Reversible Data Hiding using Prediction Error Adoption

Article · February 2022

Mohankumar Mylsamy
Sri Eshwar College of Engineering

Reversible Data Hiding using Prediction Error Adoption

M. Mohan Kumar, M. Midhuna, R. Ramya Priya, P. Megha and K. Mohanappriya

***Abstract*---**Reversible data hiding in encrypted images is a technique that embedded additional data into an encrypted image without accessing the content of the original image, the embedded data can be extracted and the encrypted image can be recovered to the original one. In this work, two reversible data hiding methods in encrypted images, namely a joint method and a separable method, are introduced by adopting prediction error. In this paper, we propose joint and separable RDH techniques using an improved embedding pattern and a new measurement function in encrypted images with a high payload. The first problem in recent joint data hiding is that the encrypted image is divided into blocks, and the spatial correlation in the block cannot fully reflect the smoothness of a natural image. The second problem is that half embedding is used to embed data and the prediction error is exploited to calculate the smoothness, which also fails to give good performance In the joint method, data extraction and image reconstruction are performed at the same time. The reversibility, number of incorrect extracted bits are significantly improved while maintaining good visual quality of recovered image, especially when embedding rate is high. In the separable method, data extraction and image recovery are separated. The separable method also provides improved reversibility and good visual quality of recovered image for high payload embedding.

***Keywords*---**Image Encryption, Image Recovery, Reversible Data-Hiding. Joint Method, Separable Method.

I. Introduction

REVERSIBLE data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. A number of reversible data hiding methods have been proposed in recent years. There are various Earth Observation Satellites (EOS), provide the large number of image database. These images are subjected to many threats and accidental damage. There would be loss of bits or data in the image. Due to this disadvantages, Secure transmission of data in the social networks as well as from the satellite towards the base station. This proposed method consists image encryption in the field of social media as well as in the satellite images. In the olden days, data security in the satellite is limited with the encryption process and the security in the social media also less. Because of the lesser security basis there would be more amount of terrorists attacks [1].

There are various process which is recommended by the consultative committee for the Space Data Systems(CCSDS) (CCDS,2015), which has the communication systems that has spread rapidly throughout the space. There are various number of threats which is existing due to improper transmission of mission data. By, knowing the mission data hackers can damage the space mission by knowing the secret data. So, due to these disadvantages, it will be necessary to secure the data from the social media, satellite transmission data.

So, it is necessary to consider the method which is used to transmit data confidentially and with proper authentication. There are various information which is available in the existing work which gives the encryption method. The image encryption which is used for the satellite transmission is Digital Encryption Standard, International Data Encryption Algorithm (IDEA), Triple Data Encryption Standard (3-DES) and the Advanced Encryption Standard [1].

Images which are used for encryption have the certain key features such as sharpness, contrast and huge data size. In this images, there will be strong correlation between the two adjacent pixels which reduce the redundancy of the original bits. Encryption of image by the proposed method can reduce the various factors namely encryption speed, loss of data. There are various traditional encryption algorithm such as AES, DES, 3DES [2][3][4]. The best analyzing of encryption of images was proposed by [5] which is used for the AES algorithm of encryption method. The main objective of the proposed work is to encrypt the satellite images and the images which are on the social network. These images are analyzed by the Single Event Upset (SEU), which has the lesser complexity and power consumption, for embedded satellite image encryption.

The watermarking method[6] is capable of withstanding incidental image processing operations such as compression and identifies any malicious tampering done on the host image. Several Steganographic techniques are described in the survey[7] The major algorithm which includes the applying the chaotic block to image encryption method[8]. There are various procedures in the chaotic block which includes the traditional algorithm for image encryption techniques [9][10].

Manuscript received on April 08, 2020, review completed on April 10, 2020 and revised on April 19, 2020.

M. Mohan Kumar is with the Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

M. Midhuna is with the Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

R. Ramya Priya is with the Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

P. Megha is with the Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

K. Mohanappriya is with the Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

Digital Object Identifier: DMKE052020004.

In this paper, they developed the encryption method using the AES and two chaotic maps which includes 2D cat map and Henon attractor is used in decryption. There are various steps which is included in the proposed work based on chaotic mapping. This new method of encryption technique is the new image encryption method which has the lesser power consumption and higher throughput[3][11][12] [13][14][15].

