Research on Reversible Watermarking Algorithms in Image Encryption Domain Based on ZUC Algorithms

Shuai Lian[a], Haiyang Ding[b, *] and Zichen Li[c]

College of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China

[a]904347410@qq.com, [b]13810284215@163.com, [c]lizc2020@163.com

*Corresponding author

Keywords: Image encryption, ZUC stream cipher, reversible watermark, image recovery

Abstract: This paper designs and implements an image encryption domain reversible watermarking algorithm based on ZUC stream cipher. The content owner encrypts the carrier image with ZUC encryption algorithm. The watermark embedder uses the LSB method to embed the watermark information, and the receiver first decrypts the encrypted image containing the embedded watermark. Then, according to the spatial correlation of natural images, the smoothness of each image block in each group is compared to find the modified image block, thereby realizing correct extraction of watermark information and image recovery. The simulation results of MATLAB show that the algorithm is simple, novel, and has high efficiency, and has high PSNR value and NC value.

1. Introduction

With the rapid development of information technology and the popularity of Internet technology in life, the content format of traditional media has gradually changed to digital. Digital technology makes it very convenient to store and propagate some multimedia data such as images, audio, video and text. [1].Copyright infringement, content tampering and other illegal activities have become easier, the copyright, integrity and validity of digital works are not guaranteed, which seriously damages the interests of the owner of the work, so how to implement effective copyright protection in the network environment and Information security means have become an urgent real problem [2].

Digital watermarking [3-4] is a hot topic in the field of information security. Reversible watermarking can not only extract secret information from the confidential image, but also reduce the carrier image without loss. The existing encryption domain reversible watermark hiding methods can be divided into four categories: (1) no processing before encryption, by simply modifying part of ciphertext data to embed information [5-8]; (2) compressing ciphertext data to Make room for additional information [9-11]; (3) pre-process the encrypted image, reserve space for information embedding [12-15]; (4) encrypt the carrier data with public key mechanism, use encryption The homomorphism of technology embeds information [16]. Generally, reversible watermarking in encrypted domain adopts a simple encryption method and has potential security problems. Using ZUC algorithm to encrypt digital image can not only ensure the security of image encryption transmission, but also reduce the complexity of the encryption algorithm.

2. Related Information

2.1 ZUC stream cipher

ZUC is a stream cipher algorithm named after the initials of ZU Chong Zhi, a famous mathematician in ancient China. It is called ZUC algorithm in Chinese. ZUC algorithm is the core of 3GPP confidentiality algorithm EEA3 and integrity algorithm EIA3. Its function is to generate keys for encryption and decryption. The process of encryption at the sender is that the key generated by ZUC algorithm is bit-exclusive or the input plaintext is bit-exclusive, the process of decryption at the receiver is that the input ciphertext is bit-exclusive or the same key as the above-mentioned encryption process, and the decryption can be realized. ZUC algorithm logically adopts three-tier structure design [17]. As shown in Fig.1, the functional structure of the ZUC algorithm is shown. The upper layer is a linear feedback shift register (LFSR). Each register of LSFR is 31bit. The middle layer of ZUC algorithm is bit reorganization (BR), which realizes data conversion from LFSR data unit to non-linear function F and key output Z, as shown in Fig.1. The high 16 bits of LFSR's corresponding registers and the low 16 bits of the corresponding registers are reassembled into four 32 bits of data for the use of the non-linear function F and the key output Z. The lower level of ZUC algorithm is nonlinear function F. In the design of nonlinear function F, ZUC algorithm draws lessons from the design techniques of block cipher, using S-box and linear transformation L with high diffusion characteristics.

