Fast Encryption Algorithm for Streaming Video over Wireless Networks

[1]Mr.Rahul Bambodkar [2]Mr.Avinash Wadhe
[1]*Lecturer (CSE),D.M.I.ET.R, Salod (HIrapur) Wardha.*
[2]*G.H Raisoni College of Engineering, Amravati.*

ABSTRACT*:*

Wireless networks are poised to enable a variety of existing and emerging video streaming applications.

However, video streaming over wireless suffers from piracy and malicious attack. Also, it is well-known that video decompression on the handheld devices is constrained by the power and other computation resource. Therefore, video encryption should be designed to be lightweight and efficient. In this paper, we designed a new lightweight, efficient, scalable, format-compliant video encryption algorithm, which is based on the DCT (Discrete Cosine Transformations) coefficients scrambling. The simulation shows that the proposed video encryption algorithm consumes low computation resource while achieves high scalability and confidentiality, which is in compliance with the design goal of video streaming over wireless applications.

Keywords— *video, encryption, security, wireless networks*

I. INTRODUCTION

Advances in multimedia and wireless technologies have led to the recent wide deployment of streaming video over wireless applications and services that suffer from piracy and malicious attack. The security becomes a critical issue in the design and development of such multimedia applications. Assuring a certain level of security is a strong requirement for a large deployment of multimedia applications. Failure to meet security requirement poses potential threats to the service providers and customers. Encryption for the video bit stream should be designed to be lightweight and format-compliant. Since video decompression on the handheld devices is constrained by the limited power and other computation resources, conventional ciphers such as data standard encryption (DES) or advanced encryption standard (AES) to wireless applications over handheld devices are intensive computation tasks. Therefore, it is not efficient to apply conventional ciphers for wireless multimedia applications. Selective encryption algorithms are proposed to be an economical and secure video encryption algorithm where only I-frames are encrypted. However, it has been reported as not good choices in the encryption of digital video since encrypting I-frames alone may not be sufficiently secure for digital video [1]. Compression-Logic based encryption is widely studied and several algorithms have been proposed [2,3,4,5,6,7,8,9,10,11]. However, these compression-based algorithms suffer either vulnerability or low-efficiency problem. In this paper, a new compression-based video encryption algorithm is proposed. The new algorithm overcomes the reported vulnerability and at the same time, relatively low computation complexity, low compression overhead, high scalability are maintained. Also, the new algorithm confines the encryption-incurred error propagation. Quick recovery from bit errors and fast resynchronization from packet losses are feasible..

II. RELATED WORK

The output of video compression is a sequence of three types of frames: I-frame (Intra picture), P-frame (Forward Predicted) and B-frame (Bidirectional Predicted: Forward-Prediction and Backward-Prediction). I-frame is reference frame and is self-contained. A P-frame specifies the difference between the previous I-frame and itself; while a B-frame is an interpolation between the previous and subsequent frame of I or P type. To compress an I-frame, the process starts from dividing the frame into macro-blocks. Each macro-block is of size 16×16 pixels. And each macro-block is composed of six blocks, four of them represent luminance and the other two represent chrominance. Each block of size 8×8 is through a discrete cosine transformation.

The transformed DCT (Discrete Cosine Transformation) coefficients are uniformly quantized in conjunction with a pre-defined quantization table. The quantized DCT coefficients are arranged in accordance with a zig-zag order. Finally, the zig-zag sequence is compressed by the Run Length Encode (RLE) mechanism to generate video bit stream. Encoding a P or B frame depends on the same block compression process and the motion compensation. The motion compensation is a technique used to compute the best-match region in the reference frame for a target macro-block in a P or B frame. The vector that points to the best-match region from the target macro-block, known as motion vector, is encoded by the Run Length Encode. Then difference or interpolation of the target macro-block and the best-match region is encoded in the same way as encoding macro-blocks of an I-frame. As we know, amplitudes of the DCT coefficients with low frequencies are relatively larger than the amplitudes of other DCT coefficients. Random permutation (interchangeably with scrambling) of coefficients of a single block does not necessarily hide those large coefficients. It has been demonstrated that video decompression based on only a few low frequency DCT coefficients could generate acceptable video playback quality. Since the low-frequency DCT coefficients with relatively large amplitudes can be easily identified after the scrambling, malicious attackers could recover significant amount of video data from cipher-text by simply performing IDCT (Inverse DCT) based on a few coefficients with relatively larger amplitudes from the permutated DCT block. The sensitivity of low frequency DCT coefficients to malicious attack is called DCT vulnerability.

Davis Pan [5] said that the MPEG compression algorithm is the first international standard for digital compression for high-fidelity audio. MPEG is one part of three part compression standard.

Tha MPEG standard addresses the compression of synchronized video and audio. Dr. S.R. Ely [6] said that MPEG has been outstandingly successful in defining the standards for video compression coding, serving a wide range of applications, bit-rates, qualities and services. The standards are based upon a flexible toolkit of techniques of bit-rate reduction. The picture quality obtained through an MPEG codec depends strongly upon the picture content, but as experience with MPEG coding grows, the bitrate needed for a given picture quality is likely to reduce.

