Copyright © 2019 Tech Science Press CMC, vol.58, no.1, pp.1-13, 2019

High Capacity Data Hiding in Encrypted Image Based on Compressive Sensing for Nonequivalent Resources

Di Xiao[1, *], Jia Liang[1], Qingqing Ma[1], Yanping Xiang[1] and Yushu Zhang[2]

Abstract: To fulfill the requirements of data security in environments with nonequivalent resources, a high capacity data hiding scheme in encrypted image based on compressive sensing (CS) is proposed by fully utilizing the adaptability of CS to nonequivalent resources. The original image is divided into two parts: one part is encrypted with traditional stream cipher; the other part is turned to the prediction error and then encrypted based on CS to vacate room simultaneously. The collected non-image data is firstly encrypted with simple stream cipher. For data security management, the encrypted non-image data is then embedded into the encrypted image, and the scrambling operation is used to further improve security. Finally, the original image and non-image data can be separably recovered and extracted according to the request from the valid users with different access rights. Experimental results demonstrate that the proposed scheme outperforms other data hiding methods based on CS, and is more suitable for nonequivalent resources.

Keywords: Compressive sensing, encrypted image, data hiding, prediction error, nonequivalent resources.

1 Introduction

There are many application scenarios in Internet of Things or Cloud Computing where different entities possess nonequivalent resources. For example, in wireless multimedia sensor networks (WMSNs), various nodes, such as common scalar sensors, multimedia sensors, multimedia processing hubs and sink, have different requirement about resources. Especially general sensors are typically resource- constrained devices which cannot afford a huge number of computation, while multimedia processing hubs and sink will have comparatively large computational resources [Akyildiz, Melodia and Chowdury (2007)]. Due to the resource limitation, there are lots of challenges in its corresponding security application [Li, Zhang, Chen et al. (2018)]. Fortunately, the emergence of compressive sensing (CS) opens up a new vision for multimedia data security with nonequivalent resource limitation.

CS has gained wide attention since it was introduced. CS can achieve compression and

[1] College of Computer Science, Chongqing University, Chongqing, 400044, China.

[2] School of Information Technology, Deakin University, Victoria 3125, Australia.

[*] Corresponding Author: Di Xiao. Email: xiaodi_cqu@hotmail.com.

CMC. doi:10.32604/cmc.2019.02171 www.techscience.com/cmc

encryption together through matrix multiplication [Rachlin and Baron (2008)]. Compared with the stream cipher encryption, the encrypted data based on CS can reduce bandwidth resources effectively. Due to this feature of CS, research results based on CS often serve multimedia data compression and representation [Wu, Yu, Yuan et al. (2016)]. Meanwhile, CS has a low computation cost in the sensing part while the computation of recovery is rather complex at the receiving end.

Information hiding plays an important role in protecting various information from being destroyed [Cao, Zhou, Sun et al. (2018)]. Within the current application of CS in reversible data hiding, there are two main types: the first one usually embeds data in the samples of DCT/DWT and then uses CS to compress [Xiao and Chen (2014)]. The other one embeds data in the measured value [Cao, Du, Wei et al. (2016); Li, Xiao and Zhang (2016); Pan, Li, Yang et al. (2015)]. However, both of the two schemes have some defects. The first one is more suitable for digital watermarking rather than data hiding, which focuses on the protection of the copyright about the carrier and the robustness of the watermark. But, data hiding puts more emphasis on the capacity and security of the embedded information itself. The scheme proposed by Pan et al. [Pan, Li, Yang et al. (2015)] is a watermarking scheme for plain image only which does not provide security for the cover. The scheme proposed by Cao et al. [Cao, Du, Wei et al. (2016)] is not suitable for nonequivalent resources, although this scheme has a brilliant performance on recovery. The reason is that sparse representation to vacate room for data embedding in the preprocessing operation is very complicated. The scheme proposed by Li et al. [Li, Xiao and Zhang (2016)] is a smart data hiding scheme based on block compressive sensing, but its capacity is limited by block size. To design a qualified hiding scheme in encrypted image based on CS for nonequivalent resources, the computational complexity in the sensing part should be focused on.