As, the proposed method, [15]'s scheme which have the new method of cryptography adapted for the spectral images as well as social network images. In [15] (1998) proposed that the block cipher algorithm based on the two steps which is mainly confusion by using two-dimensional map followed by the diffusion technique. Many of the researchers may have discussed the principle of robust cryptosystem [3][16][17][18]. In this proposed work, the adaptation of Fridrich's method for the encryption of spectral images will be suitable for the analyze of transmission of secret data from the satellite towards base station. Experimental analysis is done using the simulation software MATLAB which would explain the performance measure of the proposed work. Thus, the proposed method would have the lesser power consumption, lesser PSNR rate and the lesser MSE range. This would increase the encryption of data without loss of information and the secured transmission. The image encryption method is based on the chaotic map which consists of following steps. There is different Online Social Networks (OSN) that is used to upload the images with the different pixel range. Thus, these are the most suitable methods of stegnography. There are various tested algorithm of stegnography which would reduce the power consumption. There are several social networks such as Facebook and google+ that have the encryption of data. This data encryption method is used for the lossless embedding of message into the images. The proposed work consists of following section II which consists of proposed work, section III consists of online social network encryption, section IV consists of results and discussion, section V consists of conclusion work.

II. Related Work

The existing RDH-EI methods can be classified into two categories: "vacating room before encryption (VRBE)" and "vacating room after encryption (VRAE)". In VRBE, the content owner creates room for embedding data in the cover image before encryption [13,14]. As VRBE requires the content owner to do an extra preprocessing before content encryption, so this method might be impractical. In this sense, the VRAE method is more practical. In VRAE methods, the original content is encrypted by the content owner, and the data-hider embeds the additional information by modifying a small part of the encrypted data [15–23]. The VRAE methods can be further divided into two categories: joint method and separable method.

In joint methods [15–20], with an encrypted image containing additional data, a receiver may first decrypt it using the encryption key, and then extract the embedded data and recover the original image from the decrypted image using the data-hiding key. In 2011, Zhang [15] proposed a novel reversible data hiding technique in encrypted images. In 2012, Hong et al. [16] improved Zhang's technique by using a side match technique. Zhang's and Hong's systems were further enhanced with other techniques [17,18]. In these systems, the encrypted image is divided into blocks, and the spatial correlation in the block cannot fully reflect the smoothness of natural images, especially when the block size is small. In 2014, Li et al. [19] introduced a new scheme where a random diffusion strategy is used for embedding and accurate prediction is used to measure the smoothness. In 2014, Wu and Sun [20] proposed a different joint RDH system based on prediction error. However, the smoothness calculation from using prediction error fails to perform well.

Nevertheless, in joint methods, the embedded data can only be extracted before image decryption. In other words, a receiver having a data-hiding key but no encryption key cannot extract any information. Moreover, when the payload is high, it is not possible to get error-free extracted bits with all these joint methods. To overcome these problems, a separable reversible data-hiding scheme is required.

In separable methods [20–23], with an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional bits from the marked encrypted image directly, while if the receiver has the encryption key, he can decrypt the received data which is similar to the original one.

III. The Proposed Joint Data Hiding System

A. Procedures of Proposed Method

The proposed joint system has three phases: image encryption, data hiding, and joint data extraction and image restoration, as represented in Figure 1. In the image encryption phase, by using an encryption key, a content owner encrypts an original uncompressed image and creates an encrypted version of the original image. In the data hiding phase, by exploiting a data-hiding key, a data hider inserts some additional data within the encrypted image by modifying a small portion of the encrypted data. However, the data hider does not know any information about the original image. The encrypted image is divided into four sets, instead of blocks, and two sets can be used for data hiding, which helps to increase the embedding capacity. Besides, for security purposes, the information is further encrypted using data-hiding key. In the joint data extraction and image restoration phase, a receiver first decrypts the embedded encrypted image by using the encryption key to obtain a directly decrypted image that is similar to the original. Moreover, with the aid of a data-hiding key, the receiver can extract the embedded data and restore the original image from the directly decrypted image. In the proposed system, for fluctuation calculation, the actual value of pixels and the absolute difference between neighboring pixels are more preferred than an estimated value and prediction error, respectively. The detailed procedures are as follows.

