An Improved Method for LSB Based Color Image steganography Combined with Cryptography

[1]Xinyi Zhou, [2]Wei Gong, [3]WenLong Fu, [4]LianJing Jin
[1,2,4]Information Engineering School, Communication University of China,CUC
[1,3]Neuroscience and Intelligent Media Institute, Communication University of China
Beijng, China
xinyi_M@126.com

***Abstract*—In this paper, an improved LSB information hiding algorithm of color image using secret key is be proposed, combining information hiding and cryptography, increasing the human eye visual features, and the identity authentication based on digital signature and encryption technology to improve the security of information hiding. Finally through the experiment and the comparison of the peak signal-to-noise ratio (PSNR) and safety, the improved LSB image steganography algorithm using the encryption technology is better than general LSB image steganographic method with better security and higher PSNR.**

Keywords—image hiding; information security; secret key; LSB; encryption;

I. Introduction

As to the attention of the network information security problem, the application of network information security technology has been further research. As cornerstones of security mechanism, the cryptography method, in a certain extent, meet the part requirement of information security, but today the traditional cryptography method has not suitable for solving the problems of the multimedia aspects, in order to better solve the problem of multimedia information security, information hiding learning arises at the historic moment. Nowadays information hiding as main means in some areas such as secure communications, protection of intellectual property rights and content authentication, has been widely studied and applied.

Image information as the main source for people obtaining information from the world, and associated information hiding technology is increasingly becoming an important research field of information security [1]. Among them, the least significant bit (LSB) embedding algorithm because of its features such as simple algorithm, encryption fast, easy to implement, a large amount of hidden, although it is one of the most common algorithm [2], still occupies an important position in the field of information hiding and LSB algorithm and its derived algorithm are mostly used on the Internet common steganography software.

This paper is on the improved LSB color image steganalysis algorithm [3] combined with human visual characteristic, entered into the key ideas of cryptography and RSA algorithm of public key encryption system for further enhancing the LSB algorithm security and application in color image.

II. Cryptography and Steganography

Essence of cryptography method is by upsetting the information content, make it look like random code to achieve the purpose of protecting information content. Information hidden technology is the study of how to hide certain information in another public information, and then to pass hidden information by transferring public information [4]. The technology of information security which is based on cryptography and information security which is based on steganography, is not contradictory and competing with each other but rather complementary. This article is a cryptography and information hiding techniques combined.

A. RSA Algorithm

In this paper, we use the RSA public key cryptosystem, which is the first public key algorithm which can be used in digital encryption and digital signature [5]. It has the advantages of easy to understand and easy to operate. The mathematical theory of RSA algorithm is based on a composite number with large number factors is decomposed into two prime numbers is very difficult. In this paper, we use the digital signature system of RSA to authenticate and strengthen security. We should first sign and then encrypt in the realization process [6].

B. Least Significant Bit

Least significant bit (LSB) algorithm used in this paper is a spatial domain steganography in substitution method, the principle is to replace information in the least bit of cover image with confidential information. For 256 gray scale cover image, the gray scale value of each pixel can be used to represent 8-bit binary, taken out a certain bit of all pixels constitute a certain bit plane, for example, the least significant bit of all the pixels constituting the least significant bit plane. The higher the bit plane, the greater the contribution of the gray value, and the lowest bit plane is similar to random noise [7]. As shown in Figure 1, it is the eight bit plane of Lena gray image.

978-1-5090-0806-3/16/$31.00 copyright 2016 IEEE
ICIS 2016, June 26-29, 2016, Okayama, Japan

