Hindawi
Security and Communication Networks
Volume 2018, Article ID 1326235, 9 pages
https://doi.org/10.1155/2018/1326235

Research Article

Improved Encrypted-Signals-Based Reversible Data Hiding Using Code Division Multiplexing and Value Expansion

Xianyi Chen, Haidong Zhong, Lizhi Xiong, and Zhihua Xia

Jiangsu Engineering Center of Network Monitoring, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

Correspondence should be addressed to Zhihua Xia; xia_zhihua@163.com

Received 28 September 2017; Revised 1 December 2017; Accepted 21 January 2018; Published 15 February 2018

Academic Editor: Rémi Cogranne

Compared to the encrypted-image-based reversible data hiding (EIRDH) method, the encrypted-signals-based reversible data hiding (ESRDH) technique is a novel way to achieve a greater embedding rate and better quality of the decrypted signals. Motivated by ESRDH using signal energy transfer, we propose an improved ESRDH method using code division multiplexing and value expansion. At the beginning, each pixel of the original image is divided into several parts containing a little signal and multiple equal signals. Next, all signals are encrypted by Paillier encryption. And then a large number of secret bits are embedded into the encrypted signals using code division multiplexing and value expansion. Since the sum of elements in any spreading sequence is equal to 0, lossless quality of directly decrypted signals can be achieved using code division multiplexing on the encrypted equal signals. Although the visual quality is reduced, high-capacity data hiding can be accomplished by conducting value expansion on the encrypted little signal. The experimental results show that our method is better than other methods in terms of the embedding rate and average PSNR.

1. Introduction

Encryption and data hiding are two common approaches for protecting against information leakage [1–3]; the former is used to protect the content itself [4], whereas the latter is used to protect the hidden data [5]. While it is a problem for sensitive applications, such as military images and medical images, reversible data hiding (RDH) is an effective method for these special scenarios, which aims to recover both embedded data and the original image. In the past two decades, many classic RDH algorithms have been proposed, such as lossless image compression-based methods [6], difference expansion- (DE-) based methods [7], histogram shifting- (HS-) based methods [8], integer-to-integer transform-based methods [9], and dual-image-based methods [10].

However, with the popularity of outsourced storage services [11, 12], the traditional RDH is not suitable in these scenarios, especially with regard to the requirement of high security. Therefore, the research of privacy protection in cloud computing has attracted considerable attention in recent years [13–15]. Among these studies, encrypted-image-based reversible data hiding (EIRDH) provides the possibility that the image owner can encrypt the image before uploading it to the service provider, and then the service provider can embed some additional message into the incomprehensible encrypted image for steganography or authentication. The authorized users or receivers can recover both the additional message and the original image. The existing EIRDH methods can be grouped into three categories: vacating room after encryption (VRAE) methods [16–22], reserving room before encryption (RRBE) methods [23–25], and reversible image transform (RIT) methods [26, 27].

The framework of “VRAE” was proposed by Zhang [18], in which secret bits can be embedded after encrypting the original image. Specifically, the data hider can divide the encrypted image block into two sets and embed secret bits by flipping three LSBs of a set. To decrease the extracted-bits error rate, Hong et al. [19] and Liao and Shu [20] evaluated the complexity of image blocks. Recently, Yi and Zhou [21] proposed a novel EIRDH method using binary-block embedding for joint decryption and extraction, in which a bit-level scrambling process can prevent secret bits from loss. The methods [18–21] can embed an additional message from the decrypted image. To extract secret bits in the encrypted image, Zhang [22] proposed a novel separable EIRDH method, in which three cases are considered according to the encryption key or data hiding key.

However, it is hard to use the traditional RDH method for the data hider in the VRAE since the correlation between neighbor pixels in the encrypted image is destroyed.

The framework of "RRBE" was designed by Ma et al. [23]. The data owner can reverse the room of LSBs using the traditional RDH method and then encrypt the self-embedded image. After that, the data hider embeds secret data into the reversed LSBs of the encrypted image. Cao et al. [24] compressed pixels in the local patch by sparse representation and achieved a higher reversed room than other previous methods.

To transform the original image into an encrypted image which looks like the target image, Zhang et al. [26] proposed the EIRDH framework based on RIT, in which an image block is paired by similar means and standard deviation between the original and target images. Since the correlation of transformed images is not destroyed, the data hider can embed secret bits by the traditional RDH method. However, this method has high image distortion since much auxiliary information must be self-embedded into the transformed image for recovering the original image. Recently, Hou et al. [27] improved the visual quality of camouflage images and reduced the auxiliary information for recording block indexes by adopting k-means clustering.

Different from the EIRDH, Chen et al. [28] designed an encrypted-signals-based reversible data hiding (ESRDH) method, in which the data owner divides each pixel of the cover image into two signals and then encrypts them by a public key. After that, the data hider embeds secret bits into the encrypted signals by the additive homomorphism. To reduce data expansion, Shiu et al. [29] adopted a difference expansion method to embed the message. Zhang et al. [30] proposed a lossless, a reversible, and a combined data hiding scheme for ciphertext images, respectively, which were encrypted by a public key cryptosystem with homomorphic properties. Recently, Wu et al. [31] presented an improved ESRDH method, in which the original image can be recovered completely by decrypting all signals. The method can achieve a higher embedding capacity and better quality of decrypted images than previous ESRDH methods. In addition, compared to the traditional EIRDH method, the cost spent, on a reliable key management system in a multiparty environment, is reduced since the receiver can share the public key with other identities.

In this paper, we propose an improved ESRDH method using code division multiplexing (CDM) and value expansion (VE), in which the traditional CDM technology is utilized to achieve lossless visual quality of decrypted signals, and VE technology is designed according to the RDH method based on DE for further increasing the embedding capacity. Compared to the current ESRDH method, the proposed method achieves a high embedding capacity and good visual quality.

The rest of this paper is arranged as follows. In Section 2, the related works are described. In particular, communication technology based on CDM, RDH method based on DE, and ESRDH method based on signal energy transfer are given. Section 3 presents a lossless visual quality ESRDH method using code division multiplexing and high embedding capacity ESRDH method using value expansion. Section 4 displays the performance of the proposed method by experimental results and Section 5 concludes this paper.