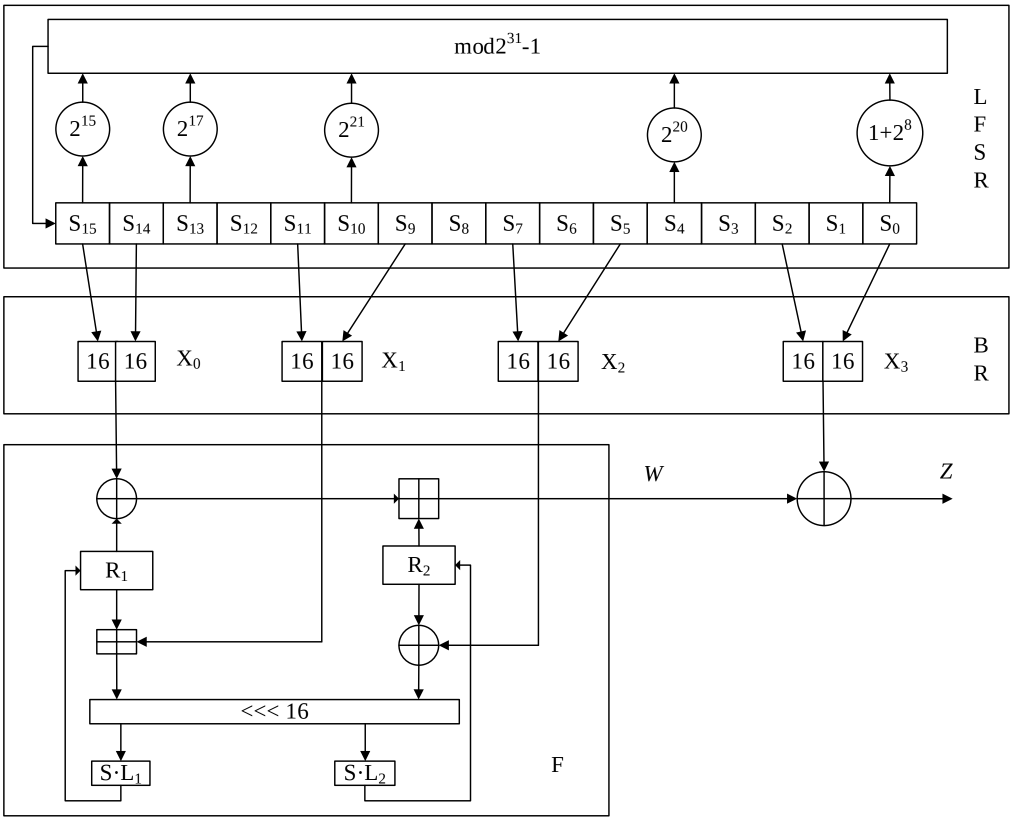

Figure 1. ZUC algorithm architecture

2.2 LSB Watermarking Algorithm

The LSB algorithm is the first proposed spatial domain information hiding algorithm. It uses a specific encryption key to generate a random signal through a pseudo-random sequence generator, then arranged according to certain rules into a two-dimensional watermark signal, and embedded in the lowest significant bit of corresponding pixel values of the original image. Since the watermark signal is hidden at the lowest significant bit, it is equivalent to superimposing a weak signal, so visually difficult to detect. As a method of information hiding for large data volumes, LSB still occupies a very important position in hidden communication.

2.3 Image Encryption Technology

Digital image is one of the most popular multimedia forms, and it is widely used in politics, economy, national defense, education, etc. Digital images have high confidentiality requirements for certain special areas such as military, commercial and medical. In order to achieve digital image secrecy, in practice, the two-dimensional image is generally converted into one-dimensional data, and then encrypted by a conventional encryption algorithm. Unlike ordinary text information, images are temporal, spatial, visually perceptible, and lossy compression is also possible. These features make it possible to design more efficient and secure encryption algorithms for images. Since the 1990s, researchers have used these features to propose a variety of image encryption algorithms. To sum up, the concept of image encryption technology is a technology that uses the characteristics of digital images to design encryption algorithms to improve the security and computational efficiency of encryption.