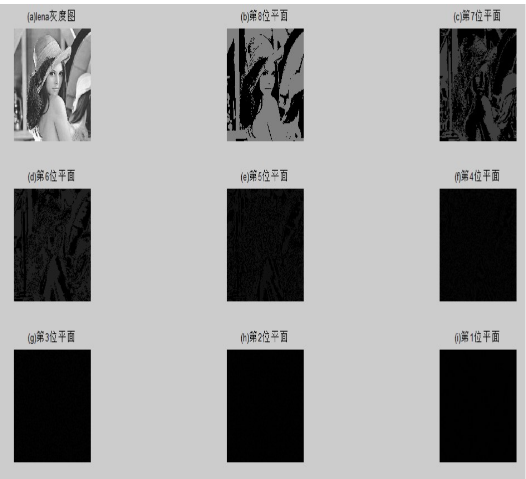


Fig. 1. Bit plane decomposition of Lena gray scale image

C. Peak Signal-to-Noise Ratio

In the objective evaluation method, the most commonly used index is the peak signal to noise ratio (Signal to Noise Ratio Peak, PSNR) [8]. In the calculation of PSNR, we must first calculate the Square Error Mean (MSE) between the hidden image and the cover image. The equation is represented as below.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(c_i - s_i)^2 \tag{1}$$

C_i and S_i respectively represent the i pixel of the cover image and the hidden image, N for the total number of pixels. Then use the MSE to get the PSNR value of the hidden image as follows, the unit is dB:

$$PSNP = 10\lg\left(\frac{255^2}{MSE}\right) \tag{2}$$

Generally speaking, the larger the value of PSNR, the more similarity between the hidden image and the cover image. In experience, the quality of the image is acceptable if the PSNR value is higher than 28dB .

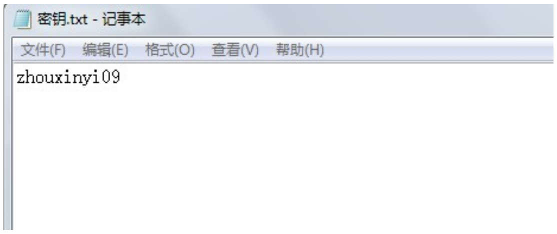
III. PROPOSED METHOD FOR LSB BASED COLOR IMAGE STEGANOGRAPHY COMBINED WITH CRYPTOGRAPHY

We start with the improvement of the randomness of the LSB embedding position, and encrypt the message which control embedded position, so the hidden information can not be extracted without the corresponding private key. In order to prevent the forgery of the hidden information, we also add a digital signature to authenticate, only the right sender just to extract the hidden information. Through this encryption technology for embedding position of the random LSB, original algorithm has greatly improved its security.

We choose to hide a gray image in a color image, in which the size of the cover color image is 256*256, the size of the gray image is 90*90. As shown in Figure 2.

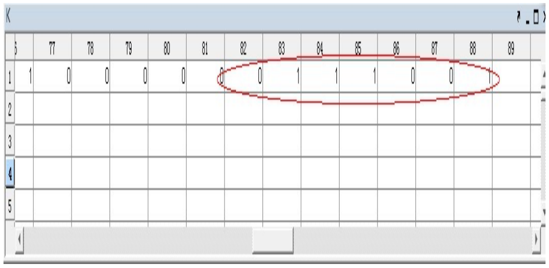
Fig. 2. The cover image and the secret image

First, we generate the control messages which determine the embedding position. This message can be a sequence of random values, or can be any combination of letters, numbers, and symbols set by us. In the experiment, the control message is set to zhouxinyi09, like Figure 3. Control messages firstly convert to bit stream before indicating the embedding of the secret message. As shown in Figure 4.



zhouxinyi09

Fig. 3. The control message



	6	77	78	79	80	81	82	83	84	85	86	87	88	89
1	1	0	0	0	0	0	0	1	1	1	0	0	1	
2														
3														
4														
5														

Fig. 4. The bit stream of control message

The sender for control messages do sign first and then encrypt with RSA algorithm. Some online source code can be used to generate a public key and private key for encryption and decryption. When the sender sends a control message M, first with his own private key d1 to encrypt the message to produce the ciphertext d1 (M), then with the recipient's public key e2 to do second encryption generating ciphertext e2 (d1 (M)). After the recipient receives the ciphertext, first with his private key to decrypt d2 for the first time, restore the ciphertext d1 (M), that is d2 (e2 (d1 (M))) = d1 (M), and then with sender's public key e1 to do second decryption getting the control message M, that is e1 (d1 (M)) = M.

