International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.59-70
http://dx.doi.org/10.14257/ijsia.2016.10.7.06

Reversible Data-hiding Algorithm in Encrypted Image for Security Application in Cloud Computing

Zhang Jing

1.Changchun vocational technical institute
Zjzqy2@foxmail.com

Abstract

There is a shortcoming in reversible data-hiding algorithm in encrypted images, it is the low capacity. we put forward a new algorithm oriented security application in cloud computing, in the new algorithm of reversible data-hiding algorithm in encrypted image, we bring in cloud computing service and singular value decomposition based on matrix. Using the powerful computing and storage capacity, compute the singular value decomposition of some selected bit planes of the encrypted image, and store the recovery dictionary that generated in this process, in the end ,we directly embed the information into the singular value matrix. Experimental results show that under the premise of ensured image privacy security and higher image fidelity, the embedding capacity has been significantly improved, and the image can be fully recovered after information extraction. In the same time, the processes of information extraction and image restoration are separable. Compared with other algorithms, it has higher embedding capacity.

Keywords: *encrypted image; reversible data-hiding; cloud computing; singular value decomposition*

1. Introduction

The information hiding technology which embedded some secret information into plain image directly usually by modifying the image pixel values, such as the literature[1].But in some cases, the owner of the image in order to guarantee the privacy of the image, need to encrypt the image, and the one who want to hide information into the encrypt image need to encrypt the image information in the case of without knowing the original image content. The receiver received the cipher text image that including embedded information, he can extract information and restore the original image. Therefore, we need to research the scheme of information hiding in encryption image .Literature[2] based on the correlation of natural image pixels, embed 1 bit by modifying a part of the least significant bit (LSB) of encryption image. Literature[3] enhance the extraction and recovery rate by improving the recovery algorithm of literature[2]. Literature [4] data hiding ones compress the encryption image, get a sparse space, used to embed data. Literature [5] and [6] consider the effect is not good that hide information of the cipher text whit bigger entropy, compare to the method of deal with the plaintext first and hide the cryptographic cipher text second. Literature[7] in order to hide information, modifies the traditional histogram translation algorithm, and applied it in difference domain of cipher image. But the algorithms above all have smaller capacity of embedding information, or cannot meet the needs of cloud computing security applications.

ISSN: 1738-9976 IJSIA

2. Related Work

Singular Value Decomposition (SVD) is a kind of numerical techniques to diagonalize matrix, from the perspective of image processing, it can show the image of the inner algebraic properties. Matrix singular value of image as very good stability, when image is applied small perturbation, the singular value does not have obvious changes [8], therefore, singular value decomposition has wide application in digital watermarking. In order to resist common attacks, literature [9] proposed a better robustness color image watermarking scheme based on SVD. Literature [10] combine the DWT and SVD, proposed a adaptive algorithm for color image, it coordinate the transparency and robustness of watermarking system. In order to improve the watermark robustness, the literature [11] based on DWT and SVD and Fibonacci transformation, presents a robust color image blind watermarking algorithm. Literature [12] proposes a color image watermarking algorithm combined with biorthogonal lifting wavelet and SVD, and make the blind watermark image inspection become true. SVD has many applications for gray image also, Literature[13] in view of the current watermarking contradiction problem between robustness and transparency, proposed a adaptive robust watermarking algorithm based on singular value transform and wavelet packet decomposition. Literature [14] under the framework of compression perception, studied the image sparse representation by SVD as a basal, shortening the time of image reconstruction effectively. To solve the problem of high false alarm rate, the literature [15] proposed a multiple watermarking algorithm using the singular value to adjust the original image non-subsample coefficient matrix of Contourlet region remaining subband.

Assuming the integer matrix M is a $\mathrm{r}\times r$ order matrix, and $M \in [0,7]$, Just is the after three of a gray image, SVD of the M :

$$M = U \cdot \sum \cdot V^{T} \tag{1}$$

Where U is $r\times r$ order unitary matrix, $\sum$ is positive semidefinite order diagonal matrix, and V^{T} , the Conjugate transpose of V ,is $r\times r$ order unitary matrix. The diagonal elements in $\sum$ are singular value of M ,that is $\sum = diag(\lambda_1, \lambda_2, \cdots\cdots \lambda_r)$.

