International Journal of Digital Crime and Forensics
Volume 11 • Issue 4 • October-December 2019

A New Kind of High Capacity and Security Reversible Data Hiding Scheme

Bin Ma, College of Information, Qilu University of Technology (Shandong Academy of Sciences), Jinan, China
Xiao-Yu Wang, College of Information, Qilu University of Technology (Shandong Academy of Sciences), Jinan, China
Bing Li, College of Information, Qilu University of Technology (Shandong Academy of Sciences), Jinan, China

ABSTRACT

A novel high capacity and security reversible data hiding scheme is proposed in this article, in which the secret data is represented by different orthogonal spreading sequences and repeatedly embedded into the cover image without disturbing each other in the light of Code Division Multiple Access (CDMA) technique, and thus the embedding capacity is enlarged. As most elements of orthogonal spreading sequences are mutually canceled in the process of repeated embedding, it keeps the distortion of the embedded image at a low level even with high embedding capacity. Moreover, only the receiver who has the spreading sequence and the embedding gain factor the same as the sender can extract the secret data and achieve the original image exactly, thus the proposed scheme achieves high embedding security than other schemes. The results of the experiment demonstrates that the CDMA based reversible data hiding scheme could achieve higher image quality at moderate-to-high embedding capacity compared with other state-of-the-art schemes.

KEYWORDS

Capacity, Code Division Multiple Access (CDMA), Data Hiding, Reversible

1. INTRODUCTION

Reversible data hiding (RDH) is a kind of distortion-free data embedding method, it allows one to hide the secret data into an image in such a way that the original image can be reconstructed completely from the marked image after the embedded data having been extracted correctly. For some sensitive applications, such as military and medical imaginary, the cover image is so important that even a very slight change of pixels is unacceptable. In this case, any changes may affect the intelligence of the image that always require access to the original data, and thus the reversible data hiding is highly desired is such scenery.

Many reversible data hiding schemes have been developed in recent years. Early reversible data hiding schemes were mainly based on lossless compression techniques, in which certain bits of an image pixel are compressed to create vacancies for data embedding losslessly (Fridrich, Goljan, & Du, 2002; Celik, Sharma, Tekalp & Saber,2005). Fredrich et al. proposed a reversible data hiding method by compressing the least significant bit planes of the host image and embedded the secret data into the saved space. Celik et al. enhanced Fredrich et al.'s approach and presented a high-performance scheme through compressing quantization residues with more efficient compression technique, however, these schemes often suffer from large distortion with low embedded capacity and lack of

DOI: 10.4018/IJDCF.2019100108

safety control algorithm. Later on, many efficient algorithm shaving been proposed that emphasize on increasing data embedding capacity at low image distortion.

Ni et al. (Ni, Shi, Ansari & Su, 2006) proposed an efficient reversible data hiding solution named histogram shifting scheme, in which a gap is created near the highest histogram bin by shifting image gray levels with one position, and the embedded bits are encoded by using the highest bin of pixels. From then on, many histogram modification schemes are proposed. Lee et al. (Lee, Suhand & Ho, 2006) employed the difference-image to embed more data than Ni et al.'s scheme. Yang et al. (Yang & Tsai,2010) proposed an interleaving prediction method and increased the number of prediction errors as many as the pixels, by which the embedding capacity is improved effectively. Xuan et al. (Xuan, Tong, Teng, Zhang & Shi, 2012) embedded data into image prediction-errors with histogram pair method, and four thresholds are introduced for performance optimization, by which they achieved excellent results at low-to-moderate embedding capacity. Recently, Li et al. (Li, Zhang, Gui &Yang, 2013) proposed an adaptive reversible data hiding scheme to enhance the embedding performance at high embedding payload.

Difference expansion is another fruitful research direction introduced by Tian (Tian, 2003), in which the pixel differences are expanded and the secret data are added to the expansion created space furtherly. Thodi and Rodriguez (Thodi & Rodriguez, 2007) enhanced the difference expansion technique with a method called prediction-error expansion, which exploits the correlation inherent in the neighborhood of a pixel than the difference-expansion scheme, and thus the distortion of the cover image is reduced after data embedding. Sachnev et al. (Sachnev, Kim, Nam, Sures & Shi, 2009) presented a prediction-error expansion method-based scheme without using a location map in most cases, it allows to embed more data into the image with less distortion. Li et al. proposed to embed 1 or 2 bits into expandable pixels adaptively according to the local complexity with prediction-error expansion method.

