Send Orders for Reprints to reprints@benthamscience.ae

Open Access

Research on a Robust Method for Image Steganography Transmission in Network

Yiran Wang*

School of Computer Science and Technology, Zhoukou Normal University, Zhoukou, 466001, China

Abstract: Images carrying the important information are often cracked by hackers when they are transmitted in the network. We propose a method in the paper for avoiding information leakage. It presents some significant evaluation parameters to analyze image scrambling algorithms for encryption level. Then images are encrypted with the algorithm and transmitted in the network by hiding in the open video. In order to prevent the loss of packet or frame, we advance a robust data hiding method which can use paired-coefficient and BCH code to recover error bit. It encodes the secret information with different BCH codes and embeds them into the paired-coefficients positions. The experimental results show that the method can avert intra-frame distortion drift and achieve high error resilience capacity. The research has a certain reference value and guiding significance for image steganography.

Keywords: Distortion, error correction, image encryption, robustness, scrambling.

1. INTRODUCTION

With the development of Internet, more and more image data are transferred in the network. In order to protect the privacy and improve the security of image transmission, scholars propose many image encryption algorithms [1]. How to distinguish their performance and assess safety, analysis for these algorithms are very necessary. The encrypted image can be hidden into the open video and transmitted in the network. Now, H.264/AVC video standard is the main direction of international telecommunications and broadcasting system, which has achieved great success [2]. More and more high-definition television, online video and 3G telephone are using the standard. The communication through information hiding in the 2D/3D H.264/AVC video is a new development direction [3].

2. THE RELATED RESEARCH

Usually there are some classical image scrambling and encryption technology, such as technology based on matrix transform or pixel replacement, on secret sharing and image segmentation, on secret key image and hybrid. But there are less relevant research on testing their performance. Now, Video Steganography is one of the hottest research fields. When H.264/AVC videos are transmitted over the network which hide the secret information, some serious errors may lead some important information not to be recovered at the terminal. These errors include the loss of packet or frame because of harsh physical environment [4], and some network attacks (such as tampering, playback or recoding).Therefore, how to effectively protect the information to prevent the leak of information becomes more and more important. In [5], the author first analyzes hiding algorithm based on video information, and points out that the existing video algorithm can’t be directly used in the H.264/AVC video standard. For information hiding, many of the current study mainly concentrate on watermarking field. Digital watermarking in DCT domain has high robustness and good flexibility, and is widely used at present. However, the watermark makes property identification through logo embedded in video. It emphasizes that the works were not modified, deleted and detection. So it can’t be directly used for steganography algorithm. The method of quantitative DCT can reduce the influence of embedding on rate, and be realized through the partial entropy decoding and coding. So, how to further enhance the robustness of built-in video hiding algorithm in the H.264/AVC video standard has more important theoretical and practical significance.

3. ANALYSIS OF IMAGE ENCRYPTION ALGORITHM

There are many methods of image encryption which have different security strength. But no matter what method it is, the encryption transformation belongs to the following three categories. The first is only the image pixel position transformation encryption. The second is only the image gray value transformation image encryption. The third is that pixel position and gray value images are both changed. The purpose of image encryption is to achieve the image secure transmission or save. Now many algorithms claim that they have very high security and can resist various attacks, but how are the performances of them in the end? How to evaluate the safety strength of these different conversion types or of the different methods in the same type? Solving this problem will have important significance in research of image encryption, and it will be able to increase the security.

3.1. Scrambling Encryption Parameters

The paper will give some parameters to analyze the relationship between parameters and image scrambling degree or safety degree. In the following analysis, Symbols represent certain meaning. $G=(g_{ij})_{M\times N}$, presents the original image which size is M×N. g_{ij} is the pixel gray value in the image, $C=(c_{ij})_{M\times N}$ is the disposed image after G is encrypted.

Definition 1. Fixed point ratio

It points the fixed points as a percentage of all pixels. It can be described as following equation (1).

$$BD(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)}{MN}\times 100\%, f(i,j)=\begin{cases}1 & g_{ij}=c_{ij}\\ 0 & g_{ij}\neq c_{ij}\end{cases} \quad (1)$$

In general, the value of BD is smaller, the difference of G and C is bigger. And the scrambling effect is better.

Definition 2. Information entropy

It is used to measure the uncertainty of information contained in images. Supposed the gray level of G is L, x_i represents the i grey, $p(x_i)$ is the proportion of x_i in G, and $\sum_{i=1}^{n}p(x_i)=1$

$$H(G)=-\sum_{i=1}^{L}p(x_i)\log_2 p(x_i) \quad (2)$$

Information entropy can measure the distribution of image gray value. The gray level is more distributed well-proportioned, the image information entropy is more bigger.

