Send Orders for Reprints to reprints@benthamscience.ae

768 *The Open Cybernetics & Systemics Journal,* 2014, *8,* 768-772

Open Access

Research on Real-Time Video Encryption Algorithm Based on Moving Objects

Wei Chen* and Changan Ding

Center of industry, Nanjing Institute of Technology, Nanjing, 211167, China and School of Computer Engineering, Nanjing Institute of Technology, Nanjing, 211167, China

Abstract: How to ensure the security and efficiency of real-time video transmission in the existing network environment is increasingly becoming an urgent problem to be solved. This paper presents a moving object-based video encryption algorithm, which can satisfactorily resolve the tradeoffs between security and efficiency of real-time video transmission. A real-time video encryption algorithm based on moving objects is proposed, which combines the extraction of moving objects with the entropy coding-based encryption algorithm, and encrypt only the extracted moving objects. Experimental results show that the algorithm has small computational overhead, and good encryption real-timeliness, which can achieve favourable tradeoffs between security and coding efficiency, and meet real-timeliness requirements.

Keywords: Entropy coding, moving object, video encryption.

1. INTRODUCTION

With the rapid development of computer and network technologies, network multimedia services have become a new field of application of network services. However, due to the openness and anonymity of network, multimedia contents transmitted over the network are vulnerable to attacks [1]. The existence of vandalism, theft and piracy of video data has made video security coding gain more and more attention. Conventional video encryption algorithms are unable to meet the requirements of video encryption with different application needs, so they cannot protect the security of video contents [2]. Due to some inherent characteristics of videos (such as large data size, high real-timeliness requirements and diverse storage formats), encryption of video streams using conventional algorithms is somewhat inefficient, while the selective encryption algorithms which have higher efficiency are not secure enough; so how to design an encryption algorithm to obtain a favorable tradeoff between security and coding efficiency is a concern [3]. This paper focuses on discussing the entropy coding-based encryption method, and designs a real-time video encryption algorithm based on moving objects, in order to meet the needs of video privacy protection [4].

2. RESEARCH STATUS AND REQUIREMENTS ON VIDEO ENCRYPTION

Research on video encryption began in the mid-1990s; with the constant expansion of the application scope of digital videos, demand for digital video encryption has also been increasing. Researchers at home and abroad have been looking for and developing algorithms with high encryption speed plus high security level that have less impact on video data. In this area, some foreign universities, companies and research institutes started earlier. For example, DePaul University established the Networking and Security Lab for this purpose, and some of the world's leading information industry companies like Microsoft, IBM and NEC have all invested rather substantially in this area. Important conferences in the field of computer research such as IEEE and SPIE have also published quite a few papers on video encryption in their proceedings. Domestically, Tsinghua University, Shandong University and Xi'an Jiaotong University are the early starters. Onets company's products have been developed and put into use. But they are still somewhat away from achieving video security in a real sense.

In consideration of the inherent characteristics of video data such as large data size, high redundancy and high real-timeliness, and given that the compressed video data are required to have functions such as data location indexing and coding rate control, the encryption of video data, in general, should meet the following requirements [5]:

Security: It is generally believed that when the cost for deciphering an encrypted video or restoring a video to tolerable watching conditions is greater than the cost for directly purchasing a video, the encryption system is secure.

Compression ratio: Encrypted video data are required to have a compression ratio similar to the unencrypted data, so as to maintain data size basically constant.

Real-timeliness: Video data are often required to be transmitted and accessed in real time, so the encryption and decryption processes should not bring too much delay to the whole process.

Video format: This requirement is often referred to as compatibility feature. For video data, such a requirement is common, that is, we hope we can make some typical video

1874-110X/14

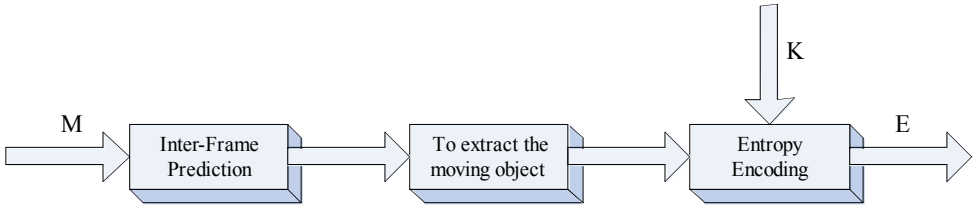

Fig. (1). Algorithm flow chart.

