Send Orders for Reprints to reprints@benthamscience.ae

Research on the Steganography Robustness Method of BCH Single Coefficient

Yiran Wang[1,*] and Xingjin Zhang[2]

[1]*School of Computer Science and Technology, Zhoukou Normal University, Henan Zhoukou, 466001, China*

[2]*School of Information Engineering, Zhengzhou University, Henan Zhengzhou, 450001, China*

Abstract: Being aimed at the problem that general steganography algorithms always destroy the original videos after extracting the information, the paper adopts analysis and experiment to propose a BCH robustness method of single coefficient which can restore error bits. Before embedding the data, the method encodes the secret information with BCH and makes use of prediction mode to select special embedding block to control the inter-frame distortion drift. Then it applies single coefficients to decrease the modification of original videos. When extracting the information, we first make error correction and try to recover the original video. The experimental results show that the method not only can efficiently recover the secret information, but also restore the original medium as far as possible and protect them.

Keywords: BCH, Distortion, Embed, h.264, Robustness, Video.

1. INTRODUCTION

When transmitting over the network, the H.264/AVC video [1] hidden information could lose packets or frames for the harsh physical environment, and lead to secret information not to be restored. On the other hand, some network attacks (such as tampering, playback, re-quantization and recoding) also destroy the information. Therefore, how to effectively protect the information and to prevent the leak of information becomes more and more important. The general steganography algorithms always destroy the original videos [2] after extracting the information, and the original videos couldn't be used again. If the demand of video quality is not high, we can try our best to restore it by some algorithms. On extracting the secret information, the algorithm considers the medium recovery, and encodes the secret information into BCH codes. When the algorithm makes the reversible operations, it can prevent error bits which are caused by transmission, packet loss, attack or the H.264/AVC video processing. In the paper, we utilize BCH to resist the error bits in the H.264/AVC environment, and realize the steganography robustness algorithms which can restore the original videos.

2. THE RELATED RESEARCH

Literature [3] is a kind of typical built-in algorithm. It chooses the space hiding information to be quantized as DCT coefficients. The algorithm randomly selects the position information to ensure the security. But its embedded capacity is tiny. Its advantages are that the algorithm can finish the information implanting the video by the DCT coefficients, and modulate its function on the basis of human visual characteristics. It can get the strong anti-attack ability. Luohuai proposes a steganography algorithm based on motion vector phase [4, 5]. It divides phase space of motion vector into 2 interval sets to match the embedding binary information. These algorithms require to completely decode the video, and carry out the inter-frame prediction, motion estimation and compensation, and subsequent code again. That the information is implanted in motion vector will cause inter-frame distortion drift, and also limit the embedding capacity.

*Address correspondence to this author at the School of Computer Science and Technology, Zhoukou Normal University, Henan Zhoukou, 466001, China; Tel: +8613526256979; E-mail: 286206308@qq.com.

3. THE METHOD RESEARCH

3.1. The Theoretical Basis

(1) H.264 standard codec

The codec in the H.264/AVC standard takes macro-block as unit to dispose. The original H.264/AVC videos are first divided into 16*16 blocks. These blocks are macro-blocks. In order to facilitate the dealing with the information in the practical coding process, the 16*16 blocks are often classified into sixteen 4×4 sub-macro blocks. Then we respectively take the sub-macro block operations such as inter-frame prediction, DCT coefficient transform, quantization and entropy coding. It makes the detailed complex region to obtain more precise processing. The processing procedure of video encoding which takes macro-block as unit is shown in Fig. (**1**).