Although most schemes try to exploit ample small prediction errors for data hiding so as to lighten the image distortion, but a lot of big-value prediction errors would still be involved for data hiding when the payload is high, and the image quality drops rapidly with the increase of embedding capacity. In this paper, a CDMA based high performance reversible data hiding scheme is presented for reversible data hiding. The secret data are represented by different orthogonal spreading sequences and embedded repeatedly into the cover image to enlarge its embedding capacity, as most elements of different spreading sequences are mutually canceled in the process of the repeated data embedding, that keeps the image in good quality even at high embedding capacity. Moreover, according to the speciality of the proposed scheme, only the receiver who has the spreading sequence and the embedding factor the same as the sender can extract the secret data and achieve the original message exactly, which improves the security of the system.

The rest of the paper is organized as follows. Section 2 introduces the CDMA based data hiding method in detail. In section 3, a CDMA based reversible data hiding scheme is provided, the experimental results are provided and discussed in section 4. The conclusions are drawn in section 5.

2. CDMA BASED REVERSIBLE DATA HIDING

Code Division Multiple Access (CDMA) is a kind of spectrum spreading technique for signal transmitting, in which various signals are represented by different orthogonal spreading sequences and transmitted together in a single channel and thus the frequency resource is saved (A data hiding scheme can also be viewed as a communication system, in which the massage is the secret data and the transmission channel is the cover image). The principle of a CDMA based data transmitting scheme is as follows:

Suppose $S = \left(s_\sigma\right)_{1\times m}$ is a zero-mean sequence with size of $1\times m$ and satisfies the following conditions:

$$s_\sigma \in \{-1,1\}, \sum_{\sigma=1}^{m} s_\sigma = 0 \tag{1}$$

Thus, the cross correlation of any two different sequences satisfies:

$$\left\langle S_i, S_j \right\rangle = S_i \cdot S_j^T = 0 \quad (i \neq j) \tag{2}$$

In a CDMA based transmitting system, the sender is assigned with an antipodal spreading sequence for signal transmission, the secret bit "1" is represented by the sequence itself and "0" is represented by its negative. Suppose the compound signals in the encoding side is

$$I = i_1 \pm i_2 \cdots \quad \pm i_j \cdots \quad \pm i_n \tag{3}$$

where, n is the number of spreading sequences, I is the compound signals to be transmitted in the same channel. At the decoding side, the specific data bit can be extracted as

$$\frac{I \cdot i_j}{\left|i_j\right|^2} = \frac{\left(i_1 \pm i_2 \cdots \quad \pm i_j \cdots \quad \pm i_n\right) \cdot i_j}{\left|i_j\right|^2} = \frac{\pm i_j \cdot i_j}{\left|i_j\right|^2} = \pm 1 \tag{4}$$

where, $|\ |^2$ is the module-square. i_j is the specified spreading sequence. The result "+1" represents the data bit "1" and "-1" represents the data bit "0". According to the orthogonality of different spreading sequences, clearly, only the receiver who has the same spreading sequence as the sender can achieve the objective data correctly. Therefore, different signals can be transmitted simultaneously in the same channel and the channel capacity is enlarged. For example, suppose two orthogonal sequences $S_1 = (1,-1,1,-1)$, $S_2 = (1,-1,-1,1)$. Apparently, S1 and S2 are zero-mean sequences and orthogonal to each other. Two secret data bits "1" and "0" are represented by S_1 and $-S_2$ respectively; thus, the two spreading sequences can be transmitted together in a CDMA based transmitting system, and the compound signal is calculated as $S=S_1+(-S_2)=S_1-S_2=(0, 0, 2, -2)$. At the receiver side, for the decoder with secret code S_1, the decoding result can be calculated as $\frac{S \cdot S_1}{\left|S_1\right|^2} = \frac{(S_1 - S_2) \cdot S_1}{\left|S_1\right|^2} = \frac{S_1 \cdot S_1}{\left|S_1\right|^2} = 1$, which represent the bit "1"; while, for the decoder with the secret codes S_2, the decoding result can be calculated as $\frac{S \cdot S_2}{\left|S_2\right|^2} = \frac{(S_1 - S_2) \cdot S_2}{\left|S_2\right|^2} = \frac{-S_2 \cdot S_2}{\left|S_2\right|^2} = -1$, which represent the bit "0". As we can see, the result would be neither 1 nor -1 if other sequences are employed to decode the compound signal. As the orthogonal spreading sequence can be generated in different ways and it is impossible for intruders to guess the spreading code, the CDMA based signal transmitting system can provide high data transmitting capacity and security.