Definition 3. Average change value of gray

$$GAVE(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|g_{ij}-c_{ij}\right|}{MN} \quad (3)$$

When G=C, GAVE=0. But if C=G^{-1}, GAVE=L. Obviously, the image scrambling effect and security of encryption are the worst in these two kinds of circumstances. When the gray values of two images generate uniform change, scrambling effect is the best. The best situation should be that GAVE= L/2.

Definition 4. The self correlation of r-m

$$R^{r,m}(G)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|G_{i,j}^{r,m}\right|}{\left|G_{i,j}^{r,255}\right|}}{MN}\times 100\% \quad (4)$$

This parameter represents the related degree of pixels within adjacent areas. When r and m change, the value of the parameter R will change too. The values of r and m are smaller, The parameter R more accurately portray the association degree of pixel gray value in the image. The greater the parameter value is, that image of the self -correlation is high.

Fig. (1). Lena.bmp.

Definition 5. Image similarity

In the real world, people often want to compare whether the two images are similar. In image encryption, the comparison is more important. If the encrypted image and the original image have many similar places, so the security degree of the encrypted image is very poor.

$$XSD(G,C,\alpha,\beta)=1-\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[c_{i+\alpha,j+\beta}-g_{ij}]^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}g_{ij}^{\ 2}} \quad (5)$$

For image encryption, the similarity of the original image and encrypted is smaller, the security is more high.

3.2. Experiment Results Analysis

The following study to test and verify the reliability of parameters with chaotic encryption scheme based on 3D Cat mapping. The encryption thought is described as the following.

Step 1. Enter a 128 bit key, divide it into 8 groups, and generate parameters of 3D CAT mapping, initial conditions of Logistic mapping and initial value of the iterative operation .

Step 2. Make the two-dimensional image into a plurality of cube image.

Step 3. Make use of 3D CAT mapping to scramble the cube image.

Step 4. Generate parameters of images iteration by using Logistic mapping, and make use of XOR operation on the image to scramble it confusing.

Step 5. Convert the scrambled and confused image into a two-dimensional encryption image.

From these steps above, we can see that the plan realizes the image encryption after confusion and scrambling many times. The encrypted image not only changed the pixel position of the original image, but also changed the gray value. We encrypt an image named Lena.bmp in Fig. (**1**) and the

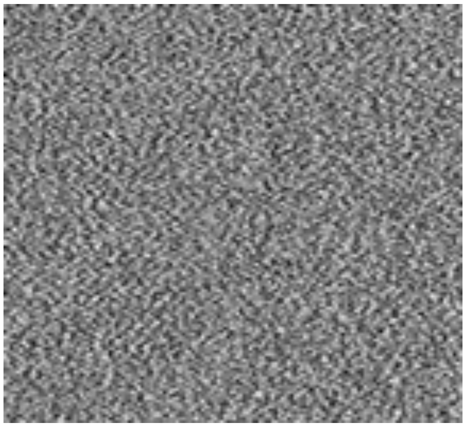

Fig. (2). Lena_3catA.bmp.

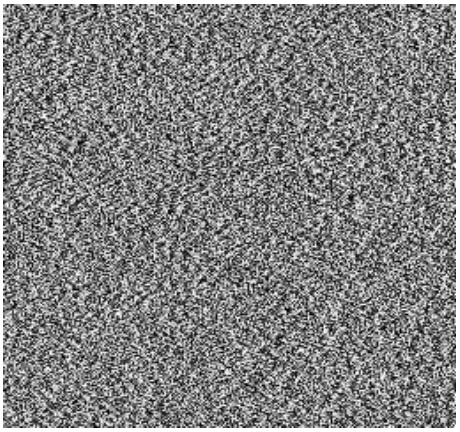

Fig. (3). Lena_3catB.bmp.

experiment results show as Fig. (**2**) and Fig. (**3**) by using plan above when the key adopts the value respectively "1234567890123456" and "1234567890123458".

Test results of each scrambling parameter by the encryption scheme are listed as following.

Compared with the original image, the fixed point ratio of encrypted image lena_3catA.bmp is only 0.4074%, lena_3catB.bmp is 0.3921%. They are very small, and it illustrates that the scrambling effect is very good. Two information entropy of image encryption are H(lena_3catA.bmp)=7.9974 and H(lena_3catB.bmp)= 7.9971. They have very small differences, and are close to the maximum entropy of 256 gray level images. This shows that the gray distribution of two encrypted images is very uniform and it achieves the good encryption effect. The average change values of gray of two encryption images are 72.85 and 73.28. They are much larger than the values of Arnold transform and magic transform encryption. It once again illustrates that encrypted image is very sensitive to the key. Small changes of the key will lead to a great change in encrypted image. We calculate the self correlation of r-m of images which meet the conditions, r=1 and 0<m<21. The results are shown in Table **1**.