2.4 Reversible Watermarking

Digital watermarks will get different classification results according to different classification criteria [24]. According to the embedded watermark information, whether the original carrier can be recovered without damage can be divided into two categories: reversible watermark and irreversible watermark [25]. The reversible watermark is also called lossless watermark. Not only the embedded watermark information can be completely extracted, but also the original carrier can be recovered completely without damage after the watermark is extracted [26]. This technology is generally used for integrity verification, lossless recovery, etc. of multimedia work, it is widely used in digital images with high security, high security and high precision, such as medical images, military images, electronic invoices, legal documents and so on.

3. Design of Reversible Image Watermarking Algorithms in Image Encryption Domain Based on ZUC Algorithms

3.1 Algorithm Introduction

The basic framework of the algorithm is shown in Fig.2. First, the content owner uses ZUC algorithm to encrypt the original carrier image and get the encrypted image. Secondly, after the watermarking embedder gets the encrypted image, the LSB method is used to embed the image watermarking information into the encrypted image, and the encrypted image containing the watermarking information is obtained. Finally, the recipient uses ZUC algorithm to decrypt the image to get the decrypted image containing the watermarking information, and then recovers the image and extracts the watermarking information.

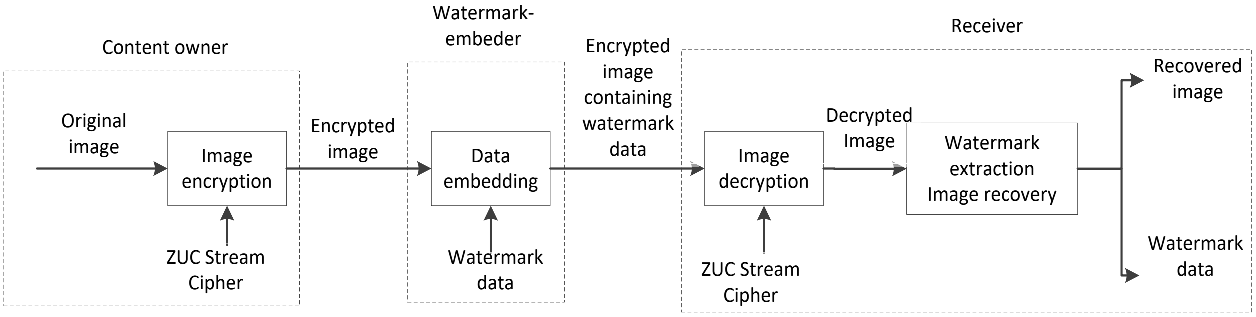

Figure 2. The frame of Watermark embedding system

3.2 Image Encryption

For an uncompressed grayscale image, the value range of any 1 image pixel $p_{i,j}$ is [0,255], (i, j) indicates the position of the pixel in the block, and $p_{i,j,k}$ can be represented by 8 bits. Let the bit of each pixel be $b_{i,j,1}, b_{i,j,2}, \ldots b_{i,j,7}$

$$b_{i,j,k} = [\frac{p_{i,j,k}}{2^k}] \bmod 2, \quad k=0,\ 1,\ldots..,7 \tag{1}$$

$$p_{i,j,k} = \sum_{k=0}^{7} b_{i,j,k} \bullet 2^k \tag{2}$$

Where [•] means rounding down, The content owner uses ZUC algorithm to generate a pseudo-random bit stream $r_{i,j,k}$, and performs XOR operations bit by bit with each bit $b_{i,j,k}$ of the image pixel.

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \tag{3}$$

The resulting $B_{i,j,k}$ is the result of image pixel $p_{i,j,k}$ encryption. The encrypted image is then transferred to the watermarking embedder.