Our scheme is inspired by the principle of CDMA based signal transmitting system and will be fully described in the following paragraphs.

2.1. CDMA Based Secret Data Embedding

Suppose $W_{in} = [\omega_1, \omega_2, \cdots, \omega_n] (\omega_i \in \{1,0\},\ i \in \{1,2,...,n\})$ is an original binary secret sequence to be embedded. The elements of the sequence are changed to a series of antipodal bits with the formula:

$$b_i = \begin{cases} 1 & if\ \omega_i = 1; \\ -1 & if\ \omega_i = 0; \end{cases} \tag{5}$$

Where, $b_i \in \{-1,1\}$, $i \in \{1,2,...,n\}$ .The original secret sequence $W_{in} = [\omega_1, \omega_2, \cdots\cdots, \omega_n] (\omega_i \in \{1,0\},\ i \in \{1,2,...,n\})$ is changed to $W_c = [b_1, b_2, \cdots\cdots, b_n]$. Choose k mutually orthogonal spreading sequences as $S_i = \{s_1, s_2 \cdots\cdots, s_l\} (i \in \{1,2,...,k\})$ from a specific *Hadmard* matrix. Here, the length of each sequence "l" is set to an even number, and the number of "1"and "-1" is equivalent in each spreading sequence. Thus, the candidate spreading sequences are zero-mean and orthogonal to each other.

Let I be the original image, the size of I is $N \times N$, Choose pixels of the image to form the vectors $i_j = [x_1, x_2, \cdots\cdots, x_l] (j \in \{1,2,..., N \times N / l\})$, where, "$l$", the same as the length of S_i, is the length of the vector i_j, Then, the secret data can be embedded into the image by the following expression:

$$i_j^{'} = i_j + \alpha[b_1 S_1 + b_2 S_2 + \cdots + b_k S_k] \tag{6}$$

The expression (6) shows that k bits of secret data can be embedded to each vector i_j. Here k is the number of the bits to be embedded (which equals to the number of orthogonal spreading sequences employed for data embedding). α is a positive integer represents the embedding gain factor, which controls the embedding intensity. The bigger the value of α, the stronger the data embedding and the noisier the image would be. Finally, the embedded image is obtained by replacing all i_j vectors with $i_j^{'}$.

2.2. CDMA Based Secret Data Extraction

Let $I^{'}$ be the marked image, and constructing $i_j^{'}$ with the same method as embedding stage. Thus, the secret bits can be extracted by calculating the cross correlation between $i_j^{'}$ and spreading sequence S_i.

$$\begin{aligned} &\langle i_j^{'}, S_i \rangle = i_j^{'} \cdot S_i^T = i_j \cdot S_i^T + \\ &\alpha \left[b_1 S_1 \cdot S_i^T + b_2 S_2 \cdot S_i^T + \cdots + b_k S_k \cdot S_i^T \right] \end{aligned} \tag{7}$$

Since the spreading sequences are orthogonal to each other. The formula (7) can be simplified as:

$$\langle i_j^{'}, S_i \rangle = i_j \cdot S_i^T + \alpha b_i S_i \cdot S_i^T \tag{8}$$

Where, α is a positive integer and $S_i \cdot S_i^T$ is always positive. So, the sign of expression $\alpha b_i S_i \cdot S_i^T$ is determined by b_i. Therefore, in the case of $\left| i_j \cdot S_i^T \right| < \left| \alpha b_i S_i \cdot S_i^T \right|$, we achieve

$$b_i = sign\langle i_j^{'}, S_i \rangle \qquad if \left| i_j \cdot S_i^T \right| < \left| \alpha b_i S_i \cdot S_i^T \right| \tag{9}$$