Then we use control information for image information hiding. A 24 bit RGB color image can be divided into three matrix which are two-dimensional , namely the Red matrix, Green matrix, Blue matrix, like figure 5. Figure 6 is the Green matrix.

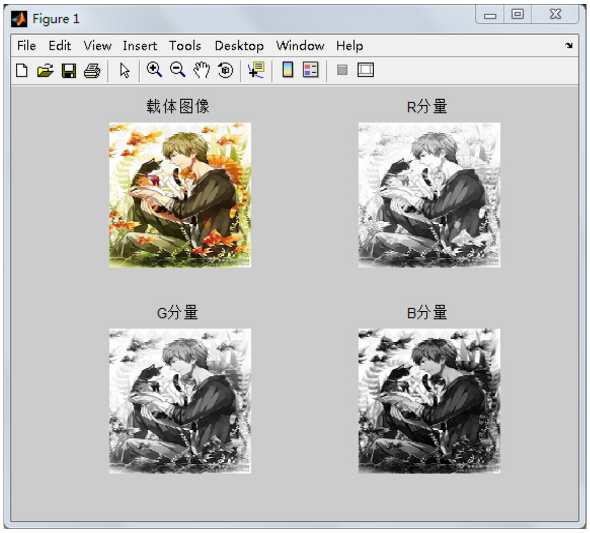
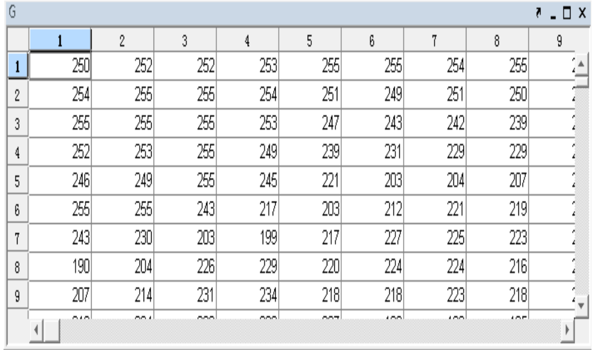


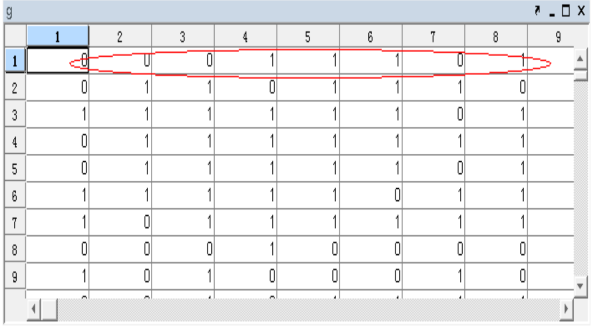
Fig. 5. The color image into the Red, Green, Blue of the three matrix



	1	2	3	4	5	6	7	8	9
1	250	252	252	253	255	255	254	255	
2	254	255	255	254	251	249	251	250	
3	255	255	255	253	247	243	242	239	
4	252	253	255	249	239	231	229	229	
5	246	249	255	245	221	203	204	207	
6	255	255	243	217	203	212	221	219	
7	243	230	203	199	217	227	225	223	
8	190	204	226	229	220	224	224	216	
9	207	214	231	234	218	218	223	218	

Fig. 6. Green matrix

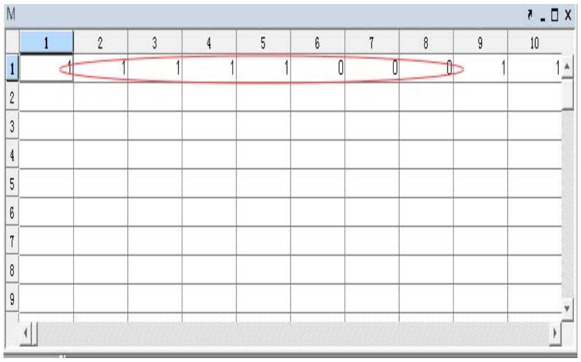
Data of each matrix can be represented by a decimal number between 0 to 255, further more the value of each pixel can be represented by a binary number with 8 bit. Then each component can take out the least bit from all pixels to compose the same size matrix which the value is 0 or 1, so that you can get the three matrix composed of the least bit from Red matrix, Green matrix and Blue matrix. Figure 7 is the matrix composed of the least bit of G matrix.