When decoding, we will make the macro-block do entropy coding, reordering and produce the quantized transformation coefficients, X. Then it goes through the inverse quantization and inverse transformation, and gets the

1874-4443/15 2015 Bentham Open

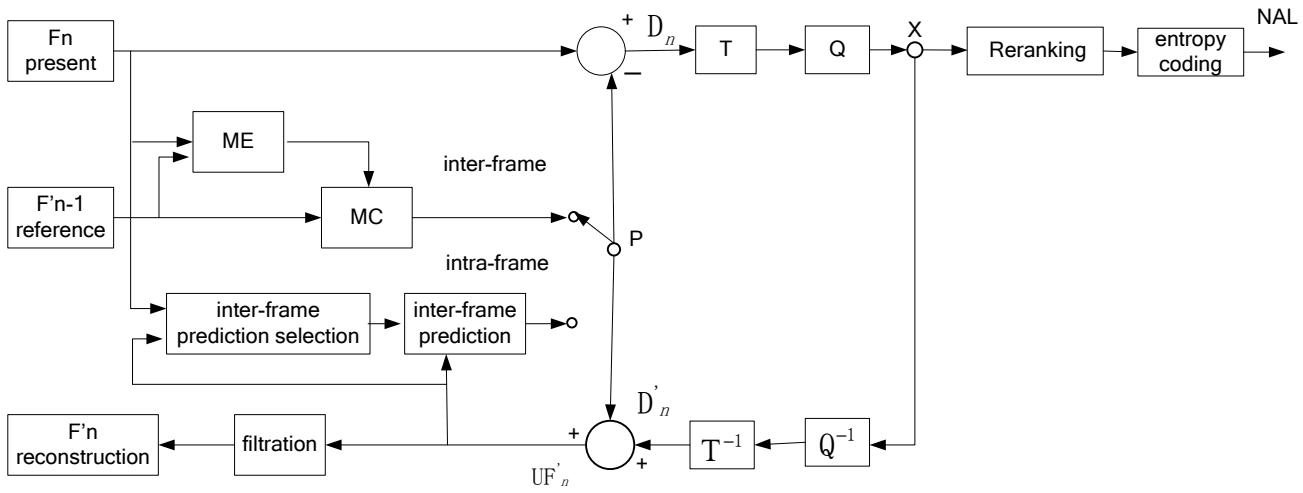

Fig. (1). H.264/AVC Coding Process Structure.

residual error, $V=QH^T$. We acquire P on the basis of decoding reference frame image during frame prediction. P adds $V=QH^T$, and the result is uFn'. We filter the uFn', and get the decoding frame image.

(1) BCH code

Because the BCH code has strict algebraic structure and good properties, so it has extremely important status in error correction of coding. It is one of the codes that has been studied thorough and detailed, and acquired many achievements. We suppose that binary BCH(n, k, t) can correct t errors. In BCH(n, k, t), n is the code length, and k is the information bit. Its check matrix is shown in formula (1).

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2t-1} & (\alpha^{2t-1})^2 & \cdots & (\alpha^{2t-1})^{n-1} \end{bmatrix} \quad (1)$$

In formula (1), α is the primitive element on $GF(2^m)$. Suppose the original binary data stream which cannot be encoded with BCH is $Q=\{q_0,q_1,\cdots q_{n-1}\}$, the video stream in which are implanted the secret information is $V=\{v_0,v_1,\cdots v_{n-1}\}$, then we can get the formula (2).

$$V=QH^T \quad (2)$$

After channel transmission, the client receives the codes stream which can be expressed as $S=\{s_0,s_1\cdots s_{n-1}\}$. In $GF(2^m)$, V and S can be described with polymerization such as $V(X)=v_0+v_1x+v_2x^2+v_3x^3+\cdots v_{n-1}x^{n-1}$ and $S(X)=s_0+s_1x+s_2x^2+s_3x^3+\cdots s_{n-1}x^{n-1}$.

The difference of S and V will be named E. Then we get the formula (3).

$$S=V+E \quad (3)$$

Making use of formulas (2) and (3), we get formula (4).

$$Y=(S-V)H^T=EH^T \quad (4)$$

Y is called syndrome of received vector R. S with secret information can be calculated by formula (3). The secret information can be restored with formula (2).

3.2. The Method Analysis

The single coefficient steganography method achieves robustness through the BCH code. It chooses the single coefficient which meets 3 conditions of.