The formula (9) shows that if the result of expression $\left|\alpha S_i \cdot S_i^T\right|$ is greater than $\left|i_j \cdot S_i^T\right|$, the secret data can be extracted correctly. Since S_i is a zero-mean spreading sequence, the expression of $i_j \cdot S_i^T$ equals to calculate the difference of certain pairs of adjacent pixels and then added them together. Therefore, the magnitude of $i_j \cdot S_i^T$ would be quite small if the elements of i_j are similar. Fortunately, according to the redundancy of natural image content, the neighboring pixels are very similar to each other, especially in the flatten areas of an image. Therefore, the product of $i_j \cdot S_i^T$ is usually very small, which enables more secret data be embedded. At the same time, the higher the value of α is, the larger the magnitude of $\alpha S_i \cdot S_i^T$ is, the more pixels would be involved to form original vector i_j and thus the embedding capacity is enlarged. Furthermore, as the reversible data embedding of the proposed scheme is achieved with different spreading sequences and embedding gain factors, the secret data can be repeatedly embedded into the object image without disturbing to each other. The embedding capacity is then can be estimated with the formula

$$C = \left(T^* M^* N / l\right) - \varepsilon \tag{10}$$

Where, C is embedding capacity, T is embedding times, M and N are the rows and columns of object image, l is the length of orthogonal spreading sequence, and ε is the size of the extra message.

2.3. CDMA Based Original Image Recover

After the correct extraction of the secret data from the marked image (the spreading sequence S_i and the gain factor α are already known apparently), the original image can be completely recovered by this the formula:

$$i_j = i_j^{'} - \alpha\left[b_1 S_1 + b_2 S_2 + \cdots + b_k S_k\right] \tag{11}$$

Moreover, as the sender can embed the secret data with different embedding sequences and gain factors, only the receiver who has the spreading sequence and the embedding gain factor the same as the sender can extract the corresponding secret data and obtain the original image exactly, consequently, the proposed reversible data hiding scheme also achieves higher data embedding security than other schemes.

3. DESIGN OF A CDMA BASED REVERSIBLE DATA HIDING SCHEME

In this section, unlike most CDMA based communication systems adopt long orthogonal spreading sequences for data transmitting; we employ short spreading sequence with only 2 elements for reversible data hiding. Since two pixels can only hide one secret bit for single embedding, it can be calculated that the maximum achievable embedding rate is 0.5BPP (Bit Per Pixel) when the length of spreading sequence is 2for single embedding. On the other hand, as the two orthogonal spreading sequences derived from *Hadmard* matrix are (1,-1) and (1, 1), it can be obtained from formula (9) that all adjacent pixels whose difference or sum belong to {-1, 0, 1} are satisfied for data embedding. Moreover, multiple levels data embedding can also be employed to improve image embedding capacity, in which different orthogonal spreading sequences are repeatedly embedded into the object image. For example, suppose the two to-be-embedded data bits are 1 and 0, the vector i_1 formed from the prediction-error image is (0, 1) and the two orthogonal spreading sequences are (1,-1) and (1, 1). The first secret bit 1 represented by spreading sequence (1,-1) and added to the vector, the embedded

vector becomes (1,0); the second secret bit 0 is represented by (-1,-1), the embedded vector is then changed to (0,-1) after double embedding.

At the decoding side, the embed data bit 0 and 1 can be extracted and the original vector can be recovered exactly according to the following steps:

$$\begin{aligned} &Step1:\begin{cases}(0,-1)\times(1,1)=-1<0\ \ \omega_2=0;\\ (0,-1)-(-1,-1)=(1,0);\end{cases}\\ &Step2:\begin{cases}(1,0)\times(1,1)=1>0\ \ \omega_1=1;\\ (1,0)-(1,-1)=(0,1);\end{cases}\end{aligned} \tag{12}$$

Notice that the order of data bit extraction is inverse to that of the embedding. In the process of data extraction, only the value of second pixel changes 2, other elements of embedded spreading sequences are mutually canceled in multiple levels data embedding. As most elements of different spreading sequences are mutually canceled in multiple levels data embedding, the proposed scheme achieves high embedding capacity while introduce low distortion to the cover image.

Furthermore, suppose the spreading sequence is $S_1=[1,-1]$ and the secret data bit is "1" at first, each pixel of vector i_1 change 1 in value after single embedding denoted as $i_1^{'}$ (it is clear that the modification on prediction errors will finally reflected on pixel values). In the second level data embedding, the bit to-be-embedded maybe "0" or "1" and the probability is 50% respectively. If the to-be-embedded data bit is "0", $-S_1=[-1,1]$ would be added to the modified vector $i_1^{'}$, the final change of the elements in i_1 are $S_1+(-S_1)=[0,0]$; If the to be embedded data bit is "1", $S_1=[1,-1]$ will added to the modified vector $i_1^{'}$, the final change of the elements in i_1 would be $S_i+S_i=[2,-2]$. Thus, considering the data bit probability, the *probable Mean Square Error* (*pMSE*) can be computed as $pMSE=\left(\left(\frac{0^2+0^2}{2}\right)+\left(\frac{2^2+2^2}{2}\right)\right)\Big/2=2$. Similarly, we can obtain the *pMSE* after third levels embedding is $pMSE=3$, and so on. The value of *pMSE* just equals to the embedding levels, therefore, the proposed scheme introduces low image distortion even at high embedding capacity.