The Image similarities among three images are respectively as following.

XSD(lena.bmp,lena_3catA.bmp)=0.5603,

XSD(lena.bmp,lena_3catB.bmp)= 0.5550,

XSD(lena_3catA.bmp,lena_3catB.bmp)= 0.4946

There are great differences between original image and encrypted image. But the differences between lena_3catA.bmp and lena_3catB.bmp are larger than that. The security of encryption is better.

From above result analysis, we can see the parameters of chaotic encryption scheme based on 3D Cat mapping is far superior to other encryption scheme. It proves that it is a good performance and high security encryption scheme.

4. DESIGN AND IMPLEMENTATION OF BCH CODES ROBUST METHOD OF DOUBLE COEFFICIENT STEGANOGRAPHY

BCH code is a powerful tool against bit errors which is widely used in digital watermarking or image information hiding [6]. However, these studies are not based on H.264/AVC video. Now, there are two kinds of questions in H.264/AVC video steganography. One is the intra frame distortion drift which can lead to serious visual distortion for embedded video. The other is modification of DCT coefficient which can cause the decline of embedding capacity and robust performance. So we put forward higher requirements on the study of robust video steganography based on

Table 1. Image self correlation(r=1).

m	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Lena	0.3613	0.4838	0.5719	0.6336	0.6799	0.7156	0.7449	0.7687	0.7890	0.8064
Lena_3catA	0.1218	0.1283	0.1349	0.1416	0.1480	0.1545	0.1609	0.1675	0.1739	0.1804
Lena_3catB	0.1221	0.1291	0.1361	0.1431	0.1497	0.1566	0.1632	0.1700	0.1765	0.1831
m	11	12	13	14	15	16	17	18	19	20
Lena	0.8219	0.8350	0.8467	0.8572	0.8667	0.8756	0.8831	0.8901	0.8968	0.9027
Lena_3catA	0.1872	0.1941	0.2008	0.2076	0.2145	0.2211	0.2278	0.2344	0.2410	0.2474
Lena_3catB	0.1896	0.1958	0.2021	0.2085	0.2148	0.2214	0.2280	0.2344	0.2407	0.2474

H.264/AVC. In the paper, we use BCH code to achieve robustness against hidden bit errors.

4.1. Intra Frame Distortion Drift Prediction Model

Distortion drift of a 4 x 4 luma block is passed on to its neighboring blocks by the edge pixel values embedding information. Similarly, the intra frame distortion drift can be avoided when we calculate current block prediction value not to adopt the edge pixels of adjacent blocks which hide the secret message. We give some conditions about adjacent blocks of the current block.

Condition 1 Right adjacent block $\in\{0,3,7\}_{4\times4}\cup\{0\}_{16\times16}$, The intra frame prediction mode of right adjacent block is 4 x 4 luma block of $\{0,3,7\}$or 16 x 16 macro block of zero.

Condition 2 Bottom-left adjacent block $\in\{0,1,2,4,5,6,8\}_{4\times4}\cup\{0,1,2,3\}_{16\times16}$, Nether adjacent block $\in\{0,8\}_{4\times4}\cup\{1\}_{16\times16}$. The intra- frame prediction mode of bottom-left adjacent block is 4 x 4 luma block of $\{0,1,2,4,5,6,8\}$or 16 x 16 macro block of $\{0,1,2,3\}$. Nether adjacent block is 4 x 4 luma block of $\{0,8\}$or 16 x 16 macro block of $\{1\}$Condition 3 Bottom-right adjacent block $\in\{0,1,2,3,7,8\}_{4\times4}\cup\{0,1,2,3\}_{16\times16}$, The intra frame prediction mode of bottom-right adjacent block is 4 x 4 luma block of $\{0,1,2,3,7,8\}$or 16 x 16 macro block of $\{0,1,2,3\}$.