	1	2	3	4	5	6	7	8	9
1	0	0	0	1	1	1	0	1	
2	0	1	1	0	1	1	1	0	
3	1	1	1	1	1	1	0	1	
4	0	1	1	1	1	1	1	1	
5	0	1	1	1	1	1	0	1	
6	1	1	1	1	1	0	1	1	
7	1	0	1	1	1	1	1	1	
8	0	0	0	1	0	0	0	0	
9	1	0	1	0	0	0	1	0	

Fig. 7. the matrix composed of the least bit of G matrix

At the same time, the secret information (text messages or images) should be transformed into the binary bit stream, which is convenient for embedding,like figure 8.



	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	0	0	0	1	1
2										
3										
4										
5										
6										
7										
8										
9										

Fig. 8. The bit stream of secret information

According to the characteristics of human vision [9], we know that the sensitivity of three components of the color image is different, the most sensitive to green, followed by the red, the least sensitive to blue. So we use the least bit of Green do XOR with original control information and embed in Red and Blue, but not in the Green, as possible to ensure the visual effect of original color image. After a least bit of Green doing XOR with a bit from the bit stream of control information, if the result is 1, we choose the bit in the same position of Red to replace, and if the result is 0, we select Blue to replace. Repeat the process until all the hidden information is embedded.

Figure 9 is to contrast the image after embedding the hidden information with the original image , it can be seen that the human eye can not distinguish the existence of hidden information. Further more, from the comparison of Figure 10, we can see that the histogram of them are basically the same.

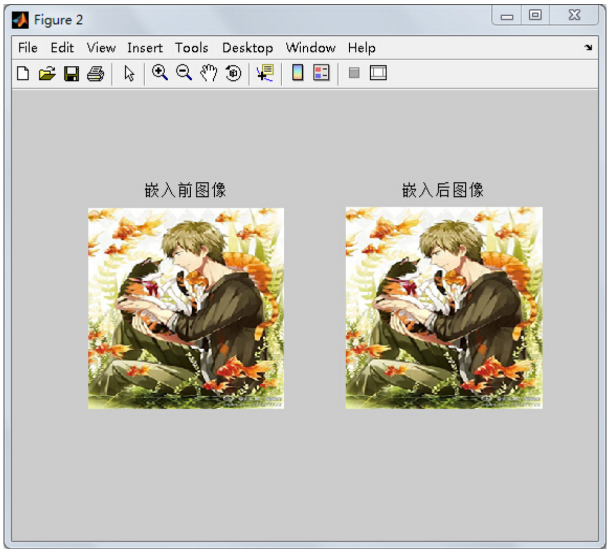


Fig. 9. the image after embedding with the original image

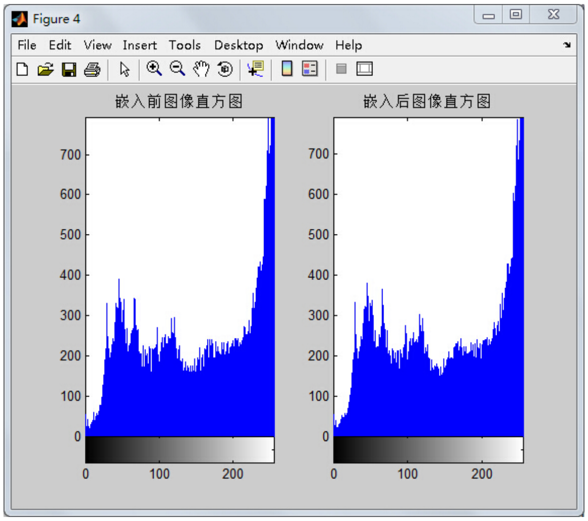


Fig. 10. Histogram comparison

IV. Results

We contrast the improved LSB algorithm in this paper with traditional LSB algorithm from two aspects including the peak signal-to-noise ratio (PSNR) and the security.