Because the content of 16*16 block changes slightly, the visual imperceptibility of embedding secret information is not strong. So we select DCT coefficient of 4*4 block as a carrier for embedding information. The method first encodes the secret information with BCH before embedding. Then it is based on the prediction direction (a 4*4 of bright block at the same time meets the conditions of 1, 2, 3) to select block to embed the secret information in single coefficients. The characteristic of this method can effectively improve the survival rate of the embedded bit. It will try to restore the video after extracting the secret information. It also can choose the number of embedding coefficients according to the capacity.

3.3. The Process of Embedding and Extracting

(1) Embedding process

In order to restore error bits correctly, we first encode the secret information with BCH before dealing with them. Then we select the current macro-block which satisfies simultaneously the conditions 1, 2 and 3 for the sake of preventing distortion drift. In order to improve the embedding capacity, we choose high frequency coefficient such as N. The embedding operation flow chart is shown in Fig. (**3**)

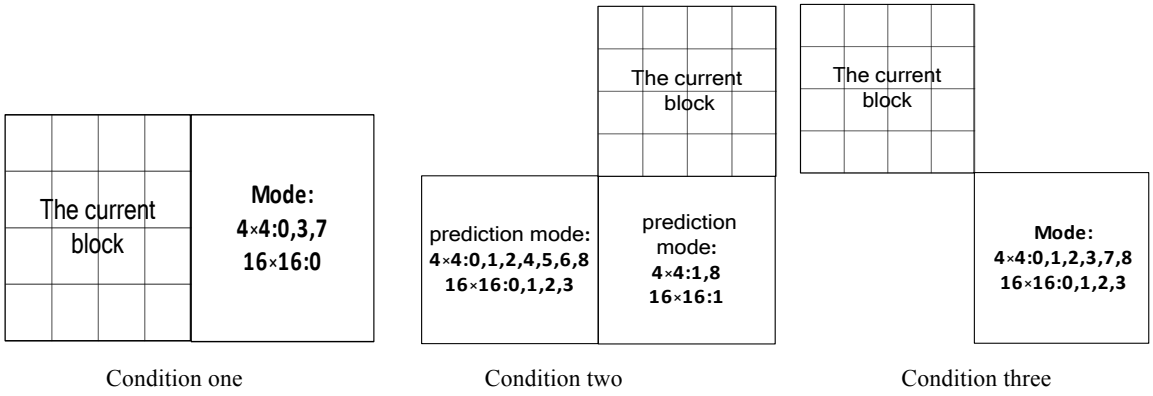

Fig. (2). The Representation Graph of Three Conditions.

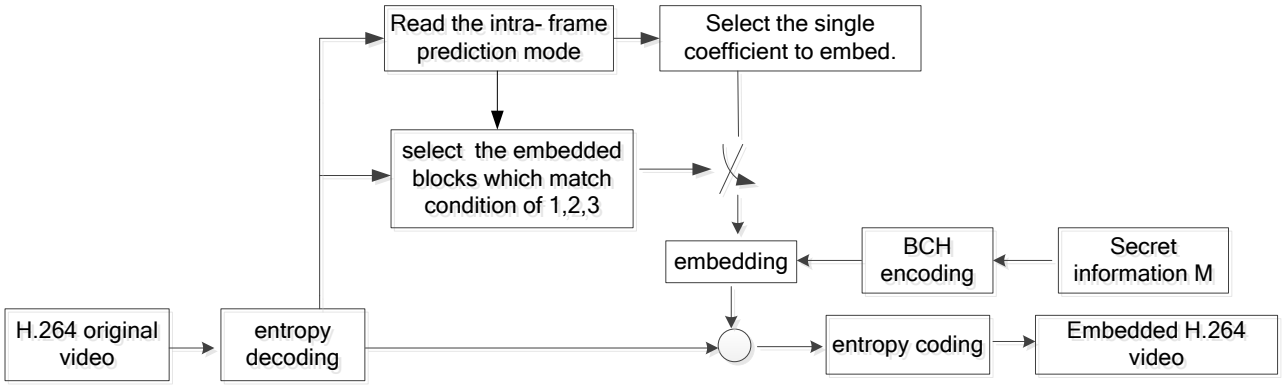

Fig. (3). The Embedding Operation Process of Single Coefficient BCH Robustness Method.