2. Related Works

2.1. Communication Technology Based on CDM. In communication systems, CDM is a kind of spectrum spreading technology for ensuring secure information transmission and channel multiplexing, in which the sender encodes to-be-transmitted bits with a predetermined spreading sequence, and then the receiver can obtain the secret bits by the same spreading sequences. So, the sequences that are derived by Walsh Hadamard matrix play an important role in CDM-based communication technology. Walsh Hadamard matrix consists of 1 and −1. In addition to the first row (column) of the matrix, other row (column) vectors are selected as the spreading sequences, and they have two properties. First, the sum of elements is equal to 0 for any sequence. Second, they are orthogonal to each other of any two different sequences, so the cross-correlation is 0.

Suppose the spreading sequences generated by Walsh Hadamard matrix are S_z, $z = \{1, \ldots, q\}$ and the compound sequence C is the linear combination of S_z; when the secret bit is 0, the coefficient of S_z is set as −1. Otherwise, the coefficient is set as 1. Thus, the receiver can decode the secret bits according to the results of dot product between S_z and C.

For example, three spreading sequences from a 4-level Hadamard matrix are$S_1 = (1, -1, 1, -1)$, $S_2 = (1, 1, -1, -1)$, and $S_3 = (1, -1, -1, 1)$. Obviously, S_1, S_2, and S_3 are zero means and orthogonal to each other. Suppose the secret bits are "010"; then, the sequences are denoted as S_1, $-S_2$, and S_3, respectively, and the three sequences are added to form the compound sequence $C = S_1 - S_2 + S_3 = (1, -3, 1, 1)$.

On the receiver side, for the receiver with the spreading sequence S_1, the decoding result is $(C \cdot S_1)/|S_1|^2 = ((S_1 - S_2 + S_3) \cdot S_1)/|S_1|^2 = (S_1 \cdot S_1)/|S_1|^2 = 1$, which represents the notion that the secret bit is 1; for the receiver with S_2, the result is $(C \cdot S_2)/|S_2|^2 = (-S_2 \cdot S_2)/|S_2|^2 = -1$, which represents bit 0; for the receiver with S_3, the result is $(C \cdot S_3)/|S_3|^2 = (S_3 \cdot S_3)/|S_3|^2 = 1$, which represents bit 1. Therefore, the secret bits can be extracted. Moreover, since a large number of secret bits are represented and transmitted by the compound sequences in different ways and it is impossible for an intruder to guess them, the CDM-based communication technology is secure and can provide high capacity.

2.2. RDH Method Based on DE. The RDH method based on DE was proposed by Tian. Assume the two neighbor pixels of

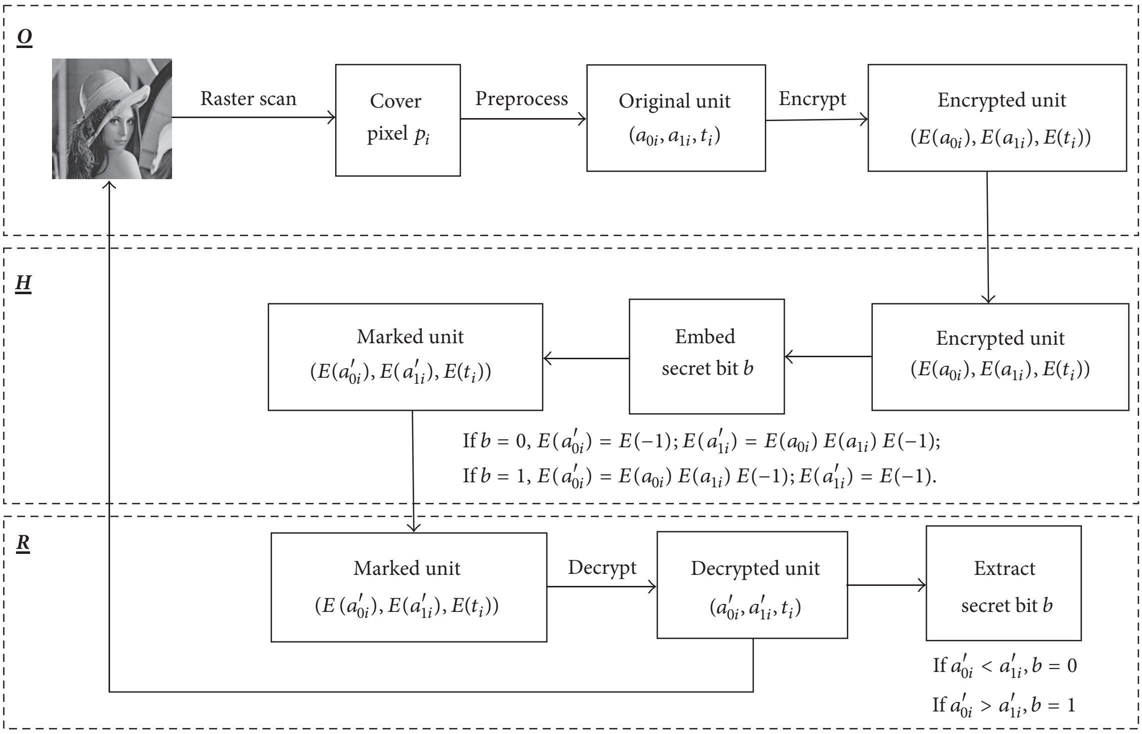

O
Raster scan
Cover pixel p_i
Preprocess
Original unit (a_{0i}, a_{1i}, t_i)
Encrypt
Encrypted unit $(E(a_{0i}), E(a_{1i}), E(t_i))$
H
Marked unit $(E(a'_{0i}), E(a'_{1i}), E(t_i))$
Embed secret bit b
Encrypted unit $(E(a_{0i}), E(a_{1i}), E(t_i))$
If $b = 0$, $E(a'_{0i}) = E(-1); E(a'_{1i}) = E(a_{0i})\, E(a_{1i})\, E(-1)$;
If $b = 1$, $E(a'_{0i}) = E(a_{0i})\, E(a_{1i})\, E(-1); E(a'_{1i}) = E(-1)$.
R
Marked unit $(E(a'_{0i}), E(a'_{1i}), E(t_i))$
Decrypt
Decrypted unit (a'_{0i}, a'_{1i}, t_i)
Extract secret bit b
If $a'_{0i} < a'_{1i}, b = 0$
If $a'_{0i} > a'_{1i}, b = 1$