The singular values $\lambda_1 (i \in [1,r])$ we get from formula (1) are the Compression results we need. Original matrix from $\mathrm{r}\times r$ order matrix change into $\mathrm{r}\times 1$vector. M is a integer matrix, but the values of $\sum$ are not integer, it need to round into integer.

$$\sum^{'} = round(\sum) \tag{2}$$

From $\sum^{'}, U$ and V^{T} ,we can recover the matrix $M^{'}$, that is :

$$U \cdot \sum^{'} \cdot V^{T} = M^{'} \tag{3}$$

$\sum^{'} \approx \sum$, so $M^{'} \approx M$,during the period of SVD, the value precision of U ,V^{T} and $\sum$ can be reach 10^{-3}. Round the singular value matrix $\sum$ we get the $\sum^{'}$, use $\sum^{'}$ and unitary matrix U ,V^T ,reconstitute matrix $M^{'}$ .under the condition of the precision is integer 1, the $M^{'} \approx M$ can be further refined (The matrix element value range[0,7]).

Use 20 images of 512 512 from the image library [16](experiment with plain image and cipher image respectively) , Take out after three LSB plane convert into integer matrix, block with size, each 512 512 image includes 16384 matrix, 20 images totally have the matrix number is ,after the experiment we get a conclusion (plain image represents the property of various kinds of natural images, and cipher image, contains property of random matrix):

(4)

Due to the higher precision characteristic of SVD, we consider use it into information hiding of Encryption image, here propose a cipher image domain information hiding scheme based on cloud computing and SVD. Some bit plane of cipher image carry out SVD is implemented in the cloud, and store the recover dictionary and ,the information hidden ones embed the data into original bit plane to hide information.

3. Proposed Reversible Data-hiding Algorithm

3.1. Image Encryption

In the sending side, the image I with size need to process, its pixel gray value range is, denote 8 bit of a pixel in coordinate :

(5)

In order to encrypt image, we use the secret key of to generate pseudorandom sequence S with length of:

(6)

Use the bits of I and the bits of pseudo random sequence to carry on xor operation,:

(7)

Turn into decimal express, get the encryption image:

(8)

The sending side sends to information hider by channel. Information hider has no secret key of, he cannot recover the original image, guarantee the privacy of the image.

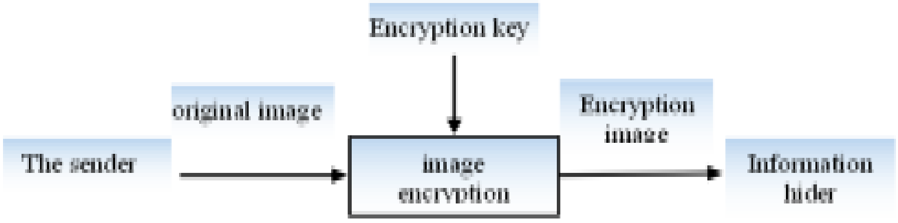


Figure 1. Encryption Processing

3.2. Data Embedding

Firstly, information hider divided the cipher image into n layers LSB-planes and m layers MSB-planes (n can be 3, 2, 1), secondly, send n layers LSB-planes to the cloud, by getting these data from cipher image, they need not encrypt again. The rest of m layers MSB-planes reserve to combine with next processing results.

The cloud side receive the n layers LSB-planes and block them ,each block size is .when n is 3, get the 3 layers LSB-planes of corresponding block ,turn them into decimal number from 1 to 7,and we get a integer matrix called ,next, perform SVD for . The are the recovery dictionary for recover the original cipher matrix (the elements value in matrix are decimals in interval(-1,1)),they saved in cloud side. We know these two dictionary are used to recover ciphertext, and there have no secret key of, original image cannot recover in here, so, it is not necessary to encrypt the two dictionary.

The singular value matrix is diagonal matrix, compare with the matrix, have many 0 value elements, these element can be used to embed data. In order to keep the elements of are integer and can turn into binary bits, round the element of ,then get the matrix ,save the four values of matrix .next , process all the blocks in the same way, and save all the recover dictionary to the cloud side orderly, the singular values, on another hand send to the information hider. Only have the singular values, without have secret key of, one cannot recover original image , so, the singular values are need not encrypt again either.