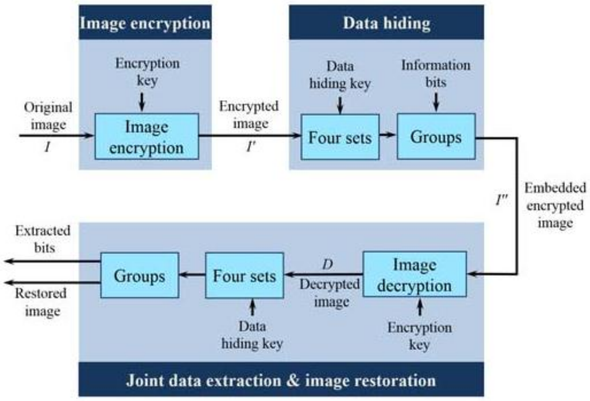


Fig 1 Block Diagram of the Proposed Joint Data Hiding System.
Image Encryption

Since the content owner does not want the data hider to know any information about the original image, he encrypts the original image with an encryption key using a standard stream cipher. Among various papers for image encryption, we adopt the image encryption algorithm identical to Zhang's [15] and others [16–20], in order to compare them conveniently and impartially.

It is assumed that I is a gray-level image of uncompressed format sized $X \times Y$, in which every pixel with a gray value is represented by eight bits. Let $I_{i,j}$ be a pixel at position (i,j), where $I_{i,j}$ belongs to [0, 255] and $1 \leq i \leq X$, $1 \leq j \leq Y$. $I_{i,j,k}$ denotes eight-bit binary digits of each pixel with a gray value, where k = [1, 8]. The relation between bits in a pixel and pixels with a gray value is denoted by

$$I_{i,j,k} = \left\lfloor \frac{I_{i,j}}{2^{k-1}} \right\rfloor \bmod 2 \qquad (5)$$

To encrypt the original image, random sequence $R_{i,j,k}$ is generated according to the encryption key using a standard stream cipher. Then, bits of pixel $I_{i,j,k}$ can be encrypted by a bitwise exclusive-or (XOR) of I and R:

$$I'_{i,j,k} = I_{i,j,k} \oplus R_{i,j,k} \qquad (6)$$

From the bits of the encrypted pixel in (6), a pixel in the encrypted image can be written as follows:

$$I'_{i,j} = \sum_{k=1}^{8} I'_{i,j,k} \cdot 2^{k-1} \qquad (7)$$

B. Data Hiding

After the encryption phase, the encrypted image is sent to the data hider. Although the data hider does not know anything about the original image, the data hider can embed additional data into the encrypted image by changing a small portion of it. Before embedding, Q bits of information are permuted by using the data-hiding key; let $A(1)$, $A(2)$, . . . , $A(Q)$ be the permuted information bits to be embedded. It is assumed that $Q = Q_B + Q_W$, where Q_B and Q_W are nonnegative integers for the number of embedded information bits in the two sets. In the data hiding phase, according to the data-hiding key, the pixels except the border pixels in the encrypted image, are divided into four sets, B_1, B_2, W_1, and W_2, where pixels in B_1 and W_1 can be used for embedding Q_B and Q_W information bits, respectively, and pixels in B_2 and W_2 can be used for data extraction. Border pixels can be the elements of B_2 or W_2 but cannot be the elements of B_1 or W_1, i.e., border pixels can be used for data extraction but cannot be used for data embedding. To embed one information bit, it is assumed that G pixels are considered. Therefore, the elements of B_1 and W_1 are Q_BG and Q_WG, respectively.