Figure 1: The framework of ESRDH method based on signal energy transfer.

the image are x and y. The sender can compute the average m and the difference h between x and y:

$$m = \left\lfloor \frac{x+y}{2} \right\rfloor, \qquad h = x - y. \tag{1}$$

Then, the secret bit b can be embedded as the least significant bit (lsb) of h. And the new difference value h' can be obtained:

$$h' = 2h + b. \tag{2}$$

Finally, the corresponding values x' and y' can be computed and transmitted by the sender:

$$x' = m + \left\lfloor \frac{h'+1}{2} \right\rfloor, \qquad y' = m - \left\lfloor \frac{h'}{2} \right\rfloor. \tag{3}$$

From the pixels pair (x', y'), the receiver can extract secret bits and recover the original image. The initial average value m and new difference value h' can be computed:

$$m = \left\lfloor \frac{x'+y'}{2} \right\rfloor, \qquad h' = x' - y'. \tag{4}$$

The secret bit b and difference value h can be obtained by h':

$$b = \mathrm{LSB}\left(h'\right), \qquad h = \left\lfloor \frac{h'}{2} \right\rfloor. \tag{5}$$

And the original pair (x, y) can be recovered by m and h:

$$x = m + \left\lfloor \frac{h+1}{2} \right\rfloor, \qquad y = m - \left\lfloor \frac{h}{2} \right\rfloor. \tag{6}$$

DE is a simple and efficient RDH method that utilizes the redundancy between two neighbor pixels to embed secret bits and achieve reversibility. In addition, we can use the data-embedding algorithm for an image more than once for multiple-layer embedding. When the difference is small, a higher embedding capacity and better visual quality of the cover image can be achieved. However, the transformed values x' and y' should be restricted in the range of $[0, 255]$.

2.3. ESRDH Method Based on Signal Energy Transfer. ESRDH method based on signal energy transfer was proposed by Wu et al. It consists of three phases: image encryption phase, data-embedding phase, and data extraction and image recovery phase. There are three active identities in this method. They are image owner O, data hider H, and receiver R. The framework of this method is described in Figure 1.

Suppose the size of the cover image is $N_1 \times N_2$ and the pixel is $p_i \in [0, 255]$, $1 \le i \le N_1 \times N_2$. Inspired by the signal energy transfer, one signal can be represented by the sum of other signals. Therefore, p_i can be represented as $a_{0i} + a_{1i} + t_i$, where a_{0i} is selected randomly from $\{0, 1, 2, \dots, x_i\}$, x_i is obtained by $x_i = 2\lfloor p_i/2 \rfloor$, a_{1i} is equal to a_{0i}, and t_i is set to be $t_i = p_i - 2a_{0i}$. And then, the image owner can encrypt the three signals according to the public key that was generated by the Paillier encryption algorithm.

Let the encrypted pixels be represented by $(E(a_{0i}), E(a_{1i}), E(t_i))$. The data hider embeds the secret bit b into $E(a_{0i})$ and $E(a_{1i})$ and generates the marked signals $E(a'_{0i})$ and $E(a'_{1i})$. If the secret bit is 0, then $E(a'_{0i}) = E(a_{0i} - a_{1i} - 1)$, $E(a'_{1i}) = E(a_{0i} + a_{1i} + 1)$. If the bit is 1, then $E(a'_{0i}) = E(a_{0i} + a_{1i} + 1)$, $E(a'_{1i}) = E(a_{0i} - a_{1i} - 1)$. Since $a_{0i} = a_{1i}$ and Paillier encryption maintains the additive homomorphic properties, then the embedded formulas can be reduced to

$$E\left(a'_{0i}\right) = \begin{cases} E(-1), & \text{if } b = 0, \\ E\left(a_{0i}\right) E\left(a_{1i}\right) E(1), & \text{if } b = 1, \end{cases}$$
$$E\left(a'_{1i}\right) = \begin{cases} E\left(a_{0i}\right) E\left(a_{1i}\right) E(1), & \text{if } b = 0, \\ E(-1), & \text{if } b = 1. \end{cases} \tag{7}$$

To extract the secret bit and recover the cover image, the receiver can decrypt the marked signals $(E(a'_{0i}), E(a'_{1i}), E(t_i))$ according to the private key generated by Paillier encryption and obtain the decrypted unit (a'_{0i}, a'_{1i}, t_i). Then, the decrypted pixel is denoted by $p_i = a'_{0i} + a'_{1i} + t_i$. Because of $a'_{0i} + a'_{1i} = a_{0i} + a_{1i}$, the decrypted image is a cover image. After that, the bit b can be extracted by comparing a'_{0i} and a'_{1i}:

$$b = \begin{cases} 0, & \text{if } a'_{0i} < a'_{1i}, \\ 1, & \text{if } a'_{0i} > a'_{1i}. \end{cases} \tag{8}$$

This method achieves a lossless visual quality since the decrypted image is the original one. It also can process encoded multimedia since each separated unit of the encoded multimedia can be recovered completely. Therefore, there is no underflow or overflow problem and there is no need to embed any auxiliary information.

3. The Proposed Method

3.1. Lossless Quality ESRDH Method Based on CDM. To maintain the lossless quality of the decrypted image and improve the embedding capacity, inspired by communication technology based on CDM, we propose a lossless visual quality ESRDH method only using CDM.

Suppose that the generated spreading sequences are $S_z, z = \{1, \dots, q\}$ and the length is denoted as $l = q + 1$, where l must be the power of 2 such as $2, 4, 8$. Therefore, the preprocess and encryption can be summarized as follows. Firstly, divide each pixel unit p_i as $p_i = a_{1i} + \cdots + a_{li} + t_i$, where t_i is obtained by $t_i = p_i \bmod l$ and $a_{1i}, \dots, a_{li}$ are set to be $(p_i - t_i)/l$. Secondly, define the vector $V_i = [a_{1i}, \dots, a_{li}]$ as an embedded vector, so each unit p_i can be represented as (V_i, t_i). Finally, the image owner encrypts each unit by a public key generated by Paillier encryption, and the encrypted unit $(E(V_i), E(t_i))$ is generated, where $E(V_i) = [E(a_{1i}), \dots, E(a_{li})]$.

