDH. According to (2), one can see that DE is actually a kind of IT, and DE can be viewed as the first IT-based RDH. Later on, Alattar [27] proposed a new method by generalizing DE from the viewpoint of IT. Specifically, Alattar improved Tian's method by generalizing DE from pixel pair to pixel block of arbitrary size. The embedding rule of Alattar's method can be simply summarized as the following IT

$$\begin{cases} y_0 = 2x_0 - \left\lfloor \dfrac{2\sum_{i=0}^n x_i + \sum_{i=1}^n m_i}{n+1} \right\rfloor + \left\lfloor \dfrac{\sum_{i=0}^n x_i}{n+1} \right\rfloor \\ y_1 = 2x_1 - \left\lfloor \dfrac{2\sum_{i=0}^n x_i + \sum_{i=1}^n m_i}{n+1} \right\rfloor + \left\lfloor \dfrac{\sum_{i=0}^n x_i}{n+1} \right\rfloor + m_1 \\ \quad \cdots\cdots \\ y_n = 2x_n - \left\lfloor \dfrac{2\sum_{i=0}^n x_i + \sum_{i=1}^n m_i}{n+1} \right\rfloor + \left\lfloor \dfrac{\sum_{i=0}^n x_i}{n+1} \right\rfloor + m_n \end{cases} \tag{4}$$

where $(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}$, $(y_0, y_1, \ldots, y_n) \in \mathbb{Z}^{n+1}$, and $(m_1, \ldots, m_n) \in (\mathbb{Z}_2)^n$ represent respectively the cover pixel block sized $n+1$, marked pixel block, and the hidden data to be embedded. One can verify that (4) includes (2) as a special case by taking $n = 1$. Clearly, with this transformation, n bits are embedded into $n+1$ pixels, and it is possible to increase the maximum embedding rate to 1 bpp by taking sufficient large n. In [28], Coltuc and Chassery proposed a method based on the so-called reversible contrast mapping which is an IT of integer pair. A specific feature of this method is that, compared with DE, it does not need additional lossless data compression, and thus it is efficient in terms of computational complexity. In [29], based on invariability of the sum of pixel pairs and pairwise difference adjustment, DE is improved by Weng *et al.* by using two different ITs of pixel pair considering the magnitude of difference value. In [30], Wang *et al.* generalized DE also by using a new IT. They showed that the embedding rule of DE can be reformulated as a transformation of integer pair and gave a novel algorithm by extending the transformation. The method [30] is recently extended by Qiu *et al.* in [31] exploiting adaptive embedding. In [32] and [33], from another IT viewpoint for DE, the authors proposed a new IT which maps the cover pixel block $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}$ and the secret message $\mathbf{m} = (m_1, \ldots, m_n) \in (\mathbb{Z}_k)^n$ to the marked pixel block $\mathbf{y} = (y_0, y_1, \ldots, y_n) \in \mathbb{Z}^{n+1}$ as

$$\begin{cases} y_0 = kx_0 - a_{n,k}(\mathbf{x}) \\ y_1 = kx_1 - a_{n,k}(\mathbf{x}) + m_1 \\ \cdots\cdots \\ y_n = kx_n - a_{n,k}(\mathbf{x}) + m_n \end{cases} \tag{5}$$

where n and k are given integers, and $a_{n,k}(\mathbf{x})$ is an integer-valued function such that (5) is reversible. By (5), $n \log_2 k$ bits can be embedded into a pixel block sized $n+1$, and thus the embedding rate in this block is $\frac{n}{n+1} \log_2 k$. Moreover, the function $a_{n,k}(\mathbf{x})$ is selected to minimize the embedding distortion, i.e., the expected value of l^2-error $\|\mathbf{y} - \mathbf{x}\|^2_{l^2}$. This yields that

$$a_{n,k}(\mathbf{x}) = \left\lfloor \frac{2(k-1)\sum_{i=0}^{n} x_i + (k-1)n}{2(n+1)} \right\rfloor. \tag{6}$$

In [34], based on a fine investigation of DE, Coltuc proposed a new IT called low-distortion transformation to embed one bit into a pixel quad. In general, IT-based methods first divide cover image into blocks and then embed data in a block-wise manner. It advantages in reducing the impact of location map to the embedding performance. However, for IT-based schemes, it usually uses a less efficient prediction in which the average value of a block is used to predict each pixel within the block. On the other hand, unlike other efficient reversible embedding techniques such as HS, the maximum modification to cover pixels cannot be controlled by IT. Based on these observations, we argue that IT-based RDH is relatively more efficient for large amount data embedding.

2) PREDICTION-ERROR EXPANSION (PEE)

Among various extensions of DE, PEE has attracted considerable attention since this approach has the potential to well exploit the spatial redundancy in natural images. Unlike in DE where only the correlation of two adjacent pixels is considered, the local correlation of larger neighborhood is exploited in PEE, and thus a better performance can be expected. PEE is firstly proposed by Thodi and Rodriguez in [35] and [36], and this technique has been widely adopted by many subsequent RDH works [37]–[52]. In PEE, instead of considering the difference operator as the decorrelation operation in DE, a pixel predictor is utilized. Specifically, take the median-edge-detector (MED) as example, a pixel x is first predicted using its right, lower and diagonal neighbors to derive its prediction value $\widehat{x}$. Then, the prediction-error of x is computed as $e = x - \widehat{x}$. After that, e is expanded to $e^* = 2e + m$ to embed one bit $m \in \{0, 1\}$. Finally, determine the marked pixel value as $\widehat{x} + e^*$. In the extraction stage of PEE, decoder first determines the prediction value $\widehat{x}$, and this value should be the same as the one obtained by encoder. Then, from the marked pixel value y, the marked prediction-error is computed as $e^* = y - \widehat{x}$. Finally, the embedded data is extracted as the LSB of e^*, and the cover pixel value is recovered as $y - \lceil e^*/2 \rceil$. The common feature of DE and PEE is the expansion-based embedding operation, in which the difference value and the prediction-error are respectively expanded in DE and PEE for data embedding. Since only one bit may be embedded into a pixel pair by DE, and thus its maximum embedding rate is 0.5 bpp. However, with PEE, one bit may be embedded into a pixel, and thus a maximum embedding rate of 1 bpp can possibly be achieved. As a result, compared with DE, an improved capacity is derived by PEE. Moreover, as discussed in [36], the expansion-based embedding operation of PEE can be used by HS for performance enhancement. We then stop here for the presentation of PEE and will come back later to this technique with more details.

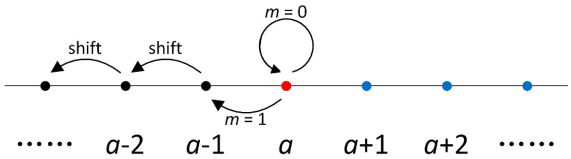
3) ADAPTIVE EMBEDDING

The first adaptive RDH scheme is the one proposed by Kamstra and Heijmans [53] which is based on DE and sorting. In this work, Tian's DE method [26] is improved by sorting pixel pairs according to the local variance before data embedding. Notice that in DE, the integer average value of two pixels in a pair is invariant and only the difference value is altered, and thus these embedding-invariants can be utilized by both encoder and decoder to compute the local variance to sort pixel pairs. Clearly, if the local variance of a pixel pair is small, the pair is located in a flat image region and it is more probably to be expandable with a small difference value. Therefore, by sorting, the location map can be remarkably compressed compared with the original DE method. The experiments reported in [53] indicated significant improvement over the original DE. In some recent works [40], [44], [46], [48], [49], [54]–[60], the authors illustrated that combining adaptive embedding strategy such as sorting or pixel-selection with other reversible techniques such as PEE, can dramatically improve the embedding performance. The basic idea of adaptive embedding is to utilize smooth image pixels to derive a better cover medium and then implement reversible data embedding by modifying only the generated cover medium which is a subset of the cover image. For example, by considering only the pixels located in flat image regions while ignoring the noisy ones, an accurate prediction can be made and a more sharply distributed prediction-error histogram can be generated. With this adaptively generated histogram, the performance of PEE can be then enhanced [40], [55], [56]. Adaptive embedding is an important strategy of RDH and a better utilization of this strategy is very helpful for performance enhancement.

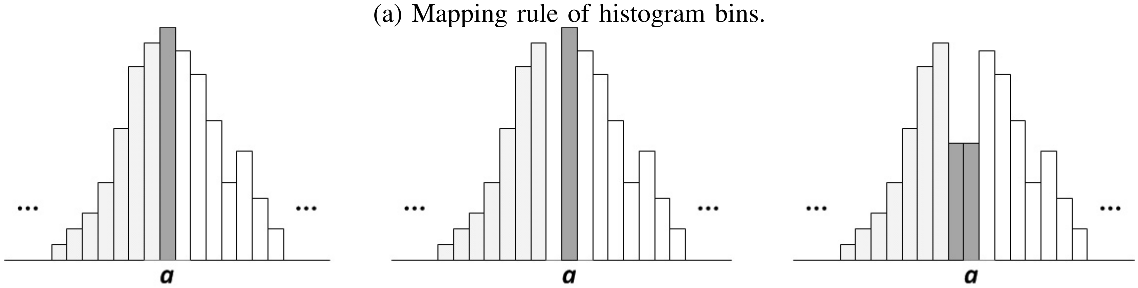
C. HISTOGRAM SHIFTING (HS)

1) NI *et al.*'s HS-BASED RDH

Besides DE, HS is another most successful approach for RDH. By this approach, a histogram is first generated, and then reversible data embedding is realized by modifying the generated histogram. HS-based RDH is first proposed by Ni *et al.* in [61] and [62]. And, the same idea of HS is independently presented in Leest *et al.*'s work [63] only a few months later. We now present the HS-based RDH of Ni *et al.* with a slight modification for better illustration. In this method,



(a) Mapping rule of histogram bins.



(b) Histogram before (left), and after (right) data embedding.

FIGURE 1. Illustration of Ni *et al.*'s HS-based RDH [61], [62]. Here, for the middle histogram of (b), it illustrates that the bins less than *a* are shifted towards left hand by 1 to create a vacant bin for data embedding. Moreover, for the right histogram of (b), without loss of generality, we assume that the number of binary 0 and the number of binary 1 to be embedded are equal. (a) Mapping rule of histogram bins. (b) Histogram before (left), and after (right) data embedding.

for a given integer a, the secret message is embedded into the cover image I in the following way to get the marked image J

$$J_{i,j} = \begin{cases} I_{i,j} - 1, & \text{if } I_{i,j} < a \\ I_{i,j} - m, & \text{if } I_{i,j} = a \\ I_{i,j}, & \text{if } I_{i,j} > a \end{cases} \tag{7}$$

where (i, j) represent the pixel coordinate in the cover image and $m \in \{0, 1\}$ is a to-be-embedded bit. In this procedure, each pixel value is modified at most by 1, and thus the PSNR of marked image versus the original one is at least 48.13 dB. Consequently, a high visual quality of marked image is guaranteed. Moreover, the integer a can be taken as the histogram peak to maximize the capacity. On the decoder side, it can extract the embedded data and restore the original image by simply reading marked pixel values, i.e., for each marked pixel $J_{i,j}$

- If $J_{i,j} < a - 1$, there is no hidden data in the pixel and its original value is $J_{i,j} + 1$.
- If $J_{i,j} \in \{a - 1, a\}$, the pixel is used to carry secret data and its original value is a. The embedded bit is $m = a - J_{i,j}$.
- If $J_{i,j} > a$, the pixel is kept unchanged in data embedding and its original value is $J_{i,j}$ itself.

Fig. 1(a) shows an illustration of this method for the mapping rule of histogram bins, in which black values are shifted, the red one is moved towards left hand to embed a binary 1 or remain unchanged to embed a binary 0, and blue ones are unchanged in data embedding. The illustration of the cover image histogram, before and after data embedding, is shown in Fig. 1(b). This simple yet effective method can well illustrate the general mechanism of HS-based RDH scheme when a histogram is generated: for data embedding, certain histogram bins are shifted to create vacant spaces whereas some others are expanded to carry hidden data by filling those vacant spaces.

2) SOME EXTENSIONS OF NI *et al.*'s HS-BASED RDH

So far, Ni *et al.*'s HS method is extensively investigated and many subsequent works are proposed. We then give a brief review for some representative extensions of HS. In [64], Fallahpour and Sedaaghi proposed to apply HS for image blocks instead of the whole image. In this method, the cover image is first divided into several blocks. Then, for each divided block, its histogram is generated and Ni *et al.*'s HS method is applied for data embedding. With the block-based HS [64], the EC can be increased with a reduced embedding distortion. In [65], Lee *et al.* proposed a new method by using the histogram of difference image. Compared with the ordinary image pixel-intensity histogram, the difference-histogram is better for RDH since it is a Laplacian-like distribution and has a much higher peak point. As a result, the spatial correlation of natural images is exploited in Lee *et al.*'s method and thus an improved performance is obtained. In [66], based on modification of the histogram generated from high-frequency IWT coefficients, Xuan *et al.* proposed a new HS-based method which can provide better performance compared with HS [62], DE [26] and some other works such as [28], [53], and [67]. In this method, for a given payload, appropriate histogram pair is selected and utilized to minimize the embedding distortion. Here, a histogram pair is defined as two consecutive integers $u < v$ with either $h(u) = 0$ and $h(v) > 0$, or $h(u) > 0$ and $h(v) = 0$, where h is the histogram counting IWT coefficients of high-frequency sub-bands. In [68], a general construction for designing HS-based RDH is proposed and this construction includes many previous schemes as special cases. In this general framework, the cover image is first divided into non-overlapping blocks such that each block contains n pixels. Then, the n-dimensional histogram is generated by counting the frequency of each divided block. Finally, data embedding is implemented by modifying the resulting n-dimensional histogram. Notice that the pixel block is an element of $\mathbb{Z}^n$, it is then divided into two disjoint sets, one set is used to carry hidden data by expansion based on a predefined embedding function, and the other set is simply shifted based on a predefined shifting function to create vacant spaces to ensure the reversibility. By this framework, one only needs to design a partition of $\mathbb{Z}^n$ and the corresponding embedding/shifting functions to derive a RDH scheme.

3) HS AND PEE

Now, as a continuation of Section II-B.2, we emphasize that PEE [36] can be and have been widely utilized by HS for performance enhancement as well. In this way, a large payload can be embedded into the cover image by modifying the prediction-error histogram, and the embedding distortion can be controlled by simultaneously utilizing expansion and shifting. By summarizing typical HS and PEE (HS-PEE) based schemes [36]–[40], we introduce HS-PEE embedding procedure containing the following two basic steps.

- (Pixel prediction and histogram generation) First, under a specific scan sequencing, the cover pixels are collected into a sequence as $(x_1, \ldots, x_N)$. Then, a predictor is used to determine the prediction of x_i denoted as $\widehat{x}_i$. Next, the prediction-error is computed by $e_i = x_i - \widehat{x}_i$ (suppose here for simplicity that $\widehat{x}_i$ is an integer). Finally, the prediction-error sequence $(e_1, \ldots, e_N)$ is derived and the prediction-error histogram is generated by counting the frequencies of prediction-errors. Usually, the prediction-error histogram obeys a Laplacian-like distribution centered at 0.
- (Histogram modification) Embed data by modifying the prediction-error histogram through expansion and shifting. Specifically, for each e_i, it is expanded or shifted as

$$e_i' = \begin{cases} 2e_i + m, & \text{if } e_i \in [-T, T) \\ e_i + T, & \text{if } e_i \in [T, +\infty) \\ e_i - T, & \text{if } e_i \in (-\infty, -T) \end{cases} \tag{8}$$

  where T is a capacity-dependent integer-valued parameter, and $m \in \{0, 1\}$ is a to-be-embedded bit. Here, the bins in $[-T, T)$ are expanded to embed data, and those in $(-\infty, -T) \cup [T, +\infty)$ are shifted outwards to create vacancies. Finally, each pixel value x_i is modified to $x_i' = \widehat{x}_i + e_i'$ to obtain the marked image. According to (8), one can see that the maximum modification to each pixel value is limited by the capacity-parameter T, and the marked image quality can be well controlled by taking a proper T. In general, for a given capacity, the parameter T is usually taken as the smallest one such that the required payload can be successfully embedded.

An illustration of this embedding procedure with the mapping rule of histogram bins and the change of prediction-error histogram (before and after data embedding), is shown in Fig. 2 for $T = 1$ and $T = 2$. Comparing Fig. 1(a) with Fig. 2(a) and (c), one can see that HS-based RDH can be simply illustrated using a mapping of histogram bins.