For convenience, it is assumed that B_1 and B_2 can be located at position (i,j), where $(i + j) \bmod 2 = 0$. Similarly, the elements of W_1 and W_2 can be located at position $(i + j)$, where $(i + j) \bmod 2 = 1$ as shown in Figure 3. In the first round, according to the data-hiding key, pixel $I'_{i,j}$ is selected, and pixel $I'_{i,j}$ is assigned to B_1 or W_1, if $(i + j) \bmod 2$ is 0 or 1, respectively. Then, neighboring pixels $I'_{i+1,j}$, $I'_{i-1,j}$, $I'_{i,j+1}$, and $I'_{i,j-1}$ are assigned to W_2 or B_2, respectively. For the next round, we choose a new pixel $I'_{i,j}$ with i and j that are different from i and j in the previous round. If $(i + j) \bmod 2$ is 0, then the chosen pixel $I'_{i,j}$ becomes an element in B_1, regardless of whether the chosen pixel $I'_{i,j}$ is an element of B_2 or not, and neighboring pixels $I'_{i+1,j}$, $I'_{i-1,j}$, $I'_{i,j+1}$, and $I'_{i,j-1}$ are elements of W_1 or W_2 or not. However, the neighboring pixels that are not in W_2 become elements in W_2. The neighboring pixels in W_1 or W_2 are not changed. Similarly, if $(i + j) \bmod 2 = 1$, then the chosen pixel $I'_{i,j}$ is assigned to set W_1, and the neighboring pixels not in set B_2, become elements of B_2. For example, as shown in Figure 3, we choose a pixel at position (2, 2) where i = 2 and j = 2. Since (2 + 2) mod 2 = 0, the first chosen pixel belongs to set B_1 and neighboring pixels will be the elements in set W_2. If the second selected pixel is located at the (3, 3) position, the chosen pixel belongs to set B_1 since (3 + 3) mod 2 = 0. Since the top and left pixels are already in set W_2, only the bottom and right pixels will be the elements in set W_2. The third chosen pixel at position (5, 2) will belong to set W_1 as (5 + 2) mod 2 = 1 and adjacent pixels will be the elements in B_2. The next pixel can be selected at position (4, 3) and will belong to set W_1. Though this pixel was already an element of set W_2, the pixel can belong to W_1 and the neighboring pixels that are not in B_2 become the elements of B_2. The selection process terminates when the elements of B_1 and W_1 become Q_BG and Q_WG.

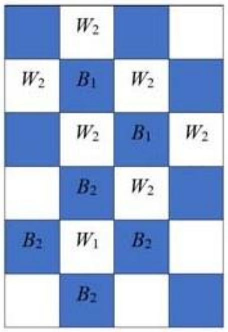


Fig 2. Pixels Allocation in Sets.

After that, let C be a union of the positions of pixels in B_1 and W_1, and the number in C is QG. The set C can be divided into Q groups: Q_1, Q_2, . . . , Q_Q, sequentially. Then, the d th group, Q_d, can be written as $\{(i_{1,d}, j_{1,d}), (i_{2,d}, j_{2,d}), . . . , (i_{G,d}, j_{G,d})\}$, where $d = 1, 2, . . . , Q$. The d th group can embed the d th permuted information bit $A(d)$. If an information bit to be embedded is 1, that is $A(d) = 1$, one bit of G pixels where positions are in Q_d will be flipped. It is assumed that the t th bit can be flipped, where t is 4, 5, or 6. Here, the t th bit is flipped instead of the three LSBs to make the pixels more fluctuated. If an information bit to be embedded is 0, that is $A(d) = 0$, the t th bit of G pixels where the positions are in Q_d will remain the same. When all the bits, $A(1)$, $A(2)$, . . . , $A(Q)$ are embedded, an embedded encrypted image, I'', will be constructed and sent to the receiver.

C. *Joint Data Extraction and Image Restoration*

In this phase, if receivers have both the encryption and data-hiding keys, then they can extract the embedded information bits and restore the original image. To do this, receivers first generate a random sequence, $R_{i,j,k}$ according to the encryption key using a standard stream cipher. Then, a bitwise XOR of I'' and R is performed using the following equations:

$$D_{i,j,k} = I^{\mathrm{JJ}}$$

$$R_{i,j,k} \qquad (8)$$

IV. The Proposed Separable Data Hiding System

In the joint data hiding system, data extraction and image restoration are inseparable as they are extremely related. If someone has the data-hiding key but not the encryption key, he cannot extract the embedded information bits from the embedded encrypted image.

In this section, we present a separable reversible data hiding system in encrypted images, where data extraction and image restoration are separable. There are four phases: image encryption, data hiding, data extraction, and image restoration is demonstrated in Figure 6. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image with the aid of a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. When, he has only the encryption key, he can decrypt the received data and obtain a filtered decrypted image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and restore the original image without any error. In the proposed system, to calculate the fluctuation, we have exploited the real value of pixels and the absolute difference between adjacent pixels in place of an estimated value and prediction error, respectively. Herein, data extraction must be carried out before image decryption.