application-related operations, such as addition, deletion and clipping, on videos without decrypting the encrypted videos. Such a requirement actually puts forward a request for the weak homomorphism of video encryption, that is, on the premise of ensuring security, the format and flag bit information of video data are remained unchanged or made able to be normally decoded as far as possible [6]. In this way, the security of video consists purely in the video data itself, while the encrypted video data can still be decoded normally from a format perspective.

Data operability: In some cases, operations such as rate control, image tile clipping, pasting, addition and deletion may be needed on video data. At this time, encryption algorithms are required to be able to maintain the operability of the data encrypted.

Many encryption algorithms for video streams proposed over the past decade satisfy security requirements of different levels in certain areas of the above requirements, of which major improvements are mostly targeting the real-timeliness requirements [7]. Because for network video applications, ensuring real-timeliness is sometimes even more important than the security requirement itself; besides, this requirement is in fact also closely related with the compression ratio requirements. Under normal circumstances, these algorithms are distinguished in the following manner:

Direct encryption algorithms: This category of algorithms is actually the direct application of common encryption algorithms in video encryption field, which encrypts video data directly as normal binary data [8];

Selective encryption algorithms: These algorithms only selectively encrypt part of data during video encoding process;

Entropy coding encryption algorithm: It is an encryption algorithm which combines the video encoding and compression processes.

In summary, despite the different applications of existing three mainstream video encryption schemes in different application fields owing to their respective advantages and disadvantages, tradeoff problems are widely present in the aspects of security and compression ratio, security and operability, as well as security and universality. This paper preferably solves the tradeoff between security and real-timeliness through the encryption of moving objects only [9].

3. MOVING OBJECTS-BASED ENCRYPTION ALGORITHM

3.1. Extraction of Moving Objects

Moving object is an important region of interest in the video [10]. In this paper, moving objects are extracted using the motion vectors generated during video encoding process. The algorithm flow chart is shown in Fig. (**1**), where M denotes the original data stream, K denotes the key, and E indicates the video data after encryption.

3.1.1. MV Prediction Method

To reduce the computational complexity of MV prediction, researchers have proposed a variety of fast MV prediction techniques, including: (1) special search mode; (2) motion vector (MV) prediction; (3) dynamic search range (SR) adjustment; (4) threshold-based search stopping technology; (5) block distortion reuse; (6) inter mode decision, etc.

However, computational complexity and rate-distortion performance of MV prediction are two factors difficult to balance [11]. To address high computational complexity of MV prediction algorithms with better rate-distortion performance, this paper proposes a fast MV prediction algorithm.

In fact, movements of objects with a two frame difference are generally rigid translational motion without large displacement, so a frame of image is often divided into several M×N blocks, and motion vectors are assigned in units of blocks, which greatly reduces the overall code rate. The translational motion of the rigid body is shown in Fig. (**2**).

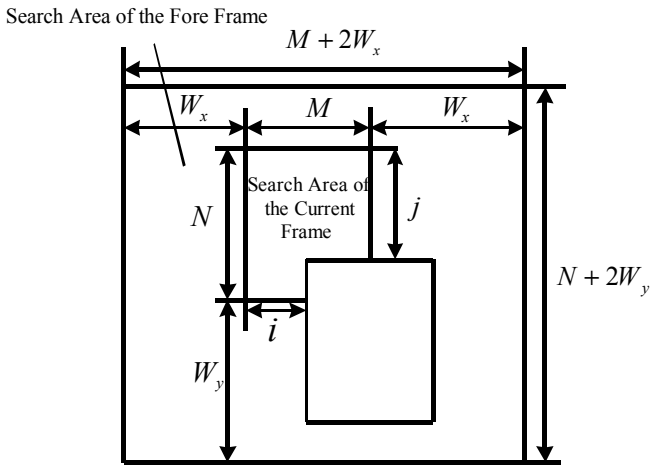

Fig. (2). The translational motion of the rigid body.