4) RECENT ADVANCE IN HS-PEE

Based on the two major steps of HS-PEE, histogram generation and histogram modification, many improved methods have been proposed so far. One type of improved methods focuses on exploiting advanced prediction techniques to generate a more sharply distributed prediction-error histogram [40], [42], [49]–[51], [55], [69]–[77]. For instance, for better utilizing the full-enclosing context information, the rhombus prediction is adopted in Sachnev *et al.*'s work [40] (i.e., the center pixel is predicted using the integer-valued-average of its four nearest neighbors), and a double-layered embedding mechanism is used in this method to guarantee the reversibility. Here, for double-layered embedding, the cover image is divided into two sets denoted as "cross" and "dot" (see Fig. 3), and then successively, the cross and dot sets are embedded with half of the secret message, respectively. In addition, a sorting strategy is also used in [40] for performance enhancement, and this method works rather well with an improved performance compared with the prior arts [36], [53], [67]. In [42], Luo *et al.* proposed an interpolation-based predictor which computes the pixel prediction as the weighted average of its four nearest neighbors. In [49], Qin *et al.* proposed an inpainting-assisted prediction in which the image inpainting technique based on partial differential equations is exploited for RDH. In a recent work [50], Dragoi and Coltuc investigated the use of local prediction and aimed to provide a distinct predictor for every single pixel without increasing any additional information. Compared with the prior arts which are based on global predictor, e.g., MED or rhombus prediction [40], the local-prediction-based method [50] can provide better performance. Later, in [51], the authors improved their previous work [50] by reducing the computational complexity, and computed the predictors for pixel groups instead of a single pixel.

Another type of improved methods exploited an optimal expansion-bins-selection mechanism for HS-PEE [54], [78]–[87]. An illustration of this mechanism is shown in Fig. 4 by presenting two examples of mapping rules for histogram bins. Comparing this figure with Fig. 2, the expansion bins here are adaptively selected instead of simply using the bins with high frequencies (i.e., the bins close to 0). For example, instead of using bins -1 and 0 for expansion in (8) when $T = 1$, one can use the bins 1 and -3. In the latter case, only the bins larger than 1 or smaller than -3 need to be shifted, while the bins -2, -1 and 0 are unchanged in data embedding. Formally, in the case of only two expansion bins, instead of using the bins -1 and 0, for any two integers $a < b$, one may take a and b as expansion bins, i.e., unlike (8), each

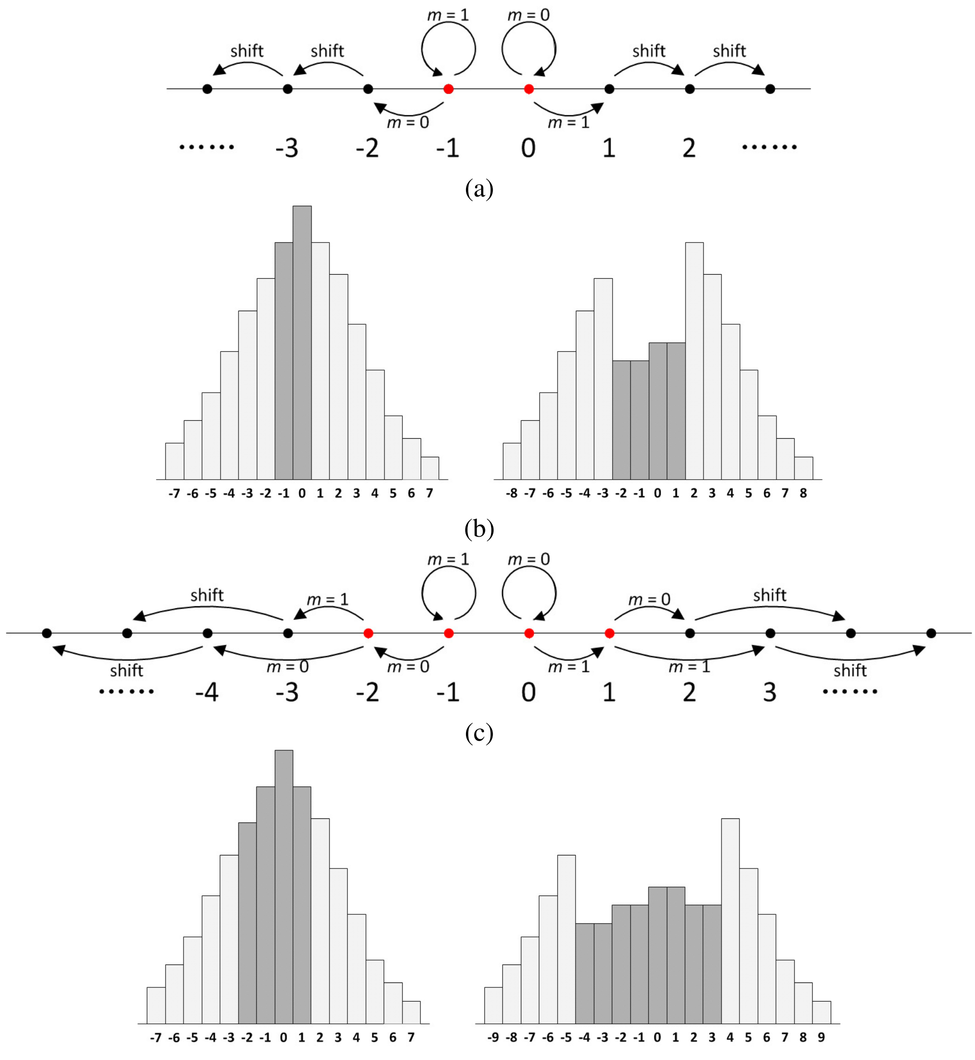


FIGURE 2. Illustration of HS-PEE for $T = 1$ and $T = 2$. (a) Mapping rule of histogram bins, $T = 1$. (b) Prediction-error histogram, before (left) and after (right) data embedding, $T = 1$. (c) Mapping rule of histogram bins, $T = 2$. (d) Prediction-error histogram, before (left) and after (right) data embedding, $T = 2$.

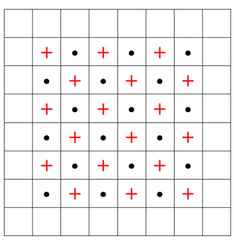
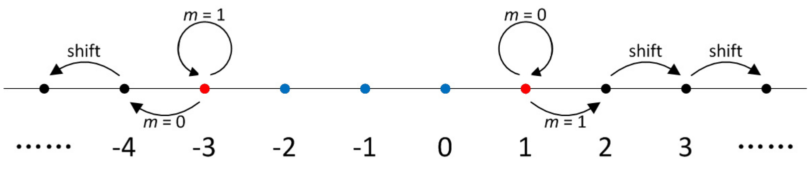


FIGURE 3. Cross/dot pixels partition in Sachnev *et al.*'s work [40].

prediction-error e_i can be expanded or shifted as

$$e_i' = \begin{cases} e_i - 1, & \text{if } e_i < a \\ e_i - m, & \text{if } e_i = a \\ e_i, & \text{if } a < e_i < b \\ e_i + m, & \text{if } e_i = b \\ e_i + 1, & \text{if } e_i > b \end{cases} \tag{9}$$

where $m \in \{0, 1\}$ is a to-be-embedded bit. And, multiple pairs of (a, b) can be selected and the predication-error histogram can be iteratively modified according to (9) to embed the required payload. Notice that, the data embedding based on (9) includes (8) ($T = 1$) as a special case when taking $a = -1$ and $b = 0$. In general, for a given capacity, considering the specific distribution of the generated histogram, the optimal expansion bins are selected such that the embedding distortion is minimized. With (9) and the optimal expansion-bins-selection mechanism, more general expansion-based reversible data embedding is exploited, and better performance of HS-PEE can be derived compared with the data embedding based on (8). This mechanism is first proposed in Xuan *et al.*'s work [66] and it is proved efficient for the performance enhancement of RDH. Later on, in [81], Xuan *et al.* proposed an improved method of [66]. Instead of IWT coefficients used in [66], the prediction-errors derived



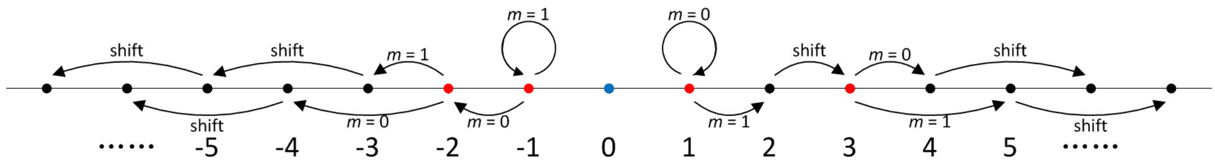


FIGURE 4. Two examples of optimal expansion-bins-selection for HS-PEE. Here, only mapping rules of prediction-error histogram bins are presented.

from the cover image are exploited for data embedding in [81]. Specifically, their method is based on HS-PEE with the following three strategies: adaptive embedding, optimal expansion-bins-selection, and histogram shrinking. By adaptive embedding, a threshold (named fluctuation threshold in [81]) is used to select smooth local area of pixels in which only those prediction-errors whose associated neighbor fluctuation does not exceed this threshold are selected for data embedding. Moreover, the expansion bins are iteratively selected according to (9). In addition, two thresholds, the left and right shrinking thresholds, are used to shrink the cover image histogram from the left and right for avoiding overflow/underflow, respectively. Then, for a given payload, the adaptive embedding threshold, expansion bins, and shrinking thresholds are determined such that the corresponding embedding distortion is minimized, and then the reversible embedding is carried out with the optimized parameters. With HS-PEE and optimized parameters, state-of-the-art embedding performance is achieved by [81]. For example, for the standard 512×512 sized Lena image at an embedding rate of 0.1 bpp, the derived PSNR is 55.44 dB. In particular, for the 960×768 sized Woman image which is a JPEG2000 test image, one can get a high PSNR of 45.38 dB for 0.5 bpp. In the latter case, the histogram of Woman image has peaks on both of its right and left ends, and the shrinking strategy is effective for performance enhancement.

In a recent work [87], Wang *et al.* developed a rate-distortion model for multiple-layered HS-PEE, in which multiple pairs of different peak and zero bins are utilized for HS-PEE to minimize the embedding distortion. Due to the massive solution space, in order to guarantee a fast search, instead of the global optimal solution, a nearly optimal embedding is derived based on the proposed model and an evolutionary optimization algorithm, i.e., genetic algorithm.

Bedsides the aforementioned extensions of HS-PEE, new HS-based embedding mechanisms based on two-dimensional-histogram-modification and multiple-histograms-modification are also proposed in some recent works as well [57], [58], [88]–[91].

D. CDM BASED RDH

Recently a novel code division multiplexing (CDM) based RDH scheme is reported in [92]. The secret data is denoted by different orthogonal spreading sequences and embedded into the cover image. The Walsh Hadamard matrix is employed to generate orthogonal spreading sequences, via which the data can be overlappingly embedded without interfering each other, thus enlarging the embedding capacity. Moreover, most elements of different spreading sequences may be mutually cancelled during the multilevel data embedding, thus resulting in good image quality even with a high embedding payload. Note that, instead of using the location map, the histogram manipulation is utilized to avoid overflow/underflow. The CDM-based RDH scheme can currently achieve the best performance at the moderate-to-high embedding capacity compared with other state-of-the-art schemes.

It is expected that other more advanced technologies and schemes for RDH will be developed and reported so as to move the RDH ahead in the future.

E. THEORETICAL INVESTIGATION ON RDH

One basic problem for RDH is, for a given distortion constraint, what is the upper bound of the payload that can be reversibly embedded into a cover medium. For a specific cover which is an independent and identically distributed (i.i.d.) integer sequence, this problem has been solved by Kalker and Willems [93] who formulated RDH as a special rate-distortion problem, and obtained the upper bound under a given distortion constraint Δ as

$$\rho_{rev}(\Delta) = \max\{H(Y)\} - H(X) \tag{10}$$

where ρ_{rev} denotes the reversible embedding capacity, X and Y denote respectively the cover and marked sequence, and H is the entropy function. The maximum entropy in (10) is over all transition probability matrices $P_{Y|X}(y|x)$ satisfying the distortion constraint

$$\sum_{x,y} P_X(x)P_{Y|X}(y|x)D(x,y) \le \Delta \tag{11}$$

where the metric $D(x, y)$ is usually defined as the square error distortion, i.e., $(x - y)^2$. Eq. (10) indicates that the amount of secret data carried by a marked sequence in a reversible manner, is just the difference of entropies between the marked and cover sequence. Notice that, in practical embedding schemes, for a cover image, it is usually projected to a low-dimensional space to derive an i.i.d. cover sequence (e.g., the prediction-error sequence), and then one applies (10) to the generated i.i.d. cover sequence instead of the cover image itself.

Recently, in order to derive practical embedding methods to asymptotically approach the rate-distortion bound according to (10), some lossless-compression-based RDH methods are proposed [94]–[100]. Since all these methods can be viewed as improved versions of the recursive code construction proposed in [93], we take the recursive-histogram-modification (RHM) method [98] as an example to briefly introduce such lossless-compression-based schemes. First, RHM should solve the problem (10) to estimate the optimal probability transition matrix $P_{Y|X}(y|x)$ and $P_{X|Y}(x|y)$. Second, RHM divides the cover sequence into disjoint blocks and embeds the message by recursively modifying the histogram of each block with the compression and decompression algorithms of an entropy coder according to the optimal probability transition matrices. As RHM behaves exactly the same within each block, we take a single block here to concisely illustrate the data embedding. Assume the block sequence $\mathbf{x} = (x_1, \ldots, x_K)$ is a K-tuple composed of K samples drawn with probability distribution P_X, where $x \in \{0, \ldots, B - 1\}$. According to the probability transition matrix $P_{Y|X}(y|x)$, for x-valued elements, one can decompress $S = KP_X(x)H(\mathbf{Q}_{\mathbf{Y}|x})$ bits of message $\mathbf{m} = (m_1, \ldots, m_S)$ into a $KP_X(x)$-bit sequence $\mathbf{y}'$ and replace all the symbols "x" in $\mathbf{x}$ with $\mathbf{y}'$. Repeat the decompression for x from 0 to $B - 1$, the data embedding for the block is completed. Note that the message is usually encrypted before embedded, so we assume $\mathbf{m}$ is a binary random sequence. Afterwards, in order to restore the original $\mathbf{x}$ at the receiver side, a compressed version of $\mathbf{x}$ is generated according to the probability transition matrix $P_{X|Y}(x|y)$, denoted by $O(\mathbf{x})$, and is embedded into the next block. The data extraction and cover restoration are executed in a backward manner. For a given cover sequence and a desired payload, the capacity-approaching codes can minimize the embedding distortion. Therefore, with such codes, designers of RDH only need to pay their attention to generating the cover signal X with small entropy. This may explain why exploiting effective prediction technique is very helpful for efficient RDH. Actually, with a better prediction method, a more concentrated prediction-error histogram can be generated. However, the optimal performance in RHM depends on the perfect lossless compression for the cover signal, and this requirement cannot be meet for short sized cover sequence. On the other hand, the cover sequence is usually correlated and not i.i.d., and thus a higher rate-distortion bound may exist in a memory host. There is a long way to narrow the performance gap between theoretical upper-bound and practical methods, especially for short or non i.i.d. cover sequence.

F. SUMMARY AND CONCLUDING REMARKS

RDH is an active research topic of digital data hiding. The reversibility of image RDH mainly relies on the lossless compressibility of natural image. Although many effective methods have been proposed so far in the literature, an insightful understanding of complex image structure and a better redundant information exploitation may further enhance the embedding performance of RDH. We would like to give the following comments as concluding remarks of this section.

- For image RDH, the most important technical issue is how to guarantee the reversibility while keeping high marked image quality. Moreover, the overflow/underflow is also an inevitable problem of RDH and should be carefully handled when designing RDH algorithms.
- HS is now the major approach of current RDH studies. Instead of spatial domain embedding as in Ni *et al.*'s original HS-based method [61], [62], the data embedding in transform domain (e.g., considering difference values [26] or prediction-errors [36], or utilizing IWT [66]) is more appropriate for performance enhancement.
- Adaptive embedding strategies considering local image properties such as sorting [40], [53] or embedding-location-selection [54], [55], [81] are very helpful for improving the reversible embedding performance. Generally speaking, adaptive embedding can be incorporated into most RDH schemes to achieve better performance.
- There are two different effective solutions to avoid the overflow/underflow problem in RDH. One is based on location map [26], [38] and the other one is based on histogram shrinking [66], [81].
- How to establish a theoretical rate-disposition model so as to achieve optimal embedding performance for RDH without i.i.d. assumption for cover images? For example, one interesting question is that, for a specific cover such as the 512×512 sized gray-scale Lena image and a given payload such as 10,000 bits, what is the maximum PSNR of the marked image that can be achieved in RDH?
- Unlike the case of gray-scale images, RDH for color images is a rarely studied topic. However, color images are more popular than gray-scale ones in reality. RDH for color images should be emphasized in the future research. The key issue for color image RDH is how to utilize the correlations of different channels.

