Research on Video Encryption Algorithm in Android Platform

Tao Sun [a], Wenjie Meng [b]

Qilu University of Technology, Jinan 250353, China

[a]tutorsun@163.com, [b]1425166646@qq.com

Keywords: digital video, perceptual encryption algorithm.

Abstract. In order to manage the copyrights for digital video on Android operation system, on the basis of summarizing traditional video encryption algorithm proposed a new video encryption algorithms, perceptual encryption algorithm. This algorithm can select important data to encrypt, and can control the intensity of encryption. The results show that the algorithm is able to meet the requirement of video copyright management when we use perceptual encryption algorithm to simulate the video encryption and decryption.

Introduction

Android OS is an operating system which based on Linux kernel, it has become the most popular smartphone operating system along with the development and popularization of intelligent mobile terminal, and so targeting Android operating platform for copyright protection of digital video has become increasingly important. Digital Video Rights Management (DRM), which is use some algorithm to managing and protect the digital video. On the basis of the Summarize and conclude traditional encryption algorithms characteristic to present a new video encryption algorithm that is perceived encryption algorithm. Which has ability to select important data, and is able to control encryption strength.

Digital Video Encryption

Digital video uses the principle of still images in the process of encoding, in order to achieve better playback which should consider online video processing capabilities in the video encryption process, so the decryption time reaches a certain speed. To this end, there are three types of encryption schemes:

Direct encryption algorithm. Direct encryption algorithm for all video streams directly with cryptography to encrypt and decrypt data, commonly referred to as traditional domestic encryption method (see Figure 2-1). Will video data as General of II into business data to for processing, and used more complex of algorithm to on video data for encryption [1], as traditional of password algorithm RSA, and IDEA, and DES,, these are is more mature of password algorithm, if not considered specific of video data flow features, can directly using password algorithm on II dimension or multidimensional data said of image and the video signal for encryption.

Selective encryption algorithm. Through the study on signal characteristics of video data stream, combine the video technology with code principle then we proposed one kind algorithm that only encrypt part of the data[2], that means only select key data to be encrypted (Figure 1). This algorithm first is divided according to the signal characteristic of the video stream flow which means just to encrypt important data in the selected signal flow.

Selective encryption method need to ensure the among compatibility among the encrypted data stream format after encrypting the important video data which means to ensure the stability of the encrypted control information and data format[3].

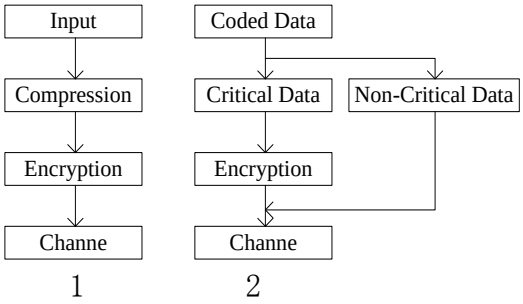

Figure 1

Through the comparison of the above general video encryption methods as can be seen all kinds of video encryption algorithms have their advantages and disadvantages, no single encryption algorithm meets the requirements of video encryption on Android operation system. It is necessary to adopt a comprehensive video encryption that include the characteristics of different encryption algorithms. This method need to select the important data in the data stream to encrypt such that no decrypt video data not be able to play normally, achieve the aim of copyright management, and to control the encryption intensity by setting parameters, this method is called perceptual encryption.

Implementation of Perceptual Encryption Algorithms

Choose encrypt data. Based on the analysis of the H.264 semantic layer, select following morpheme to encrypt.

1. Motion vector (MV) difference. In the B-frame or P-frame, each macro block can bi divided 16*16, 16*8, 8*16,8*8 (as shown in Figure 2-1)four modes. If the dividing method is 16*8, then it will generate two sub-macro blocks, and each of the pixel sub-macroblock is 16*8[4]. And the resulting sub-macro block can continue to divide (as shown in Figure 2-2), this dendritically structure is a kind of motion compensation scheme based on the sub-macroblock and zoning.

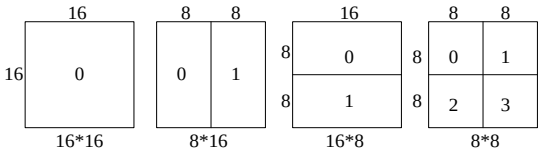

Figure 2-1

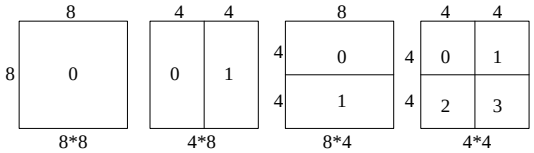

Figure 2-2

The motion vector for each P partition needs a certain number of bits to encode, in order to reduce the number of bits in the coded, can select neighboring motion vector predictive encoding, namely at the back of the motion vector can be forecast by the in front of motion vector[5], we can encode their difference MVD. In order to maintain the semantic structure of the video and enhance coding efficiency requires only to encrypt the motion vector difference value of the sign bit (Figure 3).