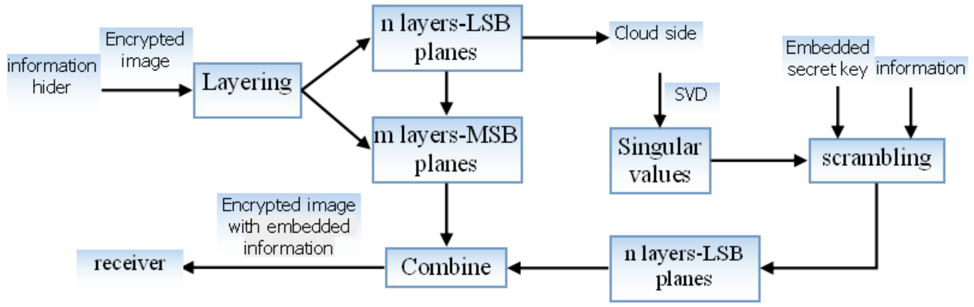


Figure 2. Process of Embed Information

Information hider receive all the singular values, for each ciphertext block, only 4 singular values are saved, its equal to compress 3 bits LSB 16=48bits of ciphertext block ,the rest position can be used to embed information. According by statistics, when block size is ,use 3 layer LSB-planes, the value will be no more than 28, it can be expressed by 5 bits, the value will be no more than 15, it can be expressed by 4 bits, the value will be no more than 15, it can be expressed by 4 bits, the value will be no more than 7, it can be expressed by 3 bits, totally we use 5+4+4+3=16 bits, the rest 48-16=32 bits can be used to embed information(corresponding to the first row of data in Table 3). Embedding capacity is matrix bits minus 4 singular values occupy bits.

For condition of the block size are and, We keep 8 and 16 singular value respectively. Due to the singular value matrix is a diagonal matrix, there are a large number of value of 0 elements, and we can use these elements to embed information. When block size is, 3 layers LSB-planes of each block have bits, we save these 8 singular value need occupy 32 bits (estimate the bit occupation by experiment to statistics the biggest value of this eight singular value), the rest bits, can be used to embed information (corresponding to the second row of data in table 3). When block size is, 3 layers LSB-planes of each block have bits, we save these 16 singular value need occupy 65 bits, the rest bits , can be used to embed information(corresponding to the third row of data in Table 3). And it is similar to deal with the 1 layer LSB and 2 layers LSB.

Table 1 to 3 show the relationship between different block size and different information length when we choose the layer of LSB-planes is 1, 2 and 3.

Table 1. Embedding Capacity when Choose 1 Layer bit Plane (bit)

Block size	Embedding capacity
	9
	50
	225

Table 2. Embedding Capacity when Choose 2 Layer bit Plane (bit)

Block size	Embedding capacity
	20
	105
	464

Table 3. Embedding Capacity when Choose 3 Layer bit Plane (bit)

Block size	Embedding capacity
	32
	160
	703

This scheme is directly process the bit of cipher, therefore, for all the gray image ,if the block size and layer of bit are fixed, the length of the embedded information is the same。

Information hider convert singular value of the current block into binary bit sequence(16 bits), combine with each embedding information(here we choose 32 bits), then we get the 3 layers LSB-planes, use the embedded secret key to scramble(Arnold scrambling[17]) all the bit layer. Next, information hider combines the each new 3 layers LSB-planes and 5 layers MSB-planes of the original location of block get a new embedded information block. Merged all the embedded information block and get a new cipher image with embedded information, and send it to receiver.

3.3. Data Extraction and Image Restoration

The receivers, according to the different authority (different number of secret keys) has different operation:

Case 1: Receiver only has decryption key, can be directly decrypt image. Use the cipher image with embedded information and secret key, the decryption image can be obtained. And although we modify part of bit plane of cipher image to get the, the recover image still include vast majority of the original image I. From Figurer 6(c) we can observe that the visual difference can ignore compare with original image (Figure 6(a)).