In addition, to further increase the embedding capacity, we employ the prediction-error matrix of the cover image generated through rhombus error prediction method for multilevel data embedding. Generally, the prediction errors of the proposed error prediction method are very small and quasi-Laplace distribute sharply around zero, and then the vectors with similar small elements are obtained and the embedding capacity is enlarged. In the proposed error prediction method, denote the image pixel value as $u_{i,j}$, where i and j are subscripts of row and column. Its four neighbors $\left(u_{i,j-1},u_{i+1,j},u_{i,j+1},u_{i-1,j}\right)$ are employed to predict the value of $u_{i,j}$ as

$$u_{i,j}^{'}=\left\lfloor\left(u_{i,j-1},u_{i+1,j},u_{i,j+1},u_{i-1,j}\right)\Big/4\right\rfloor \tag{13}$$

The prediction error is obtained as $d_{i,j}=u_{i,j}-u_{i,j}^{'}$. Then, the secret data is embedded by modification of $d_{i,j}$ to $D_{i,j}$, and the original pixel value $u_{i,j}$ is changed to $U_{i,j}=D_{i,j}+u_{i,j}^{'}$, which are employed to constructs the marked image. The decoding process of rhombus error prediction method is an inverse of encoding stage, and the trivial description is omitted here.

4. EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Comparisons on Three Popular Test Images

Three images of "Lena", "Baboon" and "Airplane" from USC_SIP database are employed to evaluate the performance of our proposed data hiding scheme. To facilitate comparison, the size of all images is 512×512×8bits. As most of the sensitive images in hospital and military areas are in grayscale, thus, we choose grayscale image for reversible data hiding experiments and our study mainly focuses on them. Furthermore, as far as color images are concerned, they can be regarded as the compound of the three gray images which come from R/G/B color Channels. Meanwhile, all experiments are performed by embedding and decoding a random binary sequence generated by the Matlab function *randint*(), and a location map is adopted to indicate the data hiding positions, whose size is usually quite small according to the redundancy of natural image. The embedding rate-distortion behavior is employed to evaluate the performance of the proposed scheme.

Figure 2-4 show the PSNR (Peak Signal Noise Ratio)-BPP curves of proposed scheme compared with some state-of-the-art reversible data hiding schemes, which include the histogram shifting based scheme presented by Xuan et al. and Li et al., the difference expansion-based schemes presented by Sachnev et al. and Li et al. The results demonstrate that the performance of our proposed scheme achieves higher PSNR values than those schemes at moderate-to-high embedding capacity. Figure 2 shows that the PSNR values of our proposed scheme exceed Xuan et al.'s result at 0.2 BPP, Li et al.'s result at about 0.13BPP, Sachnev et al.'s result at 0.16BPP and Li et al.'s result at around 0.21BPP, respectively on test image Lena Figure 1. At the same time, Figure 3-4 illustrate that the PSNR of our proposed scheme exceed other state-of-the-art schemes at 0.08BPP, 0.36 BPP respectively on image Baboon and Airplane.

The reason is that when the payload embedded into the image is small, the value of two pixels would be changed at least for one bit embedding even the spreading sequence length is 2 in the proposed scheme; thus, the image distortion is larger than other schemes at low data embedding rate. But with increase of the payload, the spreading sequences which represent different secret bits are repeatedly embedded into the watermarked image, and most elements of different spreading sequences are mutually canceled. The distortion introduced by the proposed scheme drops down and the PSNR-BPP curve declines slowly. Hence, the proposed scheme achieves higher PSNR value than others at the moderate-to-high data embedding capacity.