We decode the H.264 videos received from the network and get the DCT coefficients and inter-frame prediction mode of 4*4 block. Then we choose the alternative embedded block according to the absolute value of DC in DCT coefficients and custom parameters, threshold. We select the right embedded blocks according to the current blocks whether they meet the conditions of 1, 2 and 3 simultaneously. The secret information encoded with BCH is hidden in the DCT coefficient. At last, all of DCT coefficients have been recoded and it formed the object videos hiding the information. In order to clearly describe the method, we choose a positive integer named N, and a coefficient named $\tilde{Y}_{ij}$ as a sample to depict the process [6].

There are 2 steps in the main process. Step one is that encodes the secret information with BCH before embedding. Step two is to choose the bright macro-block to hide the information. If the current block simultaneously satisfies the condition 1, 2 and 3, it is the embedding block. The method of embedding the information is described as follows.

If $\left|\tilde{Y}_{ij}\right|$=N+1, or $\left|\tilde{Y}_{ij}\right| \neq$ N, we will amend $\tilde{Y}_{ij}$ in the light of formula (5). If the embedding bit is 1 and $\left|\tilde{Y}_{ij}\right|$=N, $\tilde{Y}_{ij}$ will be revised according to formula (6). If the embedding bit is 0 and $\left|\tilde{Y}_{ij}\right|$=N, then $\tilde{Y}_{ij}$ would not need to be modified.

$$\tilde{Y}_{i,j} = \begin{cases} \tilde{Y}_{i,j}+1, & \text{if } \tilde{Y}_{i,j} \geq 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+1}, \\ \tilde{Y}_{i,j}-1, & \text{if } \tilde{Y}_{i,j} < 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+1}, \\ \tilde{Y}_{i,j}, & \text{if } \left|\tilde{Y}_{ij}\right| \neq \text{N}. \end{cases} \quad (5)$$

$$\tilde{Y}_{i,j} = \begin{cases} \tilde{Y}_{i,j}+1, & \text{if } \tilde{Y}_{i,j} \geq 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N}, \\ \tilde{Y}_{i,j}-1, & \text{if } \tilde{Y}_{i,j} < 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N}. \end{cases} \quad (6)$$

(2) Extracting process

Fig. (**4**) shows the extracting operation flow chart. We will extract the information which lies in coefficient of $\tilde{Y}_{30}, \tilde{Y}_{21}, \tilde{Y}_{31}, \tilde{Y}_{12}, \tilde{Y}_{22}, \tilde{Y}_{32}, \tilde{Y}_{03}, \tilde{Y}_{13}, \tilde{Y}_{23}, \tilde{Y}_{33}$.

The method extracts the H.264 video received from the network and gets the DCT coefficients and prediction mode of 4*4. We select the suitable DCT coefficient of 4*4 block to extract the secret information according to two qualifications. One is that the absolute value of DC in DCT coefficients is a greater threshold [7]. The second qualification is