Now, the data hider can embed secret bits b_{iz} $(z = \{1, \dots, q\})$ into $E(V_i)$ using CDM. This means the number of bits which can be embedded into the ith $(1 \le i \le N_1 \times N_2)$ pixel is q. At the beginning, the secret bits b_{iz} can be transformed to w_{iz} which consist of –1 and 1:

$$w_{iz} = \begin{cases} -1, & \text{if } b_{iz} = 0 \\ 1, & \text{if } b_{iz} = 1. \end{cases} \tag{9}$$

Then, we can obtain the compound sequence C_i by $C_i = w_{i1}S_1 + \cdots + w_{iq}S_q$; the elements of C_i are $[C_i(1), \dots, C_i(l)]$. They can be encrypted by the public key and can generate an encrypted compound sequence $EC_i = [E(C_i(1)), \dots, E(C_i(l))]$. Since Paillier encryption has additive homomorphic properties, EC_i can be embedded into $E(V_i)$ by the following formula:

$$\begin{aligned} E\left(V'_i\right) &= \left(E\left(a'_{1i}\right), \dots, E\left(a'_{li}\right)\right) \\ &= \left(E\left(a_{1i} + C_i(1)\right), \dots, E\left(a_{li} + C_i(l)\right)\right) \\ &= \left(E\left(a_{1i}\right) \times E\left(C_i(1)\right), \dots, E\left(a_{li}\right) \times E\left(C_i(l)\right)\right), \end{aligned} \tag{10}$$

where the new vector $E(V'_i)$ can be denoted as $E(V'_i) = [E(a'_{1i}), \dots, E(a'_{li})]$.

Finally, the receiver can decrypt the marked signals $(E(V'_i), E(t_i))$ by a private key and obtain (V'_i, t_i). V'_i can be represented by $V'_i = [a'_{1i}, \dots, a'_{li}]$ or $V'_i = V_i + C_i$. Because of $a_{1i} = \cdots = a_{li}$ and for any different spreading sequences, they are zero means and orthogonal to each other; the result of dot product between V'_i and S_z $(z = \{1, \dots, l\})$ can be summarized as

$$V'_i \cdot S_z = C_i \cdot S_z = l^2 \times w_{iz}. \tag{11}$$

Therefore, w_{iz} can be obtained by the following formula:

$$w_{iz} = \frac{V'_i \cdot S_z}{l^2} = \operatorname{sign}\left(V'_i \cdot S_z\right). \tag{12}$$

And b_{iz} can inversely be transformed by formula (9). Since the sum of elements is equal to 0 for any spreading sequences, we have

$$a'_{1i} + \cdots + a'_{li} = a_{1i} + \cdots + a_{li}. \tag{13}$$

The directly decrypted pixel is p'_i, and we have $p'_i = a'_{1i} + \cdots + a'_{li} + t_i = p_i$. As a result, the decrypted pixel is the original one. In other words, based on CDM, ESRDH achieves lossless visual quality of images. And the data-embedding process does not cause an underflow/overflow problem. In addition, the embedding rate can be improved to be q bits per pixel (bpp) such as $q = \{1, 3\}$. So, it can be determined by the number of spreading sequences q.

3.2. High Embedding Capacity ESRDH Method Based on VE. In Wu et al.'s method and ESRDH method based on CDM, the signal t_i is not used to embed secret bits. To further increase the embedding capacity, the ESRDH method based on VE is proposed. In Wu et al.'s method, the range of t_i is $[p_i - 4\lfloor p_i/2 \rfloor, p_i]$, which will decrease the visual quality of the decrypted image because the absolute value of t_i is too large. However, in the ESRDH method based on CDM, the range of t_i is $[1, q]$, and it is enough small, so the ESRDH based on VE is an efficient method.

In Section 3.1, the pixel unit (V_i, t_i) is encrypted and sent to the data hider. Instead of only embedding secret bits into V_i, t_i also can embed bits in this section. Suppose t_i is expanded 2^k $(k = 1, 2)$ times and the decimal number of $(b_{i1} \cdots b_{ik})_2$ is D_i. So, k LSBs of t_i can be emptied to embedded secret bits by $t_i' = 2^k \times t_i + D_i$. Then, p_i' can be constructed by the sum of $a_{1i}', \ldots, a_{li}', t_i'$, and it can be reduced to $p_i + t_i' - t_i$. Since $p_i \in [0, 255]$ and $t_i' - t_i \in [0, R\max]$, thus $p_i' \in [0, 255 + R\max]$, where $R\max = (2^k - 1) \times (q + 1)$. Therefore, data embedding can possibly cause an overflow problem. To solve this problem, t_i should be preprocessed, and the formula can be summarized as

$$ts_i = \begin{cases} t_i, & 0 \le p_i \le 255 - R\max, \\ t_i - R\max, & 255 - R\max < p_i \le 255. \end{cases} \tag{14}$$

The range of t_i is changed from $[0, q]$ to $ts_i \in [-R\max, q - R\max] \cup [0, q]$. So, if $ts_i < 0$, ts_i is the changeable one. Otherwise, it is the original one.

Firstly, the encrypted unit $(E(V_i), E(ts_i))$ can be obtained by a public key.

Secondly, D_i should be encrypted to $E(D_i)$ by the same key. And then it is embedded into $E(ts_i)$, so a new encrypted value $E(ts_i')$ can be generated, which can be summarized as

$$E\left(ts_i'\right) = E\left(2^k \times ts_i + D_i\right) = E\left(ts_i\right)^{2^k} \times E\left(D_i\right). \tag{15}$$

Thirdly, the receiver decrypts $E(ts_i')$ by the corresponding private key and denotes it as ts_i'. After that, the embedded bits $(b_{i1} \cdots b_{ik})_2$ can be obtained by extracting k LSBs of ts_i'. So, ts_i can be calculated by

$$ts_i = \frac{ts_i' - D_i}{2^k}, \tag{16}$$

where D_i is the decimal number of $(b_{i1} \cdots b_{ik})_2$.