On the other hand, considering the difference expansion-based scheme adopted by *Sachnev et al*. and *Li et al.*, the distortion introduced to the cover image can be expressed as2p or 2p+1(p is the absolute value of prediction errors employed for data embedding). The pixel value changes "0" or "1" when the prediction error "0" or "-1" are employed for data embedding, but the pixel value changes would be "2" or "3" if the difference "1" is chosen, and so on. Thus, the distortion of the cover image grows fast when the payload increases. As for the histogram shifting scheme adopted by Xuan et al. and Li et al. its performance relies on the height of the highest histogram bins (generally is bin "0" and "-1"), when the amount of the to-be-embedded data less than the highest histogram bins, the distortion introduced to the cover image is 0 or 1, but all of the non-involved pixels are also change 1 in value to ensure the reversibility. Moreover, when the payload is large than the highest histogram bins, Multiple levels data embedding should be adopted and all of the non-involved pixels need to change 2 in value to vacate space for data embedding, and so on. Then the image quality would also degrade rapidly when the payload increases. However, in our proposed scheme, the spreading sequence is directly added to prediction-error vector and no histogram bins need to be shifted. The pixel value changes only "+1" or "-1" for each data embedding step, and all differences belongs to {-1,0,1} are involved for data embedding. Therefore, once the amount of prediction errors (histogram bins) "0" or "-1" are exhausted for data hiding in the schemes of difference expansion or histogram shifting, the image distortion caused by data embedding in those schemes would be larger than our proposed scheme apparently.

Furtherly, Figure 2-4also shows that the performance of our proposed scheme exceeds other schemes at different data embedding rate. The PSNR values of marked image exceed other schemes at low embedding rate in image with more texture areas (e.g., Baboon), however, it oversteps other schemes at moderate embedding rate in image with more flatten areas (e.g., Airplane and Lena). Since the prediction error histogram of image with more flatten areas distributes much concentrated around the zero (in fact, the value of most prediction errors is 0), the image distortion caused by data embedding by conventional data hiding schemes is less than those with more texture areas especially at low payload. Thus, only after more secret data are embedded, the proposed scheme can exceed their performance.

4.2. Comparisons on JPEG2000 Test Image

To further evaluate the performance of our proposed scheme, one of JPEG2000 test image Woman Figure 5 is employed in our experiments. Unlike those widely used images generally have the two empty ends of their histogram, the both ends of histogram of the image Woman have peaks. Thus, the data embedding in image Woman is more challenge than others. Furtherly, the size of the image has been reduced from 1920 × 1536 to 960 × 768 to facilitate the comparison. The performance comparison in terms of PSNR versus BPP with Xuan et al.'s histogram modification method is shown in Figure 6. As Xuan et al.'s method makes use of four thresholds to search for optimal performance in the process of reversible data hiding, it achieves better performance as the payload is no more than

Figure 1. Test images of Lena, baboon, and airplane

Figure 2. The performance of proposed scheme on image Lena compared with other schemes

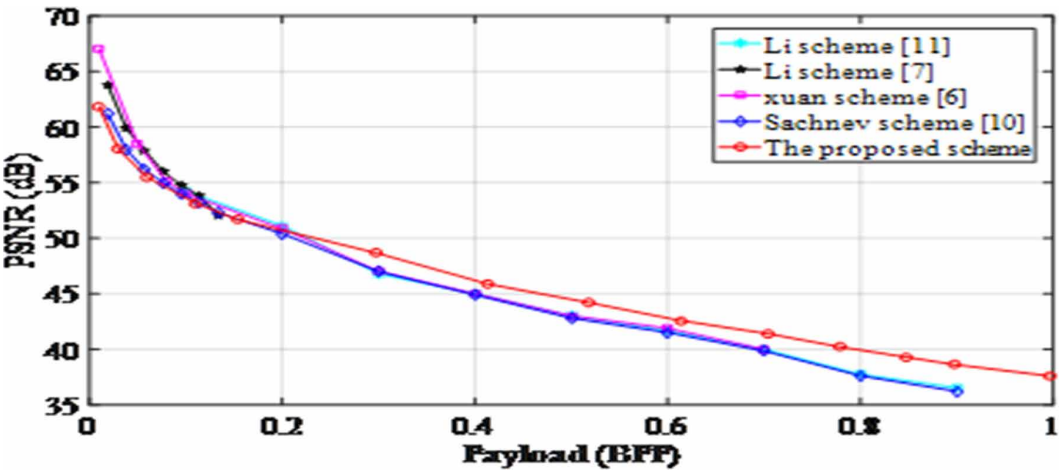


Figure 3. The performance of proposed scheme on image baboon compared with other schemes