In this paper, we propose a high capacity data hiding scheme in encrypted image based on CS for nonequivalent resources. Multimedia sensor nodes take pretreatment on covers to vacate room and encrypt them by CS. General sensor nodes get non-image data, then encrypt them. Multimedia processing hubs gather data from sensor nodes and embed the encrypted scalar data into the processed image. Sink node is in charge of managing and processing data from hubs, and will extract the embedded data and recover image for the valid user with different access rights. Due to the properties of CS, the processes of encryption and embedding are simple and suitable for resources constrained device. This feature falls in with nonequivalent resources on this point while the process of embedding secret data into encrypted image can reduce the data transmission. The main advantages of our scheme include the adaptability to nonequivalent resources, the separable processing according to different access rights, the improvement of the embedding rate and the quality of recovery image.

The rest of this paper is organized as follows. Section 2 introduces the theory of CS. Section 3 provides detailed description of the proposed scheme. The experimental results and analysis are shown in Section 4. Finally, this paper is concluded in Section 5.

2 Compressed sensing

Given a sparse signal $X, X \in R^n$, an observation system wants to obtain m linear measurements:

$$Y = \Phi X \tag{1}$$

Where Φ is a matrix of size $m*n, Y \in R^m$. In general, $m << n$. If there exists a constant $\delta_k \in [0,1]$, for all $X \in \sum_k$,

$$(1-\delta_k)\|X\|_2^2 \le \|\Phi X\|_2^2 \le (1+\delta_k)\|X\|_2^2 \tag{2}$$

Then the matrix Φ satisfies the k-th order restricted isometry property (RIP). The matrix approximately preserves the distance between k vectors, and the sparse coefficients can be accurately reconstructed from the measurements. In the sampling process, one fact is that real world data X may not be always sparse. But as long as it can be represented as a $n \times 1$ sparse vector α under some properly chosen sparse basis $\varphi \in R^{n\times n}$ via $X = \varphi\alpha$, we can still use CS theory and have $Y = \Phi X = \Phi\varphi\alpha$. Here, let $\mathrm{A} = \Phi\varphi$, If matrix A satisfies RIP, then the sparse X could be recovered with high probability from y by solving an l_1-minimization problem.

$$\min \|\alpha\|_1 \text{ subject to } Y = A\alpha \tag{3}$$

Rachlin et al. [Rachlin and Baron (2008)] pointed out that compressed sensing is computationally secure, although CS does not reach the perfect security definition of Shannon. So, CS can compress and encrypt when sampling. The standard CS can be interpreted as a symmetric encryption system where the original signal X is a plaintext, the measurements Y is a ciphertext, and the encryption algorithm is a linear transformation operated by a key which is a measurement matrix.

3 Proposed scheme

In this section, we present the detailed procedures of our scheme. As illustrated in Fig. 1, it involves five entities: multimedia sensor nodes, general nodes, multimedia processing hubs, sink nodes and valid users.

3.1 Image pretreatment and encryption

For an 8-bit grayscale image I of size $N \times N$, let the pixel value at the position (i,j) be $p_{i,j}$, where $1 \le i \le N, 1 \le M \le N$ and $p_{i,j} \in [0,255]$. As shown in Fig. 1, at the multimedia sensor nodes, the original image is first divided into two parts according to a checkerboard style. If the indices i and j satisfy $(i+j)\bmod 2 = 1$, then $p_{i,j}$ is classified into J part. And the rest pixels in I fall into H part.

For J part, each pixel $p_{i,j}$ can be represented by 8 bits as its value range is from 0 to 255:

$$p_{i,j}(d) = \left\lfloor \frac{p_{i,j}}{2^d} \right\rfloor \bmod 2, d = 0,1,...,7 \tag{4}$$