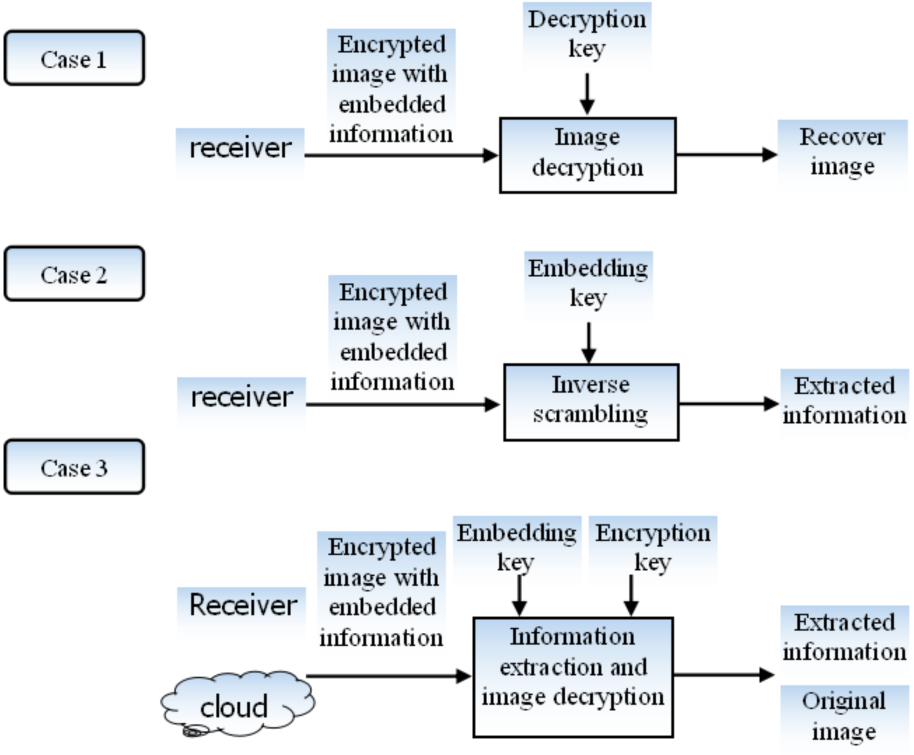


Figure 3. The Extraction and Recovery Process

Case 2: Receiver only has decryption key, can be directly extract the information. First, block the cipher image, then from the present block , get 3 layers LSB-planes and convert to binary sequence. There're a total of 48 bits in this case, inverse scrambling according to embedding key. Take out the corresponding 32-bit hidden information bits, repeat operation for all block, and get all the embedded information.

Case 3: The receiver has embedding and decryption keys simultaneously, can extract information and recover the original image. First, block the cipher image, then from the present block, get 3 layers LSB-planes. According to the embedded key, extract 16 bits singular value of the 3 layers LSB-planes of original cipher and the embedding 32 bits information. Convert these 16 bits data into integer singular value matrix and send it to the cloud side.

The cloud side use the, and , execute singular value reverse decomposition, , and is the decimal matrix of the current cipher block . convert to the 3 layer LSB-planes of current cipher block, repeat the operation for all the block, then the 3 layers LSB-planes of the original cipher text image can be gotten. Here we got the 3 layers LSB-planes are part of the encrypted cipher image, there has no secret key in the cloud side, and original image cannot recover so, need not encryption for these data here. Next, send the result to receiver and combine with the rest of 5 layers MSB-planes, can accurately recover the original cipher images. the receiver use the encrypted key of ,finally recover the original image.

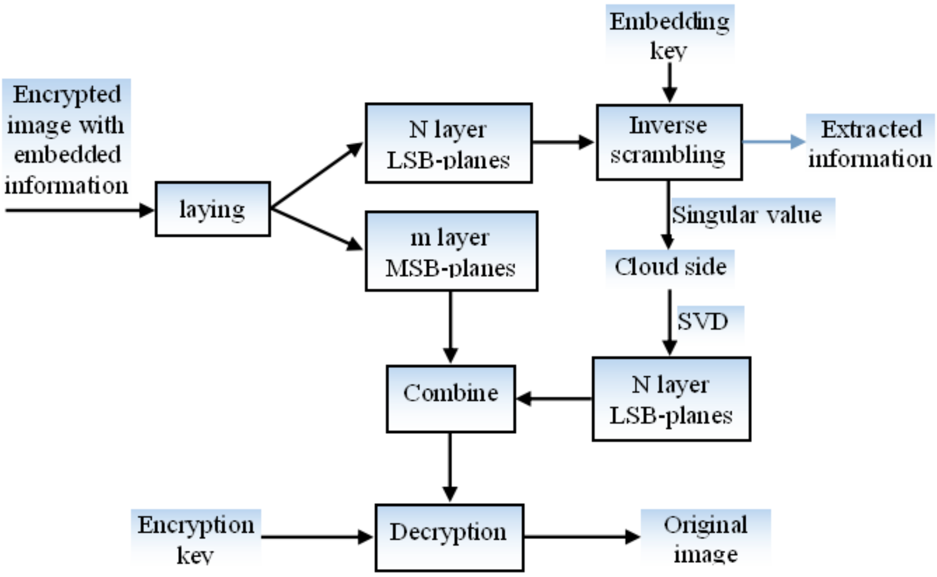


Figure 4. The Third Kind of Circumstance

4. Experiments and Analysis

4.1. Experiment Results

We choose 4 gray images with size as the test image, they are shown in Figure 5, and we finish the simulation experiment by matlab2012.