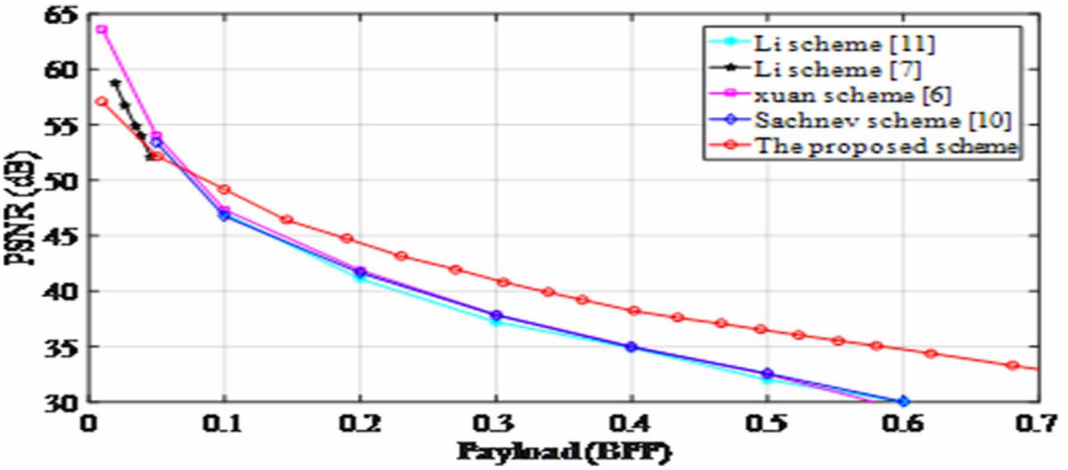
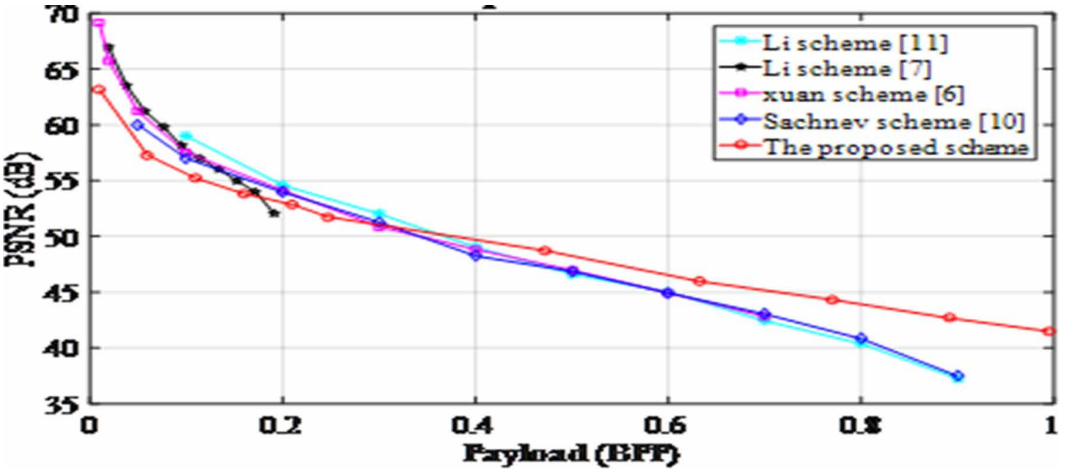


Figure 4. The Performance of proposed scheme on image airplane compared with other schemes



0.55 BPP. However, as the payload increases, most elements of different spreading sequences are mutually canceled in the process of multilevel data embedding, Hence, our proposed scheme achieves higher PSNR values than Xuan et al.'s method when the embedding capacity larger than 0.55 BPP.