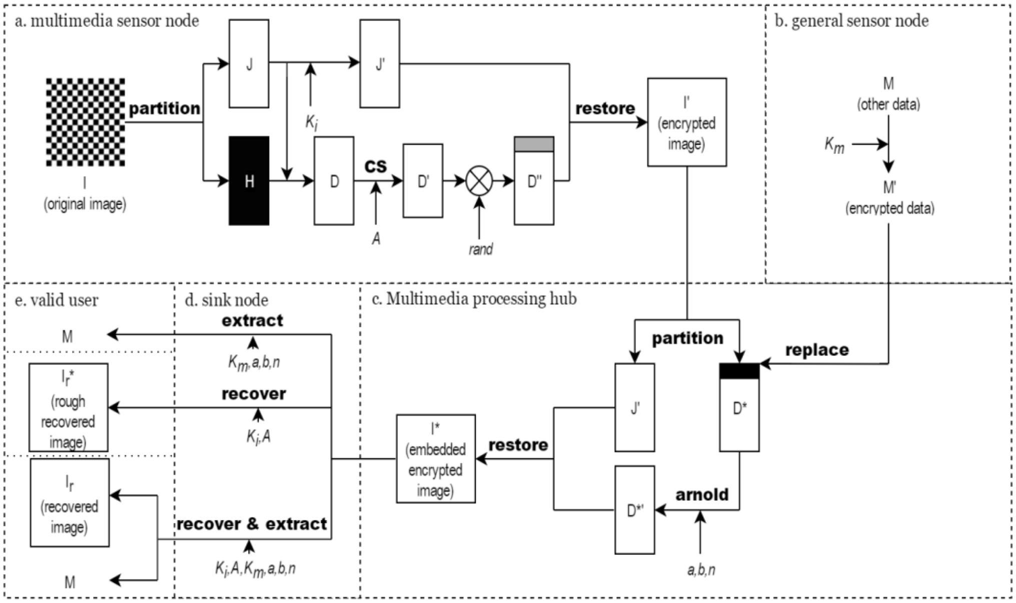


Figure 1: The flow chart of the proposed scheme

Where $\lfloor \cdot \rfloor$ is a round operator towards minus infinity. The d-th bit of $p_{i,j}$ is encrypted through exclusive-or(Xor) operation:

$$E_{i,j}(d) = p_{i,j}(d) \oplus r_{i,j}(d) \tag{5}$$

Where $r_{i,j}(d)$ is generated by a pseudo-random generator with the encryption key. Finally, J part is encrypted into J'.

Before J has been encrypted, interpolation technique [Luo, Chen, Chen et al. (2010)] is used to estimate H' from J, and the errors between H' and H are set as D:

$$D(i,j) = H(i,j) - H'(i,j) \tag{6}$$

Then, D is encrypted and compressed into D' by CS:

$$D' = \Phi \times D = \Phi \times \Psi \times \theta = A\theta \tag{7}$$

Where Φ is known as the measurement matrix, D is the original prediction errors, Ψ is set as a sparse matrix for D, θ is known as the sparse coefficients of D, and the sensing matrix A can be regarded as an encryption key. During this process, the restricted isometric property should be satisfied.

Next, pseudo-random bits are padded in front of D' to let D'' have the same size with D, and the number of padded bits is the embedding capacity which is determined by the compression ratio. The last step is to embed the embedding capacity in the first three positions of D'', as the front of D'' is vacated for data embedding.

Finally, the encrypted image with vacated room, I', is generated by restoring the corresponding position of J' and D'' in the checkerboard, where K_i and A can be considered as the encryption key.

3.2 Message encryption

General sensor nodes gain other types of data M such as temperature, humidity and position. For security, these data need to be encrypted as well. Here, a standard stream cipher is used to encrypt the data into M' by bitwise exclusive-or operation with a pseudo-random bit sequence generated by the key K_m. This process is similar to Eq. (5).

3.3 Data hiding in the encrypted images

At the multimedia processing hubs, the encrypted image should be partitioned into J' and D'' at first, and the embedding capacity is extracted from the first three positions in D''. Then, the encrypted data M' is embedded into D'' by replacing the former padded pseudo-random bits. As the data is embedded in the front of D'', if image is directly restored according to the corresponding location, the embedded data will be in dangerous. In order to improve the security, the block with embedded data, D^*, will be lightly encrypted into $D^*{}'$ by digitized Arnold transform:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \left(\bmod N \right) \tag{8}$$

where a, b and n are positive integers, and they can be considered as the key for embedding secret data.

In the last step, $D^*{}'$ and J' should be restored to the original position to obtain I^*, the encrypted image with embedded data. And the message encryption key K_m and Arnold transform's parameters a, b and n are known as the data hiding key.

3.4 Data extraction and image recovery

Sink node will extract data and restore image according to the request from valid users with different access rights.

If valid user can access comprehensive data including image and embedded data, sink node will recover image, extract embedded data and send them to user by both data hiding key and encryption key. The processes in the extracting and recovering are the inverse of data embedding and image encryption, so they are not elaborated here. CS reconstruction is a solution of the minimal l_1 norm [Donoho (2006)].