III. REVERSIBLE DATA HIDING INTO JPEG IMAGES

As Joint Photographic Experts Group (JPEG) standard [101] offers a good trade-off between the compression rate and the visual quality of the compressed image, it is the most popular

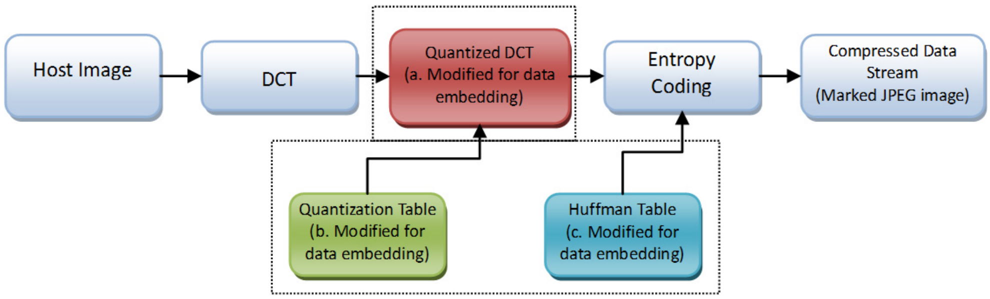


FIGURE 5. Three different data embedding methods in JPEG compression (a) Quantized DCT coefficients based; (b) Quantization table based; (c) Huffman Table based.

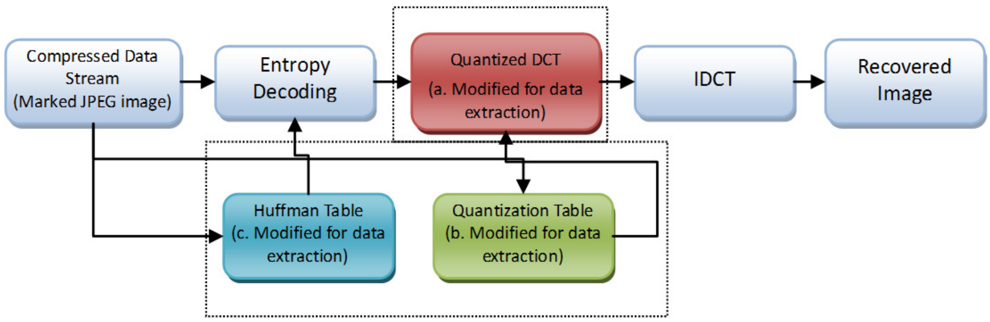


FIGURE 6. Three different data extraction methods in JPEG decompression (a) Quantized DCT coefficients based; (b) Quantization table based; (c) Huffman Table based.

image format that is widely adopted by digital cameras and other photography capture devices. Therefore, JPEG images are ideal candidates as cover objects for RDH. However, the RDH in the compressed images has not received attention from the community as much as the RDH received in the un-compressed images. This is partly due to the fact that the technique of RDH aims at keeping the quality of original images while JPEG compression often reduces the image size by eliminating some high frequency components of the image.

Quite some number of RDH techniques designed for JPEG images have been reported in the literature. This number is, however, much smaller than that of the published RDH techniques designed for un-compressed images. So far, three major approaches have been developed for the RDH into JPEG images. They are the RDH based on the manipulation of quantized DCT coefficients, the RDH based on the modification of quantization tables, and the RDH based on the modification of Huffman codes. Each of the three reversible data hiding approaches has its distinctive characteristics and therefore has achieved different performances, respectively. In Fig. 5 and Fig. 6, the three approaches are shown; they work differently during image compression and image decompression.

A. RDH WITH QUANTIZED DCT COEFFICIENTS MODIFICATION

The first category of RDH in JPEG images is based on manipulating the quantized DCT coefficients. In [102], Fridrich *et al.* proposed the idea of compressing the LSB plane of the selected DCT coefficients in a JPEG image in a lossless way so as to create space for RDH. In [103], Xuan *et al.* proposed a lossless data hiding scheme for JPEG images by using histogram pairs. The method divides the histogram of quantized DCT coefficients into three parts: (a) the part suitable for data embedding; (b) the non-modified part where the absolute value of coefficients is smaller than the established threshold; (c) the shifted part for the absolute value of coefficients is larger than the threshold. The embedding and extraction procedure can be expressed as follows,

$$x' = \begin{cases} 2x+b-|S|, & \text{if } |S| \le x \le T \\ 2x-b+|S|+u(S), & \text{if } -T \le x \le -|S|-u(S) \\ x, & \text{if } -|S|-u(S) < x < |S| \\ x+T+1-|S|, & \text{if } x > T \\ x-T-1+|S|+u(S), & \text{if } x < -T \end{cases} \tag{12}$$

where, T is the selected threshold, S is the stop position, x is the value of quantized DCT coefficient before data embedding, x' is the value of quantized DCT coefficient after data embedding, u is unit step function ($u(S) = 1$ when $S \ge 0$, and $u(S) = 0$ when $S < 0$), and $b \in \{0, 1\}$ is a message bit. This method has also proposed to execute with an optimal search strategy to minimize the image distortion. In order to make the data embedding unperceivable, only low- and mid-frequency coefficients are selected for data embedding. Sakai *et al.* [104] improved Xuan *et al.*'s scheme by avoid embedding data into the blocks located in the noisy part of the image. The proposed method can determine whether a block of 8×8 DCT coefficients is located in smooth part of image by examining the fluctuation of the DC coefficients of its neighboring blocks. Thus, they could select the smooth parts of a JPEG image for data embedding. Later on, Li *et al.* [105] proposed to embed massage bits into the quantized DCT coefficients belonging to some specific frequencies such that it introduces less change to the original JPEG images. In [106], Efimushkina *et al.* aimed at embedding messages to some selected coefficients with small magnitudes (i.e., the coefficients with values of 0, 1, 2) to ensure that the data hiding introduces less distortion in the host JPEG images. The approach has gained about 44% increase in average payload compared with that achieved by the un-optimized counterpart at the same image distortion. In [107], Nikolaidis et al. proposed a data hiding scheme for JPEG image by relying on modification of the quantized DCT coefficients with the value of zero. In contrast to the most prevailing methods which make use of non-zero quantized DCT coefficients for data embedding, it provides significantly lower distortion on similar embedding capacity; but the size of the marked JPEG image is not discussed in this paper. Recently, Huang *et al.* [108] have provided some insights on how to select quantized DCT coefficients for RDH. A new histogram shifting-based RDH scheme was proposed, in which the zero coefficients remain unchanged and only coefficients with values of 1 are expanded to carry message, thus the storage size of the marked JPEG image is well preserved. In their scheme, the histogram bins 1 and -1 are employed for data embedding. The embedding algorithm can be described as follows

$$x' = \begin{cases} x + sign(x)b, & \text{if } |x| = 1 \\ x + sign(x), & \text{if } |x| > 1 \end{cases} \tag{13}$$

where x and x' are respectively the non-zero quantized DCT coefficient before and after data embedding, and $b \in \{0, 1\}$ is a message bit. As all of the non-zero coefficients in the DCT domain would be modified by one at most, the quality of the marked-image is maintained. Moreover, a block selection strategy according to the number of zero coefficients in each 8×8 blocks is designed to adaptively choose blocks rich in zero coefficients for data embedding, by which the distortion of the marked JPEG image is minimized.

Different from the RDH applied to un-compressed image, the storage size of the marked JPEG file is another important index for the performance evaluation of a RDH scheme for JPEG image. The RDH based on modifying the quantized DCT coefficients can achieve acceptable embedding capacity and good visual quality while preserving the storage size of the marked JPEG image. As the embedding capacity, image fidelity and the storage size of the marked JPEG file can be well balanced, this category of RDH method becomes the most popular approach and have received increasing attention in the past few years. Exploiting more efficient data embedding techniques to enhance the embedding capacity might be one promising direction of this kind of scheme.

B. RDH WITH QUANTIZATION TABLE MODIFICATION

The second approach is based on the modification of the JPEG quantization tables. In [109], Fridrich *et al.* firstly modified the quantization table to losslessly embed one bit per DCT coefficients. Specifically in the case where the quantization factor $Q(i, j)$ is even, it would be divided by two and the corresponding coefficient $D(i, j)$ is multiplied by two (the result is denoted by $D'(i, j)$) without changing the visual appearance of the image at all. As $D'(i, j)$ is even, the bit can be embedded into the LSB of $D'(i, j)$, the data embedding is certainly invertible. The idea can be shown as,

$$\begin{cases} Q'(i, j) = \lfloor Q(i, j)/2 \rfloor \\ D'(i, j) = 2D(i, j) \\ D''(i, j) = D'(i, j) + b \end{cases} \tag{14}$$

where $b \in \{0, 1\}$ is a message bit. However, this technique has two drawbacks. One drawback is that a non-standard quantization table is used, which must be included in the header of the JPEG image with the hidden data. Another drawback is that the modified stream of quantized coefficients will be less compressible in the process of Huffman coding, and the overall compression efficiency of the marked JPEG image, i.e., the JPEG image with the hidden data, would be decreased. In [110], Chang *et al.* presented a RDH scheme to modify the specific entries of quantization table and hide secret messages in the cover image with its middle-frequency coefficients of the quantized DCT table. Considering some areas are not utilized by Chang *et al.*'s method, Lin and Shiu [111] proposed another method called the layer-1 data embedding stratagem to improve the hiding capacity of Chang *et al.*'s scheme while maintaining the visual quality of the marked image. Recently, Chen *et al.* [112] employed the JPEG compressed stream of an image as the cover medium. Two quantization tables (original and modified) map the DCT coefficients of each block to some larger ones and thus the data are embedded. The scheme could achieve high performance in terms of both data hiding rate and image visual quality at the expense of the increase of the storage size of the marked JPEG file. Wang *et al.* [113] proposed to divide the entries of quantization table by an integer, and then multiply the corresponding quantized DCT coefficients with the same integer to make the space for data embedding; hence, the high embedding capacity and fidelity are achieved.

However, as the original quantization table of JPEG files offers a trade-off between the file size and visual quality, the category of RDH in JPEG images based on modifying the JPEG quantization tables may inevitably break the balance between the visual quality and their storage sizes. With this category of RDH methods, the storage size of the JPEG images generally increases significantly after the data have been embedded.

C. RDH WITH HUFFMAN TABLE MODIFICATION

The third approach is based on the modification of the Huffman table. In [114], Mobasseri *et al.* exploited the fact that only a fraction of JPEG code space is actually used by available encoders. Data embedding is performed by mapping a used variable length code (VLC) to an unused VLC, through which the file size is maintained or even decreased despite carrying a payload. Qian and Zhang [115] have mapped the unused VLC codes to usable codes according to the statistical results of VLC usage in a cover. During data hiding, parts of codes in bit-stream are replaced by the mapped codes according to the secret bits. Later on, Hu *et al.* [116] took full advantage of the unused VLCs by mapping Huffman codes according to a specific mapping strategy to enhance the embedding capacity, and resulting in high data capacity. Wu and Deng [117] proposed a new integer-vector conversion algorithm and applied it to JPEG Huffman tables so that the bit stream changes synchronically with the embedded message. Moreover, the scheme is applicable to any JPEG bit-stream even if its Huffman tables are optimized.

Although these methods can ensure the fidelity and preserve the storage size of the marked JPEG image, the embedding capacity is rather limited. Therefore, it can only be employed for image authentications where low payload embedding is satisfied.

D. DISCUSSION AND SUMMARY

Apart from the above mentioned, there are still some other interesting ideas for the RDH into JPEG images. In [118], Zhang *et al.* proposed a reversible watermarking scheme for JPEG image authentication. In [119], Chen *et al.* presented a quantized DCT coefficients based RDH, in which a triplet consisting of one non-zero coefficient and two zero-valued coefficients is used to accommodate one additional bit. Moreover, Kuo *et al.* [120] proposed a RDH scheme based on exploiting modification direction (EMD) and JPEG compression technology, Ohyama *et al.* [121] presented a RDH method for JPEG2000 compressed image.

Although quite some number of RDH for JPEG images have been proposed in the past, the RDH into JPEG image is still challenging because the process is more complicated than the RDH into un-compressed images. As the information redundancy in JPEG images is much less than that in uncompressed image, any modification made in the compressed domain may result in obvious or even serious distortion in the host JPEG images. Furthermore, apart from the embedding capacity and fidelity (imperceptibility) that need to be considered like for the case of uncompressed image, the storage size of the marked-image also should be taken into consideration in the JPEG scenario. Among various data hiding schemes discussed above, the number of reported RDH techniques for JPEG images is still rather limited and there is a huge need to enhance the fidelity of the marked image and the data embedding capacity while keeping the size of JPEG file without increasing largely.

+	−	+	−	+	−	+	−
−	+	−	+	−	+	−	+
+	−	+	−	+	−	+	−
−	+	−	+	−	+	−	+
+	−	+	−	+	−	+	−
−	+	−	+	−	+	−	+
+	−	+	−	+	−	+	−
−	+	−	+	−	+	−	+

FIGURE 7. The pattern of difference pair in each block.

IV. ROBUST REVERSIBLE DATA HIDING

In this section, the definition and motivation of the so-called robust RDH (RRDH) is firstly introduced followed by the descriptions of some representative methods that have been published in the literature.

A. MOTIVATION

In some applications, an image with some hidden data may undergo some processing. If the processing is irreversible, the original image will not be recovered completely in general. Nevertheless, it is appealing that the hidden data can be extracted as much as possible from the processed image. So the property of robustness is often desired in the applications of RDH. In the past decades, quite a few RRDH methods have been reported for digital images. In the following, some representative methods are discussed.

B. REPRESENTATIVE METHODS FOR ROBUST RDH

The first RRDH scheme was proposed by Vleeschouwer *et al.* [122], [123], which is based on the correlations existed among the neighboring pixels. As reported, the method is robust to JPEG compression to some extent. To avoid the overflow/underflow problems, additions and subtractions are conducted via using the modulo-256 scheme. After modulo-256 addition, white pixels may be changed to black ones while black ones may be changed to white ones, resulting in the so-called ąřsalt-and-pepperąś noise and thus lowering the image visual quality.

After pointing out this drawback existed in [122] and [123], Ni *et al.* [124], [125] presented a RRDH scheme to avoid the salt-and-pepper noise. Specifically, a robust statistical quantity based on patchwork theory is identified and employed for data hiding. The host image is firstly divided into blocks (e.g., with the size of 8×8 as shown in Fig. 7). By adopting the Error Correction Coding (ECC) and permutation techniques, the reversibility can be achieved if the image has not gone through some kind of non-reversible process, and the robustness can be achieved if the image has gone through, say, some kind of the JPEG compression. As shown in Fig. 7, each 8×8 block is split into two sets (denoted by A, consisting of all elements marked by '$+$', and B, consisting of all elements marked by '$-$',) of pixels. Then the difference value of these two sets, i.e., A and B, is calculated by

$$\alpha = \frac{1}{n}\sum_{i=1}^{n}(a_i - b_i) \tag{15}$$

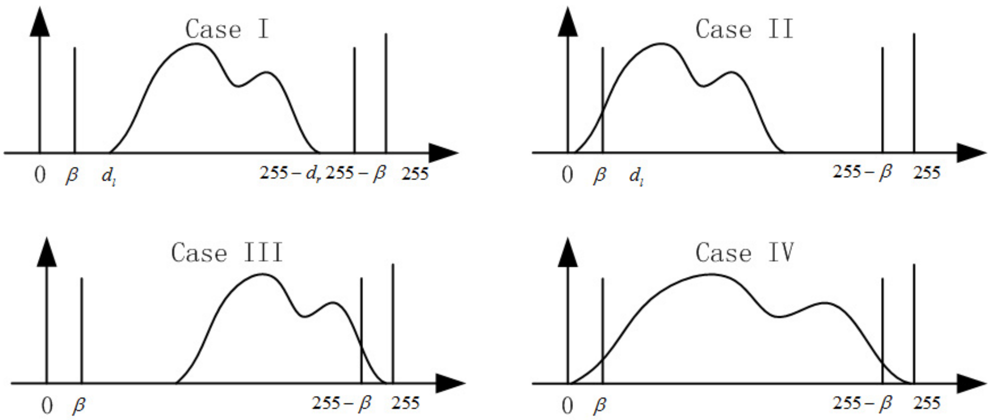
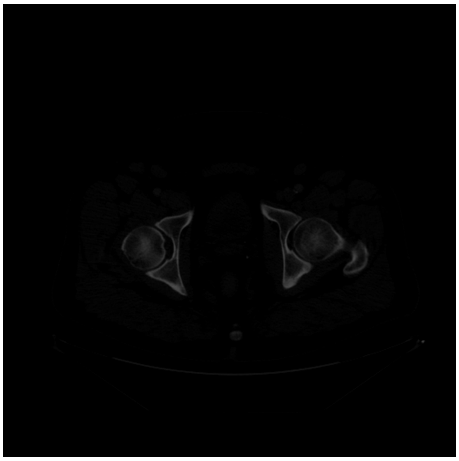


FIGURE 8. Block histogram distribution for different cases.