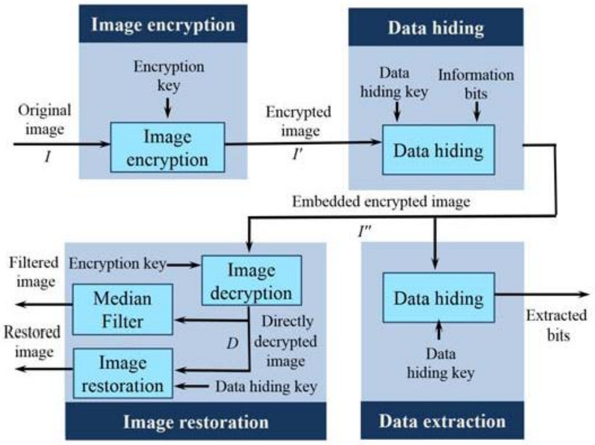


Fig 3. Block Diagram of the Proposed Separable Data Hiding System.

A. *Image Encryption*

In the image encryption phase, by using an encryption key, a content owner encrypts the original uncompressed image to obtain an encrypted image. The encryption procedure is the same as that in the joint system.

B. *Data Hiding*

In data hiding phase, a data hider embeds additional information bits into the encrypted image, I'. The detailed embedding steps are as follows.

Step 1: Before embedding, Q bits of information are permuted by using the data-hiding key; let $A(1)$, $A(2)$, . . . , $A(Q)$ be the permuted information bits to be embedded.

Step 2: Then, according to the data-hiding key, the data hider pseudo-randomly selects Q pixels from the encrypted image. The selection process is the same as that in the data hiding phase of the joint system. Let I'(1), I'(2), . . . , I'(Q), be the Q selected pixels in the encrypted image.

Step 3: The t th bits of the I'(1), I'(2), . . . , I'(Q), pixels are collected, where $t \geq 7$. Then, the information bits are embedded by replacing the t th bits of the corresponding selected pixels with $A(1)$, $A(2)$, . . . , $A(Q)$. Herein, the information bits are concealed in the most significant bits or the second most significant bits. Then, the embedded encrypted image I'' is sent to the receiver.

C. *Data Extraction*

In this phase, we consider that the receiver only has the data-hiding key. With the aid of data-hiding key, the receiver extracts the embedded information bits by adopting following steps.

Step 1: The receiver pseudo-randomly selects Q pixels from the embedded encrypted image according to the data-hiding key as did in the data hiding phase. Let I''(1), I''(2), . . . , I''(Q), be the Q selected pixels in the embedded encrypted image.

Step 2: The t th bits of I''(1), I''(2), . . . , I''(Q) pixels are collected and these bits are the permuted extracted information bits. Let $E(1)$, $E(2)$, . . . , $E(Q)$ be the extracted bits. The t th bits can be extracted by using following equation

$$E(d) = \left\lfloor \frac{I^{JJ}(d)}{2^{t-1}} \right\rfloor \bmod 2,\ 1 \le d \le Q \qquad (14)$$

Step 3: By exploiting the data-hiding key, the permuted extracted bits $E(1)$, $E(2)$, . . . , $E(Q)$ are inverse permuted to get the actual information bits.

Note that, because of the pseudo-random pixel selection and permutation of information bits, any attacker without the data-hiding key cannot obtain the pixel locations, and therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

D. Image Restoration

In the image restoration phase, we consider two cases: (1) the receiver only has the encryption key; and (2) the receiver has both the data hiding and encryption keys.

When the receiver has the encryption key but does not know the data-hiding key, undoubtedly, he cannot extract the embedded data without data-hiding key. However, the original image content can be roughly restored. To do this, receivers first generate a random sequence, $R_{i,j,k}$ according to the encryption key using a standard stream cipher. Then, a bitwise XOR of I" and R is performed to decrypt the encrypted image. Since some most significant bits or second-most significant bits are modified in the separable method, it introduces salt-and-pepper noise on the directly decrypted image. Then, a median filtering is applied to the directly decrypted image to suppress the noise, and a filtered decrypted image is obtained.

When the receiver has both the data hiding and encryption keys, he can extract the embedded bits and resort the encrypted image to the original version. The detailed steps are as follows.

Step 1: With the aid of data-hiding key, pixels with hidden bits are selected and by fetching the t th bit of the corresponding chosen pixel, embedded bits are extracted. By using the data-hiding key, the extracted bits are inverse permuted to get the actual information bits.