In the second case, if the valid user can only access embedded data, sink node will extract data by the hiding key and deliver it to user.

In the third case, if the valid user can only access approximate image, sink node will decrypt the J' part in I^* by the encryption key and then provide an approximately recovered image without embedded data through interpolation.

For the latter two cases, the resource consumption can be effectively reduced because CS reconstruction is not in need.

4 Experimental results and analysis

In this section, eight 512×512 standard images, including Lena, Cameraman, Baboon, Barbara, Boat, Plane, Peppers and Mondrian, are used in the experiment. Besides, another test image set containing 100 images is formed by randomly selecting from Corel database which is available from CorelDraw version 10.0 software. And the selected image is cropped to 512×512 pixels and turned into grayscale. The prediction error is calculated by interpolation technique. The sampling operator is scrambled dense FFT [Candes and Romberg (2006)]. The sparsifying transform is the 9-7 wavelet transform used in the JPEG 2000 standard and the optimizer is based on the GPSR program [Figueiredo, Nowak and Wright (2008)].

4.1 Evaluation of the proposed scheme

In our scheme, the vacated room for embedding data is obtained by CS. Therefore, the embedding rate is directly related to the compression rate of CS on D part in Fig. 1. Since only half of each image is processed by CS, for an 8-bit gray image, the relation is

$$ER = 0.5\times(1-\alpha)\times 8 = 4\times(1-\alpha) \tag{9}$$

Table 1: The relation between embedding rate and compression rate

Compression ratio α of D part	Compression ratio for image	Embedding rate (bpp)
0.4	0.7	2.4
0.6	0.8	1.6
0.8	0.9	0.8

Table 2: PSNR(dB) with different embedding rates for different test images

Embedding rate(bpp)	2.4	1.6	0.8	Recovered image with only encryption key
Lena	41.1628	43.6153	47.2990	38.4794
Camera	32.7707	34.6330	38.0325	31.0552
Baboon	30.0623	32.3724	36.0897	27.7775
Barbara	32.4655	36.4079	41.5642	29.0003
Boat	36.1654	38.3364	41.8668	33.9686
Plane	40.2079	43.0778	47.4222	37.1712
Peppers	37.8241	40.1419	43.6617	35.3252
Mondrian	41.9096	43.9259	47.2470	36.2618
Average	36.5710	39.0638	42.8979	33.6299

where α is the compression rate of D part, and *ER* is the embedding rate, as listed in Tab. 1. The first three columns in Tab. 2 show the recovered image PSNR with both the encryption key and data hiding key under different embedding rates for different images. It indicates that the PSNR will rise with the decrease of embedding rate. Fig. 2 shows more detailed experimental results. And the last row in Tab. 2 lists the average of each column. It also shows that even if the embedding rate is as high as 2.4 bpp, the lowest PSNR is larger than 30 and hence acceptable. We also test the selected set with 100 images, and give the results in Fig. 3. Both the fourth column of Tab. 2 and Fig. 3(d) show PSNR of the recovered approximate image in the case of with the encryption key only. Meanwhile, for different images with unique textures, their distributions of prediction errors are disparate, so the errors caused by CS on prediction errors D are also slightly different. Tab. 2 shows that the smoother the image is, the better the experimental result will be.