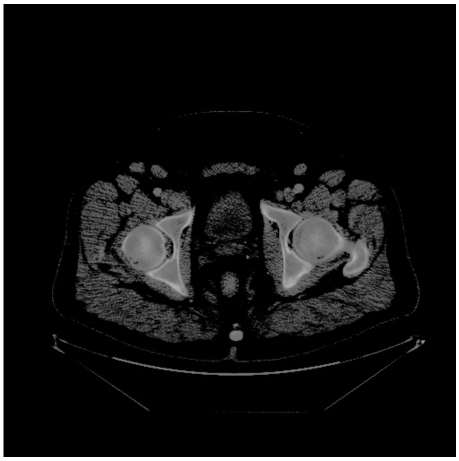
where a_i and b_i are pixels contained in the sets A and Set B, respectively. Since the pixels' grayscale values are often highly correlated in the same block, the difference value α is expected to be close to 0 most likely. Moreover, as the difference value α is based on the statistics of all pixels in a block, even though some pixels in the block have been slightly changed after JPEG compression, this statistic value likely remains unchanged. This statistical quantity is intrinsically robust to JPEG/JPEG2000 compression and to other small incidental alterations. In the proposed scheme, each block is used to embed one bit, the block size will thus affect data embedding capacity apparently. The robustness of embedded bits would be stronger if the block size is larger. Therefore, a compromise between the data embedding capacity and the robustness of hidden data needs to be made according to different applications. As shown in Fig. 8, in order to overcome the overflow/underflow problem, the blocks are classified into four different categories, and for each category a specified bit-embedding scheme is applied. In Case I, the pixel grayscale values of a block under consideration are far away from the two bounds of the histogram (0 and 255 for an 8-bit grayscale image), i.e., the distance $d = \min(d_l, d_r)$ satisfies $d \geq \beta$ (where β is a selected quantity). The difference value α is kept unchanged to embed bit "0", and is shifted beyond a specified threshold, K, to embed bit "1". In Case II, when binary "0" is to be embedded, do nothing; when binary "1" is to be embedded, the algorithm only shift the histogram towards the right hand by K. In Case III, when binary "0" is to be embedded, do nothing; when binary "1" is to be embedded, the algorithm only shift the histogram towards the left hand by K. In Case IV, because some pixel grayscale values of the block under consideration are close to the left and some others are close to the right bounds of the histogram, all the pixel values would be kept intact to avoid the overflow/underflow of the pixels grayscale values. Hence, if binary "0" is to be embedded, no problem occurs. If binary "1" is to be embedded, however, an error is then to be produced, which will be corrected via using ECC to correct them. Later on, most of RRDH schemes have been developed based on this framework.

Inspired by the idea in [125], Zou *et al.* [126] developed a robust digital watermarking system based on the shifting the absolute mean values of IWT coefficients. In [45] and [127], Gao *et al.* reported an improved version of Ni *et al.*'s method, in which the ECC is not needed. This improvement has been achieved by the following two measures. One is to skip some selected blocks in data embedding; another is a theoretical analysis conducted to guarantee the reconstruction of the original host image without distortion. To better exploit the statistical characteristics of a host image, a framework has been further proposed by incorporating the merits of the generalized statistical quantity histogram (GSQH) and the histogram-based embedding so that the embedding capacity and robustness are improved. Later, An *et al.* [128], [129] constructed a RRDH scheme by histogram shifting and clustering in IWT domain, which are efficient to improve the robustness and reduce the computing complexity. The problem of overflow/underflow is handled by adopting the method of property-inspired pixel adjustment (PIPA). Some improved techniques have also been proposed to solve the problem of salt-and-pepper noise and to improve the imperceptibility of the image with the hidden data.

Recently, Tsai *et al.* [130], [131] presented a kind of zero-watermark RRDH scheme based on α-trimmed mean algorithm and support vector machine (SVM). In their method, the cover image is unchanged because the embedded message has been memorized by the trained SVM so that data extraction can be accomplished by the estimation of the trained SVM algorithm. The α-trimmed mean algorithm is utilized in the method to resist the noise attacks. Yin *et al.* have built a selection and evaluation method of non-overlapping feature regions for RRDH. Besides the aforementioned, the RRDH methods that can resist geometric attacks [132], [133] and can be robust against H.264/AVC video compression [134], [135] have also been reported in the literature



(a)



(b)

FIGURE 9. A medical image acquired with poor illumination and the one obtained after contrast enhancement. (a) Original medical image. (b) Contrast-enhanced image: PSNR=18.66dB.

C. CONCLUDING REMARKS

For many applications such as medical and military images, RDH is needed. If an image with the hidden data has not been changed, the original image can be completely recovered and the hidden data can be correctly extracted. However, if the image with the data hidden inside has undergone some processing or incidental alterations, e.g., the lossy JPEG compression, the hidden data is expected to be able extracted correctly, even though the original image may not be completely recovered. Hence the robust RDH is useful in reality. The future work may aim at developing some more efficient RRDH schemes.

V. REVERSIBLE DATA HIDING WITH CONTRAST ENHANCEMENT

In this section, the RDH methods with contrast enhancement are reviewed. Firstly, the motivation of developing the image RDH with contrast enhancement is introduced. Then the RDH methods in [136]–[139] are reviewed one by one, in which the quality of the host images can be preserved by contrast enhancement instead of keeping PSNR as high as possible. After that, image quality assessment in the scenario of RDH with contrast enhancement is discussed. At the end of this section, the topics that are worth exploring in future are pointed out.

A. MOTIVATION OF RDH WITH CONTRAST ENHANCEMENT

RDH has been developed originally for authentication purpose in the distortion sensitive applications such as in medicine, military and satellite. The perceptual quality of the host image plays an important role and should be preserved as well as possible. To measure the difference between the original image and the one with the hidden data, the PSNR between them is often utilized. As an objective measurement, the PSNR value decreases when more distortions are introduced into image content by the operations of data embedding. Normally, there exists a trade-off between the PSNR and the embedding capacity. So the curve of the PSNR versus the hiding rate is often plotted to evaluate the performance of the image RDH methods, such as those reviewed in Section II.

Although the quality of the image with the hidden data can be preserved by keeping PSNR high, such as using the state-of-the-art RDH methods (e.g., [51], [87], [90]), the visual quality can hardly be improved because more or less distortions are introduced by data hiding. For the images with poor quality, such as those acquired with poor illumination, preserving the image quality is not enough but improving the visual quality is more important. For instance, contrast enhancement of the medical or satellite images is often desired to show the details for visual inspection. As shown in Fig. 9, the visibility of image details can be improved by contrast enhancement though the PSNR value of the enhanced image is low (only 18.66 dB). It can be seen that keeping PSNR high becomes not so important in some cases.

As the PSNR is not suitable for image quality assessment in the certain scenarios, the normal RDH methods often focus on keeping the PSNR as high as possible. So a new type of RDH is in need to improve the visual quality of the host image. As contrast enhancement is often desired for some applications, the functionality has been achieved in [136] by performing the so-called histogram bin expansion operations to obtain the effect of histogram equalization [140]. Similarly, several following methods have been proposed in [137]–[139] to preserve the visual quality by contrast enhancement instead of simply keeping PSNR high in RDH. From the experimental results, it can be seen that the visual quality can be improved by applying these methods. In the following, the methods in [136]–[139] will be reviewed one by one.

B. FOUR RDH METHODS WITH CONTRAST ENHANCEMENT

In this section, four RDH methods with contrast enhancement are reviewed. The common feature of these methods is that the visual quality can be improved by contrast entrancement under some circumstances.

1) METHOD BY HISTOGRAM BIN EXPANSION IN [136]

In principle, image contrast enhancement can be achieved by histogram equalization [140]. To perform data hiding and contrast enhancement simultaneously, the method in [136] is conducted by modifying the histogram of pixel values. For a gray-level image, image histogram is firstly calculated by counting the number of every pixel value ranging from 0 to 255 in the host image. Among the non-empty bins in the histogram, the highest two are chosen and denoted by f_L and f_R, respectively. For a pixel value f scanned in raster order, the histogram bin expansion operation is performed by

$$f' = \begin{cases} f-1, & \text{if } f < f_L \\ f-b, & \text{if } f = f_L \\ f, & \text{if } f_L < f < f_R \\ f+b, & \text{if } f = f_R \\ f+1, & \text{if } f > f_R, \end{cases} \tag{16}$$

where f' is the value generated to replace f, and b is a binary value (0 or 1) in the bitstream to be hidden. After applying Eq. (16) to every pixel in the host image, the highest two bins are expanded into four bins to carry the hidden data. After that, the highest two bins in the *modified* histogram are chosen to be expanded by updating the values of f_L and f_R in Eq. (16). By repeatedly expanding the highest two bins in the modified histogram, the effect of histogram equalization can be achieved.

To avoid the overflows and underflows due to histogram bin expansion, the host image need to be pre-processed. Suppose that S pairs of histogram bins are expanded in total (it is required that $S \leq 64$). Then the range of pixel values from 0 to $S-1$ are added by S in pre-processing, while the pixels from $256-S$ to 255 are subtracted by S. To memorize the locations of those pixels modified, a binary location map with the same size as the host image is generated by assigning 1s to their locations, while 0s are assigned to the other locations. For the recovery of the original image, the location map is losslessly compressed by the JBIG standard [141] and hidden into the host image with other data.

In the process of data extraction, the values of the expanded histogram bins should be known to recover the original image. By knowing the last two expanded bins, which are denoted by f_{LL} and f_{LR}, a binary value b' can be extracted from a pixel value f' given that $f' \in \{f_{LL}-1, f_{LL}, f_{LR}, f_{LR}+1\}$, i.e.,

$$b' = \begin{cases} 1, & \text{if } f' = f_{LL}-1 \text{ or } f' = f_{LR}+1 \\ 0, & \text{if } f' = f_{LL} \text{ or } f' = f_{LR} \\ \textit{null}, & \textit{otherwise}. \end{cases} \tag{17}$$

The process of data extraction is also performed in raster order. Meanwhile, the following operation is carried out to restore the histogram bins:

$$f = \begin{cases} f'+1, & \text{if } f' < f_{LL} \\ f', & \text{if } f_{LL}-1 < f' < f_{LR}+1 \\ f'-1, & \text{if } f' > f_{LR}. \end{cases} \tag{18}$$

If the previously expanded bins are also known, the data hidden within them can be further extracted from the restored histogram by applying Eq. (17). Meanwhile, the operations in Eq. (18) are iteratively carried out to restore the histogram until the image after pre-processing is obtained.

To recover the original image, the pixels modified in pre-processing should be restored according to the location map extracted from the contrast-enhanced image. Since the pixel values originally in $[0, S-1]$ are added by S in pre-processing, a pixel value within $[S, 2S-1]$ is subtracted by S if the corresponding value in the location map is 1. For a pixel within $[256-2S, 255-S]$, it is added by S if the corresponding value in the location map is 1. Note that the compressed location map, the number of histogram bin pairs totally expanded, and all of the histogram bin values expanded for data hiding are kept in the contrast-enhanced image so that the original image can be blindly recovered in [136].

2) METHOD WITH CONTRAST ENHANCEMENT FOR MEDICAL IMAGES IN [137]

Although both high-capacity RDH and contrast enhancement can be achieved by applying the method in [136], artificial distortions may be introduced to the images with strong background. To overcome the drawback, a new RDH method is presented in [137] for medical images. Specifically, background segmentation is firstly carried out by employing Otsu's method [142] to separate the image into background and the region of interest (ROI). Then the pixel values in the segmented background above a pre-defined percentage are identified as the principle ones. By excluding the histogram bins of those principle values from being expanded, the contrast of ROI can be selectively enhanced. To alleviate the distortions caused by pre-processing, two intervals with the length of S (i.e., the number of histogram bin pairs to be expanded) are adaptively chosen in the histogram so that the minimum number of pixels are contained, respectively. The chosen intervals are overlapped by histogram shifting to minimize the "dis-ordering" of pixel values that may be caused by pre-processing. In the extraction process, the hidden data can be extracted in the similar way as in [136] because all of the expanded histogram bins are hidden in the contrast-enhanced image. Meanwhile, the original image can be blindly recovered by extracting the location map hidden in the contrast-enhanced image.

3) METHOD WITH THE CONTROLLED CONTRAST ENHANCEMENT IN [138]

To alleviate the visual distortions caused by using [136] for high-capacity data hiding, another method is proposed in [138]. To prevent the over enhancement, an upper bound of the relative contrast error (RCE) defined in [143] is set to control the degree of contrast enhancement. Since a RCE value greater than 0.5 indicates the enhanced contrast, the upper bound is set to 0.55 to preserve the visual quality. Then data hiding is further conducted in the Haar IWT domain to increase the hiding capacity. In this way, generally better image quality can be achieved in the case of high-capacity hiding.

4) AUTOMATIC CONTRAST ENHANCEMENT METHOD IN [139]

Another RDH based method to achieve reversible contrast enhancement is proposed in [139]. Unlike in [136] where the location map is generated only once, their method generates the map for every histogram expansion to avoid the artifacts that may be caused by pre-processing. Specifically, the highest histogram bin is expanded while the lowest bin is merged with one adjacent bin at the same time. To equalize the histogram, as many repetitions as possible are conducted. Automatic contrast enhancement can be performed until the embedding capacity is not sufficient to accommodate the increasing overhead information. The experimental results show that the better visual quality can be achieved for poorly exposed images by the method in [139]. Meanwhile, the effects of contrast enhancement can be achieved, similar to those obtained with the global histogram equalization function *histeq* in Matlab.

C. IMAGE QUALITY ASSESSMENT IN RDH WITH CONTRAST ENHANCEMENT

To evaluate the effect of contrast enhancement, the RCE defined in [143] is calculated in the methods of [136]–[138]. However, the RCE value cannot be used to represent the visual quality because it may be high for an enhanced image with visual distortions. Although the visual quality can be improved by applying the schemes introduced in [136]–[139] under some circumstances, the enhanced contrast does not necessarily lead to good image quality. Meanwhile, PSNR is still used in [136]–[139] as a reference of image quality due to the lack of a suitable image quality evaluator. Since PSNR is not always suitable for image quality assessment, other criteria need to be found to guide the process of RDH more efficiently. In the following, we will introduce using the Structural SIMilarity (SSIM) [144], the methods specially developed for the contrast changed images, and the no-reference methods for image quality assessment, respectively.

1) USING SSIM FOR IMAGE QUALITY ASSESSMENT

As a popular image quality evaluator, the SSIM index is calculated between two images. Different from the objective methods that quantify the errors (differences) between a distorted image and a reference image, the SSIM index is designed for quality assessment based on the degradation of structural information. The range of the SSIM index is from 0 to 1, and it equals to 1 when the two images are identical [144]. In [137], the SSIM index is used to evaluate image quality in addition to PSNR. The experimental results on the test images in [145] and [146] have shown that the SSIM index between the original and contrast-enhanced images generally decreases as the hiding rate is increased while the obtained RCE value increases with the hiding rate. The SSIM index generally decreases with the enhanced contrast, despite whether there are visual distortions introduced into image content or not. That means that the SSIM index is sensitive to both of the enhanced contrast and the visual distortions that may be caused. Therefore, it is not enough to use SSIM and PSNR for image quality assessment in RDH with contrast enhancement.