3.3 Watermark Information Embedding

For encrypted information, even if the watermark embedder does not know the content of the original image, he can still embed the watermark information into the image by modifying a small part of the encrypted information. Firstly, the watermark embedder divides the encrypted image into several non-overlapping blocks of size $s \times s$. In other words, the encryption bit $B_{i,j,k}$ in the same block satisfies $(m-1)\bullet s+1 \le i \le m\bullet s$, $(n-1)\bullet s+1 \le j \le n\bullet s$ and $0 \le k \le 7$ (m and n are positive integers). Thus, each block will be used to carry 1 additional bit. For each block, the watermark embedder randomly divides the s^2 pixels into S_0 and S_1. Here, the probability that each pixel belongs to S_0 and S_1 is 1/2. If appended as embedded 0, flip the 3 least significant bits of the secret pixel in each S_0:

$$B'_{i,j,k} = \overline{B_{i,j,k}}\,,\ (i,j) \in \mathrm{S}_0,\ \ k\text{=}0,\ 1,\ 2 \tag{4}$$

If appended as embedded 1, flip the 3 least significant bits of the secret pixel in each S_1:

$$B'_{i,j,k} = \overline{B_{i,j,k}}\,,\ (i,j) \in \mathrm{S}_1,\ \ k\text{=}0,\ 1,\ 2 \tag{5}$$

Other embedded information has not changed.

3.4 Watermark Information Extraction and Image Recovery

When receiving an encrypted image containing embedded information, the receiver first generates a key, and calculates the XOR of the received information and $r_{i,j,k}$ to obtain a decrypted image. We use $b'_{i,j,k}$ to indicate the decryption bit. Obviously, the original 5 most significant bits are correctly restored. For a certain pixel, if the embedding bit of the pixel in the image block is 0 and the pixel belongs to S_1, or the embedding is 1 and the pixel belongs to S_0. Then this data hiding will not affect any encryption bits of the pixel. So the least significant bit of the decryption must be the same as the original least significant bit. This means that the decrypted gray value of the pixel is correct. On the other hand, if the embedding bit in the pixel block is 0 and the pixel belongs to S_0, or the embedding bit is 1 and the pixel belongs to S_1, The least significant bit of this decryption is:

$$b'_{i,j,k} = r_{i,j,k} \oplus B'_{i,j,k} = r_{i,j,k} \oplus \overline{B_{i,j,k}} = r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} = \overline{b_{i,j,k}}\ , k=0,1,2 \tag{6}$$

This means that the 3-bit decrypted least significant bit must be different from the original least significant bit, in which case:

$$b'_{i,j,k} + b_{i,j,k} = 1,\ k=0,1,2 \tag{7}$$

Therefore, the sum of the decimals of the decrypted 3 least significant bits and the original 3 least significant bits is 7, and the error average energy of the decrypted and original gray values is

$$E_A = \frac{1}{8}\sum_{u=0}^{7}[u-(7-u)]^2 = 21 \tag{8}$$

The probability of LSB decryption error is 1/2, when reconstructing an image using the decrypted data, the value of PSNR in the decrypted image is approximately

$$PSNR = 10\log_{10}\frac{255^2}{\frac{E_A}{2}} = 37.9dB \tag{9}$$

The receiver extracts the embedded bits from the encrypted image and restores the original content. With the information hiding key, he can split the decrypted image into blocks and divide the pixels in each block into two groups in the same way. For each decrypted block, the receiver flips the 3 least significant bits of the S_0 pixel to form a new block, and flips the 3 least significant bits of the pixel in S_1 to form another new block. We denote these two new blocks as H_0 and H_1. One of H_0 and H_1 must be the original image block, and the other block is seriously interfered with by LSB flipping. For two image blocks of size $s\times s$, define a function that measures the smoothness of the image block

$$c_1 = \sum_{u=2}^{s-1}\sum_{u=2}^{s-1}\left| p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4} \right| \tag{10}$$

$$c_2 = \sum_{u=1}^{s}\sum_{v=1}^{s-1}\left| p_{u,v} - p_{u,v+1} \right| + \sum_{u=1}^{s-1}\sum_{v=1}^{s}\left| p_{u,v} - p_{u+1} \right| \tag{11}$$

$$f = c_1 + c_2 \tag{12}$$

In the above formula, $P_{u,v}$ is the pixel value in the square, and (u,v) is the position of the pixel in the block.c_1 represents the difference between the center position pixel and its predicted difference, and c_2 represents the difference between adjacent pixels. The smoothness of H_0 and H_1 is represented by f_0 and f_1, respectively, due to the spatial correlation of natural images due to natural images. The smoothness of the image after modification is less than before modification, therefore, the receiver can perform information extraction and image restoration by comparing f_0 and f_1. If $f_0 < f_1$, then view H_0 as the original content of the image block and let the extracted position set to 0, Otherwise H_1 is the original content of the block and the extracted bits are 1. Finally, the extracted bits are concatenated to recover the watermark information and collect the recovered image blocks to form the original image.