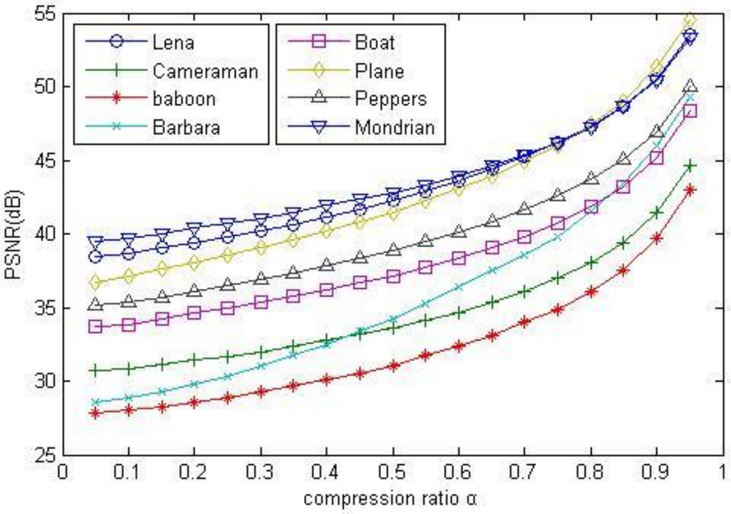
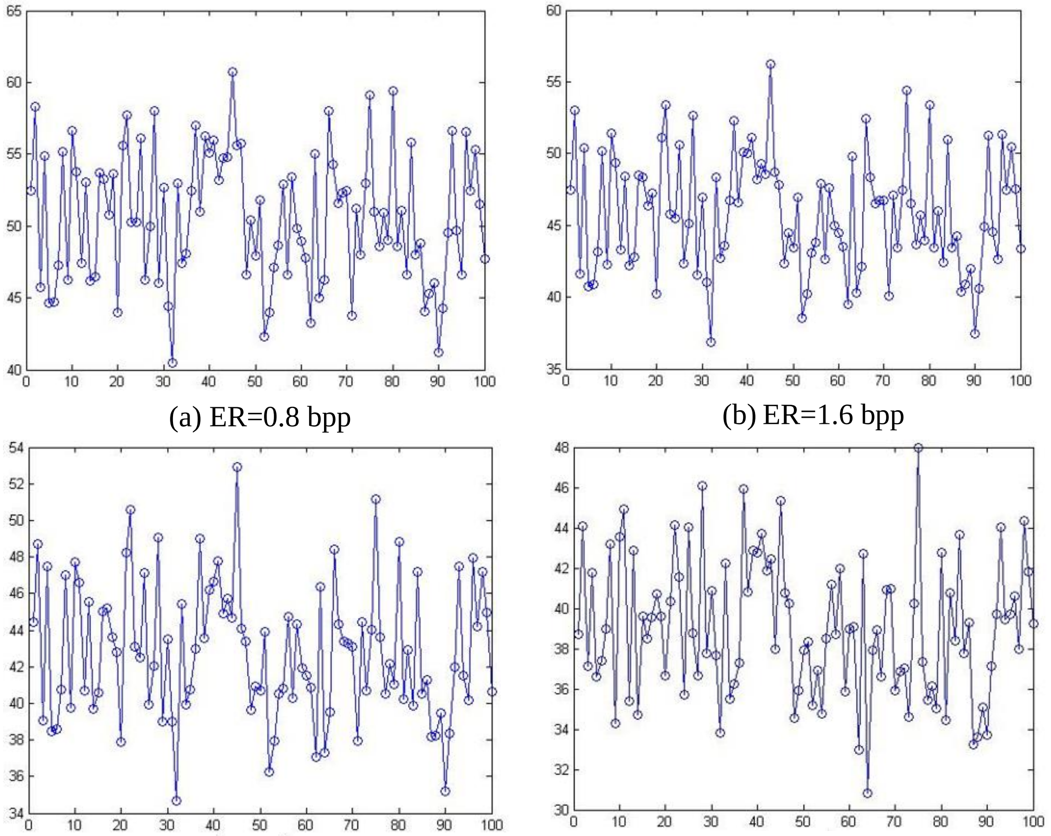


Figure 2: Relationship between compression ratio α and PSNR

In the schemes of data hiding in CS domain, both the cover data (sparse samples) and the embedded data are exactly recovered under certain noise, payload and sparsity conditions, so these methods can be qualified as conditionally reversible data hiding [Yamaç, Dikici and Sankur (2016)]. In our scheme, CS is the only part of the whole process that will bring the loss, and the sensing object of CS is the prediction error. The accuracy of Jpart, the first half of the original image, is ensured; while the other half of the original image, Hpart, can be recovered based on both the interpolation technique and the prediction error reconstructed by CS. As a result, the proposed scheme has a good recovery performance. This can be seen in Fig. 2, Fig. 3 and Tab. 2. When the compression rate is significantly low, the quality of the full recovery image is close to the one using interpolation technique only. Of course, the higher the compression rate is, the smaller the error of CS reconstruction is, and the quality of recovery image will be higher. When the compression rate approaches 0.95, the PSNR values of the full recovery image are greater than 43, and may even be close to 55.