III. VIDEO ENCRYPTION ALGORITHM

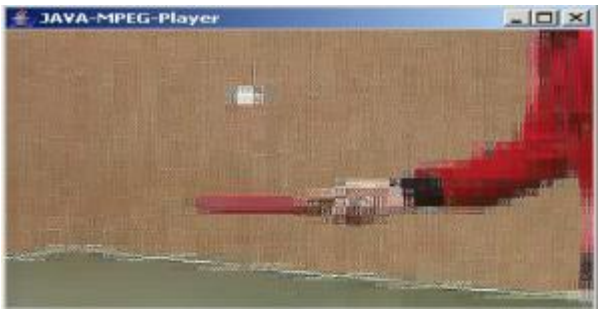

Figure 1: Before random Permutation

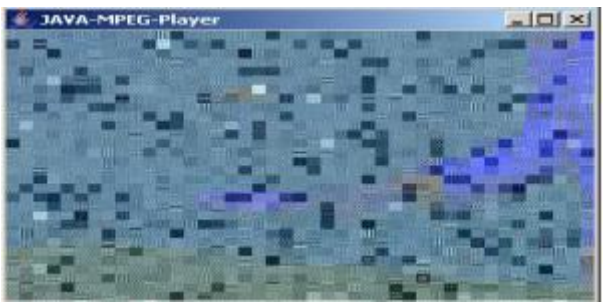

Figure 2: After random Permutation

The proposed algorithm is a Compression-Logic based video encryption algorithm. Instead of randomly permuting 8×8 coefficients of a single DCT block, the random permutation is applied to a number of permutation groups. Each permutation group contains the DCT coefficients of the same frequency (index of 8×8 DCT matrix) from every single block of a frame, regardless of I, P or B frame. Obviously, since each DCT block has 64 coefficient frequencies so that 64 permutation groups can be formed, the proposed algorithm runs random permutations on each of permutation groups to encrypt a single video frame. After random permutation, the encrypted video data is compressed by standard RLE. The resulting picture after the random permutation is shown in Figure 1(b). The idea of the random permutation is illustrated in Figure 2 by an

example. Note that blocks of a frame are indexed in row major. Figure 2 (a) shows the original DCT blocks before the random permutation. The DCT blocks after the random permutation is shown in Figure 2 (b). Figure 2 (c) shows the permutation order, which basically represents the encryption key of the proposed algorithm. Each number in Figure 2 (c) is the block index number of the corresponding coefficients in Figure 2 (a). The proposed video encryption algorithm scrambles the DCT coefficients of each permutation group. After the random permutation, the sensitive low frequency DCT coefficients still exist in the low frequency region such that the statistical distribution of DCT bock remains the same and low-frequencies DCT coefficients can not be easily identified after encryption by simply checking the amplitudes of coefficients. Therefore, the new video encryption algorithm is more secure than Tang's algorithm. The new algorithm is built on top of standard video compression scheme. It inherits most of computation steps of video compression and simply inserts permutation before entropy coding is applied. Thus no extra computational steps are introduced except encryption and decryption. The computation overhead is relatively small. In addition, since random permutation does not change DCT block statistical distribution, no compression inefficiency incurs in terms of entropy coding. The video bit stream generated by the new encryption algorithm has the same format as that of standard MPEG algorithms. Therefore, the new video encryption algorithm is format-compliant. According to the statistical distribution that high-frequency DCT coefficients tend to have zero amplitude, we know the permutation groups which include high-frequencies coefficients contain zeros mostly. Scrambling those permutation groupso does not improve data confidentiality much while the performance of the proposed algorithm is negatively impacted. It is wise to select only a small number of permutation groups with low-frequency DCT values for encryption, which further reduces the computational overhead without confidentiality breach. In summary, the advantages of the new video encryption algorithm are multi-folded. Firstly, the proposed algorithm does not suffer from DCT vulnerability. Secondly, it maintains the sam compression efficiency compared to the standard MPEG algorithms since the new algorithm has the same probability distribution of DCT coefficients after the scrambling. Thirdly, the new algorithm adds little computation overhead since the encryption and decryption has the same computational complexity as zig-zag order, which is basically linear to the number of coefficients. Furthermore, the proposed algorithm is format-compliance. Therefore, it confines the encryption-incurred error propagation. Quick recovery from bit errors and fast resynchronization from packet losses are feasible. Finally, the proposed algorithm is selective since only a small number of permutation groups can be encrypted based on the requirements of confidentiality. The proposed video encryption algorithm is extremely suitable for application of streaming video over mobile devices. As we discussed, the new algorithm guarantees the protection of source video from the exploitation of DCT vulnerability. And it is reliable against brute-force attacks due to a very large key space. Retaining format-compliance and compression efficiency makes the proposed algorithm compatible with current MPEG standards. Robustness against wireless channel error is provided by error propagation control. Selective encryption makes security protection scalable, which is necessary for user requirement and available computational resource