Finally, the original t_i should be recovered by

$$t_i = \begin{cases} ts_i, & ts_i \ge 0, \\ ts_i + R\max, & ts_i < 0. \end{cases} \tag{17}$$

And the pixel p_i can be recovered by the sum of other signals.

Based on ESRDH using CDM, the proposed method can further improve the embedding rate using VE. The embedded rate can be increased by k bpp such as $k = \{1, 2\}$. Furthermore, there is no need to embed any auxiliary information to recover the original t_i. However, there is a possibility that an overflow problem arises, which may cause image distortion.

3.3. Algorithm of ESRDH Method Based on CDM and VE. According to Sections 3.1 and 3.2, the framework of ESRDH method based on CDM and VE is shown in Figure 2, and the algorithm can be divided into three phases: preprocess and signal encryption phase, data-embedding phase, and data extraction and image recovery phase. The details are described as in Algorithm 1.

4. Experimental Results

As is shown in Figures 3(a)–3(d), four different grayscale images with different features are selected as the test images, which are Lena, Pepper, Sailboat, and Baboon. The size of these pictures is 512 × 512. The development tool is Myeclipse8.6, which is used on an Intel Core i5 CPU (2.8 GHz) with 8 GB of memory.

The embedding rate (ER) and visual quality of the decrypted image are two important indicators to measure the performance of the EIRDH method, and they can be calculated by

$$\begin{aligned} \mathrm{ER} &= \frac{\text{Embedding Capacity}}{\text{The size of cover image}}, \\ \mathrm{PSNR} &= 10 \lg \frac{255^2 \times N_1 \times N_2}{\sum_{i=1}^{N_1 \times N_2} \left(p_i' - p_i\right)^2}, \end{aligned} \tag{18}$$

where p_i and p_i' are the original and modified pixel values, respectively.

In the proposed method, if the ESRDH method based on CDM is used to embed secret bits, the ER is q bpp, and PSNR is $+\infty$. In Table 1, when $q = 1$ and $q = 3$, the embedding capacity (EC) is $512 \times 512 = 262144$ and $3 \times 512 \times 512 = 786432$, and the corresponding ER is 1 bpp and 3 bpp, respectively. And lossless visual quality of the decrypted image can be achieved. The decrypted images with the hidden data were not further processed, as shown in Figure 4. The plain text images recovered from the four encrypted images were all identical to the original one. In addition, we can utilize the VE method to further improve ER, and up to $q + k$ bpp can be achieved. In addition, PSNR will be changed by setting k. For example, 786432 bits can be embedded using CDM and VE methods when $q = 1$, $k = 2$. However, PSNR of Lena is decreased to 36.85 dB. The other results about EC, ER, and PSNR of different test images are shown in Table 1. Furthermore, although the ER of the four images is 3 bpp when $q = 1$, $k = 2$, or $q = 3$, the PSNR of these decrypted images are different.

To assess the time overheads on encryption, embedding, and decryption, we assessed the statistic efficiency performance of the proposed method for different test images when $q = 3$ and $k = 1$ in Table 2. In this table, the embedding time is small because secret bits are embedded by multiplication, which also reflects the notion that signals encryption and decryption spend a long time. However, since the operations of CDM and VE were all performed in a homomorphic encryption domain, the encrypted signals with the hidden data were protected by the Paillier cryptosystem. Therefore, the Paillier cryptosystem in our method is an important

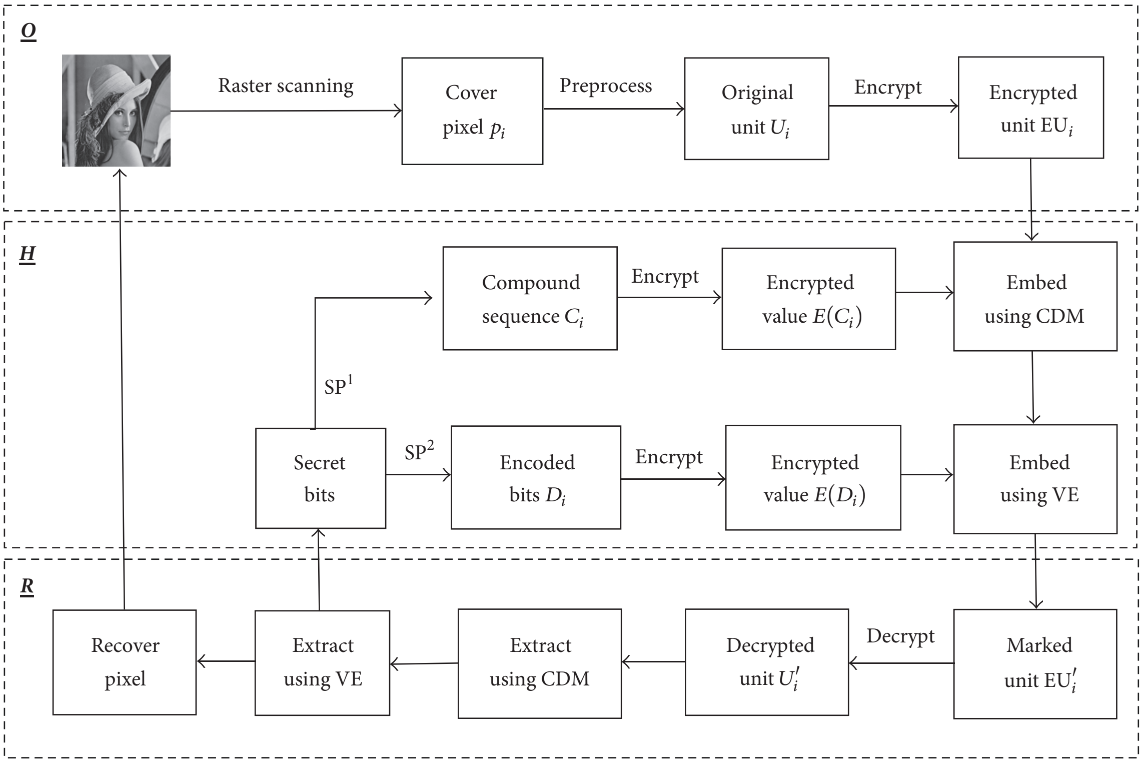


FIGURE 2: The framework of the ESRDH method based on CDM and VE.