(a) ER=0.8 bpp

(b) ER=1.6 bpp

(c) ER=2.4 bpp

(d) Recovered image with only encryption key

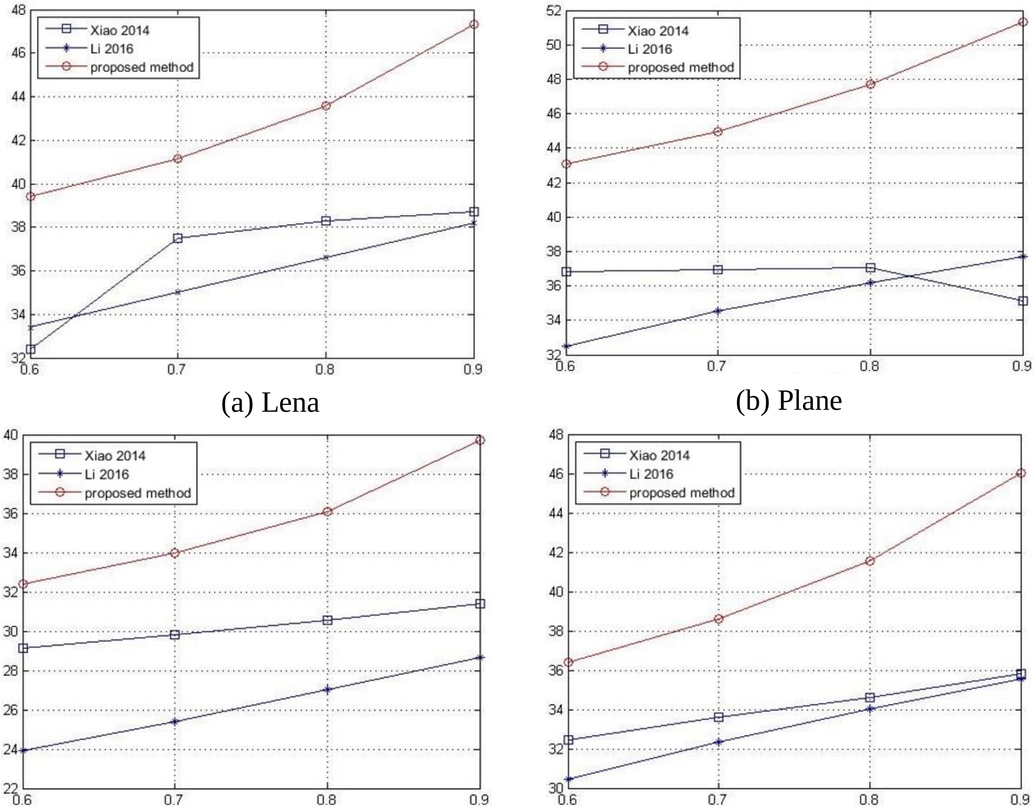
Figure 3: The PSNR under different ER values

It should be noted that the computation in the encryption and embedding processes of the proposed scheme is relatively low because there are only arithmetic and matrix multiplication. And in the process of image recovery, l_1 optimization problem is a relatively complex operation. Meanwhile, since this is a high capacity scheme, other types of non-image data and part of image data can be embedded into the cover image to reduce the transmission consumption. The comprehensive data collected in the same area can be considered as the properties of the region and has its special usage. In our scheme, the obtained comprehensive data, including the encrypted non-image data and image in the same area, can not only ensure the data security, but also be convenient for data management.

Therefore, the scheme is suitable for the applications with nonequivalent resources.

4.2 Performance comparison

When compared with other schemes based on CS, it can be seen from Fig. 4 that the proposed scheme has a better recovered image performance when using the same compression ratio for the whole image. In Fig. 4, the abscissa indicates the compression ratio, and the ordinate indicates the PSNR value of the recovered image. The reason is that only half of the data in the original image is processed and compressed by CS, and the other half is processed by the conventional stream cipher. Therefore, the quality of the restored image is ensured to be significantly better than other schemes based on CS.



(a) Lena (b) Plane

(c) Baboon (d) Barbara

Figure 4: Comparison results of the same compression ratio

Moreover, we make a comprehensive comparison among our scheme and some typical data hiding schemes based on CS in Tab. 3. According to Eq. (9), the maximal theoretical embedding rate of the proposed scheme is 4 bpp, and we calculate the average PSNR values of the recovered Lena under different embedding ratios for different schemes. It should be noted that although the title of the scheme proposed by Li et al. [Li, Xiao and Zhang (2016)] contains “reversible data hiding”, it is not a lossless scheme, so its PSNR is not infinite. Based on Tab. 3, the proposed scheme has the largest theoretical capacity so that the embedding rate can be adaptively adjusted according to different requirements.