A. PSRN

In the traditional LSB algorithm applied in color image, we respectively replace the secret information in Red, Green and Blue. Calculate its PSNR, and make a compare with the PSNR of method in this paper. The results are displayed in Table I.

TABLE I. COMPARISON PSNR WITH TRADITION LSB METHOD AND OUR LSB MATHOD

	algorithms			
PSNR	***Red***	***Green***	***Blue***	***Ours***
	53.621	53.567	53.396	56.513

It can be seen that the PSNR value of our method is more than 3dB compared with the traditional LSB, which is greatly improved.

B. The Security

From our proposed method can be seen that if the attacker intercept the camouflage pictures and control information (has been encrypted), even know the secret information is embedded in the image, the attacker will not be able to know the exact location of hiding information because can not decrypt the control information without private key. At the same time, the identity authentication mechanism is added to the control message, which can prevent the forgery of the hidden information. Image with hidden information for unauthorized users is unknown and forged can be found, which improves the security of information hiding.

V. Conclusion

The image hiding method in this paper combine the cryptography and information hiding. On the one hand, by using information hiding does not change the visual characteristic of cover image, we can embed secret information in another public image and transfer. On the other hand, by using digital signature and encryption technology of cryptography , we can make the unauthorized users can not know the location of the embedded secret information, so that the secret information can not be extracted. The effective combination of the above two means further improves the security of information hiding. We select encrypt the control message which determines the embedding position rather than the image or messages to hide because the process of the former is more simple, on the other hand the former also ensures the visual characteristics of the embedded information. In this paper, we improve the security on the basis of the traditional LSB information hiding, and join the identity authentication to prevent the forgery of hidden information. But there is no further research on the steganalysis. In the future, for improving this method, we must continue to study the related analysis of the hidden.

Acknowledgment

We would like to thank the National Key Science & Technology Pillar Program of China (The key technology research of public digital culture sharing service, 2015BAK25B03); and The Engineering Program Project of CUC, 3132014XNG1435, 3132015XNG1521.

References

[1] Zhang Yanling, Wang Yunfeng robustness analysis LSB image hiding algorithm [J] chaotic sequence enhanced Xi'an Technological University, 2015,10: 850-854.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Yan Xiaomeng Zhang Tao, Xi Ling, PING Xi build one for LSB matching steganography load new positioning algorithm [J] data acquisition and processing, 2016,01: 145-151.K. Elissa, "Title of paper if known," unpublished.

[3] S. M. Masud Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on, Dhaka, 2011, pp. 286-291.

[4] Stefan Katzenbeisser, Fabien AP.Petitcolas (a), the new Charles Ng, NIU Xin-xin, xian, etc. (translation) information hiding - steganography and digital watermarking [M] Beijing: People's Posts and Telecommunications Press, 2001,50-62.

[5] Huang Jian .RSA safety analysis and improvement of public key encryption system [J] computer and network, 2016,01: 70-73.

[6] Paragraph Hongying, Shaoze Yun, Cao Jianying RSA digital signature technology and safety research [J] Longdong College, 2015,01: 38-40.

[7] Zhang Haitao, YEW Suet, Chen Hongyu, Zhang Ye bit planes and HVS information hiding algorithm [J]. Chinese Journal of Image and Graphics, 2013,12: 1559-1566.

[8] Li Li. Study [D] based on the LSB information hiding technology, Beijing University of Posts and Telecommunications, 2011.

[9] Yang Zhenya, Wang Yong, vector Yang Zhendong, Wang Tao RGB color space - from the perspective of color difference formula [J]. Computer Engineering and Applications, 2010,06: 154-156.