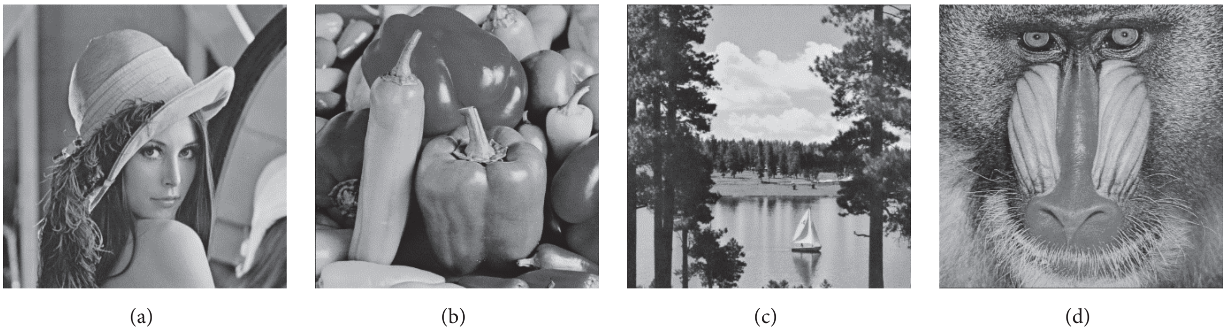


FIGURE 3: Four test images. (a) Lena, (b) Pepper, (c) Sailboat, and (d) Baboon.

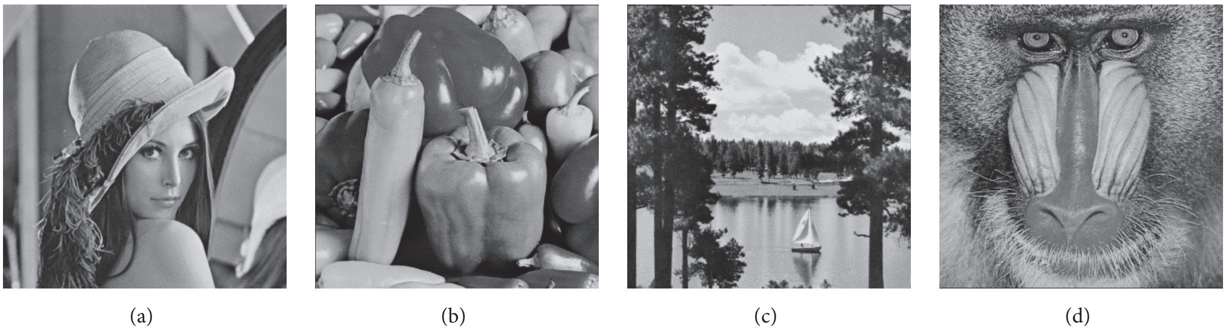


FIGURE 4: Directly decrypted images. (a) Lena, (b) Pepper, (c) Sailboat, and (d) Baboon.

```
Preprocess and signal encryption phase
Input:   An original image with a size of $N_1 \times N_2$, the number of spreading sequences $q$ ($q = \{1, 3\}$), the expanded
         parameter $k$ ($k = \{1, 2\}$), and public key $pk$.
Output:  The encrypted unit $\mathrm{EU}_i$.
Step 1:  Obtain the separated signals from the original pixel $p_i = a_{1i} + \cdots + a_{li} + t_i$, $1 \le i \le N_1 \times N_2$, which can be
         calculated in Section 3.1. Define the embedded vector $V_i = [a_{1i}, \ldots, a_{li}]$, and each pixel unit is represented
         as $(V_i, t_i)$.
Step 2:  Modify $t_i$ to be $ts_i$ by formula (14) for preventing overflow.
Step 3:  Encrypt $U_i = (V_i, ts_i)$ by $pk$ and generate an encrypted unit $\mathrm{EU}_i = (E(V_i), E(ts_i))$.
Data embedding phase
Input:   The encrypted unit $\mathrm{EU}_i$, the number of spreading sequences $q$, the expanded parameter $k$, public key $pk$, and
         secret bits.
Output:  Marked unit $\mathrm{EU}_i'$.
Step 1:  Divide secret bits into two parts $\mathrm{SP}^1$ and $\mathrm{SP}^2$, where $\mathrm{SP}^1$ contains $q \times N_1 \times N_2$ secret bits and $\mathrm{SP}^2$ contains the
         remaining bits.
Step 2:  Transform secret bits $b_{iz}$, $z = \{1, \ldots, q\}$ in $\mathrm{SP}^1$ to $w_{iz}$ using formula (9), and then obtain
         the compound sequence $C_i$ for each unit $\mathrm{EU}_i$.
Step 3:  Encrypt $C_i$ by $pk$ and denote it as $E(C_i)$.
Step 4:  Embed $E(C_i)$ into $E(V_i)$ using CDM. By formula (10), obtain a new vector $E(V_i')$.
Step 5:  Encode secret bits $(b_{i1} \cdots b_{ik})_2$ in $\mathrm{SP}^2$ to $D_i$. $D_i$ is the decimal of $(b_{i1} \cdots b_{ik})_2$ for each unit $\mathrm{EU}_i$.
Step 6:  Encrypt $D_i$ by $pk$ and denote it as $E(D_i)$.
Step 7:  Embed $E(D_i)$ into $E(ts_i)$ using VE. By formula (15), obtain a new signal $E(ts_i')$. Then,
         generate a marked unit $\mathrm{EU}_i' = (E(V_i'), E(ts_i'))$.
Data extraction and image recovery phase
Input:   The marked unit $\mathrm{EU}_i'$, the number of spreading sequences $q$, the expanded parameter $k$, and private key $sk$.
Output:  Secret bits and the original image.
Step 1:  Decrypt $\mathrm{EU}_i'$ using $sk$ to generate $U_i' = (V_i', ts_i')$.
Step 2:  Extract $q \times N_1 \times N_2$ secret bits from $V_i'$ by formulas (9) and (12).
Step 3:  Obtain $(b_{i1} \cdots b_{ik})_2$ by extracting $k$ LSBs of $ts_i'$.
Step 4:  Calculate $ts_i$ by formula (16) and recover $t_i$ by formula (17).
Step 5:  Recover the original image by calculating $p_i = a_{1i}' + \cdots + a_{li}' + t_i$.
```

Algorithm 1

Table 1: The performance of EC, ER, and PSNR for different images.