2) USING THE METHODS FOR CONTRAST CHANGED IMAGES

The methods specially developed for the contrast changed images can be adopted if the original image or its entropy is available [147], [148]. For instance, a patch-structure representation method for quality assessment of the contrast changed images can be found in [148]. Since an image patch can be decomposed into its mean intensity, signal strength and signal structure components, the perceptual distortions can be evaluated in different ways. A local contrast quality map is produced so that the patch-based contrast quality index (PCQI) method can provide accurate predictions on the human perception of contrast variations [148].

3) USING THE NO-REFERENCE METHODS

In addition to SSIM and PCQI, the no-reference methods have been proposed for image quality assessment, such as in [149]–[154]. Basically, a good no-reference method suitable for the scenario of contrast enhancement should be more tolerant to the enhanced contrast given that the image quality is well preserved. In [154], a no-reference quality assessment of the contrast-distorted images is proposed based on natural scene statistics (NSS). A large scale image database is employed to construct the NSS models by using the moment and entropy features. So the quality of a contrast-enhanced image can be evaluated based on its unnaturalness characterized by the degree of deviation from the NSS models.

D. CONCLUSION AND FUTURE WORK

From the RDH methods reviewed in this section, it can be seen that the functionality of contrast enhancement can be achieved with RDH. One important aspect of image RDH is to preserve the visual quality. That is why contrast enhancement is required for some applications instead of simply keeping the PSNR as high as possible. To achieve the better image quality, the pre-processing and the data hiding process in [136]–[139] may be improved to achieve the

TABLE 1. Terms used in this paper.

Terms	Explanations
original media	media such as images, audio, videos in plaintext form
encrypted media	media obtained by encrypting the original media
additional bits	Binary string to be embedded into the encrypted media
marked encrypted media	encrypted media containing additional bits
approximate media	the directly decrypted version close to the original media
recovered media	perfectly restored media that is identical to the original image
content-owner	owner of the original media who encrypts the original media
data-hider	one who embeds additional bits into the encrypted media
receiver	one who receives the marked encrypted media, and performs data extraction and/or reconstruction

better effects. By hiding additional information into the contrast-enhanced image, more functionalities can be enabled such as authentication and content annotation in addition to contrast enhancement.

One topic that is worth exploring is image quality assessment in RDH. By accurately assessing the visual quality, the process of RDH can be better guided to achieve the more satisfactory results. Besides the PSNR and SSIM, it will be rewarding to adopt the methods specially developed for the contrast changed images (e.g., [148]) and the no-reference methods (e.g., [149]–[154]) for image quality assessment. Since quite a few no-reference image quality assessment have been proposed in the literature, more comparative experiments should be conducted to find out the one most suitable for the contrast-enhanced images. With the proper image quality assessment, more sophisticated methods that can preserve or even improve the image quality through data hiding are expected to be proposed in future.

VI. REVERSIBLE DATA HIDING IN ENCRYPTED DOMAIN

A. MOTIVATION

As is well known, encryption is an effective and popular means of privacy protection. Recently, the research on signal processing over encrypted domain, primarily driven by the needs from Cloud computing platforms and various privacy preserving applications, has gained increasing attention. Combination of data hiding and encryption has also received some of the earliest attention. In some existing joint data-hiding and encryption schemes [155]–[157], only a part of cover data are encrypted and the rest can be used to carry the additional message. In [155], the intra-prediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In [156], the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In these joint schemes, however, since only partial encryption is involved, lead to leakage of partial information of the cover. Furthermore, the separation of original cover and embedded data from a watermarked version is not considered. Also, the data embedding is not reversible.

Most of works on RDH discussed in previous sections are suitable for plaintext domain, namely, the additional bits are embedded into the original, un-encrypted multimedia data. Along with more and more attention on signal processing over encrypted domain, the investigation of embedding additional data in the encrypted domain in a reversible fashion is triggered. In order to securely store or share multimedia file with other person, a content owner may encrypt the media data before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted media though he does not know the original content. Taking medical images administration as an example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. It may be also hopeful that the original content can be recovered exactly after decryption and data extraction at receiver side. That means RDH in encrypted domain (RDH-ED) is required. In this section, the state-of-the-art reversible embedding techniques of RDH-ED are reviewed.

As an emerging technology, RDH-ED aims at embedding additional information into cipher-data without revealing the plaintext content and recovering the original plaintext content error-free at the receiver side. For the ease of discussion, explanations of some frequently used terms are listed in Table 1.

The general framework of RDH-ED is sketched in Fig. 10. Consider the three parties in the entire workflow: *content-owner*, *data-hider*, and *receiver*, whose roles are described as follows.

- *Content-Owner:* Encrypt the original media to conceal the principal content with or without some preprocessing. An encryption key is chosen by the content-owner.
- *Data-Hider:* Embed the additional bits into the encrypted media. A data hiding key is used by the data-hider for security.
- *Receiver:* Three options are available for receivers who hold different keys. Option 1: decrypt the marked encrypted media to get approximate media. Option 2: Extract the additionally embedded bits. Option 3: generate the recovered media that is identical to the original.

The existing RDH-ED methods can be classified into two categories: "vacating room before encryption (VRBE)" and "vacating room after encryption (VRAE)". Here, we provide an overview in each category one by one.

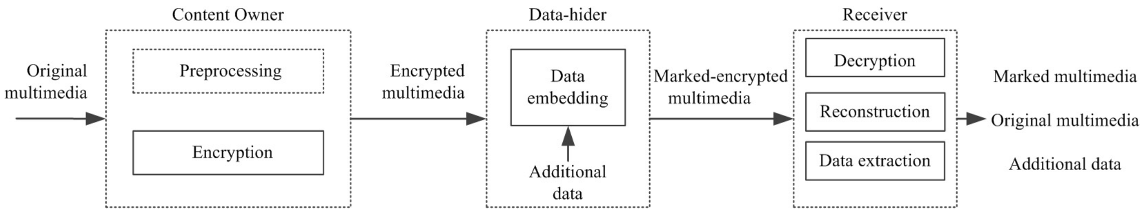


FIGURE 10. **General framework of RDH-ED.**

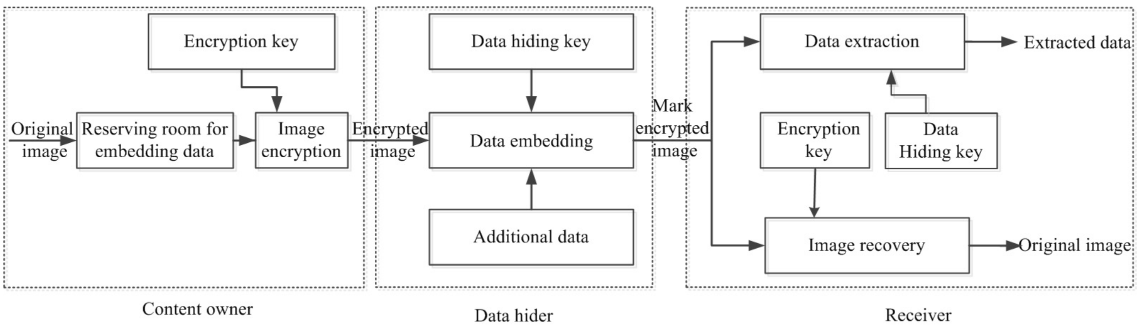


FIGURE 11. **VRBE framework.**

B. VACATING ROOM BEFORE ENCRYPTION (VRBE)

VRBE framework creates embedding room in the plaintext domain, i.e., vacating embedding room before encryption [158]–[161]. Thus, the content owner is expected to perform an extra preprocessing before encryption. Take image as example (similarly hereinafter), the sketch of VRBE framework is shown in Fig. 11.

In [158], the embedding room is created in digital images by embedding LSBs of certain pixels into other pixels using a traditional RDH method. The pre-processed image is then encrypted by the owner to generate an encrypted image. Thus, the positions of these vacated LSBs in the encrypted image can be used by the data-hider, and a large payload up to 0.5 bpp can be achieved.

With a similar idea, another method based on a prediction technique is proposed [159]. In this method, some pixels are estimated by the rest pixels before encryption and predicted errors are gained. Then, a special encryption scheme is designed to encrypt the predicted errors and a benchmark encryption algorithm (e.g. AES) can be applied to the rest pixels. Instead of embedding data in encrypted images directly, additional data can be embedded by shifting the encrypted histogram of predicted errors.

Further improvement is made by considering the patch-level sparse representation [160]. The widely used sparse coding technique has demonstrated that an image patch can be linearly represented by some atoms in an over-complete dictionary. As the sparse coding is an approximation solution, the leading residual errors are encoded and self-embedded within the cover image. Furthermore, the learned dictionary is also embedded into the encrypted image. Thanks to the powerful representation of sparse coding, a large vacated room can be achieved, and thus the data hider can embed more secret messages in the encrypted image.

In [161], embedding room is vacated by combining Paillier homomorphic encryption and a traditional plaintext RDH technique, i.e., difference expansion. In this scheme, preprocessing is required. In other words, before image encryption, the image owner has to pre-process the original image to generate a processed image with a modified difference expansion method. Then, the processed image would be encrypted by Paillier homomorphic encryption and sent to the data-hider, who will embed one bit into each pair of adjacent encrypted pixels and generate the marked encrypted image containing additional bits. Based on the homomorphic property of Paillier encryption, the receiver compares all pairs of decrypted pixels to obtain the embedded bits, and also recovers the cover-image.

VRBE framework might be impractical because it requires the content owner to perform an extra preprocessing before content encryption. In this sense, VRAE framework, what you will see in the following, is more close to practice.

C. VACATING ROOM AFTER ENCRYPTION (VRAE)

In VRAE methods, the original signal is encrypted directly by the content owner, and the data-hider embeds the additional bits by modifying some bits of the encrypted data. Also take image as example, the sketch of VRAE framework is shown in Fig. 12.

Based on the domain in which the additional data can be extracted, VRAE methods can be further grouped into three basic categories. These include data extraction in the plaintext domain, data extraction in the cipher domain and

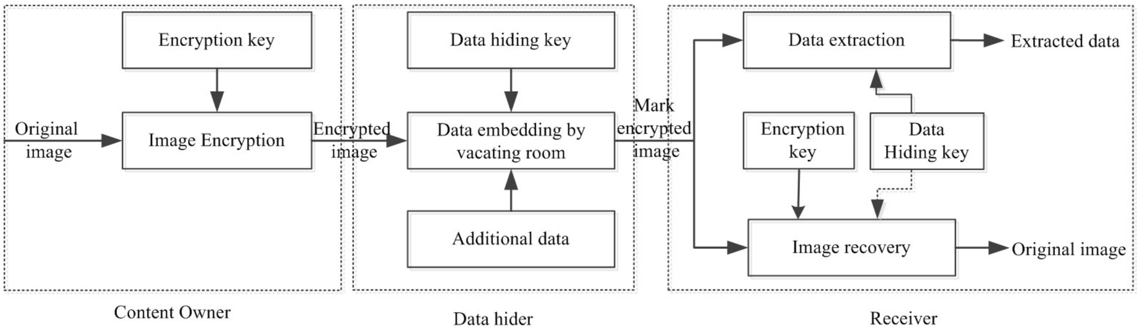


FIGURE 12. VRAE framework.

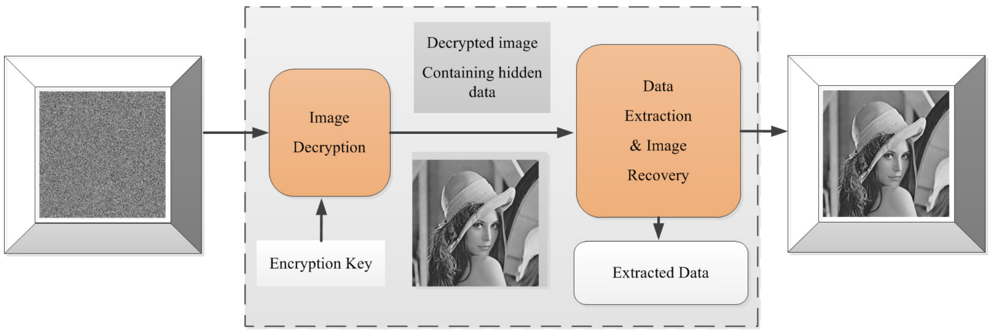


FIGURE 13. Sketch of data extraction and image recovery in plaintext domain.

data extraction in both domains. In the first place, we introduce data extraction in the plaintext domain.

1) VRAE: DATA EXTRACTION IN THE PLAINTEXT DOMAIN

In these methods, with an encrypted medium containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. The sketch of data extraction and image recovery in plaintext domain is shown in Fig. 13.

The first method is proposed by Zhang for encrypted images [162], in which the data-hider divides the encrypted image into blocks and embeds one bit into each block by flipping three least significant bits (LSB) of half the pixels in the block. On the receiver side, the marked encrypted image is decrypted to an approximate image. The receiver flips the three LSBs of pixels to form a new block and uses a function to estimate the image-texture of each block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block. Thus the embedded bits can be extracted and the original image can be recovered jointly. Embedding rate of this method depends on the block size. If an inappropriate block size is chosen, errors may occur during data extraction and image recovery. A similar method for JPEG images is proposed by Qian *et al.* [163], that hides data into the encrypted JPEG bit-stream and recovers the original bit-stream by analyzing the blocking artifacts caused by data hiding.

This method [162] has been paid great attention [164]–[169]. For example, in [164], the performance is improved by exploiting spatial correlation between neighboring blocks and using a side-match algorithm to achieve higher embedding payload with lower error rates in image recovery. The performance is further improved by introducing a flipping ratio [165] and using unbalanced bit flipping [166]. In [167], a more precise function is presented to estimate the image-texture of each image block and increase the correctness of data extraction/image recovery. Furthermore, during data embedding in [168], the LSBs of fewer pixels are flipped instead of flipping the LSBs of half pixels in the encrypted image, which leads to the significant improvement for the visual quality of the approximate image. And a new adaptive judging function based on the distribution characteristic of image local contents is utilized to estimate the image-texture of each block in the procedures of data extraction and image recovery, which decrease the errors of extracted bits and recovered image to some extent.

In [169], a two-class SVM classifier is adopted to distinguish encrypted and non-encrypted image blocks rather than the judging functions used in [162] and [164]–[168]. At the same time, this method gets a sharp rise in the embedding capacity since the data embedding is achieved through a public key modulation mechanism rather than LSBs flipping.

In addition, some researchers have achieved this kind of RDH-ED based on public key cryptosystem and homomorphic encryption [170]. In [170], it is stated that a RDH scheme

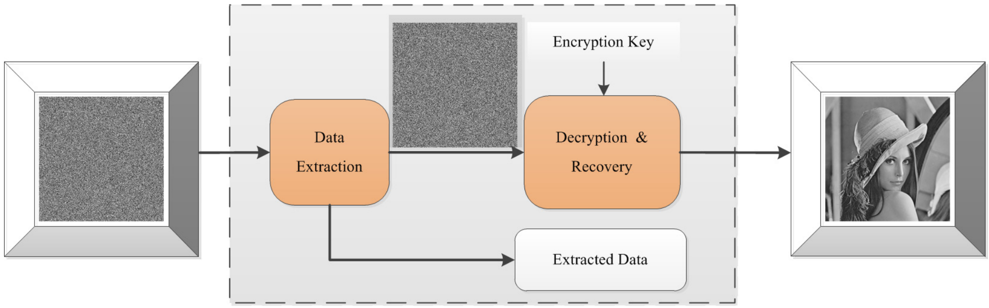


FIGURE 14. Sketch of data extraction in the cipher domain.

for any encrypted signals is proposed and digital image is taken as an example for description. During image encryption, each pixel value was segmented into two parts, i.e., seven most significant bits (MSBs) and one LSB, and these two parts were encrypted respectively. Then, two encrypted LSBs of each encrypted pixel pair were modified to reversibly embed one secret bit according to the properties of homomorphism. The receiver can easily extract the embedded bits and recover the original image by judging the relationship of the two decrypted LSBs in each pixel pair. However, in the aspect of images, the inherent overflow cannot be avoided.

These methods introduced above focus on the data extracting after decryption. In other words, the additional data must be extracted from the plaintext domain, so that the principal content is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the marked encrypted media which containing additional bits. Since the extraction of the embedded bits and the recovery of the original media are often tied together, this category is also called non-separable solution [171]. Opposite to this category, there is another type called separable solution, in which the data extraction can be separately carried out before image decryption, i.e., data extraction in the cipher domain.