At the same time, the quality of recovered image is only worse than he scheme proposed in Cao et al. [Cao, Du, Wei et al. (2016)]. However, since the background of our scheme is resource deficient device, we need to focus on the computational complexity about image pretreatment and encryption (as the embedding operation is relatively simple, and the data extraction side has more resources for complex calculation). According to the scheme proposed in Cao et al. [Cao, Du, Wei et al. (2016)], its computational complexity is $O\left(N^2KL\right)+O\left(2N^2\log N\right)+O\left(RN^2\right)+O\left(N^2\right)$, where N is the image size, K is the number of dictionary atoms, L is the nonzero element number in each coefficient vector, and R is the embedding round number. Meanwhile, the computational complexity of our scheme is $O\left(N^2\right)+O\left(MN^2\right)$ corresponding to the three main processes: stream encryption, prediction error estimation and CS, where N is the image size, and M is the row number in measurement matrix. In this aspect, our scheme is more suitable for nonequivalent resources than the scheme proposed by Cao et al [Cao, Du, Wei et al. (2016)].

All in all, the proposed scheme is a high capacity data hiding scheme which is more suitable for resource-constrained devices and has a better performance while comparing with other existing schemes.

Table 3: Performance comparison

Method	[Xiao (2014)]	[Cao (2016)]	[Li (2016)]	[Pan (2015)]	Proposed
Techniques	CS+DWT	CS+sparse coding	CS	CS+DCT	CS+predictio n error
Avg-PSNR (Lena)	36.7	∞	35.8	32.5	43.0
Max-embedding rate (bpp)	1	0.8	0.0078	0.0036	4
Encryption	Y	Y	Y	N	Y
Separable (decryption and extraction)	Y	Y	N	Y	Y
Resource limited condition	Y	N	Y	N	Y

4.3 Security of encrypted image

In this section, we will discuss the security of the encrypted image in the proposed method.

The natural images pixels are highly correlated. A qualified encryption algorithm must break the correlation between adjacent pixels to resist statistical attack. A correlation coefficient value "one" represents a highly correlated image which is susceptible to statistical attacks. Correlation Coefficient (CC) is given by

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{10}$$

Where $\mathrm{cov}(x,y)=\frac{1}{p}\sum_{i=1}^{p}[x_i-E(x)][y_i-E(y)]$, $E(x)=\frac{1}{p}\sum_{i=1}^{p}x_i$, $\mathrm{E(x)}=\frac{1}{p}\sum_{i=1}^{p}x_i$. Compression ratioα of *D* part is 0.5. 2000 pixels and their corresponding adjacent pixels along the horizontal, vertical and diagonal directions are randomly chosen for the correlation analysis. So, for an ideal cipher image, the correlation coefficient should be close to zero. From the Tab. 4, we can infer that in the proposed scheme, the correlation between adjacent pixels in the cipher image is negligible. Structural Similarity Index (SSIM) is used for measuring the similarity between the plain image and the encrypted image. Tab. 4 also shows the SSIM of our proposed method is close to zero. Compared with the traditional image encryption method through exclusive-or(Xor) operation, the proposed method can obtain similar correlation coefficients and SSIM. So the security of the encrypted image is acceptable.

Table 4: Correlation Coefficient (CC) and SSIM

Test Image	Direction	CC of Plain Image	CC of Cipher Image		SSIM	
			Proposed	Encrypted through Xor	Proposed	Encrypted through Xor
Lena	Horizontal	0.83751	0.0034	-0.0149	0.0126	0.0055
	Vertical	0.9077	0.0065	-0.0138		
	Diagonal	0.8007	-0.0058	0.0030		
Boat	Horizontal	0.8140	0.0073	0.0160	0.0072	0.0078
	Vertical	0.8189	-0.0033	-0.0243		
	Diagonal	0.7107	-0.0103	-0.0071		
Peppers	Horizontal	0.8786	0.0096	0.0094	0.0029	0.0023
	Vertical	0.8145	-0.0013	-0.0037		
	Diagonal	0.9050	0.0085	-0.0065		

The randomness of the image is measured by Entropy as

$$H(x)=-\sum_{i=1}^{N\times N}P(I_i)\log_2 P(I_i) \tag{11}$$

For an image with 256 grey levels the absolute maximum of entropy is 8 bits per pixel. The maximum entropy is obtained when the gray levels have equal probability of occurrence. Hence for a cipher image, the entropy value should be close to 8. From Tab. 5, we can infer that the lower the compression ratioα of *D* part, the greater the entropy. The encrypted image has high randomness as the entropy of cipher is close to the theoretical value of 8.