Step 2: A random sequence, $R_{i,j,k}$ is obtained according to the encryption key using a standard stream cipher. These bits are utilized to decrypt the encrypted image and directly decrypted image, D is obtained. In the directly decrypted image, only the t th bits of the Q specific pixels may differ from the original.

Step 3: From the directly decrypted image, the receiver pseudo-randomly chooses Q pixels by using the data-hiding key. Let $D(1)$, $D(2)$, . . . , $D(Q)$, be the Q selected pixels in the directly decrypted image.

Step 4: By setting the t th bit as 0 and 1, two possible values of $D(d)$ are achieved. Let $D_0(d)$ and $D_1(d)$ be the two possible values of $D(d)$, respectively.

Step 5: The fluctuation function of $D_0(d)$ and $D_1(d)$

V. Experimental Results and Discussion

In our simulation, we consider four gray-level images (Lena, Jet, Peppers, and Sailboat) sized 512 × 512 as test images, as shown in Figure 8 [24], for both joint and separable systems.

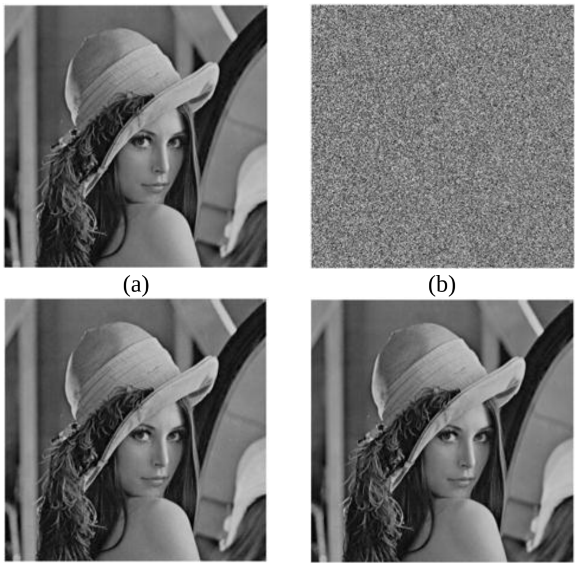
(a) (b)

(c) (d)

Fig 4. Test Images used for the Simulation (a) Lena; (b) Jet; (c) Peppers; and (d) Sailboat [24].

A. Joint System

For joint data hiding system, as shown in Figure 5a, original test image Lena is encrypted to generate Figure 5b. Then, we embed 7225 bits (equivalent to a block size of 6 × 6 [15–17]) into the encrypted image by setting t = 5 and G = 15. After that, the image was decrypted as seen in Figure 5c. Finally, the hidden bits were successfully extracted and the original image was perfectly restored from the directly decrypted image as shown in Figure 5d.



(a) (b)

(c) (d)

Fig 5. Experiment by Joint System. (a) Original Lena; (b) Encrypted Lena; (c) Decrypted Lena Containing Information bits; and (d) Recovered Lena.

Tables 1–4 show the performance analysis of the proposed system for test images Lena, Jet, Peppers, and Sailboat, respectively. For the performance analysis, we consider bit error rate (BER) and embedding rate. The BER is the ratio of unrecovered bits to the total number of embedded bits, and the embedding rate is the ratio of the total embedded bits to the total pixels in the image. Figure 6 is a graphical representation of the bit error rate (%) versus data-embedding capacity (bits) for all the images. From the tables and Figure 6, we can see that the error rate increases with an increase in the embedding rate. If we embed more bits, then the error rate will also be higher. For the Lena image (Table 1 and Figure 6), when 16,384 bits (equivalent to a block size of 4 × 4 [15–17]) are embedded, that is the embedding rate is 0.0625, the error rate is 0; however, with 28,900 bits (equivalent to a block size of 3 × 3 [15–17]), the embedding rate is 0.11, and the error rate increases to 0.01. With the Jet image, as shown in Table 2 and Figure 6, when the embedding rate increases from 0.0275 to 0.0625, the error rate also rises from 0 to 0.04. Tables 3 and 4 also show similar results.