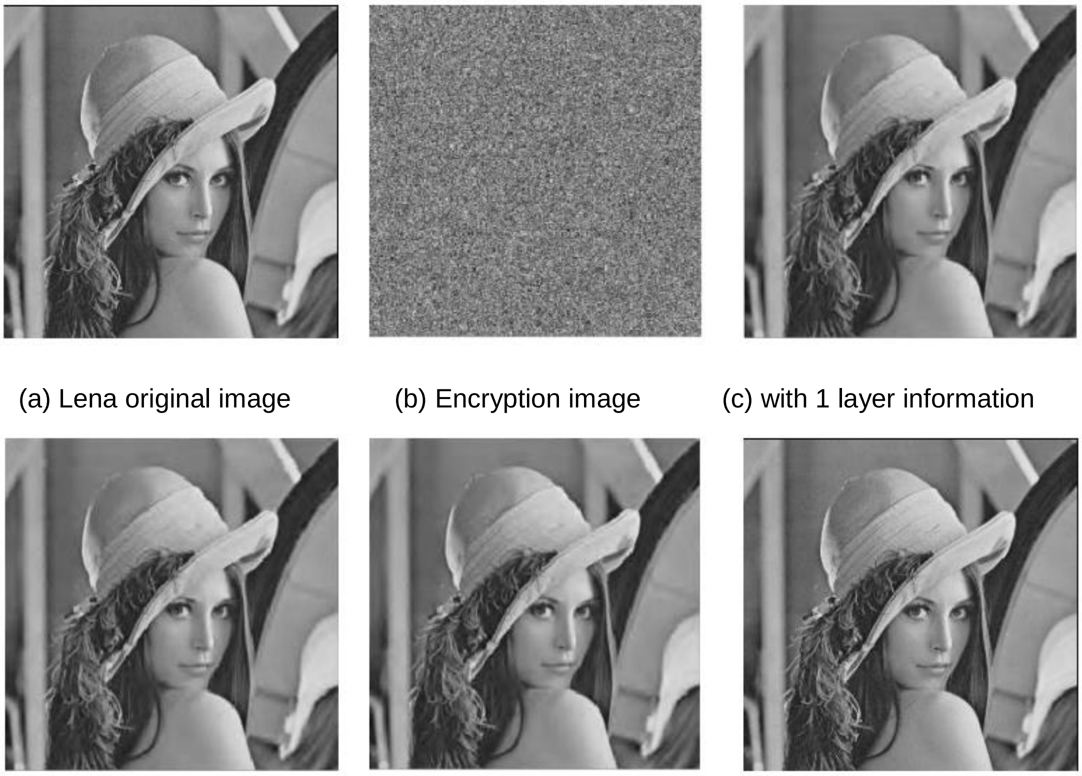
(a) Lena

(b) baboon

(c) boat (d) barbara

Figure 5. Four Standard Test Images

Take the Lena image as example, the result is shown in Figure 6, (a) is the original image of Lena, (b) is encryption image, (c) is the decrypted image in the case of block size and including 1 layer bit embedding information, PSNR value is 51.2132dB, (d) is the decrypted image in the case of block size and including 2 layers bit embedding information, PSNR value is 44.1732dB, (e) is the decrypted image in the case of block size and including 3 layers bit embedding information, PSNR value is 37.9493dB, is the recover image after extracting information.