Test image	q and k	EC (bits)	ER (bpp)	PSNR (dB)
Lena	$q = 1$	262144	1	$+\infty$
	$q = 1, k = 1$	524288	2	46.37
	$q = 1, k = 2$	786432	3	36.85
	$q = 3$	786432	3	$+\infty$
	$q = 3, k = 1$	1310720	4	29.52
Pepper	$q = 1$	262144	1	$+\infty$
	$q = 1, k = 1$	524288	2	43.39
	$q = 1, k = 2$	786432	3	36.42
	$q = 3$	786432	3	$+\infty$
	$q = 3, k = 1$	1310720	4	29.53
Sailboat	$q = 1$	262144	1	$+\infty$
	$q = 1, k = 1$	524288	2	46.37
	$q = 1, k = 2$	786432	3	36.87
	$q = 3$	786432	3	$+\infty$
	$q = 3, k = 1$	1310720	4	29.52
Baboon	$q = 1$	262144	1	$+\infty$
	$q = 1, k = 1$	524288	2	46.36
	$q = 1, k = 2$	786432	3	36.87
	$q = 3$	786432	3	$+\infty$
	$q = 3, k = 1$	1310720	4	29.52

Table 2: Efficiency performance of the proposed method.

Test images	Encryption (m)	Embedding (m)	Decryption (m)
Lena	94.76	1.79	181.70
Pepper	93.48	1.46	183.64
Sailboat	95.66	1.42	180.78
Baboon	94.74	1.51	185.29

Table 3: The signal expansion between our method and the selected methods.

Methods	Input signal (bits)	Output signal (bits)
Our method	8	$2 \times (q+2) \times 512$
Wu et al. [31]	8	6×512
Shiu et al. [29]	8	2×512
Chen et al. [28]	8	4×512

technology for protecting image content security although it is not efficient enough.

Table 3 denotes signal expansion between our method and the selected methods, including Wu et al. [31], Shiu et al. [29], and Chen et al. [28]. According to Paillier encryption, the size of the cipher space is square of the size of the message space. In the table, Paillier encryption with 512-level security is adopted, and the plain text and the ciphertext are represented by 512 bits and 1024 bits, respectively. The output signal of our method is related to q and can reach $2 \times (q + 2) \times 512$. To solve the problem of data expansion, three alternative methods can be considered. The first is to use a lower security level, such as a 128-bit security level and 64-bit security level. Thus, the length of output signal will be reduced to $2 \times (q + 2) \times 128$ bits and $2 \times (q + 2) \times 64$ bits, respectively. The second is to reduce the value of q. When $q = 1$, it is $6 \times 512 \times 512$ and the same as Wu et al.'s method. The third is to use a pixel block instead of a single pixel as the input signal. If a 512-bit security level is used, an 8×8 pixel block can be adopted since such a block consists of $8 \times 8 \times 8 = 512$ bits. Now, the length of the output signal is $2 \times (q + 2)$ times that of the input signal.

The average PSNR of different images when $q = 1$and $k = 2$ are shown in Figure 5. At the beginning, the secret bits can be embedded using CDM, and the embedding rate can reach 1 bpp. Since the decrypted image is the same as the original image, PSNR is $+\infty$. To further improve the embedding rate, the PSNR will be reduced and more secret bits will be embedded using VE. Compared with other related methods including Wu et al. [31], Shiu et al. [29], and Chen et al. [28], the proposed method has a better performance in terms of the embedding rate and PSNR.

Moreover, since the decrypted image is the original image, the proposed method, which only uses CDM, can be applied to deal with encoded media such as H.264 video and JPEG images. Besides, real reversibility can be achieved by the proposed method.

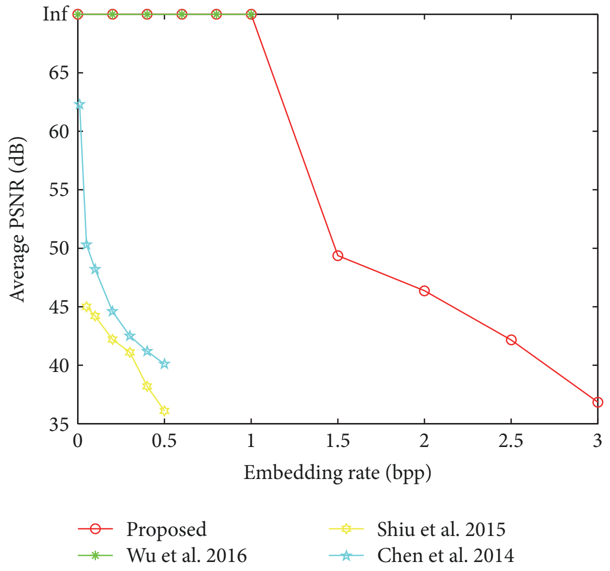


Figure 5: The average PSNR in different test images when $q = 1$ and $k = 2$.

5. Conclusion

This paper proposes improved encrypted signals-based reversible data hiding based on code division multiplexing and value expansion. When only using code division multiplexing to embed bits, lossless visual quality of directly decrypted images can be achieved, and the embedding rate can reach q ($q = \{1, 3\}$) bpp. When using code division multiplexing and value expansion method, the decrypted image will have some distortion, but the embedding rate can be improved to $q + k$ ($k = \{1, 2\}$) bpp. The secret bits and the original image can be recovered from the decrypted image completely. However, the size of the encrypted image will be expanded because of Paillier encryption. In further work, the expansion problem may be solved using other encryption ways, and the property of multiplicative homomorphism may be utilized to further improve the performance on the embedding rate and PSNR.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (NSFC) (61502242, U1536206, 61672294, 61702276, 61602253, 61373133, 61232016, 71501101, and U1405254), Jiangsu Basic Research Programs-Natural Science Foundation (BK20150925), Startup Foundation for Introducing Talent of Nanjing University of Information Science and Technology (2014r026#), Open Fund of Demonstration Base of Internet Application Innovative Open Platform of Department of Education (KJRP1402), Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) Fund, Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund, and National Ministry of Science and Technology Special Project Research (GYHY201301030, 2013DFG12860, and BC2013012).