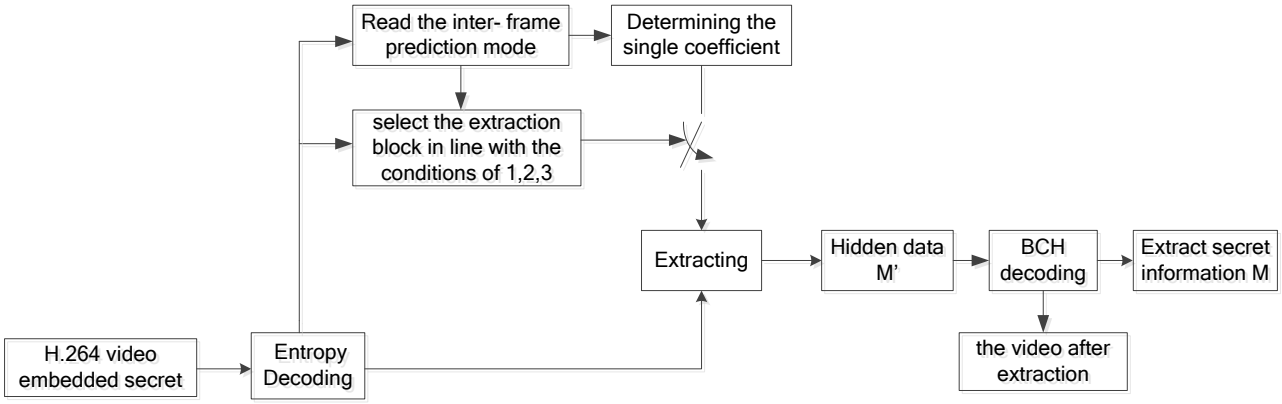

Fig. (4). The Extracting Operation Process of Single Coefficient BCH Robustness Method.

Table 1. Performance Comparison of Different BCH Code.

Video	BCH	PSNR1 (dB)	PSNR2 (dB)	The Survival Rate by not Using BCH (%)	The Survival Rate by Using BCH (%)
Mobile	(7,4,1)	34.61	44.42	91.47	94.42
	(15,11,1)	34.59	44.21	90.22	93.12
	(31,26,1)	34.59	44.22	90.76	92.71

that the prediction mode of adjacent block meets the conditions 1, 2 and 3. The method to extract the information is described as follows.

If $\left|\tilde{Y}_{ij}\right|$=N+2, or $\left|\tilde{Y}_{ij}\right| \neq$ N+2, or $\left|\tilde{Y}_{ij}\right| \neq$ N+1, we will amend $\tilde{Y}_{ij}$ in the light of formula (7). If the embedding bit is 1 and $\left|\tilde{Y}_{ij}\right|$=N+1, $\tilde{Y}_{ij}$ will be revised according to formula (8). If the embedding bit is 0 and $\left|\tilde{Y}_{ij}\right|$=N, then $\tilde{Y}_{ij}$ would not need to be modified.

$$\tilde{Y}_{i,j} = \begin{cases} \tilde{Y}_{i,j} - 1, & \text{if } \tilde{Y}_{i,j} \geq 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+2}, \\ \tilde{Y}_{i,j} + 1, & \text{if } \tilde{Y}_{i,j} < 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+2}, \\ \tilde{Y}_{i,j}, & \text{if } \left|\tilde{Y}_{i,j}\right| \neq \text{N+2 or} \left|\tilde{Y}_{i,j}\right| \neq \text{N+1}. \end{cases} \quad (7)$$

$$\tilde{Y}_{i,j} = \begin{cases} \tilde{Y}_{i,j} - 1, & \text{if } \tilde{Y}_{i,j} \geq 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+1}, \\ \tilde{Y}_{i,j} + 1, & \text{if } \tilde{Y}_{i,j} < 0 \text{ and } \left|\tilde{Y}_{i,j}\right| = \text{N+1}. \end{cases} \quad (8)$$

After extracting information M ' , we can decode the M' and achieve the secret information. The simple embedding and extracting process for the method brings great convenience to realize it. At the same time, the method has minor time-complexity [8].

4. ANALYSIS AND COMPARISON OF EXPERIMENTAL RESULTS

The method has been implemented on JM which is the standard H.264 video codec software. The test video has 300 frames and the encoding-frame rate is 30 frames /sec. The frame interval of code I is 15, and the quantization parameter is 28. The test video sequence is News which resolution is 176 * 144. For "PSNR1", Peak Signal to Noise Ratio 1, is calculated by comparing uncoding YUV video file and embedding video file. For "PSNR2", Peak Signal to Noise Ratio 2, is calculated by comparing the decoded video of H.264/AVC which does not have the embedding information and the embedding video.