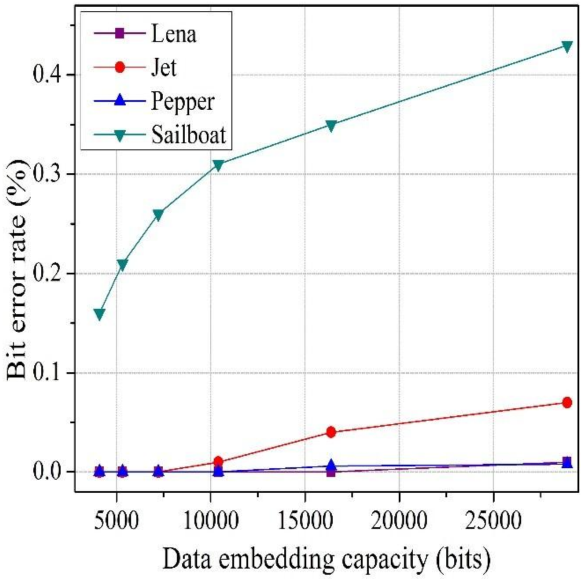


Fig 6. Bit Error Rate vs. Data Embedding Capacity.

TABLE 1
PERFORMANCE ANALYSIS OF THE PROPOSED SYSTEM FOR THE TEST IMAGE LENA.

G	*t*	**Embedded Bits**	**Embedding Rate (bpp)**	**Bit Error Rate**
10	5	4096	0.0156	0
4	6	4096	0.0156	0
15	5	7225	0.0275	0
4	6	7225	0.0275	0
4	6	16,384	0.0625	0
4	6	24,576	0.0938	0.008
4	6	28,900	0.1100	0.010

TABLE 2
PERFORMANCE ANALYSIS OF THE PROPOSED SYSTEM FOR THE TEST IMAGE JET.

G	*t*	**Embedded Bits**	**Embedding Rate (bpp)**	**Bit Error Rate**
10	5	4096	0.0156	0
4	6	4096	0.0156	0
15	5	7225	0.0275	0
4	6	7225	0.0275	0
4	6	16,384	0.0625	0.04
4	6	24,576	0.0938	0.05
4	6	28,900	0.1100	0.07

Figure 6 also shows that the BER performance with the Lena image is better than the other images, since the spatial correlation of the Lena image is stronger than the other images. For Lena, 16,384 bits can be embedded error-free, whereas in the Jet and Pepper images, 7225 bits can be embedded error-free. On the other hand, the BER performance with Sailboat is worse than the other images because of weak spatial correlation. Therefore, the BER in the data hiding system depends on spatial correlation, too.

TABLE 3
PERFORMANCE ANALYSIS OF THE PROPOSED SYSTEM FOR THE TEST IMAGE PEPPERS.

G	*t*	**Embedded Bits**	**Embedding Rate (bpp)**	**Bit Error Rate**
10	5	4096	0.0156	0
4	6	4096	0.0156	0
15	5	7225	0.0275	0
4	6	7225	0.0275	0
4	6	16,384	0.0625	0.006
4	6	24,576	0.0938	0.007
4	6	28,900	0.1100	0.008

TABLE 4
PERFORMANCE ANALYSIS OF THE PROPOSED SYSTEM FOR THE TEST IMAGE SAILBOAT.

G	*t*	**Embedded Bits**	**Embedding Rate (bpp)**	**Bit Error Rate**
10	5	4096	0.0156	0.21
4	6	4096	0.0156	0.16
15	5	7225	0.0275	0.26
4	6	7225	0.0275	0.23
4	6	16,384	0.0625	0.35
4	6	24,576	0.0938	0.41
4	6	28,900	0.1100	0.43

Bit error rate comparisons between the proposed system and the referenced systems (based on embedded bits) for test images, Lena, Jet, Peppers, and Sailboat, respectively. In Figures 11a, 12a, 13a, and 14a, the difference between the proposed system and Wu and Sun [20] is small due to the scaling factor. So, we draw Figures 11b, 12b, 13b, and 14b, to compare the proposed system and Wu and Sun [20] and to indicate the difference clearly. For Lena, when 16,384 bits are embedded, the error rates for the Zhang [15], Hong et al. [16], and Liao et al. [17] systems are 15.8, 7.9, and 6.62%, respectively; whereas, the BER of the proposed system is 0, which is significantly lower than other systems.