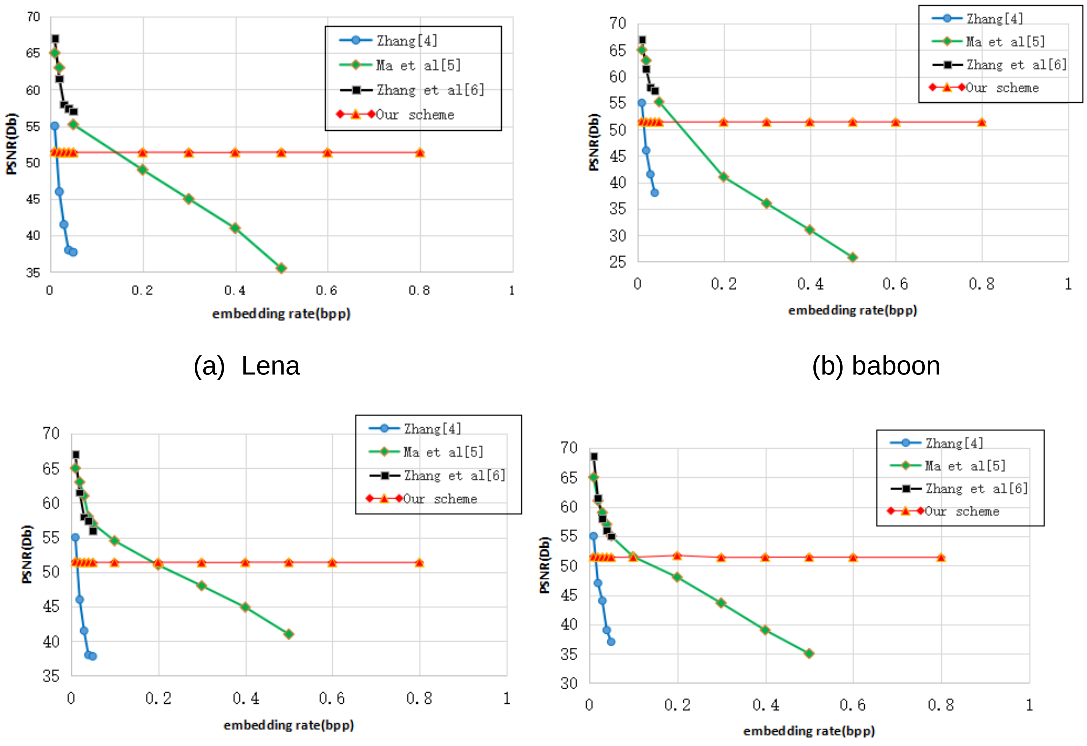
(a) Lena original image (b) Encryption image (c) with 1 layer information

(d) With 2 layers information (e) with 3 layers information (f) recover image

Figure 6. Different Stages Lena Image

Generally, when the PSNR value is more than 39dB, the image has Good visual effect. We choose 1 layer, 2 layers, 3 layers to embed information, PSNR average values in sequence are 51dB, 44dB, 38dB. As the Figure 6 shows, the scheme we proposed can keep the visual characteristics of the original image, and meet the requirements of visual invisibility for embedded information as well.

Compare the scheme we proposed with scheme [4], [5] and [6], the embedding rate (bpp) and corresponding PSNR changes use 4 test images are shown in Fig 7, from the diagram we can see that with the increase of embedding rate, the PSNR value will be significantly lower, by the time the embedding rate is close to 0.5,PSNR value of scheme[5] is lower than 40dB(embedding rate of scheme [4]and [5] cannot reach to 0.5), but the PSNR value of scheme we proposed is about 51dB. The reason is we can use the restore dictionary which store in the cloud side to refactoring cipher text image, when we embed information, we can embedded only choose the least significant bit LSB of cipher image. So in guarantee of embedding capacity increases do not causing PSNR value decreased obviously at the same time.



(a) Lena

(b) baboon

(c) boat

(d) barbara

Figure 7. Our Scheme Embedding Rate and the Corresponding PSNR Compared with Other Solutions

The embedding capacity of our scheme is bits when we choose the 1 layer plane and block size, with the layer and the block size growth, the embedding capacity will growth either, the top embedding capacity can reach bits, but at the same time , the PSNR value decline.

The cipher image information hiding scheme at present [2-6] exist three problems (1) cannot guarantee a complete recovery; (2) with the increasing of embedding capacity, PSNR will fell sharply, embedding capacity is lower. Experimental results show that our scheme will not lead to PSNR decreases obviously when increase the embedding capacity, and when the embedding rate is larger than 0.5, PSNR is significantly higher than the other schemes. Meanwhile, our scheme can choose different block size and different layer plane, so we can adjust the embedding capacity flexibility.

4.2. Security Analysis

For the first case, the receiver only has encryption key of, can only recover the main information of image, the receiver has no embedding key, so cannot extract the embedding information, and cannot recover original image. For the second case, receiver has only embedding key of, can only extract the embedding information, and cannot recover the main information of original image. For the first case, the receiver use the embedding key to extract the embedding information, and send the recover SVD to the cloud side to get the after three LSB-planes, then combine with the 5 layers of MSB – planes, finally recover the original image use the encryption key of . Therefore, the original image recovery is controlled together by encryption key and embedding key, the recovery of image and information extraction can be separated.