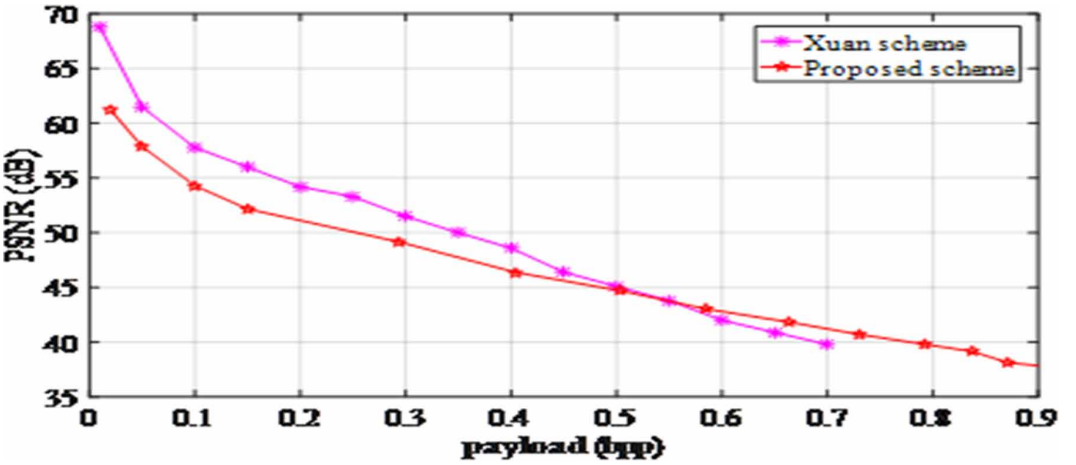
5. CONCLUSION

This paper presents a reversible data hiding scheme based on CDMA algorithm. Unlike the conventional CDMA based data transmitting system using very long spreading sequence, short spreading sequences are employed in our scheme. The secret bits represented by different orthogonal spreading sequences are repeatedly embedded into the image so that the embedding capacity is enlarged. Due to the orthogonality of the spreading sequences, most elements of different spreading sequences are mutually canceled in the process of multilevel data embedding, which retains the cover image with excellent visual quality even at moderate-to-high payload. Moreover, only the receiver who has the spreading sequence and the embedding gain factor the same as the sender can extract the

Figure 5. Test images of woman

secret data and achieve the original image exactly, which improves the security of the proposed scheme. Experimental results show that the performance of the proposed scheme is superior to those state-of-the-art-3533 reversible data hiding schemes especially at moderate-to-high embedding capacity.

Figure 6. Comparison of our proposed method and Xuan et al.'s on image woman



ACKNOWLEDGMENT

This research was partially supported by the natural science foundation of China (No. 41202206), Jinan university & institutes innovation program (JN201402005).

REFERENCES

Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2002). Reversible data hiding. In *International Conference on Image Processing Proceedings* (Vol. 2, pp. 157-160).

Fridrich, J., Goljan, M., & Du, R. (2001, August). Invertible authentication. In *Security and Watermarking of Multimedia contents III* (Vol. 4314, pp. 197–209). International Society for Optics and Photonics.

Lee, S., Suh, Y., & Ho, Y. (2006). Reversible Image Authentication Based on Watermarking. *IEEE International Conference on Multimedia and Expo* (pp. 1321-1324). IEEE.

Li, X., Yang, B., & Zeng, T. (2011). Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Transactions on Image Processing*, *20*(12), 3524-3533.

Li, X., Zhang, W., Gui, X., & Yang, B. (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. *IEEE Transactions on Information Forensics and Security*, *8*(7), 1091–1100. doi:10.1109/TIFS.2013.2261062

Ma, B., & Shi, Y. Q. (2016). A Reversible Data Hiding Scheme Based on Code Division Multiplexing. *IEEE Transactions on Information Forensics and Security*, *11*(9), 1914–1927. doi:10.1109/TIFS.2016.2566261

Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2004). Reversible data hiding. In *International Workshop on Digital Watermarking* (Vol. 2, pp.1-12). Springer.

Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(7), 989–999. doi:10.1109/TCSVT.2009.2020257

Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing,16*(3), 721-730.

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(8), 890–896. doi:10.1109/TCSVT.2003.815962

Tong, X., Wang, X., Xuan, G., Li, S., & Shi, Y. Q. (2015). Optimal Histogram-Pair and Prediction-Error Based Reversible Data Hiding for Medical Images. In *International Workshop on Digital Watermarking* (pp. 378-391). Cham: Springer.

Yang, C. H., & Tsai, M. H. (2010). Improving histogram-based reversible data hiding by interleaving predictions. *IET Image Processing*, *4*(4), 223–234. doi:10.1049/iet-ipr.2009.0316

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 a Professor with the School of Information Science, Qilu University of Technology, Shandong, China. He serves as an Editorial Board Member of a few journals such as the IEEE Transactions on Information Forensics and Security, the Journal Of Visual Communication and Image Representation, and IEEE Signal Processing, etc. and his research interests include reversible data hiding, multimedia security, and image processing. He is a member of ACM, and a member of the IEEE.

Xiaoyu Wang received the B.S. degree from Qilu University of Technology, Jinan, China in 2016. She is a postgraduate student in School of Information Science, Qilu University of Technology. Her research interest is reversible data hiding.

Bing Li received a B.S. degree from Qilu University of Technology, Jinan, China in 2017. She is currently a postgraduate student in the School of Information Science, Qilu University of Technology. Her research interest is reversible data hiding.