VI. Conclusions

In this work, two (joint and separable) reversible data hiding systems using an enhanced embedding pattern and a new measurement function in encrypted images which offer a high payload are proposed. In the joint system, data extraction and image restoration are done jointly. Here, the encrypted image is divided into four sets, instead of blocks, and two sets can be used for data hiding, which helps to increase the embedding capacity. Moreover, we consider the actual value of pixels, instead of an estimated value, and we exploit the absolute difference between neighboring pixels in preference to prediction error to calculate the smoothness. By avoiding block division and prediction error, we use the spatial correlation property of the natural images fully. For this reason, performance of the proposed work is superior to the performance of other works. In the separable method, data extraction and image recovery are separable and the hidden information bits are extracted without any error. Besides, as we avoid prediction error for separable method too, the proposed separable scheme outperforms other works in terms of reversibility. Furthermore, before hiding data, we can encrypt the information bits to further increase the security of the system.

References

[1] Hong, W.; Chen, T. A novel data embedding method using adaptive pixel pair matching. IEEE Trans. Inf. Forensics Secur. 2012, 7, 176–184. [CrossRef]

[2] Hussain, M.; Wahab, A.W.A.; Javed, N.; Jung, K.H. Hybrid data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images. Symmetry 2016, 8, 1–21. [CrossRef]

[3] Hong, W.; Chen, T.S.; Yin, Z.; Luo, B.; Ma, Y. Data hiding in AMBTC images using quantization level modification and perturbation technique. J. Vis. Commun. Image Represent. 2017, 76, 3761–3782. [CrossRef]

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

[5] Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. 2006, 16, 354–362.

[6] Thodi, D.M.; Rodriguez, J.J. Expansion embedding techniques for reversible watermarking. IEEE Trans. Image Process. 2007, 16, 721–730. [CrossRef] [PubMed]

[7] Luo, L.; Chen, Z.; Chen, M.; Zeng, X.; Xiong, H. Reversible image watermarking using interpolation technique. IEEE Trans. Circuits Syst. Video Technol. 2010, 5, 187–193.

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

[9] Hong, W.; Chen, T.S.; Chen, J. Reversible data hiding using delaunay triangulation and selective embedment. Inf. Sci. 2015, 308, 140–154. [CrossRef]

[10] Kumar, M.; Agarwal, S. Reversible data hiding based on prediction error and expansion using adjacent pixels. Secur. Commun. Netw. 2016, 9, 3703–3712. [CrossRef]

[11] Lian, S.; Liu, Z.; Ren, Z.; Wang, H. Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. 2007, 17, 774–778. [CrossRef]

[12] Cancellaro, M.; Battisti, F.; Carli, M.; Boato, G.; Natale, F.G.B.; Neri, A. A commutative digital image watermarking and encryption method in the tree structured haar transform domain. Signal Process. Image Commun. 2011, 26, 1–12. [CrossRef]

[13] Ma, K.; Zhang, W.; Zhao, X.; Yu, N.; Li, F. Reversible data Hiding in encrypted images reserving room before encryption. IEEE Trans. Inf. Forensics Secur. 2013, 8, 553–562. [CrossRef]

[14] Cao, X.; Du, L.; Wei, X.; Meng, D.; Guo, X. High capacity reversible data hiding in encrypted images by patch-level sparse representation. IEEE Trans. Cybern. 2016, 46, 1132–1143. [CrossRef] [PubMed]

[15] Zhang, X. Reversible data hiding in encrypted images. IEEE Signal Process. Lett. 2011, 18, 255–258. [CrossRef]

[16] Hong, W.; Chen, T.; Wu, H. An improved reversible data hiding in encrypted images using side match. IEEE Signal Process. Lett. 2012, 19, 199–202. [CrossRef]

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

[18] Pan, Z.; Wang, L.; Hu, S.; Ma, X. Reversible data hiding in encrypted image using new embedding pattern and multiple judgements. Multimed. Tools Appl. 2016, 75, 8595–8607. [CrossRef]

[19] Li, M.; Xiao, D.; Peng, Z.; Nan, H. A modified reversible data hiding in encrypted images using random diffusion and accurate prediction. ETRI J. 2014, 36, 325–328. [CrossRef]

[20] Wu, X.; Sun, W. High-capacity reversible data hiding in encrypted images by prediction error. Signal Process. 2014, 104, 387–4