Table 5: Entropy of encrypted image

Test Image	Plain Image	Encrypted through Xor	Compression ratio α of D part		
			0.7	0.5	0.3
Lena	7.2725	7.9868	7.9188	7.9437	7.9697
Boat	7.2018	7.9884	7.9198	7.9437	7.9716
Peppers	7.5967	7.9881	7.9027	7.9345	7.9702

5 Conclusion

In this paper, a high capacity data hiding scheme in encrypted image based on CS is proposed. In this scheme, image decryption and data extraction are separable to match the requests of the users with different access rights. The experimental results have demonstrated that it performs well in the tradeoff between the embedding rate and the recovered image quality. Compared with other data hiding schemes based on CS, the proposed one is much more suitable for nonequivalent resources. In our future study, a part of image may be embedded into other image data to further reduce the transmission consumption.

Acknowledgement: The work was funded by the National Natural Science Foundation of China (Grant Nos. 61572089, 61502399, 61633005), the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjBX0008), the Project Supported by Graduate Student Research and Innovation Foundation of Chongqing (Grant No. CYB17026), the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018), the Chongqing University Postgraduate Education Reform Project (Grant No. cquyjg18219) and the Fundamental Research Funds for the Central Universities (Grant Nos. 106112017CDJQJ188830, 106112017CDJXY180005).

References

Akyildiz, I. F.; Melodia, T.; Chowdury, K. R. (2007): Wireless multimedia sensor networks: a survey. *IEEE Wireless Communications Magazine*, vol. 14, no. 6, pp. 32-39.

Candes, E.; Romberg, J. (2006): Robust signal recovery from incomplete observations. *IEEE International Conference on Image Processing*, pp. 1281-1284.

Cao, X.; Du, L.; Wei, X.; Meng, D.; Guo, X. (2016): High capacity reversible data hiding in encrypted images by patch-level sparse representation. *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1132-1143.

Cao, Y.; Zhou, Z.; Sun, X.; Gao, C. (2018): Coverless information hiding based on the molecular structure images of material. *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197-207.

Donoho, D. L. (2006): For most large underdetermined systems of linear equations the minimal l1-norm solution is also the sparsest solution. *Communications on Pure & Applied Mathematics*, vol. 59, no. 6, pp. 797-829.

Figueiredo, M. A. T.; Nowak, R. D.; Wright, S. J. (2008): Gradient projection for sparse reconstruction: application to compressed sensing and other inverse problems. *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 586-597.

Li, J.; Zhang, Y.; Chen, X.; Xiang, Y.; Li, J. et al. (2018): Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, vol. 72, pp. 1-12.

Li, M.; Xiao, D.; Zhang, Y. (2016): Reversible data hiding in block compressed sensing images. *ETRI Journal*, vol. 38, no. 1, pp. 159-163.

Luo, L.; Chen, Z.; Chen, M.; Zeng, X.; Xiong, Z. (2010): Reversible image watermarking using interpolation technique. *IEEE Transactions on Information Forensics & Security*, vol. 5, no. 1, pp. 187-193.

Pan, J. S.; Li, W.; Yang, C. S.; Yan, L. J. (2015): Image steganography based on subsampling and compressive sensing. *Multimedia Tools & Applications*, vol. 74, no. 21, pp. 9191-9205.

Rachlin, Y.; Baron, D. (2008): The secrecy of compressed sensing measurements. *46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 813-817.

Wu, Z.; Yu, Z.; Yuan, J.; Zhang, J. (2016): A twice face recognition algorithm. *Soft Computing*, vol. 20, no. 3, pp. 1-13.

Xiao, D.; Chen, S. (2014): Separable data hiding in encrypted image based on compressive sensing. *Electronics Letters*, vol. 50, no. 8, pp. 598-600.

Yamaç, M.; Dikici, Ç.; Sankur, B. (2016): Hiding data in compressive sensed measurements: A conditionally reversible data hiding scheme for compressively sensed measurements. *Digital Signal Processing*, vol. 48, pp. 188-200.