IV. ALGORITHM ENCRYPTION STRENGTH ANALYSIS

The new encryption algorithm can be described by the following formula:

$$Y=E(K,X)$$

Where X is the DCT coefficients before the scrambling while Y is the coefficients after the scrambling; K is the scrambling order, which represents the encryption key. To protect the algorithm from brute-force attack, the key space can be used to measure the strength of the encryption algorithm. Tang's algorithm is based on permutation of 64 coefficients of a DCT block. In theory, the key space of Tang's algorithm is factorial of 64. However, by exploiting the DCT vulnerability, the attackers can recover significant amount of video info from only a few DCT coefficients without exhaustively working through the key space in Tang's algorithm. The key space of the proposed video encryption algorithm is proportional to the frame size. For a video frame of M×N pixels, the number of luminance DCT blocks, K, can be computed as follows:

$$K= \quad \times \quad = \frac{M}{\epsilon}$$

Since the scrambling is performed on DCT coefficients of permutation group, the key size of the proposed algorithm is factorial of K. As an example, ITU QCIF (Quarter Common Intermediate Format 176×144 pixels) video has 396 luminance blocks, which means the key space for QCIF video is factorial of 396, which is much larger than that of Tang's algorithm. More importantly, as we discussed in section 4.1, the proposed algorithm does not suffer from DCT vulnerability. Therefore, it is impractical to brute-force attack the video encrypted by the proposed algorithm.

V. ALGORITHM EFFICIENCY ANALYSIS

In Tang's algorithm, the number of permutation operations performed on a single video frame is exactly the number of blocks of that frame. In the case of QCIF (176×144), permutation operation will be applied 594 times to a single frame. Each permutation computes 64 DCT coefficients. Overall, Tang's algorithm has time complexity) (MN O , which is linear in terms of number of pixels of a frame. Based on the statistical distribution that a large portion of high-frequency DCT coefficients tend to have zero amplitude, the proposed algorithm can improve the computational efficiency by encrypting only those permutation groups which contains low-frequency DCT coefficients. If we only encrypt a small number of permutation groups, say r, then the running-time complexity of the proposed algorithm.

Can be reduced to O( ) ,where r < k.

VI. CONCLUSIONS

This paper, proposed a computationally efficient, yet secure video encryption scheme. It uses RC5 for encryption of the DCT coefficients and ECC for small key sized generation .The proposed scheme is very fast, possesses good security and adds less overhead on the codec. It slightly decreases the compression rate of the video, which is negotiable for higher security. In fu-ture it would be to reduce the encrypted video size by modifying the default Huffman tables and hence come up with an ideal video encryption algorithm which takes less encryption time and causes no overhead on video size. It can also be extended to videos like MPEG-4, H.261, and H.264 etc

REFERENCES

[1] I. Agi, L. Gong. "An empirical study of secure MPEG video transmission", In Proceedings of the Internet Society Sumposium on Network and Distributed System Security,

[2] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiency", in Proc. Fourth ACM Int. Multimedia Conference. (ACM Multimedia'96), 1996, pp.201-206S..

[3] W. Zeng, S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video", IEEE Transaction on Multimedia, Vol. 5, No.1. March

[4] C. Wu, C, Kuo, "Efficient multimedia encryption via scrambling by spatially shuffling codewords of compressed bitstreams", in Proc. SPIE Security and watermarking of Multimedia Contents III, vol. 4314, San Jose, CA, Jan.

[5] J, Wen, M. Severa, W. Zeng, M. Luttrell and W. Jin, "A format compliant configurable encryption framework for access control of multimedia", in IEEE Workshop on Multimedia Signal Processing, pp. 435-440, Oct. 2001.*FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[6] J, Wen, M. Severa, W. Zeng, M. Luttrell and W. Jin, "A format compliant configurable encryption framework for access control of video", IEEE Transaction. CSVT, Special Issue on Wireless Video, 2002.

[7] 7. A. S. Tosun and W. Feng, "A light-weight mechanism for securing multi-layer video streams", Proc. IEEE International Conference on Information Technology:

[8] C. Yuan, B. B. Zhu, Y. Wang, S. Li and Y. Zhong, "Efficient and fully scalable encryption for MPEG-4 FGS", in Proc. IEEE Int. Symp. Circuits and Systems, vol.2, Bangkok, Thailand, May 2003, pp 620-623.

[9] 9. B. Zhu, C. Yuan, Y. Wang, S. Li, "Scalable protection for MPEG-4 fine granularity scalability", IEEE Transactions on Multimedia, vol.7, No.2, April 2005. 10. st

[10] L. Qiao and K. Nahrstedt, "A new algorithm for MPEG video encryption", in Proc. 1 Int. Conf. Imaging Science, Systems & Tech, Las Vegas, Jun, 1997, pp 21-29. 11. C. Shi and B.Bhargava, "A fast MPEG video encryption algorithms", Int. J. Comput. & Graph., vol.22, No.3, 1998.

[11] Mr.Avinash P. Wadhe,Mrs Lekha Bhandari "Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3)