2) VRAE: DATA EXTRACTION IN THE CIPHER DOMAIN

In these methods, with a marked encrypted medium, a legal receiver having the data-hiding key can extract the additional bits in the cipher domain directly, while a receiver having the encryption key can decrypt the received data to obtain an edition similar to the original one, i.e., the approximate medium. If the receiver has both the data-hiding and encryption keys, he can extract the additional bits and recover the original medium error-free. Sketch of data extraction in the cipher domain is shown in Fig. 14.

The idea was first proposed by [172], in which the owner encrypts the original image by Advanced Encryption Standard (AES), and the data-hider embeds one bit in each block containing n pixels, meaning that the embedding rate is $\frac{1}{n}$ bpp. On the receiver side, data extraction and image recovery are realized by analyzing the local standard deviation after decryption of the marked encrypted image. Although this method provides a good embedding rate, two drawbacks are fatal on the recipient side. On the one hand, the attacker may break some information from the enciphered bits by statistical analysis. Since each block is encrypted independently using AES with an encryption key, redundancy in an image may result in the reduplicative encrypted blocks. On the other hand, if the receiver directly deciphers the marked encrypted image, quality of the decrypted image is rather poor, which is far from the human vision requirements.

To overcome the drawbacks in [172] and solve the problem that additional data can only be extracted from the decrypted domain, Zhang further proposed an RDH-ED method for stream-enciphered images using the idea of compressing the encrypted bits to accommodate the additional bits [171]. The data-hider pseudo-randomly permutes and divides the encrypted image into groups with size of L. The P LSB-planes of each group are compressed with a matrix G sized $(PL - S) \times (PL)$ to generate corresponding vectors. Thus, S bits are available for data embedding. On the receiver side, a total of $8 - P$ most significant bits (MSB) of pixels are obtained by decryption. The receiver then estimates the P LSBs by the MSBs of neighboring pixels. By comparing the estimated bits with the vectors in the coset Ω corresponding to the extracted vectors, the receiver can recover the original bits of the P LSBs. Because the additional bits are embedded in LSBs of the encrypted images, they can be extracted directly before image decryption.

This method [171] ignites researchers' passion again [173]–[179]. Qian *et al.* use histogram shifting to encipher the original image and then additional bits can be embedded into the encrypted image by using an n-nary data hiding scheme [173]. In [174], the cover image is partitioned into non-overlapping blocks and encrypted by multi-granularity encryption. The additional data is then embedded into the blocks in a sorted order with respect to block smoothness by using a novel local histogram shifting. Both of them [173], [174] provide satisfactory embedding payload and nice image quality. However, as the original image is encrypted with pixel permutation and affine transformation, leakage of image histogram is inevitable under exhaustive attack.

Some other methods further vacate embedding room by encrypted bits compression [175], [178], [179]. Zhang *et al.* extended the lossless compression based RDH approach to the encrypted domain [175]. Half of the 4th LSBs of the encrypted image are losslessly compressed via low density parity check (LDPC) code to create space for data hiding. In [179], authors encode the selected bits taken from the stream-ciphered image using LDPC codes into syndrome bits to make spare room to accommodate the additional data. In [178], the least significant bits of pixels in encrypted image are losslessly compressed by the Hamming distance calculation between the LSB stream and auxiliary stream.

In some application scenarios, a content owner encrypts the plaintext media, e.g., images, and asks a telecommunication operator or a channel provider to deliver the encrypted data to some users. Although the telecommunication operator/channel provider does not know the plaintext content, he may hope to insert a visible watermark into the encrypted data and deliver the marked encrypted data to the users, so that the users who have not paid for data transmission can only obtain a visibly marked version, i.e., a quality-degraded image, by decrypting the received data, while the users authorized both by the content owner and the telecommunication operator/channel provider can obtain the original image after data extraction and content recovery. That means the reversible visible watermark embedded in the encrypted domain is needed. In [180], a reversible visible watermarking scheme for encrypted images based on wet paper codes is proposed. In this scheme, the exclusive-or operation is employed for encryption, and a part of encrypted data corresponding to the black pixels of watermark image is altered to insert the visible watermark and carry some additional data used for content recovery. Although the watermark is inserted in encryption domain, it is invisible through the encrypted data and visible after direct decryption at receiver side, i.e., a direct decryption would result in a visibly marked image. If the data-hiding key is available, the receiver can employ the wet paper decoding to extract the embedded bits from the marked encrypted image and a joint decryption-extraction recovery operation may retrieve the original plaintext image error-free if both of the keys are available.

In addition, while most RDH-ED methods are based on stream cipher, Qian *et al.* presents an alternative method feasible for block-enciphered images [177]. Before uploading data to a remote server, the content owner encrypts the original image with a block cipher algorithm using an encryption key. Then, the server embeds additional bits into the encrypted image with an embedding key to generate the marked encrypted image. On the recipient side, the additional bits can be extracted from the encrypted domain if the receiver has the embedding key. Compared with the existing block cipher based RDH-ED method [172], image security and quality can be improved.

Besides, in [176], a universal reversible data embedding method applicable to any encrypted domain is described. It has stated that the coding redundancy of any encrypted signal can be exploited by partitioning it into segments and using Golomb-Rice codewords (GRC) to entropy encode them. Then two bits can be embedded into each segment GRC code in a reversible manner. The experimental results shown in the article have demonstrated that, for every bit of the encrypted signal, an average embedding payload of 0.169 bit can be achieved.

With the methods mentioned above, although the embedded data can be extracted in encrypted domain by using the data-hiding key, it is impossible to perform the data extraction in decrypted domain. Thus, there is one key problem of the works discussed so far, that the embedded data can only be extracted either before (shown in Fig. 14) or after (shown in Fig. 13) decryption. That means that a legal receiver who has the data hiding key but no decryption key he cannot extract the embedded bits from the cipher domain directly, or, on the other hand, a legal receiver who has the data hiding key and the decrypted media containing additional bits he cannot extract the embedded data. So, a kind of new RDH-ED framework in which the embedded bits can be extracted from both plaintext domain and cipher domain is desirable.

3) VRAE: DATA EXTRACTION IN BOTH DOMAINS

In this framework, with the marked encrypted media containing additional bits, a legal receiver who knows the data-hiding key can extract the embedded data from the cipher domain directly. And a content user with the encryption key may decrypt the encrypted data to obtain a similar edition to the original one. If someone receives the approximate media and has the data-hiding key, he can also successfully extract the additional bits and perfectly recover the original image. The sketch of data extraction in both domains is shown in Fig. 15.

In [181], the first solution based on pseudorandom sequence modulation is provided. In this scheme, a part of data in LSB planes of encrypted image is replaced with the additional data and the rest data in LSB planes are modified by the pseudorandom sequences modulated by the replaced bits and embedded data. Then, the additional-data user with the data-hiding key can easily extract the additional data in encrypted domain. Since the data embedding operation affects only the LSB, a direct decryption may result in an image with principal original content. By finding the modulated sequences corresponding to the minimal fluctuation, the embedded data can be extracted from the decrypted image and the original content can also be recovered without any error when the embedding rate is not too high.

In some methods, RDH-ED is achieved by means of embedding data into space not being affected by encryption [182]–[186]. In [182], the gray values of two neighboring pixels are masked by same pseudo-random bits. Then, the additional data are embedded into various bit planes with a reversible manner, and a parameter optimization method is used to ensure a good payload-distortion performance. Because the data space used for accommodating the additional data is not affected by the encryption operation, the data insertion/extraction can be performed in both the plain and

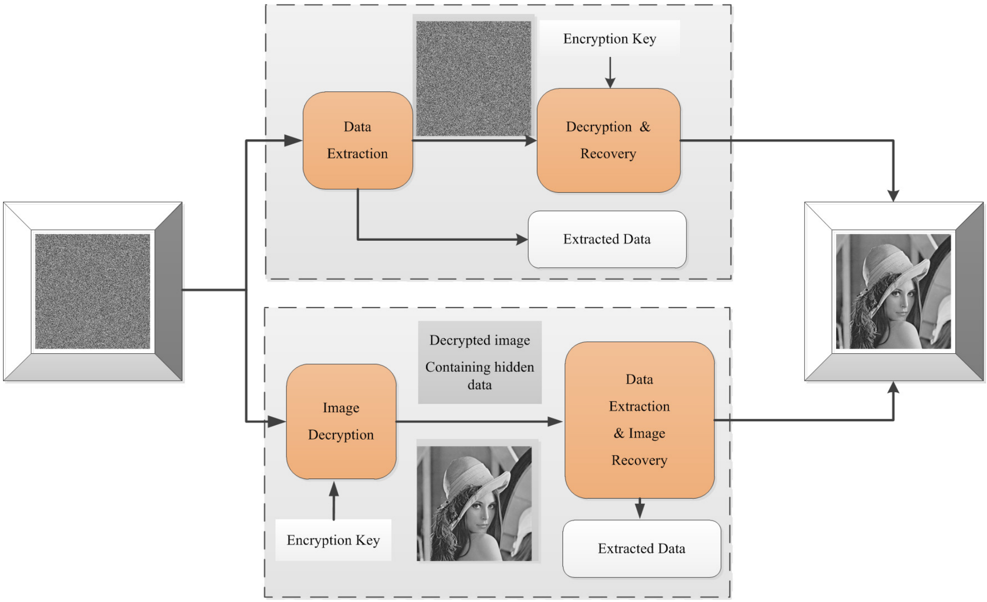


FIGURE 15. Sketch of data extraction in both domains.

encrypted domains, and the ways of data insertion/extraction in the two domains are same. In [183], a complete separable RDHEI method is proposed based on block division, RC4 encryption and block histogram modification. At first, the original image is divided into non-overlapping blocks. Then all the pixels within each block can be encrypted by RC4 with the same key. Thus each encrypted block keeps structure redundancy to carry additional bits and RDH is achieved by block histogram shifting. The embedded data can be extracted error-free both from the marked encrypted image (cipher domain) and directly decrypted image (plaintext domain). However, this method is not suitable for images containing saturated pixels. A similar idea is proposed in [184], where the image is divided into groups by cross division and all the pixels within each group are encrypted by RC4 with the same key. Thus the difference histogram is maintained after image encryption. Then additional bits can be reversibly embedded by using difference histogram shifting. In [185], the cover image is first encrypted by permutation in both block- and pixel-wise manners using a chaotic mapping. Then, the PVO embedding [71] is adopted to reversibly embed additional bits into each permuted block. Since the pixel value order is unchanged in each block after PVO embedding, the embedded data can be exactly extracted using the inverse PVO whether the marked image is decrypted or not. In [186], a stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels. Then, additional bits can be embedded into the interpolation-error by modified histogram shifting and difference expansion technique. Then, data extraction can be done either in the encrypted domain or in the decrypted domain. However, just as described in the experimental results of the paper, the leakage of image contour is inevitable.

In another method, RDH-ED is achieved with the benefit of Homomorphic encryption [187]. This paper proposes a lossless, a reversible, and a combined data hiding schemes for cipher images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the cipher pixels are replaced with new values to embed the additional bits into several LSB-planes of cipher pixels by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

D. FUTURE WORK

Undoubtedly, RDH in encrypted domain is a new topic and also an emerging technology. In our view, in the near future, the research on theory, framework, methodology and applications on RDH-ED should be deeply developed. Firstly, we need new theory about RDH-ED to give the achievable rate-distortion performance suitable for the statistical properties of plaintext data and the usability of cryptographic key. Secondly, a generalized framework is desired. Thirdly, we need more methods on RDH-ED to improve actual rate-distortion performance. At last, new techniques are on-demand for special application scenarios such as the privacy protection and security management of massive data.

VII. VIDEO AND AUDIO REVERSIBLE DATA HIDING

In addition to image RDH, the RDH into video and into audio have also moved ahead recently, however, in a much smaller scale. In this section we briefly discuss these two subjects.

A. VIDEO REVERSIBLE DATA HIDING

The research works on RDH mainly focus on still image. In contrast, the research on video/audio RDH has obtained less attention. Liu *et al.* [135] developed a video RDH scheme based on histogram modification. The to-be-embedded data is encoded by using BCH syndrome code before data hiding to improve robustness. Then the encoded data is embedded into the quantized DCT coefficients of the 4×4 blocks of intra-frame. Song *et al.* [188] took Multi-Vide Coding (MVC) videos as the carrier, and presented a reversible video steganography scheme for hiding secret data into the motion vector of each block. The idea of the inner product between the motion vector and the modulation vector is introduced to achieve reversibility. To increase the embedding capacity of histogram based reversible watermarking techniques, Zhao *et al.* [189] proposed a RDH algorithm based on two-dimensional (2D) histogram modification. Two quantized DCT coefficients are randomly selected from each embeddable 4×4 luminance block for embedding data with 2D histogram modification, which can provide the better capacity-distortion performance. Vural and Barakli [190] presented a reversible video watermarking method based on motion-compensated frame interpolation error expansion. Unlike the current reversible video watermarking approaches that are based on the modification of the motion-compensated prediction error histogram, this method is based on motion-compensated frame interpolation error expansion. Consequently, it allows high-capacity data insertion to video, and causes small distortion in the original video. In addition, RDH-based approach for intra-frame error concealment in H.264/AVC are presented [10], [191]. By using the histogram modification technique, these methods embed the motion vector (MV) of a macroblock (MB) into other MB within the same intra-frame. If an MB is corrupted at the decoder side, the embedded MV can be extracted from the corresponding MB for the recovery of the corrupted MB.

Due to the security and privacy-preserving requirements for cloud data management, it is sometimes desired that video content is accessible in an encrypted form. RDH for encrypted H.264/AVC videos is proposed recently [192], [193]. The data-hider can embed the secret data into the encrypted video using the modified histogram shifting method, even though he does not know the original video content.

B. AUDIO REVERSIBLE DATA HIDING

The papers on researches on audio RDH is even less that reported for video RDH. Yan and Wang [194] proposed an audio RDH scheme based on prediction error expansion. The secret information is embedded into the expanded prediction error. The location map technique is adopted to solve the underflow/overflow problem. The compressed location map needs to be embedded together with the secret information in order to ensure the reversibility. Similar to [194], Nishimura [195] has proposed to use the Burg's method to calculate the predicted coefficients. A higher SNR and a larger embedding capacity are thus obtained. Considering on the capacity control capability, Nishimura [196] proposed a variable expansion method which is combined with the prediction error expansion. A smaller expansion factor results in a smaller payload and less degradation. It has been shown that with a random payload of less than 0.4 bits per sample embedded into CD-format music signals, the stego audio still maintains with acceptable objective quality. The method is also applied to G.711 μ-law-coded speech signals. Wang *et al.* [197] proposed a reversible audio data hiding scheme based on improved prediction error expansion and histogram shifting. Different from using the fixed set of linear prediction coefficients in [194], the optimal linear prediction coefficients are determined by the differential evolution algorithm. Histogram shifting technique is applied to reduce the embedding location information dramatically. The results have shown that this algorithm can enhance the capability to control capacity.

In [198], Nishimura proposed another reversible audio data hiding scheme based on quantization index modulation (QIM). The secret information is embedded into the apertures in the amplitude histogram created by amplitude expansion in QIM. The objective perceptual evaluation shows that the proposed method can achieve good imperceptibility. However, the technique is not reversible when applied to modified stego audio. In [199], Nishimura improved the scheme reported in [198]. The improved scheme is reversible for unmodified stego audio and is semi-reversible for perceptually coded stego audio. Direct-sequence spread-spectrum (DSSS) modulation is applied to embed the secret information. The sequence is determined from the amplitude expansion in time and frequency of integer modified discrete cosine transform (MDCT) coefficients. Similar to [198], the reversible payload is embedded into the apertures in the amplitude histogram. The results show that the mean objective difference grade (ODG) is better than "perceptible, but not annoying" for the stego audio. Semi-recovery from the perceptually coded stego audio is realized in terms of small differences in ODG between the recovered and coded audio.

VIII. SUMMARY

With digital images used as the main media together with video and audio, this survey paper has addressed the following six subjects for the reversible data hiding (RDH).

They are the RDH into digital images in the spatial domain, the RDH into digital images in the JPEG domain, the semi-fragile RDH into digital images that have gone through some lossy compression, the image quality measure used for RDH which is different from the PSNR, the RDH into encrypted digital images and the RDH for video and audio. For each subject, the typical algorithms and the methodologies behind them are presented, analyzed and discussed. It is expected that the research on the RDH and the applications of the RDH will continue to move ahead in the future. Furthermore, it is noticed that all of the first five subjects mentioned above are presented and addressed with digital images as media. This is because there is only a much smaller number of papers published in the literature that have addressed RDH in the field of video and in the field of audio. It is expected that this will be changed in the near future in the research on RDH because of the increased importance of video and audio in our digital society.