References

[1] J. Shen, D. Liu, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive & Mobile Computing*, 2017.

[2] Z. Fu, F. Huang, X. Sun, A. V. Vasilakos, and C. Yang, "Enabling semantic search based on conceptual graphs over encrypted outsourced data," in *Proceedings of the IEEE Transactions on Services Computing*, vol. 99, 1939.

[3] C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Communications*, vol. 13, no. 7, pp. 60–65, 2016.

[4] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, 2016.

[5] X. Chen, S. Chen, and Y. Wu, "Coverless information hiding method based on the Chinese character encoding," *Journal of Internet Technology*, vol. 18, no. 2, pp. 313–320, 2017.

[6] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," *EURASIP Journal on Applied Signal Processing*, no. 2, pp. 185–196, 2002.

[7] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[8] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[9] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 321–330, 2007.

[10] H. Yao, C. Qin, Z. Tang, and Y. Tian, "Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion," *Signal Processing*, vol. 135, pp. 26–35, 2017.

[11] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 9, pp. 2546–2559, 2016.

[12] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594–2608, 2016.

[13] Y. Kong, M. Zhang, and D. Ye, "A belief propagation-based method for task allocation in open and dynamic cloud environments," *Knowledge-Based Systems*, vol. 115, pp. 123–132, 2017.

[14] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[15] Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-preserving Smart Semantic Search based on Conceptual Graphs over Encrypted Outsourced Data," *IEEE Transactions on Information Forensics Security*, no. 99, p. 1, 2017.

[16] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," *Journal of Visual Communication and Image Representation*, vol. 25, no. 2, pp. 322–328, 2014.

[17] L. Xiong, Z. Xu, and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images," *Multidimensional Systems and Signal Processing*, pp. 1–12, 2017.

[18] X. P. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[19] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[20] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *Journal of Visual Communication and Image Representation*, vol. 28, pp. 21–27, 2015.

[21] S. Yi and Y. Zhou, "Binary-block embedding for reversible data hiding in encrypted images," *Signal Processing*, vol. 133, pp. 40–51, 2017.

[22] X. P. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[23] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[24] 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 Transactions on Cybernetics*, vol. 46, no. 5, pp. 1132–1143, 2016.

[25] W. M. Zhang, K. D. Ma, and N. H. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, no. 1, pp. 118–127, 2014.

[26] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469–1479, 2016.

[27] D. Hou, W. Zhang, and N. Yu, "Image camouflage by reversible image transformation," *Journal of Visual Communication and Image Representation*, vol. 40, pp. 225–236, 2016.

[28] Y.-C. Chen, C.-W. Shiu, and G. Horng, "Encrypted signal-based reversible data hiding with public key cryptosystem," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1164–1170, 2014.

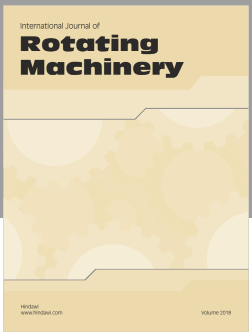
[29] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," *Signal Processing: Image Communication*, vol. 39, pp. 226–233, 2015.

[30] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 9, pp. 1622–1631, 2016.

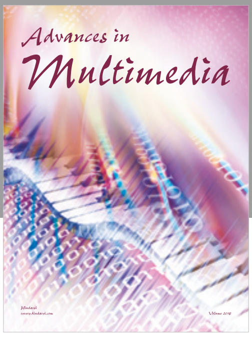
[31] X. Wu, B. Chen, and J. Weng, "Reversible data hiding for encrypted signals by homomorphic encryption and signal energy transfer," *Journal of Visual Communication and Image Representation*, vol. 41, pp. 58–64, 2016.

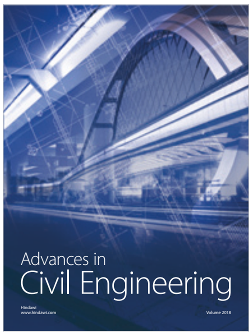
Journal of
Engineering

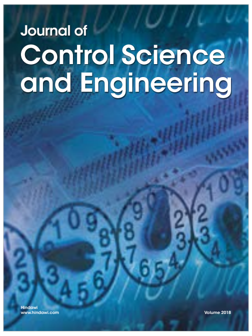
The Scientific World Journal


International Journal of
Rotating Machinery

Journal of
Sensors

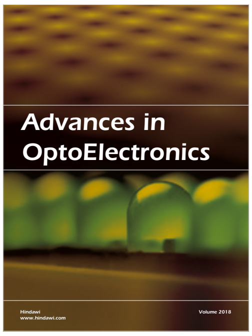

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science and Engineering

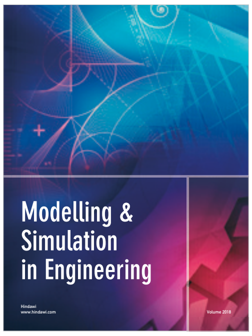
Journal of
Robotics

Journal of
Electrical and Computer Engineering

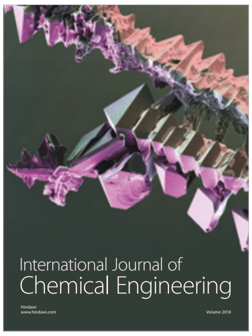

Advances in
OptoElectronics

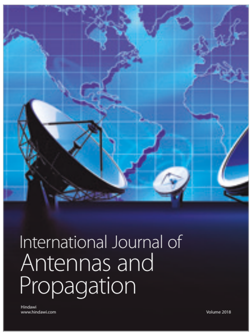
VLSI Design

International Journal of
Navigation and Observation

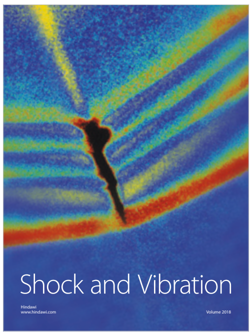

Modelling & Simulation in Engineering

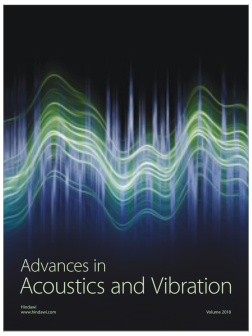
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration