An Effective Selective Encryption Scheme for HEVC based on Rossler Chaotic System

Fei Peng†, Han-yun Li†, Min Long‡

† College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan, PRC, 410082
‡ College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, Hunan, PRC, 410014

Abstract–To strengthen the protection of privacy information in videos, a selective encryption scheme for high efficiency video coding (HEVC) is proposed in this paper. In this scheme, the pseudo random binary sequence generator is first constructed based on Rossler chaotic system. After that, the generated key stream is used to encrypt the motion information and residual coefficients of HEVC. Especially for the encryption of residual coefficients, the improved scrambling effect is achieved by encrypted DC coefficients. Experimental results and analysis show that the proposed scheme can produce a good encryption effect, and keep the encrypted stream format-compliant.

1. Introduction

HEVC is the latest video coding standard [1], which can get a lower bitrate than those of the previous video coding standards. However, the computational complexity is greatly increased. As video has the characteristics such as large amount of data, real-time demands, and diverse storage format, etc., traditional encryption algorithms which encrypt all data cannot meet the requirement of the video encryption. In addition, different application scenarios for video encryption algorithms have different security requirements.

As the encoding details of HEVC is different from that of H.264, the existed encryption algorithms for H.264 cannot directly used for HEVC. Therefore, the encryption of HEVC should consider the encoding characteristics of HEVC.

The rest of the paper is organized as follows. The related work is introduced in Section 2. The selective encryption scheme for HEVC based on Rossler chaotic system is presented in Section 3. Experimental results and analysis are provided in Section 4. Finally, some conclusions are drawn in Section 5.

2. Related works

Currently, the existed video encryption methods can be classified into two categories: full video encryption and selective video encryption.

2.1 Full video encryption

Full video encryption encrypts all video data with traditional encryption algorithms such as DES, AES and RSA. A typical full encryption algorithm is video encryption algorithm (VEA) proposed by L. Qiao [2]. A symmetric encryption algorithm international data encryption algorithm (IDEA) is used as a key generator, and the MPEG video stream is completely encrypted. Full encryption can keep the size of video stream and achieves the highest security, but the computational cost is high and capability of format-compliance is limited.

2.2 Selective video encryption

Selective video encryption only encrypts partial data of video that has the most significant influence on the construction of video image, which can achieve high computational efficiency and format-compliance of bitstream. In addition, it can encrypt different sensitive data to meet different security requirements.

In the past years, a variety of selective encryption algorithms have been proposed for H.264. J. Ahn *et al.* proposed to scramble the intra prediction modes [3]. It can obtain effective scrambling effect and keep the compression ratio. Meanwhile, it is format-compliance. Y. Wang *et al.* proposed to encrypt the sign of MVD [4]. The encryption of the sign of MVD distorts the pictures predicted by inter prediction. It can achieve a high computational efficiency. Z. Shahid *et al.* proposed to encrypt nonzero coefficients of residual coefficients [5]. As the encrypted video with error residual information results in unrecognized images, a good perceptual security is obtained.

Due to the differences between HEVC and H.264, the selective encryption algorithms for H.264 cannot be directly used for HEVC. For example, if intra prediction modes of HEVC are encrypted, the encrypted video cannot be decoded by general decoder of HEVC because the encryption of intra prediction modes of HEVC is not format-compliance. To adapt for the new characteristics, G.V.Wallendae *et al.* observed some syntax elements of HEVC which are suitable for video encryption with format-compliance [6], and a format compliance encryption algorithm for HEVC was proposed in [7]. However, the scrambling effect is limited.

From the above analysis, although some selective encryption algorithms for H.264 have been put forward,

their adaption capability for HEVC is limited. Meanwhile, as a new video encoding standard, the encryption methods which are aimed specially at HEVC are few. In this paper, based on the method in [7], a selective encryption scheme for HEVC is proposed to strength the perceptual security.

3. Proposed Encryption Scheme

3.1 Rossler Chaotic System

Chaotic system is sensitive to initial conditions and system parameters, and it has characteristics such as pseudo randomness, uncertainty, ergodicity and fractal dimension, etc. So, there has close connection between chaos and cryptography. In the past decades, some studies have been done on how to use chaos in cryptosystems [8].Several image and video encryption methods based on chaotic system are reported in [9-11].

Rossler chaotic system [12] is defined as:

$$\begin{cases} x = -y - z \\ y = x + ay \\ z = b + z(x - c) \end{cases}, \quad (1)$$

where a, b and c are the parameters of the system. When a=0.2, b=0.2, c=5.7, the chaotic system is in a chaotic state.

3.2. Generation of Chaotic Sequence

When Rossler system is in a chaotic state, the sequence $\{(x_k, y_k, z_k)|k=0, 1, 2, \ldots\}$ generated from Rossler system by fourth order Runge-Kutta method is sensitive to initial values, aperiodic and non-convergence. Therefore, the binary key sequence generator based on Rossler chaotic system is constructed as follows:

Step 1: Set the initial values (x_0, y_0, z_0) for Rossler system.

Step 2: Iterate Rossler system for $t+len$ times with fourth order Runge-Kutta method, where len is the length of key sequence and the step length h is 0.001. To avoid the transition effect in the iteration, the first t iteration results are discarded.

Step 3: For each iteration results z_n , select the continuous 8 numbers after its decimal point to form an integer number Z_n. S_n can be obtained as

$$S_n = 1 + (Z_n \bmod 12), \quad (2)$$

where $Z_n = \left\lfloor (|z_n| - \lfloor |z_n| \rfloor) \times 10^8 \right\rfloor$.

Step 4: Generation of binary sequences. Select the S_n^{th} number after the decimal point of x_n and y_n, respectively, to get X_n and Y_n. key_i can be obtained as

$$key_i = \begin{cases} 1, & both\ X_{n_i}\ and\ Y_{n_i}\ are\ odd\ or\ even \\ 0, & otherwise \end{cases}, \quad (3)$$

where $\begin{cases} X_{n_i} = \left\lfloor (|x_n| \times 10^{S_{n-1}} - \lfloor |x_n| \times 10^{S_{n-1}} \rfloor) \times 10 \right\rfloor \\ Y_{n_i} = \left\lfloor (|y_n| \times 10^{S_{n-1}} - \lfloor |y_n| \times 10^{S_{n-1}} \rfloor) \times 10 \right\rfloor \end{cases}$.

In this way, a binary sequence $key=\{key_1, key_2, \ldots, key_n\}$ is generated from Rossler system.

3.3. Description of the Encryption Algorithm

(1) Encryption of the Sign of MVD

In the entropy encoding of MVD, the sign and the absolute value are separately encoded. The encryption of the sign of MVD is represented as

$$en\_MVDSign = MVDSign \oplus key, \quad (4)$$

where key represents the key stream generated by Rossler system , $MVDsign$ and $en\_MVDSign$ represent the original sign bit of MVD and the encrypted sign bit of MVD sign, respectively, and $\oplus$ represents XOR operation.

(2) Encryption of Motion Vector Prediction (MVP) Index

Before the entropy encoding of MVP index, it is encrypted by key stream generated from Rossler system and an encrypted MVP index is obtained. The encryption is represented as

$$en\_MVPIdx = MVPIdx \oplus key, \quad (5)$$

where $MVPIdx$ and en_MVPIdx represent the original MVP index and the encrypted MVP index, respectively.

(3) Encryption of Reference Index

Similar to the encryption of MVP index, the encryption of reference index is obtained by performing XOR operation between the key steam and the reference index, and it is described as

$$en\_RFI = \begin{cases} RFI \oplus key & (RFI \neq 2\ or\ RN \neq 3) \\ RFI & (RFI = 2\ and\ RN = 3) \end{cases}, \quad (6)$$

where RFI and en_RFI represent the original reference index and the encrypted reference index, respectively, and RN represents the number of candidate reference pictures.

It should be noted that the reference index cannot be encrypted when it equals 2 when the number of candidate reference pictures in the reference picture list is 3. Because the encryption results may be 3, which will be out of the preset range (from 0 to 2), it impose influence on the format compliance of the HEVC stream.

(4) Encryption of Merge Index

In the merge mode of HEVC, the number of merging candidates is set as 5, so the range of merge index is from 0 to 4. If the merge index equal 4, the result of encryption maybe 5, which is out of the range and format compliance of HEVC stream will be influenced. Here, only the merge indices whose values less than 4 are selected for encryption, and it is described as

$$en\_MI = \begin{cases} MI \oplus key & (MI \neq 4) \\ MI & (MI = 4) \end{cases}, \quad (7)$$

where MI and en_MI represent the original merge index and the encrypted merge index, respectively.

During the encoding process of HEVC, the encryption of the matched motion parameters will results in the prediction errors in B frame or P frame in the decoding process. Thus, the video images will be scrambled.

(5) Encryption of the Sign of Residual Coefficient

The encryption of residual coefficient sign is similar to that of the sign of MVD. It is described as

$$en\_CoeffSign = CoeffSign \oplus key\ , \qquad (8)$$

where *CoeffSign* and *en_CoeffSign* represent the sign of the original residual coefficient and the sign of the encrypted residual coefficient, respectively.

Since the encryption of the above syntax are accomplished by using XOR operation with key stream generated by Rossler chaotic system, the decryption of them is just the inverse of it.

(6) Encryption of DC Coefficient

For the encryption of DC coefficient, every bit of the key stream is regarded as a switch to control whether the current DC coefficient in residual information is encrypted or not. If the current key bit is 1, the encrypting operation will be performed. Otherwise, the DC coefficient will be kept unchanged. In order to preserve format-compliance of HEVC and guarantee the decrypted DC coefficients is the same as the original one, different encryption policy is implemented for the DC coefficients with the value of 0 and 1. The encryption process is described as

$$en\_CDC = \begin{cases} CDC\text{-}2\ , (CDC \neq 1, 2) \quad (key = 1) \\ CDC\text{-}3\ , \ (CDC = 1, 2) \quad (key = 1) \\ CDC \quad (key = 0) \end{cases}\ , \qquad (9)$$

where *CDC* and *en_CDC* represent the original DC coefficient and the encrypted DC coefficient, respectively.

The decryption of DC coefficient is just the inverse process of the encryption, and it is described as

$$de\_CDC = \begin{cases} en\_CDC + 2\ , (CDC \neq -2 - 1) \quad (key = 1) \\ en\_CDC + 3\ , \ (CDC = -2, -1) \quad (key = 1) \\ en\_CDC \quad (key = 0) \end{cases}\ , \qquad (10)$$

where *de_CDC* represents the decrypted DC coefficient.

4. Experimental Results and Analysis

Experiments are performed on HEVC test Model 12.0(HM 12.0), whose encoding mode is random access mode[13]. 7 video sequences are selected for the experiments, and the comparison is also made between the encryption method in [7] and the proposed method. 50 frames are encoded for every video, and their quantization parameter (QP) is 32.

4.1. Analysis of Perceptual Security

Perceptual security specifies the perception of video contents in human's eyes. If the encrypted video contents are more difficult to be understood and identified, it demonstrates that the perceptual security of encryption is better. The encrypted results of City, Coastguard and Foreman obtained from the method in [7] and the proposed method are shown in Figure 1.

(a) (b) (c)

Figure 1 The encrypted results of Foreman with different methods. (a) represent the original video sequence, (b) represent the encryption results by using method in [7], and (c) represents the encryption results by using the proposed method

As seen from Figure 3, it can be found that the scrambling effect of the proposed method is better than that of the method in [7]. In addition, PSNR and SSIM [14] are used for the evaluation of perceptual security of the encryption methods. The results are shown in Table 1.

Table 1. PSNR and SSIM of the encrypted video sequences

Sequences	Method in [7]		Our Method	
	PSNR	SSIM	PSNR	SSIM
City	15.41	0.1337	11.91	0.0770
Coastguard	14.44	0.1239	11.37	0.0881
Flower	9.48	0.2412	7.12	0.1412
Foreman	10.94	0.2292	7.95	0.1374
Mobile	9.56	0.0807	7.65	0.0571
Soccer	11.61	0.2410	9.28	0.1517
Stefan	12.27	0.1895	10.59	0.1486
Average	11.96	0.1770	9.41	0.1144

As seen from Table 1, the PSNR and SSIM of the encrypted results of the proposed method is smaller than that of the method in [7] for every video sequence, which indicates that the good perceptual security of the proposed method.

4.2. Analysis of computation complexity

In the scheme, encryption operations are performed to approximate 50% of the syntax elements. However, the encryption operations are XOR or subtraction, whose computation complexity is relatively low. Thus the executions of proposed encryption scheme are at high speed, whose influence on encoding efficiency is very limited.

4.3. Analysis of key space

Key space specifies the number of keys for generating different key stream. A larger key space means that a good capability of resisting exhaustive attack. For the proposed algorithm, the initial value and the iteration time of Rossler chaotic system can be used as key. Given the initial values (x_0, y_0, z_0) are in double-precision floating-point format, and the range of iterations is [2000, 4000], the key space is

$$S_k = \text{Card}\{x_0\} \cdot \text{Card}\{y_0\} \cdot \text{Card}\{z_0\} \cdot \text{Card}\{t\} = 10^{15} \times 10^{15} \times 10^{15} \times 2 \times 10^3 = 2 \times 10^{48} \approx 2^{160} \quad (11)$$

where $\text{Card}\{\cdot\}$ represents the cardinality of a set.

As the key space is approximately 2^{160}, it is effective in resisting exhaustive attack.

4.4. Analysis of key sensitivity

Key sensitivity is very important for a cryptosystem. Here, experiments are done to evaluate the key sensitivity of the proposed method. When a small value 10^{14} is added to the initial value x_0 of Rossler system (the other parameters are kept the same), the results are shown in Figure 2.

(a) Decrypted video with correct key

(b) Decrypted video with changed key

Figure 2. The results of sensitivity test

As seen from Figure 2, it can be found the decrypted video with a changed key displays obvious error comparing with the correct decrypted video, which demonstrates that the proposed encryption algorithm has good key sensitivity.

5. Conclusion

In this paper, a selective encryption scheme for HEVC based on Rossler chaotic system is proposed. Experimental results and analysis show that the proposed encryption scheme is format-compliance, and has better perceptual security than the method in [7]. Furthermore, the key stream generated from Rossler system has large key space and key sensitivity, which provides high security to the proposed encryption scheme. The proposed selective encryption of HEVC has great potential in video data protection.

Acknowledgments

This work was supported in part by project supported by National Natural Science Foundation of China (Grant No. 61370225, 61402162), project supported by Hunan Provincial Natural Science Foundation of China (Grant No.2015JJ2007), project supported by Research Plan of Hunan Province (Grant No. 2014FJ4161).

References

[1] G. J. Sullivan, J. R. Ohm, W.J. Han, and T. Wiegand, "Overview of the high efficiency video coding (HEVC) standard, " *IEEE Transaction on Circuits and Systems for Video Technology*, 2012, 22(12):1649-1668.

[2] Qiao L, Nahrstedt K. "A New Algorithm for MPEG Video Encryption" *Proceedings of the First international Conference on Imaging Science, Systems and Technology* (CISST'97), Las Vegas, USA, 1997.

[3] Ahn J, Shim H J, Jeon B, et al. "Digital video scrambling method using Intra-prediction mode,"*Proceedings of the 5th Pacific Rim conference on Advances in Multimedia Information Processing* - Volume Part III. Tokyo, Japan, 2004: 386-393.

[4] Wang Yajun, Cai Mian, Tang Feng. "Design of a new selective video encryption scheme based on H.264," *Proceedings of the international Conference on Computational Intelligence and Security*, 2007: 883-887.

[5] Shahid Z, Chaumont M, Puech W. "Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns," *16th IEEE international Conference on Image Processing (ICIP)*, Cairo, 2009: 1273-1276.

[6] G. Van Wallendael, A. Boho, J. De Cock, A. Munteanu, and R. Van de Walle. "Encryption for High Efficiency Video Coding with video adaptation capabilities," *IEEE International Conference on Consumer Electroics* (ICCE), Las Vegas, USA, Jan. 2013.

[7] G. Van Wallendael, J. De Cock, S. Van Leuven, A,Boho, P. Lambert, B. Preneel, and R. Van de Walle. "Format-compliant encryption techniques for high efficiency video coding," *20th IEEE international Conference on Image Processing* (ICIP), 2013: 15-18.

[8] L. Shujun, G. Chen, and X. Zheng. "Multimedia Security Handbook." eds. B. Furht and D. Kirovski, 4, 2005.

[9] D. Arroyo, C. Li, G. Alvarez, W. A. Halang. "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm." *Chaos, Solitons & Fractals*, 2009, 41(5): 2613-2616.

[10] S. Li, X. Zheng, X. Mou and Y. Cai. "Chaotic encryption scheme for real-time digital video," RealTime Imaging VI, Proceedings of SPIE, Volume 4666, 2002:149-160.

[11] S. Lian, J. Sun, J. Wang and Z. Wang. "A chaotic stream cipher and the usage in video protection," Chaos, Solitions & Fractals, 2007, 34(3):851-859.

[12] O. E. Rossler. "An equation for continuous chaos," Phys. Letters A, 1976, 57:397-398

[13] F. Bossen, D. Flynn, and K. Suhring. "HEVC Reference Software Manual, " JCTVC-F634,6th Meeting, Jul.2011

[14] Z. Wang, A.C.Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transaction on Image Processing*, 2004, 13(4): 600-612.