ACKNOWLEDGEMENT

The authors acknowledge Dr. Dawen Xu (School of Electronics and Information Engineering, Ningbo University of Technology) and Dr. Diqun Yan (College of Information Science and Engineering, Ningbo University) for their contributions to Section VII. Their sincere appreciation goes to Professor Guorong Xuan (Dept. of Computer Science, Tongji University) for his valuable technical discussion.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.
[2] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[3] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: Fundamentals, algorithms and applications," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 2. May 2004, pp. 33–36.
[4] Y. Q. Shi, "Reversible data hiding," in *Proc. Int. Workshop Digit. Watermarking*, 2004, pp. 1–12.
[5] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," *EURASIP J. Inf. Secur.*, vol. 2010, 2010, Art. no. 134546.
[6] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U.S. Patent 5 646 997, Jul. 8, 1997.
[7] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U.S. Patent 6 278 791, Aug. 21, 2001.
[8] F. Bao, R.-H. Deng, B.-C. Ooi, and Y. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," *IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 4, pp. 554–563, Dec. 2005.
[9] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 2, pp. 158–165, Mar. 2009.
[10] K. L. Chung, Y. H. Huang, P. C. Chang, and H. Y. M. Liao, "Reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 11, pp. 1643–1647, Nov. 2010.
[11] D. Coltuc and I. Caciula, "Stereo embedding by reversible watermarking: Further results," in *Proc. Int. Symp. Signals, Circuits Syst.*, Jul. 2009, pp. 1–4.
[12] X. Tong *et al.*, "Stereo image coding with histogram-pair based reversible data hiding," in *Proc. Int. Workshop Digital-Forensics Watermarking*, 2014, pp. 201–214.
[13] X. Wang, C. Shao, X. Xu, and X. Niu, "Reversible data-hiding scheme for 2-D vector maps based on difference expansion," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 311–320, Sep. 2007.
[14] F. Peng, Y.-Z. Lei, M. Long, and X.-M. Sun, "A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion," *Comput.-Aided Design*, vol. 43, no. 8, pp. 1018–1024, 2011.
[15] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep. 2010.
[16] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," *Proc. SPIE*, vol. 4314, pp. 197–208, Aug. 2001.
[17] M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," in *Proc. 4th Inf. Hiding Workshop*, 2001, pp. 27–41.
[18] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 2, pp. 185–196, 2002.
[19] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," *Electron. Lett.*, vol. 38, no. 25, pp. 1646–1648, Dec. 2002.
[20] G. Xuan, J. Chen, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su, "Lossless data hiding based on integer wavelet transform," in *Proc. IEEE Int. Workshop Multimedia Signal Process.*, Dec. 2002, pp. 312–315.
[21] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in *Proc. IEEE Int. Conf. Inf. Process.*, vol. 2. Sep. 2002, pp. 157–160.
[22] G. Xuan *et al.*, "High capacity lossless data hiding based on integer wavelet transform," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 2. May 2004, pp. 29–32.
[23] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.
[24] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," *IEEE Trans. Image Process.*, vol. 15, no. 4, pp. 1042–1049, Apr. 2006.
[25] J. Tian, "Wavelet-based reversible watermarking for authentication," *Proc. SPIE*, vol. 4675, pp. 679–690, Apr. 2002.
[26] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
[27] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.
[28] D. Coltuc and J. M.Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.
[29] S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," *IEEE Signal Process. Lett.*, vol. 15, pp. 721–724, 2008.
[30] X. Wang, X. Li, B. Yang, and Z. Guo, "Efficient generalized integer transform for reversible watermarking," *IEEE Signal Process. Lett.*, vol. 17, no. 6, pp. 567–570, Jun. 2010.
[31] Y. Qiu, Z. Qian, and L. Yu, "Adaptive reversible data hiding by extending the generalized integer transformation," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 130–134, Jan. 2016.
[32] C. Wang, X. Li, and B. Yang, "High capacity reversible image watermarking based on integer transform," in *Proc. IEEE Int. Conf. Inf. Process.*, Sep. 2010, pp. 217–220.
[33] F. Peng, X. Li, and B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Process.*, vol. 92, no. 1, pp. 54–62, Jan. 2012.
[34] D. Coltuc, "Low distortion transform for reversible watermarking," *IEEE Trans. Image Process.*, vol. 21, no. 1, pp. 412–417, Jan. 2012.
[35] D. M. Thodi and J. J. Rodriguez, "Prediction-error based reversible watermarking," in *Proc. IEEE Int. Conf. Inf. Process.*, Oct. 2004, pp. 1549–1552.
[36] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.
[37] M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction," *IEICE Electron. Exp.*, vol. 5, no. 20, pp. 870–876, Oct. 2008.
[38] Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 2, pp. 250–260, Feb. 2009.

[39] W. Hong, T.-S. Chen, and C.-W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," *J. Syst. Softw.*, vol. 82, no. 11, pp. 1833–1842, Nov. 2009.
[40] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.
[41] W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.
[42] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[43] M. Fujiyoshi, T. Tsuneyoshi, and H. Kiya, "A parameter memorization-free lossless data hiding method with flexible payload size," *IEICE Electron. Exp.*, vol. 7, no. 23, pp. 1702–1708, 2010.
[44] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 873–882, Sep. 2011.
[45] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 8, pp. 1061–1070, Aug. 2011.
[46] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[47] J. Zhou and O. C. Au, "Determining the capacity parameters in PEE-based reversible image watermarking," *IEEE Signal Process. Lett.*, vol. 19, no. 5, pp. 287–290, May 2012.
[48] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 111–120, Jan. 2013.
[49] C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 7, pp. 1109–1118, Jul. 2013.
[50] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, Apr. 2014.
[51] I. C. Dragoi and D. Coltuc, "On local prediction based reversible watermarking," *IEEE Trans. Image Process.*, vol. 24, no. 4, pp. 1244–1246, Apr. 2015.
[52] S. Xiang and Y. Wang, "Non-integer expansion embedding techniques for reversible image watermarking," *EURASIP J. Adv. Signal Process.*, vol. 2015, p. 56, 2015.
[53] L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2082–2090, Dec. 2005.
[54] G. Xuan, Y. Q. Shi, J. Teng, X. Tong, and P. Chai, "Double-threshold reversible data hiding," in *Proc. IEEE Int. Symp. Circuits Syst.*, May/Jun. 2010, pp. 1129–1132.
[55] W. Hong, "An efficient prediction-and-shifting embedding technique for high quality reversible data hiding," *EURASIP J. Adv. Signal Process.*, vol. 2010, Feb. 2010, article ID 104835.
[56] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," *Opt. Commun.*, vol. 285, no. 2, pp. 101–108, Jan. 2012.
[57] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1091–1100, Jul. 2013.
[58] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, Dec. 2013.
[59] Q. Pei, X. Wang, Y. Li, and H. Li, "Adaptive reversible watermarking with improved embedding capacity," *J. Syst. Softw.*, vol. 86, no. 11, pp. 2841–2848, 2013.
[60] W. Hong, T.-S. Chen, and J. Chen, "Reversible data hiding using delaunay triangulation and selective embedment," *Inf. Sci.*, vol. 308, pp. 140–154, Jul. 2015.
[61] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2003, pp. II-912–II-915.
[62] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
[63] A. van Leest, M. van der Veen, and F. Bruekers, "Reversible image watermarking," in *Proc. IEEE Int. Conf. Inf. Process.*, vol. 2. Sep. 2003, pp. II-731–II-734.
[64] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," *IEICE Electron. Exp.*, vol. 4, no. 7, pp. 205–210, 2007.
[65] S.-K. Lee, Y.-H. Suh, and Y.-S. Ho, "Reversiblee image authentication based on watermarking," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2006, pp. 1321–1324.
[66] G. Xuan, Y. Q. Shi, P. Chai, X. Cui, Z. Ni, and X. Tong, "Optimum histogram pair based image lossless data embedding," in *Proc. Int. Workshop Digit. Watermarking*, 2007, pp. 264–278.
[67] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 321–330, Sep. 2007.
[68] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram-shifting-based reversible data hiding," *IEEE Trans. Image Process.*, vol. 22, no. 6, pp. 2181–2191, Jun. 2013.
[69] M. Muzzarelli, M. Carli, G. Boato, and K. Egiazarian, "Reversible watermarking via histogram shifting and least square optimization," in *Proc. ACM MM&Sec*, 2010, pp. 147–152.
[70] G. Feng and L. Fan, "Reversible data hiding of high payload using local edge sensing prediction," *J. Syst. Softw.*, vol. 85, no. 2, pp. 392–399, 2012.
[71] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Process.*, vol. 93, no. 1, pp. 198–205, 2013.
[72] W.-J. Yang, K.-L. Chung, H.-Y. M. Liao, and W.-K. Yu, "Efficient reversible data hiding algorithm based on gradient-based edge direction prediction," *J. Syst. Softw.*, vol. 86, no. 2, pp. 567–580, Feb. 2013.
[73] B. Ou, X. Li, Y. Zhao, and R. Ni, "Reversible data hiding based on PDE predictor," *J. Syst. Softw.*, vol. 86, no. 10, pp. 2700–2709, Oct. 2013.
[74] T.-C. Lu, C.-Y. Tseng, and K.-M. Deng, "Reversible data hiding using local edge sensing prediction methods and adaptive thresholds," *Signal Process.*, vol. 104, pp. 152–166, Nov. 2014.
[75] X. Qu and H. J. Kim, "Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding," *Signal Process.*, vol. 111, pp. 249–260, Jun. 2015.
[76] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 653–664, Mar. 2015.
[77] S. Hiary, I. Jafar, and H. Hiary, "An efficient multi-predictor reversible data hiding algorithm based on performance evaluation of different prediction schemes," *Multimedia Tools Appl.*, pp. 1–27, Jan. 2016. [Online]. Available: http://link.springer.com/article/10.1007%2Fs11042-015-3161-9
[78] C. Wang, X. Li, and B. Yang, "Efficient reversible image watermarking by using dynamical prediction-error expansion," in *Proc. IEEE Int. Conf. Inf. Process.*, Sep. 2010, pp. 3673–3676.
[79] H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting," *KSII Trans. Internet Inf. Syst.*, vol. 4, no. 4, pp. 655–670, Aug. 2010.
[80] H.-T. Wu and J. Huang, "Reversible image watermarking on prediction errors by efficient histogram modification," *Signal Process.*, vol. 92, no. 12, pp. 3000–3009, Dec. 2012.
[81] G. Xuan, X. Tong, J. Teng, X. Zhang, and Y. Q. Shi, "Optimal histogram-pair and prediction-error based image reversible data hiding," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2012, pp. 368–383.
[82] X. Chen, X. Sun, H. Sun, Z. Zhou, and J. Zhang, "Reversible watermarking method based on asymmetric-histogram shifting of prediction errors," *J. Syst. Softw.*, vol. 86, no. 10, pp. 2620–2626, 2013.
[83] J. Wang, J. Ni, and Y. Hu, "An efficient reversible data hiding scheme using prediction and optimal side information selection," *J. Vis. Commun. Image Represent.*, vol. 25, no. 6, pp. 1425–1431, 2014.
[84] L. Dong, J. Zhou, Y. Y. Tang, and X. Liu, "Estimation of capacity parameters for dynamic histogram shifting (DHS)-based reversible image watermarking," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2014, pp. 1–6.
[85] X. Ma, Z. Pan, S. Hu, and L. Wang, "High-fidelity reversible data hiding scheme based on multi-predictor sorting and selecting mechanism," *J. Vis. Commun. Image Represent.*, vol. 28, pp. 71–82, Apr. 2015.
[86] D. Cavagnino, M. Lucenteforte, and M. Grangetto, "High capacity reversible data hiding and content protection for radiographic images," *Signal Process.*, vol. 117, pp. 258–269, Dec. 2015.

[87] J. Wang, J. Ni, X. Zhang, and Y.-Q. Shi, "Rate and distortion optimization for reversible data hiding using multiple histogram shifting," *IEEE Trans. Cybern.*, to be published.

[88] S.-Y. Wang, C.-Y. Li, and W.-C. Kuo, "Reversible data hiding based on two-dimensional prediction errors," *IET Image Process.*, vol. 7, no. 9, pp. 805–816, 2013.

[89] I. Caciula and D. Coltuc, "Improved control for low bit-rate reversible watermarking," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2014, pp. 7425–7429.

[90] X. Li, W. Zhang, X. Gui, and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 2016–2027, Sep. 2015.

[91] I.-C. Dragoi, D. Coltuc, and I. Caciula, "Horizontal pairwise reversible watermarking," in *Proc. Eur. Signal Process. Conf.*, Aug./Sep. 2015, pp. 56–60.

[92] B. Ma and Y. Q. Shi, "A reversible data hiding scheme based on code division multiplexing," *IEEE Trans. Inf. Forensics Security*, vol 11, no. 9, pp. 1914–1927, Sep. 2016.

[93] T. Kalker and F. M. J. Willems, "Capacity bounds and constructions for reversible data-hiding," in *Proc. Int. Conf. Digit. Signal Process.*, vol. 1. 2002, pp. 71–76.

[94] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[95] S.-J. Lin and W.-H. Chung, "The scalar scheme for reversible information-embedding in gray-scale signals: Capacity evaluation and code constructions," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1155–1167, Aug. 2012.

[96] X. Zhang, "Reversible data hiding with optimal value transfer," *IEEE Trans. Multimedia*, vol. 15, no. 2, pp. 316–325, Feb. 2013.

[97] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 779–788, May 2013.

[98] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," *IEEE Trans. Image Process.*, vol. 22, no. 7, pp. 2775–2785, Jul. 2013.

[99] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 294–304, Jan. 2015.

[100] F. Balado, "Optimum reversible data hiding and permutation coding," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Nov. 2015, pp. 1–4.

[101] *The JPEG Standard*, accessed on 2016. [Online]. Available: http://www.jpeg.org/

[102] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in *Proc. Int. Conf. Inf. Technol., Coding Comput.*, Apr. 2001, pp. 223–227.

[103] G. Xuan, Y. Q. Shi, Z. Ni, P. Chai, X. Cui, and X. Tong, "Reversible data hiding for JPEG images based on histogram Pairs," in *Proc. Int. Conf. Image Anal. Recognit.*, 2007, pp. 715–727.

[104] H. Sakai, M. Kuribayashi, and M. Morii, "Adaptive reversible data hiding for JPEG images," in *Proc. IEEE Int. Symp. Inf. Theory Appl.*, Dec. 2008, pp. 1–6.

[105] Q. Li, Y. Wu, and F. Bao, "A reversible data hiding scheme for JPEG images," in *Proc. Pacific-Rim Conf. Multimedia*, 2010, pp. 653–664.

[106] T. Efimushkina, K. Egiazarian, and M. Gabbouj, "Rate-distortion based reversible watermarking for JPEG images with quality factors selection," in *Proc. Eur. Workshop Vis. Inf. Process.*, Jun. 2013, pp. 94–99.

[107] A. Nikolaidis, "Reversible data hiding in JPEG images utilising zero quantised coefficients," *IET Image Process.*, vol. 9, no. 7, pp. 560–568, Jul. 2015.

[108] F. Huang, X. Qu, H. J. Kim, and J. Huang, "Reversible data hiding in JPEG images," *IEEE Trans. Circuits Syst. Video Technol.*, to be published.

[109] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," *Proc. SPIE*, vol. 4675, pp. 572–583, Apr. 2002.

[110] C.-C. Chang, C.-C. Lin, C.-S. Tseng, and W.-L. Tai, "Reversible hiding in DCT-based compressed images," *Inf. Sci.*, vol. 177, no. 13, pp. 2768–2786, 2007.

[111] C.-C. Lin and P.-F. Shiu, "DCT-based reversible data hiding scheme," *J. Softw.*, vol. 5, no. 2, pp. 214–224, Feb. 2010.

[112] L. S.-T. Chen, S.-J. Lin, and J.-C. Lin, "Reversible JPEG-based hiding method with high hiding-ratio," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 24, no. 3, pp. 433–456, 2010.

[113] K. Wang, Z.-M. Lu, and Y.-J. Hu, "A high capacity lossless data hiding scheme for JPEG images," *J. Syst. Softw.*, vol. 86, no. 7, pp. 1965–1975, 2013.

[114] B. G. Mobasseri, R. J. Berger, M. P. Marcinak, and Y. J. NaikRaikar, "Data embedding in JPEG bitstream by code mapping," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 958–966, Apr. 2010.

[115] Z. Qian and X. Zhang, "Lossless data hiding in JPEG bitstream," *J. Syst. Softw.*, vol. 85, no 2, pp. 309–313, 2012.

[116] Y. Hu, K. Wang, and Z.-M. Lu, "An improved VLC-based lossless data hiding scheme for JPEG images," *J. Syst. Softw.*, vol. 86, no. 8, pp. 2166–2173, 2013.

[117] Y. Wu and R. H. Deng, "Zero-error watermarking on jpeg images by shuffling huffman tree nodes," in *Proc. IEEE Vis. Commun. Image Process.*, Nov. 2011, pp. 1–4.

[118] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Reversible fragile watermarking for locating tampered blocks in JPEG images," *Signal Process.*, vol. 90, no. 12, pp. 3026–3036, 2010.

[119] C.-C. Chen and D.-S. Kao, "DCT-based reversible image watermarking approach," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Nov. 2007, pp. 489–492.

[120] W.-C. Kuo, S.-H. Kuo, and L.-C. Wuu, "High embedding reversible data hiding scheme for JPEG," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2010, pp. 74–77.

[121] S. Ohyama, M. Niimi, K. Yamawaki, and H. Noda, "Reversible data hiding of full color JPEG2000 compressed bit-stream preserving bit-depth information," in *Proc. Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4.

[122] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in *Proc. IEEE Workshop Multimedia Signal Process.*, Oct. 2001, pp. 345–350.

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

[124] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jun. 2004, pp. 2199–2202.

[125] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 4, pp. 497–509, Apr. 2008.

[126] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1294–1300, Oct. 2006.

[127] X. Gao, L. An, X. Li, and D. Tao, "Reversibility improved lossless data hiding," *Signal Process.*, vol. 89, no. 10, pp. 2053–2065, Oct. 2009.

[128] L. An, X. Gao, X. Li, D. Tao, C. Deng, and J. Li, "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Trans. Image Process.*, vol. 21, no. 8, pp. 3598–3611, Aug. 2012.

[129] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng, and F. Ji, "Content-adaptive reliable robust lossless data embedding," *Neurocomputing*, vol. 79, pp. 1–11, Mar. 2012.

[130] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai, "Robust lossless watermarking using alpha-trimmed mean and SVM," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Jul. 2008, pp. 3347–3353.

[131] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai, "Robust lossless image watermarking based on *a*-trimmed mean algorithm and support vector machine," *J. Syst. Softw.*, vol. 83, no. 6, pp. 1015–1028, Jun. 2010.

[132] N. S. Narawade and R. D. Kanphade, "Robust semi-reversible watermarking using pixel averaging method against geometric attack," *IUP J. Telecommun.*, vol. 5, no. 1, pp. 46–55, 2013.

[133] N. S. Narawade and R. D. Kanphade, "Robust reversible watermarking against geometric attack using geometric transformation correction applied on spatial domain methods," *IUP J. Telecommun.*, vol. 5, no. 3, pp. 47–56, 2013.

[134] M. A. Alavianmehr, M. Rezaei, M. S. Helfroush, and A. Tashk, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," in *Proc. Int. ISC Conf. Inf. Secur. Cryptol.*, Oct. 2013, pp. 194–198.

[135] Y. Liu, L. Ju, M. Hu, X. Ma, and H. Zhao, "A robust reversible data hiding scheme for H.264 without distortion drift," *Neurocomputing*, vol. 151, pp. 1053–1062, Mar. 2015.
[136] H.-T. Wu, J.-L. Dugelay, and Y.-Q. Shi, "Reversible image data hiding with contrast enhancement," *IEEE Signal Process. Lett.*, vol. 22, no. 1, pp. 81–85, Jan. 2015.
[137] H.-T. Wu, J. Huang, and Y.-Q. Shi, "A reversible data hiding method with contrast enhancement for medical images," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 146–153, Aug. 2015.
[138] G. Gao and Y.-Q. Shi, "Reversible data hiding using controlled contrast enhancement and integer wavelet transform," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2078–2082, Nov. 2015.
[139] S. Kim, R. Lussi, X. Qu, and H. J. Kim, "Automatic contrast enhancement using reversible data hiding," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Nov. 2015, pp. 1–5.
[140] J. A. Stark, "Adaptive image contrast enhancement using generalizations of histogram equalization," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 889–896, May 2000.
[141] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W. J. Rucklidge, "The emerging JBIG2 standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8, no. 7, pp. 838–848, Nov. 1998.
[142] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Trans. Syst., Man, Cybern.*, vol. 9, no. 1, pp. 62–66, Jan. 1979.
[143] M.-Z. Gao, Z.-G. Wu, and L. Wang, "Comprehensive evaluation for HE based contrast enhancement techniques," in *Proc. Int. Comput. Symp.*, vol. 2. 2013, pp. 331–338.
[144] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[145] *The USC-SIPI Image Database*, accessed on 2016. [Online]. Available: http://sipi.usc.edu/database/
[146] *Kodak Lossless True Color Image Suite*, accessed on 2016. [Online]. Available: http://www.r0k.us/graphics/kodak/
[147] K. Gu, G. Zhai, X. Yang, W. Zhang, and M. Liu, "Subjective and objective quality assessment for images with contrast change," in *Proc. IEEE Int. Conf. Inf. Process.*, Sep. 2013, pp. 383–387.
[148] S. Wang, K. Ma, H. Yeganeh, Z. Wang, and W. Lin, "A patch-structure representation method for quality assessment of contrast changed images," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2387–2390, Dec. 2015.
[149] A. K. Moorthy and A. C. Bovik, "Blind image quality assessment: From natural scene statistics to perceptual quality," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3350–3364, Dec. 2011.
[150] M. A. Saad, A. C. Bovik, and C. Charrier, "Blind image quality assessment: A natural scene statistics approach in the DCT domain," *IEEE Trans. Image Process.*, vol. 21, no. 8, pp. 3339–3352, Aug. 2012.
[151] A. Mittal, A. K. Moorthy, and A. C. Bovik, "No-reference image quality assessment in the spatial domain," *IEEE Trans. Image Process.*, vol. 21, no. 12, pp. 4695–4708, Dec. 2012.
[152] Y. Zhang, A. K. Moorthy, D. M. Chandler, and A. C. Bovik, "C-DIIVINE: No-reference image quality assessment based on local magnitude and phase statistics of natural scenes," *Signal Process., Image Commun.*, vol. 29, no. 7, pp. 725–747, Aug. 2014.
[153] L. Liu, B. Liu, H. Huang, and A. C. Bovik, "No-reference image quality assessment based on spatial and spectral entropies," *Signal Process., Image Commun.*, vol. 29, no. 8, pp. 856–863, 2014.
[154] Y. Fang, K. Ma, Z. Wang, W. Lin, Z. Fang, and G. Zhai, "No-reference quality assessment of contrast-distorted images based on natural scene statistics," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 838–842, Jul. 2015.
[155] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.
[156] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. De Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Process., Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.
[157] R. Schmitz, S. Li, C. Grecos, and X. Zhang, "A new approach to commutative watermarking-encryption," in *Proc. 13th Joint IFIP TC6/TC11 Conf. Commun. Multimedia Secur.*, 2012, pp. 117–130.
[158] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.
[159] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Process.*, vol. 94, no. 1, pp. 118–127, Jan. 2014.
[160] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Trans. Cybern.*, vol. 46, no. 5, pp. 1132–1143, May 2016.
[161] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," *Signal Process., Image Commun.*, vol. 39, pp. 226–233, Nov. 2015.
[162] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
[163] Z. Qian, X. Zhang, and S. Wang, "Reversible data hiding in encrypted JPEG bitstream," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1486–1491, Aug. 2014.
[164] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.
[165] J. Yu, G. Zhu, X. Li, and J. Yang, "An improved algorithm for reversible data hiding in encrypted image," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2012, pp. 384–394.
[166] W. Hong, T.-S. Chen, J. Chen, Y.-H. Kao, H.-Y. Wu, and M.-C. Wu, "Reversible data embedment for encrypted cartoon images using unbalanced bit flipping," in *Proc. 4th Int. Conf. Swarm Intell.*, 2013, pp. 208–214.
[167] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *J. Vis. Commun. Image Represent.*, vol. 28, pp. 21–27, Apr. 2015.
[168] C. Qin and X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 154–164, Aug. 2015.
[169] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 3, pp. 441–452, Mar. 2016.
[170] Y.-C. Chen, C.-W. Shiu, and G. Horng, "Encrypted signal-based reversible data hiding with public key cryptosystem," *J. Vis. Commun. Image Represent.*, vol. 25, no. 5, pp. 1164–1170, 2014.
[171] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[172] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE*, vol. 6819, pp. 68191E-1–68191E-9, Feb. 2008.
[173] Z. Qian, X. Han, and X. Zhang, "Separable reversible data hiding in encrypted images by n-nary histogram modification," in *Proc. Int. Conf. Multimedia Technol.*, 2013, pp. 869–876.
[174] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *Sci. World J.*, vol. 2014, Apr. 2014, Art. no. 604876.
[175] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 322–328, Feb. 2014.
[176] M. S. A. Karim and K. Wong, "Universal data embedding in encrypted domain," *Signal Process.*, vol. 94, pp. 174–182, Jan. 2014.
[177] Z. Qian, X. Zhang, Y. Ren, and G. Feng, "Block cipher based separable reversible data hiding in encrypted images," *Multimedia Tools Appl.*, 2016.
[178] S. Zheng, D. Li, D. Hu, D. Ye, L. Wang, and J. Wang, "Lossless data hiding algorithm for encrypted images with high capacity," *Multimedia Tools Appl.*, 2016.
[179] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.
[180] X. Zhang, Z. Wang, J. Yu, and Z. Qian, "Reversible visible watermark embedded in encrypted domain," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, Jul. 2015, pp. 826–830.
[181] X. Zhang, C. Qin, and G. Sun, "Reversible data hiding in encrypted images using pseudorandom sequence modulation," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2012, pp. 358–367.
[182] X. Zhang, "Commutative reversible data hiding and encryption," *Secur. Commun. Netw.*, vol. 6, no. 11, pp. 1396–1403, 2013.

[183] Z. Yin, H. Wang, H. Zhao, B. Luo, and X. Zhang, "Complete separable reversible data hiding in encrypted image," in *Proc. 1st Int. Conf. Cloud Comput. Secur.*, 2015, pp. 101–110.

[184] M. Li, D. Xiao, Y. Zhang, and H. Nan, "Reversible data hiding in encrypted images using cross division and additive homomorphism," *Image Commun.*, vol. 39, pp. 234–248, Nov. 2015.

[185] B. Ou, X. Li, and W. Zhang, "PVO-based reversible data hiding for encrypted images," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, Jul. 2015, pp. 831–835.

[186] D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Process.*, vol. 123, pp. 9–21, Jun. 2016.

[187] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public key cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, to be published.

[188] G. Song, Z. Li, J. Zhao, J. Hu, and H. Tu, "A reversible video steganography algorithm for MVC based on motion vector," *Multimedia Tools Appl.*, vol. 74, no. 11, pp. 3759–3782, 2015.

[189] J. Zhao, Z.-T. Li, and B. Feng, "A novel two-dimensional histogram modification for reversible data embedding into stereo H.264 video," *Multimedia Tools Appl.*, vol. 75, no. 10, pp. 5959–5980, 2016.

[190] C. Vural and B. Barakli, "Reversible video watermarking using motion-compensated frame interpolation error expansion," *Signal, Image Video Process.*, vol. 9, no. 7, pp. 1613–1623, 2015.

[191] D. Xu, R. Wang, and Y. Q. Shi, "An improved reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 410–422, 2014.

[192] D. Xu, R. Wang, and Y.-Q. Shi, "Reversible data hiding in encrypted H.264/AVC video streams," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2013, pp. 141–152.

[193] D. Xu and R. Wang, "Efficient reversible data hiding in encrypted H.264/AVC videos," *J. Electron. Imag.*, vol. 23, no. 5, p. 053022, 2014.

[194] D. Yan and R. Wang, "Reversible data hiding for audio based on prediction error expansion," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2008, pp. 249–252.

[195] A. Nishimura, "Reversible audio data hiding using linear prediction and error expansion," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2011, pp. 318–321.

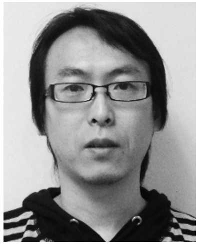
[196] A. Nishimura, "Reversible audio data hiding based on variable error-expansion of linear prediction for segmental audio and G.711 speech," *IEICE Trans. Inf. Syst.*, vol. 99-D, no. 1, pp. 83–91, 2016.

[197] F. Wang, Z. Xie, and Z. Chen, "High capacity reversible watermarking for audio by histogram shifting and predicted error expansion," *Sci. World J.*, vol. 2014, Apr. 2014, Art. no. 656251.

[198] A. Nishimura, "Reversible and robust audio watermarking based on quantization index modulation and amplitude expansion," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2013, pp. 275–287.

[199] A. Nishimura, "Reversible and robust audio watermarking based on spread spectrum and amplitude expansion," in *Proc. Int. Workshop Digit.-Forensics Watermarking*, 2014, pp. 215–229.

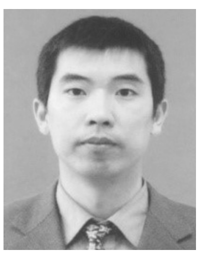
YUN-QING SHI (F'05) received the M.S. degree from Shanghai Jiao Tong University, China, and the Ph.D. degree from the University of Pittsburgh, USA. He has been with the New Jersey Institute of Technology, USA, since 1987. He has authored/co-authored more than 300 papers, one book, five book chapters, and an Editor of ten books, three special issues, and 13 proceedings, and holds 30 U.S. patents. His research interests include data hiding, forensics and information assurance, visual signal processing, and communications. He has served as an Associate Editor of the IEEE Transactions on Signal Processing and the IEEE Transactions on Circuits and Systems (II). He serves as an Associate Editor of the IEEE Transactions on Information Forensics and Security, and an Editorial Board Member of a few journals. He was the Technical Program Chair of the IEEE ICME07 and the IEEE MMSP05, a Co-General Chair of the IEEE MMSP02, and a Distinguished Lecturer of the IEEE CASS, and has been a Co-Technical Chair of IWDW since 2006. He is a member of a few IEEE technical committees.



XIAOLONG LI received the B.S. degree from Peking University, Beijing, China, in 1999, the M.S. degree from Ecole Polytechnique, Palaiseau, France, in 2002, and the Ph.D. degree in mathematics from the ENS de Cachan, Cachan, France, in 2006. Before joining Peking University as a Researcher, he was a Post-Doctoral Fellow with Peking University from 2007 to 2009. His research interests are image processing and information hiding.

XINPENG ZHANG (M'11) received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been a Faculty Member with the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. He was with the State University of New York at Binghamton as a Visiting Scholar from 2010 to 2011, and Konstanz University as an Experienced Researcher by the Alexander von Humboldt Foundation from 2011 to 2012. His research interests include multimedia security, image processing, and digital forensics. He has published more than 200 papers in these areas. He is an Associate Editor for the IEEE Transactions on Information Forensics and Security.

HAO-TIAN WU (SM'15) received the Ph.D. degree from the Department of Computer Science, Hong Kong Baptist University, Hong Kong, in 2007. From 2008 to 2009, he was a Post-Doctoral Research Engineer at EURECOM, France. From 2009 to 2013, he was a Lecturer with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China. Since 2013, he has been a Visiting Scholar with the Computer Science and Engineering Department, New York University Polytechnic School of Engineering for one year. He is currently an Associate Professor with the School of Digital Media, Jiangnan University, Wuxi, China. His research interests include image and video processing, information hiding, cyber security, and signal processing in the encrypted domain. He is a member of ACM.



BIN MA received the M.S. and Ph.D. degrees from Shandong University, Jinan, China, in 2005 and 2008, respectively. From 2008 to 2013, he was an Associate Professor with the School of Information Science, Shandong University of Political Science and Law, Jinan, China. He visited the New Jersey Institute of Technology at Newark, NJ, USA, as a Visiting Scholar from 2013 to 2015. He is currently an Associate Professor with the School of Information Science, Qilu University of Technology, Shandong, China. His research interests include reversible data hiding, multimedia security, and image processing. He is a member of ACM.