The correlation coefficient is used to characterize the correlation between the original image and the recovery image. The formula is as follows:

$$NC = \frac{\sum_{i,j} p_{i,j} p'_{i,j}}{\sum_{i,j} p^2{}_{i,j}} \tag{13}$$

In the above formula, $p_{i,j}$ and $p'_{i,j}$ represent a pixel point of the original image and the recovery image with coordinates (i, j), respectively.

4. Analysis of Results

In this experiment, a Lena grayscale image with a size of 512 pixels and 512 pixels was used as the original carrier image as Fig.3. Fig.4 is an encrypted image obtained by encrypting with an encryption key. Subjectively, the human visual system has been unable to obtain any content of the original image from the encrypted image, such as edge information, important textures, etc. Fig.5 is a watermark of 64 pixels and 64 pixels to be embedded. Here, s=8, embed watermark information in the encrypted image using the embedded key, and the encrypted image containing the watermark information is shown as Fig.6.

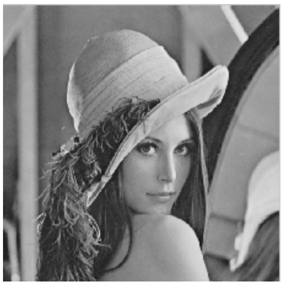

Figure 3. Original image

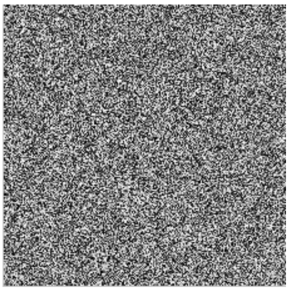

Figure 4. Encrypted image

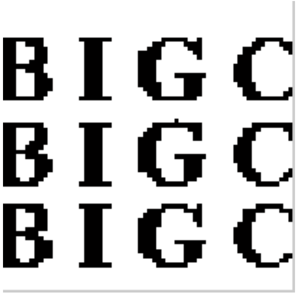

Figure 5. Watermark information

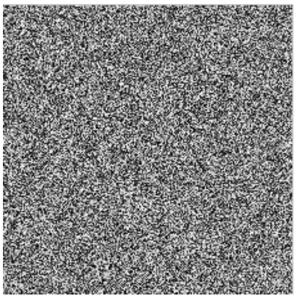

Figure 6. Encrypted image containing watermark information

After receiving the encrypted map containing the watermark information, the receiver first decrypts the image by using the encryption key to obtain a decryption image containing the watermark information as shown in Fig.7. Its PSNR is 37.9 dB. The embedded watermark is successfully extracted from the decrypted image by using the embedded key, and the original image is completely recovered. The extracted watermark and recovered image are shown in Fig.8, Fig.9 and the PSNR of the recovered image is 56 dB.

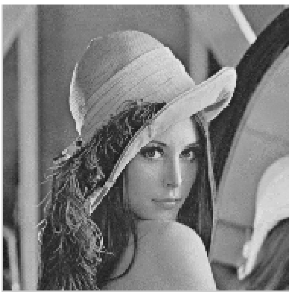

Figure 7. Decrypted image containing watermark information

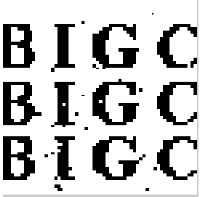

Figure 8. Watermark extraction

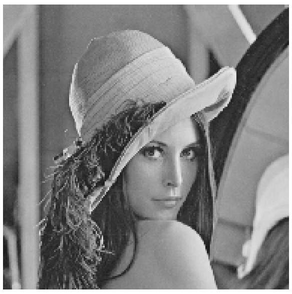

Figure 9. Recovery image

According to the image information entropy formula can calculate the information entropy of the encrypted image H$\approx$7.9913.