If the current block satisfies the condition 1, block errors caused by embedded in the information could not pass to its right adjacent block through the rightmost pixel value because the column of pixel value is not used as a reference pixel [7]. If the current block satisfies the condition 2, block errors could not pass to its bottom-left adjacent block or nether block because the row of pixel value is not used as a reference pixel. If the current block satisfies the condition 3, block errors could not pass to its bottom-right adjacent block because the bottom-right pixel value is not used as a reference pixel. If all of the edge pixel values in adjacent blocks are not used as prediction of current block in the same way, the error caused by embedding secret information in adjacent block is not delivered to the current block [8]. For example, if f a 4 x 4 luma block simultaneously satisfies condition 1, 2and 3, the error caused by embedded information can't be transferred to the surrounding adjacent blocks. It can prevent the intra frame distortion drift through condition 1,2 and 3.

4.2. Method of Analysis

The method of double coefficient steganography gets the robustness by BCH coding, avoids distortion drift through the prediction mode selection and eliminates error by coupling coefficient. We discuss the principle of BCH code how to correct errors. Now we take BCH (7,4,1) as an example to analyze the changes of DCT coefficients when using BCH code and not using it. Suppose the secret information is '01100001', and it becomes '10001101010001' after BCH(7,4,1) code. The step size of weight is 29. When the data extracts from the network, the information is still '10001101010001' because it uses the BCH code. If not, the information is '00100001'. Embedded bit can be correctly extracted only 87.5%. It shows that BCH code has the very strong error correcting capability.

4.3. Embedding and Extracting Process

In embedding process, we first make decoding operation for H.264/AVC video received from network, obtain DCT coefficients and 4 x 4 block intra-frame prediction mode. Then according to the absolute value of DC and custom parameters threshold, we select alternative of embedded block. Based on the prediction model of adjacent blocks within a frame, embedded block is chosen to eliminate the intra frame distortion drift [8]. Now we judge whether the current block accords with conditions 1(or 2). If it meets the condition, coupling coefficients from HS are selected to do embedding operation. Then BCH code is embedded into coupling coefficient, and we need adjust the compensation coefficient in order to eliminate the error [9]. At last, DCT coefficients with embedded information are entropy recode to obtain the target embedded video. The specific embedding method is as following.

Step 1 Encode the information with BCH, and select embedded block.

Step 2 Choose a non-zero coefficient and block as the embedded block.

Step 3 Select a suitable coupling coefficient, and use modulation method to embed 1 bit into it.

In extracting process, we first carry on the decoding operation according to H.264/AVC video and get DCT coefficients and 4 x 4 block intra-frame prediction mode. IF the absolute value of DC is greater threshold, and prediction mode of adjacent blocks meets the condition 1 or 2, we will select appropriate DCT coefficients to extract the secret information [10].

4.4. Analysis and Comparison of Experimental Results

The method has been realized in JM which is an encoding and decoding software for H.264/AVC video standard. Test video has 300 frames and the encoding frame rate is 30 frames/sec. The interval is 15 and the quantization parameter is 28. The test video sequence is a resolution ratio of 176 x 144. "PSNR1" is the peak signal to noise ratio, which is composed of YUV video file and embedded video file. Because all of the embedded operation are carried out in luma block, PSNR1 is the average value of I frame, B frame and P frame of PSNR1. The survival rate is the ratio of correct extraction embedding bit number and total embedded bit number.

The experiment takes the recoding attacks as a examples to test BCH technology and non- distortion drift performance. We use QP=28, $|Y_{00}|>3$, BCH (7,4,1) and the secret information embedding position is $(\overline{Y}_{32},\overline{Y}_{30})$. Table **2**. gives comparison of test results when the video named news was

Table 2. Performance comparison.

BCH Code	PSNR1 (dB)	The Survival of Non-use BCH Code (%)	The Survival of Use BCH Code (%)
(7,4,1)	38.8	93.91	99.34
(15,5,3)	39.41	94.05	99.66
(15,11,1)	38.58	93.60	98.04
(31,26,1)	38.8	93.66	96.83
(63,7,15)	38.82	93.31	100