4.1. The Error Correcting Performance of BCH

BCH code is a powerful tool to recover error bits in information hiding. It will cause the embedding bit not extracted correctly so that video processing or attack will change prediction mode and DCT coefficient [9]. Therefore, we take recoding-weight as an example to test the BCH performance of the method through embedding the information in the coefficient,

$$\tilde{Y}_{30}, \tilde{Y}_{21}, \tilde{Y}_{31}, \tilde{Y}_{12}, \tilde{Y}_{22}, \tilde{Y}_{32}, \tilde{Y}_{03}, \tilde{Y}_{13}, \tilde{Y}_{23}, \tilde{Y}_{33}.$$

Table **1** gives the comparison test results by using and not using BCH codes when recoding. The experiment for all

(a) original frame

(b) embedding frame

(c) recoding embedding frame

(d) extracting frame

Fig. (5). Four Different Frames of News.

I frames is used in fixed step size 28. From Table **1**, we can see that the value of PSNR1 is greater than 34dB, and PSNR2 is greater than 44dB. These values prove that the method has good concealment [10]. The experimental results show that BCH(7,4,1) has the strong ability to correct bit error, and the survival rate of embedded bit is 94.42%. So we adopt the BCH(7,4,1) to use in the following experiment.

4.2. The Recovery Probability Analysis of Original Video

The method takes into account the recovery of carrier in the extraction of secret information. If there are n blocks of 4*4, we select the coefficient to modify which value is N. The number of coefficient is pi when the absolute value of DCT coefficient of the i block equals to N+2. The formula (9) gives the bit recovery rate of original video.

$$\frac{1}{n}\sum_{i=1}^{n}(1-\frac{P_i}{16}) \tag{9}$$

Fig. (**5**) gives the News comparison chart which contains the original frame, embedding frame, recoding embedding frame and extracting frame. From Fig. (**5**), we can see that four contrast diagrams of News have no obvious change. The method obtains better visual hiding effect, high robustness and can recover the original video.

CONCLUSION

We have researched on the steganography robustness method of BCH single coefficient, and proposed the design scheme and implementation steps. The method takes recoding and re-quantization in video processing as an example to test the error recovery capability of BCH code. In all the test codes, BCH (7,4,1) has the most powerful error correcting capability on correcting a mistake of bits. Compared to not using the BCH method, the survival rate of embedded bits can be improved by 20% by the use of the BCH method. When the recoding attacks, the survival rate is 100% of embedded bits by BCH code. The method achieves the restoration of the original video in the extraction of secret information. The process is simple and quick, and can adapt to the requirements of real-time video.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work is financially supported by the National Natural Science Fund, China (No 61103143), basic and frontier project of Science and Technology Department of Henan province, China (No 142300410334).

REFERENCES

[1] R.B. Wolfgan, C. I. Podilchuk, and E. J. DelP, "Perceptual Watermarking for Digital Images and Video", *Phil. Trans. Roy. Soc. London*, vol. 87, pp. 1108-1126, 1999.

[2] J. Hemandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain Watermarking Techniques for Still images: Detector Performance Analysis and a New Structure", *IEEE Transactions on image Processing*, vol. 9, pp. 53-68, 2000.

[3] C. Nguyen, D. Tay, and G. Deng, "A Fast Watermarking System for H.264/AVC Video", *IEEE Asia Pacific Conference on Circuits and Systems*, APCCAS'06. Singapore, pp. 81-84, 2006.

[4] H. Luo, "Research on the algorithm of H.264 video steganography and implement in the embedded platform", *Chang sha:Hunan University*, 2009.

[5] H. J. Kim and R. Zhang, "Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding", In: *Proceedings of the 11th ACM Multimedia & Security Workshop*, pp. 131-140, 2009.

[6] Z. Ni, Y. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication", *IEEE Trans Circ Syst Video Tech*. vol. 18, pp. 497-509, 2009.

[7] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed-domain video watermarking resistance to geometric distortions", *Journal of Software*, vol. 19, pp. 70-79, 2012.

[8] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Computer Application,* vol. 89, pp. 1129-1143, 2009.

[9] 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. 21, pp. 1130-1138, 2011.

[10] Y. Hu, C. Zhang, and Y. Su, "Information Hiding for H.264/ AVC", *Acta Electronica Sinica*, vol. 36, pp. 690-694, 2010.

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