$$H(X) = -\sum_{i=1}^{n} p(X_i)\log_2 p(X_i) \tag{14}$$

The histograms of the original image and the encrypted image obtained by experiments are shown in Fig.10 and Fig.11, and Fig.10 is a histogram of the original image. In this case, the attacker can easily count the image information, and Fig.11 is the encrypted histogram. It can be clearly seen through comparison and Fig.8 that the ratio of almost pixels is relatively uniform.

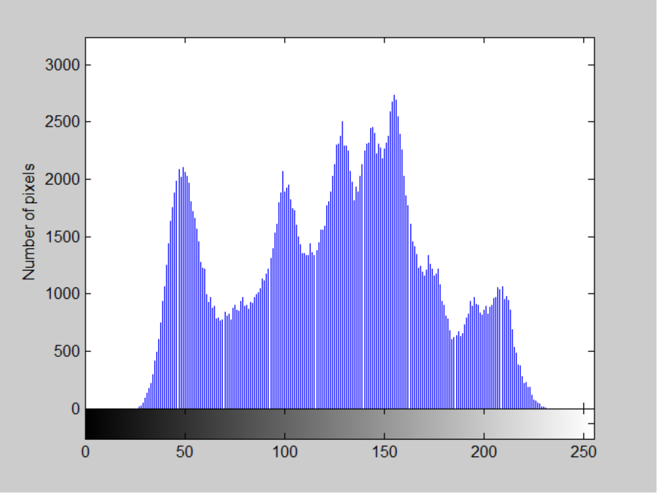

Figure 10. Original histogram

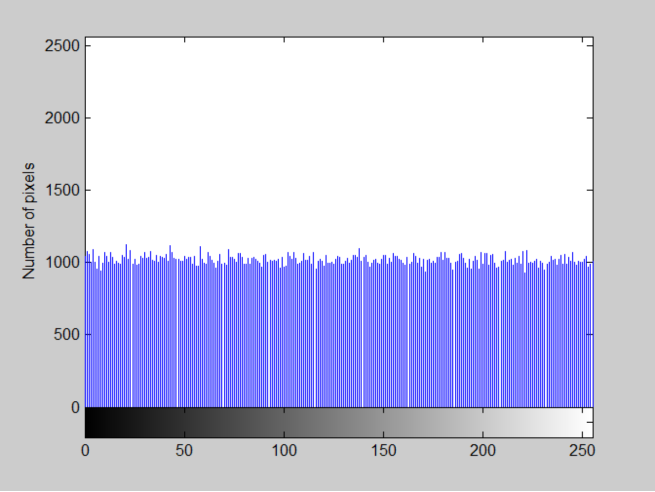

Figure 11. Encrypted image histogram

Table 1 is obtained by calculating the NC values of the original image and the recovery image. It can be seen from Table 1 that the NC value is close to 1, indicating that the restored image has a higher quality.

Table.1. NC value of the image

图像	NC值
Lena	0.9999949
Baboon	0.9999946
Camera	0.9999788
Peppers	0.9999954
Lake	0.9999785
Cell	0.9999870

5. Conclusion

Through the MATLAB experiment simulation, a reversible watermarking algorithm based on the low computational complexity of the image of ZUC algorithm is analyzed. The information entropy of the encrypted image and the histogram of the original image and the encrypted image are analyzed.

It is found that the ZUC algorithm can combine the reversible watermark well. Moreover, the ZUC algorithm can generate a 32-bit key every cycle, which satisfies the real-time and fast requirements of digital image encryption, and is very suitable for digital image encryption. And by calculating the NC values of the original image and the recovery image, it is found that the restored image has a higher quality. Secure the image by encrypting the image with the key stream generated by the ZUC algorithm. The algorithm is novel and simple, but the size of the embedded watermark and the correct rate of image restoration are related to the block size S. Therefore, further research is carried out to improve the embedding amount and improve the peak signal-to-noise ratio of the decrypted image.