5. Conclusion

Based on SVD, this paper presents a cloud computing security application oriented reversible image cipher domain information hiding scheme. Compared with literature [4-6], the embedding capacity has increased significantly, and it is separable for the extraction of embedded information and recover image, it has a certain practical meaning. And because of the Information hider and the cloud, the receiver and the cloud, are only related to the original cipher image, and the cloud cannot obtain encryption keys, so the image content of privacy can be guaranteed.

References

[1] Z. Yan, Z. MingQing and W. JiaJia, “Histogram pairs based large capacity information hiding algorithm[J]”, Application Research of Computers, vol. 30, no. 7, **(2013)**, pp. 2108-2110, 2123.

[2] Z. Xinpeng, “Reversible data hiding in encrypted images[J]”, IEEE Signal Processing Letters, vol. 18, no. 4, **(2011)**, pp. 255-258.

[3] H. Wien, C. Tungshou and W. Hanyan, “An improved reversible data hiding in encrypted images using side match[J]”, IEEE Signal Processing Letters, vol. 19, no. 4, **(2012)**, pp. 199-202.

[4] Z. Xinpeng, “Separable reversible data hiding in encrypted image[J]”, IEEE Trans on Information Forensics and Security, vol. 7, no. 2, **(2012)**, pp. 826-832.

[5] M. Kede, Z. Weiming and Z. Xianfeng, “Reversible data hiding in encrypted images by reserving room before encryption[J]”, IEEE Trans on Information Forensics and Security, vol. 8, no. 3, **(2013)**, pp. 553-562.

[6] Z. Weiming, M. Kede and Y. Nenghai, “Reversibility improved data hiding in encrypted images[J]”, Signal Processing, vol. 94, **(2014)**, pp. 118-227.

[7] X. Di and D. She, “Reversible watermarking algorithm for encrypted image based on histogram difference shifting[J]”, Application Research of Computers, vol. 31, no. 12, **(2014)**, pp. 3668-3672.

[8] C. Ning and M. Hui-jie, “Robust dual-watermarking algorithm based on Contourlet and SVD[J]”, Application Research of Computers, vol. 29, no. 7, **(2012)**, pp. 2700-2702.

[9] Z. Wen-quan, X. Xiang-guang and Y. Ai-min, “Color image watermarking algorithm based on singular value decomposition[J]”, Application Research of Computers, Application Research of Computers.

[10] F. Wang-sheng and Z. Rong, “DWT-SVD based adaptive color image watermarking[J]”, Application Research of Computers, vol. 29, no. 11, **(2012)**, pp. 4323-4326.

[11] C. Yi-jia and N. Yu-gang, “Blind watermarking algorithm for color images based on DWT-SVD and Fibonacci transformation[J]”, Application Research of Computers, vol. 29, no. 8, **(2012)**, pp. 3025-3028.

[12] Z. Li-hong and W. Yong-jun, "Research of color image watermarking algorithm based on biorthogonal lifting wavelet and singular value decomposition[J]", Application Research of Computers, Application Research of Computers, vol. 31, no. 2, **(2014)**, pp. 568-570,575.

[13] Z. Guang and Z. Jun-liang, "Adaptive robust watermarking algorithm based on SVD and wavelet packet transform[J]", Application Research of Computers, vol. 30, no. 4, **(2013)**, pp. 1230-1233.

[14] W. Xi-yu and Y. Xiao-mei, "Single value decomposition based compressed sensingMRI reconstruction algorithm[J]", Application Research of Computers, vol. 30, no. 4, **(2013)**, pp. 1247-1249,1252.

[15] L. Da-jin, "Multiple watermarks algorithm based on nonsubsampled Contourlet transform and singular value decomposition[J]", Application Research of Computers, vol. 30, no. 12, **(2013)**, pp. 3850-3853.

[16] Image database [EB/OL].http://sipi.usc.edu/database/.

[17] X. Di, L. Xiaofeng and W. Pengcheng, "Analysis and improvement of a chaosbased image encryption algorithm [J], Chaos Solitons Fractals, vol. 40, no. 5, **(2009)**, pp. 2191-2199.

Author

Zhang Jing, born in 1973, associate professor. Her research interests include image processing, information security, data encryption, and data retrieval.