Firstly, fast MV prediction algorithm forms a MV_List of adjacent blocks; then, the identical or similar MVs in the MV_List are combined to form MV_Groups; at last, each MV_Group generates a prediction motion vector that represents the motion characteristics of their respective groups [12]. MV prediction is performed on the current macro block (CMB), ideally, MV_List shall include MVs of all spatially adjacent sub-blocks, just like the MVs of twenty 4×4 blocks numbered 1-10 and 21-30 in Fig. (**3**).

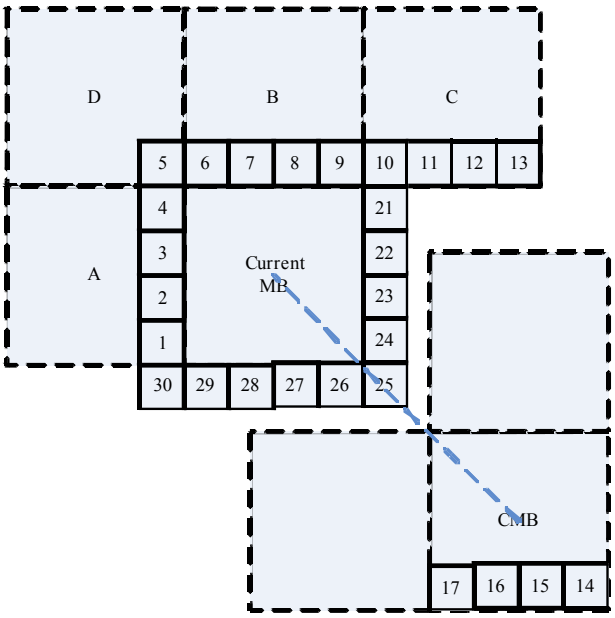

Fig. (3). The MV list.

However, since the macro blocks are encoded in raster scan order, when encoding CMB, only the adjacent macro blocks in the left, upper, right upper and left upper sides (labelled sequentially as A, B, C and D) are already-encoded, whereas the MV values of adjacent sub-blocks numbered 21-30 are unknown. To improve the MV prediction accuracy, this paper replaces the MV of sub-blocks 21-25 with MV of sub-blocks 11-13 in adjacent macro block C, and replaces the MV of sub-blocks 26-30 with MV of sub-blocks 14-17 in spatially adjacent macro block c/.

MVs contained in the MV_list are adjacent sub-blocks, whose motion trends are usually the same or similar. This paper defines MVth, the threshold for MV, to distinguish between different MVs. If two MVs satisfy Formula 1, then these two MVs are considered to have different motion trends (MVl≠MV2), otherwise, the two MVs are considered close (MVl≈MV2).

$$|MVxl-MVx2| \geq MVth \text{ or } |MVyl-MVy2| \geq MVth \quad (1)$$

MVs are grouped based on similarity; an effective approach is to sort MVs by x and y components, and then divide them into groups by threshold MVth. Since the blocks with the same motion trend are generally spatially continuous, it is highly probable that the neighboring MVs are identical; thus this paper proposes a simplified MV grouping method. MVs are arranged in numerical order shown in Fig. (**2**), and grouped using Formula (2). MV1, the first value in the MV_List, is included in the first group MV_Group1. Afterwards, MVs in the MV_List are grouped using Formula (2) in an ascending order of their serial numbers. Suppose MVi-1 belongs to MV_Groupi, if MVi is similar to MVi-1, then MVi is also included in MV_Groupi, otherwise MVi is included in the next MV group MV_Croupj+1.

MVs are grouped based on similarity; an effective approach is to sort MVs by x and y components, and then divide them into groups by threshold MVth. Since the blocks with the same motion trend are generally spatially continuous, it is highly probable that the neighboring MVs are identical; thus this paper proposes a simplified MV grouping method. MVs are arranged in numerical order shown in Fig. (**2**), and grouped using Formula (2). MV1, the first value in the MV_List, is included in the first group MV_Group1. Afterwards, MVs in the MV_List are grouped using Formula (2) in an ascending order of their serial numbers. Suppose MVi-1 belongs to MV_Groupi, if MVi is similar to MVi-1, then MVi is also included in MV_Groupi, otherwise MVi is included in the next MV group MV_Croupj+1.

$$MV_i \in \begin{cases} MV\_Group_1 & (i=1) \\ MV\_Group_j \left(\begin{matrix} i>1, MV_{i-1} \in MV\_Group_j, \\ MV_i \approx MV_{i-1} \end{matrix} \right) & \\ MV\_Group_{j+1} \left(\begin{matrix} i>1, MV_{i-1} \in MV\_Group_j, \\ MV_i \neq MV_{i-1} \end{matrix} \right) & \end{cases} \quad (2)$$

3.1.2. Encryption Module Selection based on MV

For macro block with coordinates of (i,j), its motion intensity can be defined by (3).

$$MI\_MB(i,j) = \begin{cases} \sqrt{Mv_{xi,j}^{\ 2} + Mv_{yi,j}^{\ 2}} & MB_{i,j} \text{ is inter Block} \\ 0 & MB_{i,j} \text{ is intra Block} \end{cases} \quad (3)$$

where Mvxi,j and Mvyi,j denote the motion vectors of macro block in the x and y directions, respectively. Here, if an inter macro block has plural motion vectors, then its motion vector is the mean of motion vectors of sub-blocks it contains, see Formula (4):

$$MIF\_MB(i,j) = \sum_{m,n} \frac{MI\_MB(m,n)}{S_{partition}(i,j)} \quad (4)$$

where Spartition represents the total number of sub-blocks included in a macro block. In addition, this paper defines the motion intensity of a frame of video by Formula (5):

$$MIF(i,j) = \sum_{i=0}^{N_x - 1} \sum_{j=0}^{N_y - 1} MIF\_MB(i,j) \quad (5)$$

where Nx and Ny denote the numbers of macro blocks of a frame of video in the x and y directions, respectively. Next, this paper defines the encryption region of video image based on the relationship between the value of and MV of macro block by Formula (6)

$$S_{MB(i,j)} = \begin{cases} required\ \ encryption\ \ MB(i,j) & Macroblock\, MI\_MB(i,j)\ equal\ \textbf{to}\ 0 \\ required\ \ encryption\ \ MB(i,j) & Macroblock\, MI\_MB(i,j) > MIF(i,j) + \delta \\ NOT\ encrypted\ \ Macroblock\, MI\_MB(i,j) & \leqslant MIF(i,j) + \delta \end{cases} \quad (6)$$

where δ is the encryption strength adjustment factor, the greater its value, the more quantitative the selected encrypted macro blocks, and the higher the encryption strength.

3.2. Macro Block Encryption Method

In this paper, chaotic system is used to encrypt the extracted moving objects, the reason this approach is adopted is

that the chaotic signals generated by some well-established and simple dynamic systems can exhibit very complex pseudo-randomness [13]; any small initial deviation can be amplified exponentially over time. Thus, just a small number of parameters about initial state are enough to generate chaotic cipher sequences meeting the basic characteristics of cryptography, which have natural pseudo-randomness, so it is particularly suitable for encrypting information.

Because chaotic system has both composite and diffusion characteristics, it is in full compliance with the requirements of cryptography, so it is a natural cryptosystem. Meanwhile, the irregularity of chaos on two-dimensional phase plane makes chaotic system more suitable for the encryption of image data. This paper uses Logistic chaotic sequence mapping for encryption.

After determining the region of video to be encrypted according to the above method, the following encryption algorithms are used to implement encryption process on these selected macro blocks: encrypt of MVs and low order part of DC coefficients [14].

Firstly, chaotic sequence Mi of real numbers with a length less than N is generated by setting the initial value X0 of Logistic chaotic mapping which is shown in Formula (7) and system parameter μ, where Mi is composed of k consecutive Xl (k denotes quantity) generated by Logistic mapping;

$$X_{n+1} = \mu(1 - X_{n\_})X_{n\_}, {}_{n} \in (0,1], \mu \in (0,4] \tag{7}$$

Next, the chaotic sequence Mi of real numbers generated by Logistic mapping is transformed into a binary sequence Mi according to Formula (8);

$$f(n) = \begin{cases} 0 & 0 < X_n < 0.5 \\ 1 & 0.5 \le X_n < 1 \end{cases} \tag{8}$$

Finally, bitwise XOR is performed between the DCj coefficients and motion vectors of all QDCT of macro blocks need to be encrypted and the chaotic sequence Mi to obtain the encrypted DCj coefficients and motion vectors. Here, in order to prevent the encrypted DC coefficients from exceeding the indication range of encoder, and to reduce the impact of encryption on the encoding output rate, only the low order part of encrypted DC coefficients is selected. Nonzero AC (coefficient sequence number, defines a random number S(1≤S≤Q).

The position of nonzero AC coefficients in QDCT block is scrambled. Since the scrambling only changes the position of nonzero AC coefficients in QDCT block, without changing the values of AC coefficients, run length and number of run two-tuples, from the perspectives of statistics and coding theory, the scrambling has minimal impact on encoding output rate. At last, these encrypted video data are encapsulated into video bit streams in accordance with the video coding standards, thus, the entire encryption process is completed [15].

4. PERFORMANCE ANALYSIS

4.1. Security Analysis

Security is a primary requirement for data encryption. In the paper, chaotic encryption is adopted for key macro-block DC coefficients and motion vector low part. Few parameters of chaotic system initial state are taken as secret key to generate chaotic code sequence that can satisfy the fundamental features of codes, as they possess natural pseudo randomness. In addition, encryption algorithm is of one time one code. On the one hand, in motion macro-block, DC coefficients and motion vector are key data in video stream, their damage will trigger serious degradation of video program; on the other hand, encryption on DC coefficients and motion vector in motion macro-block are from periodic Logistic mapping. Given that Logistic mapping has strong sensitivity to initial values, the paper select different secret key at every time, to ensure the security of the encryption. Then, non-nil AC coefficients in key QDCT block are scrambled. Here, the numbers of non-nil AC coefficients in key every QDCT block are different. According to the statistics of different video programs, it is reflected that, for every 8×8 size intra-frame QDCT block, there are about 8 to 17 non-nil AC coefficients. The lower 8 is taken. Hence, every non-nil AC coefficient possesses 8 possibilities of values, and every QDCT sample space is at least 64. For a common 70min standard definition video program (a resolution of 720 × 576), intra-frame image blocks alone (not considering inter-frame large range encrypted motion area), the sample space is at least 64×70×60×3×(720×576)/(16×16)×6=7,838,208,000. So, larger sample space enhances calculation difficulty of encryption attack; whereas scrambled positions of non-nil AC coefficients, chaotic DC coefficients and motion vector break subjective video information, and guarantee the security of this paper's calculation on cipher-text-only attack.

4.2. Real-Time Analysis

Encryption method of the paper is divided into two parts. The first part is intra-frame macro-block DC coefficient low position, inter-frame motion macro-block motion vector, and DC coefficient low position. The encryption is of some short chaotic sequence generated by repetition of Logistic mapping. The short chaotic sequence generates encryption secret key, and completes chaotic encryption on motion vector and DC coefficient low position. Apparently, the calculation cost is very small. As this chaotic calculation changes part of the system statistic property, video compression rate is reduced on certain degree. Yet, these partial coefficients only account for a small portion of coefficients that needed coding. And the changed coefficient statistic property does not necessarily decrease compression rate. Consequently, generally speaking, this chaotic encryption of few coefficients at low positions has little influence on coding output rate. The second part is encryption method is to scramble the positions of non-nil AC coefficient in QDCT block. This method does not change AC coefficient value, runs length, and the number of runs two- tuples. In term of statistics and coding theory, scrambling possesses extremely small impact on coding output rate. Integrating these two factors, impact on video compression rate by calculation method of this paper is controlled within certain scope.

4.3. Compatibility Analysis

Encryption calculation adopted in this paper does not modify video data header and identification information. Therefore, at reception end or communication intermediate

link, correct data type can be identified and decoded. Yet, the quality of video image is downgraded after de-coding. Thus, this encryption calculation satisfies video format compatibility requirements in communication process.

CONCLUSION

Through analysis on video motion vector, the paper conducts encryption on tested key macro-block motion vector, QDCT block DC coefficients non-nil AC coefficients. Given that the encryption process is set after quantification and is carried out in synchronization with variable length coding, this method of calculation is of low cost and good real-time property. Moreover, selective encryption is conducted on video image reconstruction of key influence macro-block. *Via* encryption on data as few as possible, certain intensity of video encryption effects are achieved. Meanwhile, this method is featured by non-evident impact on video coding speed and video standard compatibility.

CONFLICT OF INTEREST

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

ACKNOWLEDGEMENTS

This paper belongs to the project of the "Science Fund Projects", No.CKJ2011013 and QKJB2011025; Nanjing Institute of Technology.

REFERENCES

[1] Song B, Chang Y L, Li C L, "Novel fast selecting inter prediction mode algorithm based H.264," *Acta Electronica Sinica,* vol. 35, pp. 698-700, April 2007.

[2] Noureldaim Emadeldeen, Mohammed Jedra, Noureldeen Zahid, "On Segmentation of Moving Objects by Integrating PCA Method with the Adaptive Background Model," *Journal of Signal and Information Processing,* vol. 3, pp. 387-393, March 2012.

[3] Osama A. Khashan, Abdullah M. Zin, Elankovan A. Sundararajan, "Performance study of selective encryption in comparison to full encryption for still visual images," *Journal of Zhejiang University SCIENCE C,* vol. 15, pp. 435-444, June 2014.

[4] Nikola Toljic, Kaz Adamiak, G.S. Peter Castle *et al.*, "3D numerical model of the electrostatic coating process with moving objects using a moving mesh," *Journal of Electrostatics,* vol. 70, pp. 499-504, June 2012.

[5] Dae-Youn Lee, Sanghoon Sull, Chang-Su Kim, "Progressive 3D mesh compression using MOG-based Bayesian entropy coding and gradual prediction," *The Visual Computer*, vol. 30, pp. 1077-1091, October 2014.

[6] Cheung C H, L M Po, "A novel cross-diamond search algorithm for fast block motion estimation," *IEEE Transactions on Circuits Systems for Video Technology,* vol. 12, pp. 1168-1117, December 1987.

[7] Ye Yao, Zhengquan Xu, Wei Li, "Visual security assessment for video encryption," *Third International Conferenee on Communications and Networkin*g, pp. 1317-1322, August 2008.

[8] L.M. Varlakshmi, G.Florence Sudha, G. Jaikishan, "An efficient scalable video encryption scheme for real time applications," *Procedia Engineering,* vol. 30, pp. 852-860, January 2012.

[9] Bo Lei, KunDe Yang, YuanLiang Ma *et al.*, "Forward acoustic scattering by moving objects: Theory and experiment," *Chinese Science Bulletin,* vol. 57, pp. 313-319, April 2012.

[10] Song J B, Li B, Li W, Ma L, "A fast motion estimation algorithm based on mode and spatiotemporal correlation," *Acta Electionica Sinica*, vol. 35, pp. 1825-1826, October 1987.

[11] Johny Paul, Andreas Laika, Christopher Claus *et al.*, "Real-time motion detection based on SW/HW-codesign for walking rescue robots," *Journal of Real-Time Image Processing,* vol. 8, pp. 353-368, April 2013.

[12] Liu ZY, Zhou JW, S Goto, T Ikenaga, "Motion estimation optimization for H.264/AVC using source image edge features," *IEEE Transaction On Circuits Systems for Video Technology*, vol. 19, pp. 1096-1097, August 2009.

[13] L. X. Zhao, Q. Su, H. Liu, H. Peng, "Application of flexible edge matching algorithm in the field of moving object detection," *Intelligent Automation & Soft Computing,* vol. 20, pp. 515-523, April 2014.

[14] Fuwen Liu, Hartmut Koenig, "Puzzle - an efficient, compression independent video encryption algorithm," *Multimedia Tools and Applications,* vol. 73, pp. 715-735, Feburary 2014.

[15] Esam A, Qaralleh A, Chang TS, "Fast variable block size motion estimation by adapllve early termination," *IEEE Transaction on Circuits Systems for Video Technolog*y, vol. 16, pp. 1022-1023, August 2006.

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