References

[1] Gibson J, Eveleigh D, Rondeau R, Tan Qing. Benefits and challenges of three cloud computing service models//Proceedings of the 4th International Conference on Computational Aspects of Social Networks. So Carlos, Brazil, 2012: 198-205.

[2] Jin C. Digital Watermark Theory and Technology [M]. BEIJING, Tsinghua University Press, 2008.

[3] Zhang X P, Wang S Z. Efficient Steganographic Embedding by Exploiting Modification Direction [J]. IEEE Communications Letters, 2006, 10 (11): 781-783.

[4] Zhang X Q, Sun Z R, Tang Z J, et al. Hi, h Capacity Data Hiding Based on Interpolated Image [J]. Multimedia Tools and Applications, 2017, 76 (7): 9195-9218.

[5] Zhang X Q, Yu C Q, Wang X Y, et al. A Reversible Data Hiding Scheme for JPEG Images [J]. ICIC Express Letters, 2013, 7 (9): 2575-2580.

[6] ZHANG X P, Reversible data hiding in encrypted image [J], Signal Processing Letters,2011,18 (4): 255-258.

[7] HONG W, CHEN T S, WU H Y, An improved reversibledata hiding in encrypted images using side match [J], Signal Processing Letters, 2012, 19 (4): 199-202.

[8] YU J, ZHU G P, LI X L, et al. An improved algorithm for reversible data hiding in encrypted image [M] // Digital Forensics and Watermaking, Heidelberg: Springer, 2013: 384-394.

[9] LIAO X, SHU C W. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels [J]. Journal of Visual Communication and Image Representation, 015, 28: 21-27.

[10] ZHANG X P, Separable reversible data hiding in encrypted image [J]. IEEE Transactions on Information Forensics and Security, 2012, 7 (2): 826-832.

[11] ZHANG X P, QIN C, SUN G L. Reversible data hiding in encrypted images using pseudorandom sequence modulation [M] // Digital Forensics and Watermaking. Heidelberg: Springer, 2013: 358-367.

[12] ZHANG X P, QIAN Z X, FENG G R, et al, Efficient reversible data hiding in encrypted images [J]. Journal of Visual Communication and Image Representation, 2014, 25 (2): 322-328.

[13] MA K, ZHANG W M, ZHAO X F, et al. Reversible data hiding in encrypted images by reserving room before encryption [J]. IEEE Transactions on Information Forensics and Security, 2013, 8 (3): 553-562.

[14] JAGDALE M V,HINGWAY S P, SURESH S S, Reversible encryption and data hiding [J /OL], International Journal of Advance Research in Computer Science and Management Studies, 2014, 2(1): 293-299 [2015-07-30], http: //www. Ijarcsms.com/docs /paper / volume2 /issue1 /V211-0079.pdf.

[15] LATHA K, SUNDARAMBAL M. A novel encryption and extended dynamic histogram shifting modulation for reversible data hiding in encrypted image [J /OL]. International Journal of Computer Trends and Technology (IJCTT), 2014, 7 (2): 115-118 [2015-07-30], http: //www.ijcttjournal.org/ Volume7/number-2 /IJCTTV7P130.pdf.

[16] ZHANG W M, MA K, YU N H. Reversibility improved data hiding in encrypted images [J], Signal Processing, 2014, 94: 118-12.

[17] ETSI/SAGE TS 35.222—2011, Specification of the 3GPP Confiden-tiality and Integrity Algorithm 128-EEA3&128-EIA3; Document 2: ZUC Specification.

[18] YANG Y X, NIU X Y. Digital Watermark Theory and Technology [M]. Beijing: Higher Education Press, 2006.

[19] LUO J G. Research on Reversible Image Watermarking and Reversible Image Authentication Technology [D]. Guangzhou: Ph.D thesis of South China University of Technology, 2011.