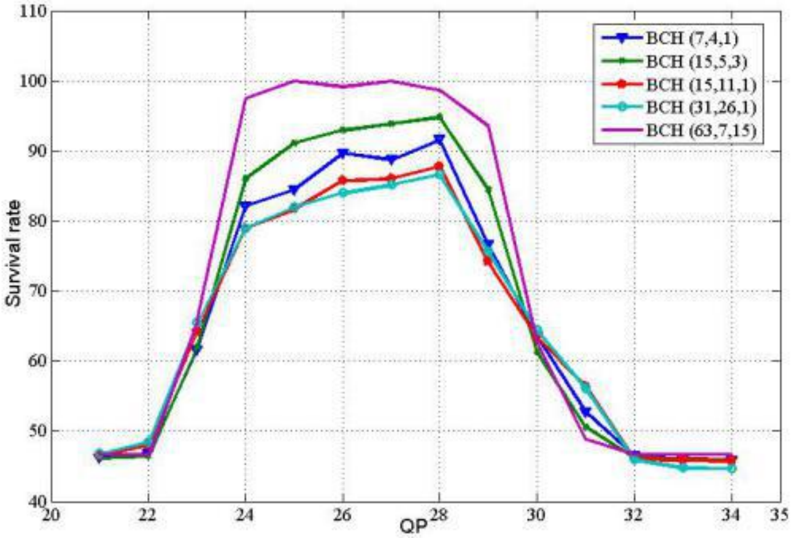

Fig. (4). Performance Comparison of Different BCH Code.

encountered heavy attacks by using and not using BCH code. Experiments show that the average survival rate is 98.77% by using the BCH code. On the contrary it reaches 93.71%. and . The average PSNR1 is not less than 38.86 dB. We can see that the survival rate is significantly higher by using BCH code than the one which does not use the BCH code.

Fig. (**4**) shows the robustness of performance comparison with the use of different BCH codes. When the QP gets the value from 24 to 29, BCH code has strong error correcting capability. The results are consistent with the one in Table **2**. In several test codes, BCH (63,7,15) is the most powerful error correcting capability [11]. For BCH (n, K, t), t is more bigger, PSNR1 is lower, and error correction capability is more strong.

CONCLUSION

Aiming at the image information transmitted in the network unsafe, we propose a new method which first encrypts images and then transmits them in network through the video steganography mode. In the selection of secure encryption algorithm, the paper presents some evaluation parameters to analyze the scramble and security. Results of experiment show that they are practical and effective. In order to prevent the loss of packet or frame, we advance a robust data hiding method which can use paired-coefficient and BCH code to recover error bit. The method takes the recoding and weight as an example to test the BCH code error recovery capability. The survival rate of embedded bit can increase at least 25% when using the method. On recoding, it can reach 100%. The process of extraction and embedding is simple and quick, and it can adapt to the real-time requirements of video.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work is supported by basic and frontier project of Science and Technology Department of Henan province, China (no 142300410334), the funding scheme for young backbone teachers of colleges and universities in Henan Province, China.

REFERENCES

[1] G.R. Chen, Y.B. Mao, and C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals* , vol. 21, pp. 749-761, 2004.

[2] P. Pradhan, R. Tewari, S. Sahu, A. Chandra and P, Shenoy, "An observation-based approach towards self-managing web servers," In: *Proceedings of ACM/IEEE Intel Workshop on Quality of Service (IWQoS),* Miami Beach, FL, May 2002

[3] L. L. Wang, Y.S. Tong, and W. T. Huang, "Technical overview of the video privacy protection", *Journal of Communications*, vol. 8, pp. 154-160, 2013.

[4] W. Lie, T.C. Lin, and D. Tsai, "Error resilient coding based on reversible data embedding technique for H. 264/AVC video," In: *IEEE International Conference on Multimedia and Expo. ICME'05*, Amsterdam, Netherlands, 2005, pp. 1174 -1177.

[5] L.Y. Wang, H.F. Ling, and F.H. Zou, "Real-time compressed-domain video watermarking resistance to geometric distortions," *IEEE Multi Media*, vol. 19, pp. 70-79, 2012.

[6] X.J. Ma, Z.T. Li, J. Lv, and W. Wang, "Data hiding in H.264/AVC streams with limited intra- frame distortion drift", *Computer Network and Multimedia Technology*, pp. 1-5, 2009.

[7] X.J. Ma, and Z.T. Li, "A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," In: *IEEE Transaction on Circuits And Systems for Video Technology*, vol. 10, pp. 1320-1330, 2010.

[8] Y.X. Liu, Z.T. Li, and X.J. Ma, "A robust data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," *Electric Information and Control engineering*, pp. 1744-1748, 2012.

[9] X.J. Ma, Z.T. Li, and J. Lv, "Data hiding in H.264/AVC streams with limited intra-frame distortion drift," *Computer Network and Multimedia Technology,* pp. 1-5, 2009.

[10] X.J. Ma, Z.T. Li, and H. Tu, "A data hiding algorithm for H.264/AVC video streams Without Intraframe Distortion Drift," *Circuits and Systems for Video Technology*, vol. 10, pp. 1320-1330, 2010.

[11] E. Esen , and A.A. Alatan, "Robust Video data hiding using forbidden zone data hiding and selective embedding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 8, pp. 1130-1138, 2011.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014

© Yiran Wang; Licensee *Bentham Open.*

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.