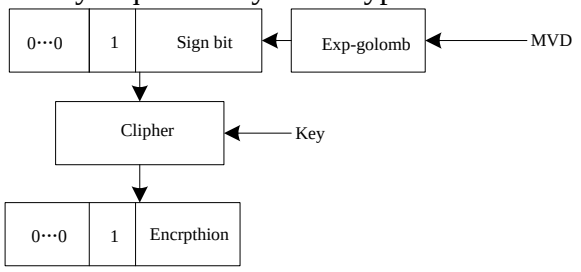

Figure 3

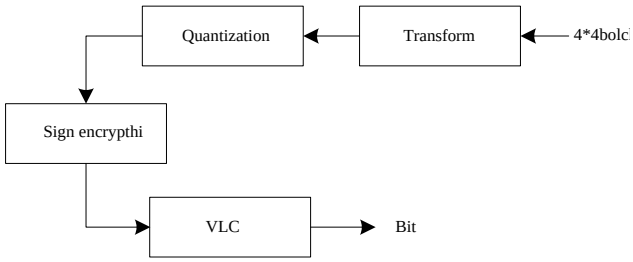

Figure 4

2. The residual coefficients. Residual coefficients encodes by CABAC and CAVLC, through CAVLC coding process, the number of the trailing, the number of non-zero coefficients, the number of the zero before the last non-zero coefficients and the number of the zero before per zero. We only encrypt the key field in the process of coding CAVLC, therefore, when we choose the residual coefficient of correlation coefficient, only calculate these two fields numerical.

Intensity of multidimensional data encryption scheme. In several kinds of video data elements mentioned above, they plays a different role for video image display, we can set different encryption intensity on them to control, for the three types of elements, the Residual coefficient, the prediction model, IPM, motion vector MVD [6], we were set its three different encryption strength control parameters, P1, P2, P3, detailed plan is as follows:

1. With the value of P1 to represent the residual coefficient of the sign bit encryption intensity, as the change of P1 corresponding to the residual coefficient of the sign bit encrypted.

2. In P2 numerical to represent the forecast word encryption intensity, according to the value of P2 size to determine the IPM encryption strength.

3. In P3 numerical to the represent MVD encryption intensity, as the change of P3 corresponding to the motion vector is encrypted.

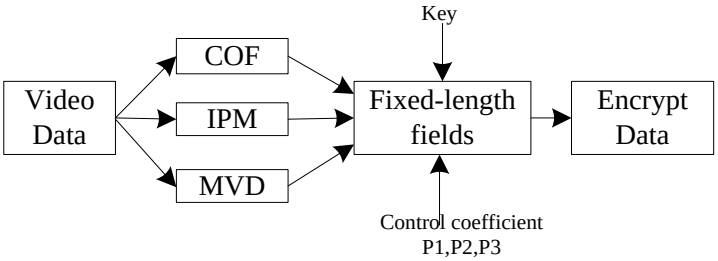

Figure 5

Solution algorithm design. In order to achieve the above control strength algorithm, first of all, to generate a random number 0 ~ 1, corresponding to the intensity of each of the above control coefficient, if s < p, to encrypt the data stream[7], otherwise, skip this element, of course, we also can use the following method to improve the speed of encryption:

1. Randomly generated a random value of 0 to 1.

2. Generate a binary array which length is N, from S [0]-S [N], randomly selected N consecutive number from 0 to 1.

3. When operating the video data stream, only when the S [I] =1 to encrypt the data elements, otherwise, not process the data elements.

This can effectively be select video data encryption and improve the calculation speed. Below is a flow diagram:

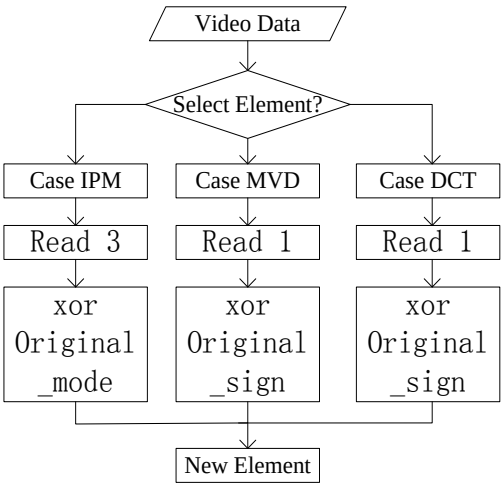

Figure 6

Simulation and Analysis

The simulation, we use tablet computers points, Android4.2, code development environment Ubuntu operating system, select the Eclipse integrated development software operating system. Selection MobePalyer player under Android system encrypted video playback, view the playback, we set the default encryption strength factor P = 0.5, while the video brightness setting, the following two figures are not player to play encrypted video and through encrypted video renderings. Through the above two figures, we can see through video encryption algorithm processing of video over ordinary player cannot correctly decompress, play, met our video copyright for the management purposes.

Figure 7 Contrast Figure

Summary

This paper compares the various types of traditional video encryption algorithms, real-time, security, the amount of data to increase the size, and other characteristics, draw their own limitations, the limitations on the basis of induction on different video encryption algorithm proposed a comprehensive video elements for each species and prioritize different encryption strength algorithm to achieve the purpose of the video resources for copyright management. In the future also on video coding technology and source characteristics for further research and exploration, providing more technical aspects of video copyright protection for distance education management, promoting better education, faster and healthy development.

References

[1] Cheng H, Li X B. Partial Encryption of Compressed Images and Videos. IEEE Transactions on Signal Processing, 2000, 48 (4):2, p.439.

[2] Tosun A S, Feng W C. Efficient Multi-layer Coding and Encryption of MPEG Video Streams. IEEE, 2000. p. 119-122.

[3] Wu C P, Kuo C C J. Fast encryption methods for audiovisual data confidentiality [A]. Proceedings of SPIE International Symposia on Information Technologies 2000[C]. Boston, USA: SPIE, 2000.p.284-295.

[4] Wu C P, Kuo C C .Efficient Multimedia Encryption via Entropy Codec Design. SPIE, the International Society for Optical Engineering, 2001, 4 313, p.128-138.

[5] Blom R, Carrara E, Mc Grew D, et al. The Secure Real Time Transport Protocol (SRPT).Internet Draft, 2001.

[6] Wallace G regory K. The JPEG still image compression standard [J]. Communication of the ACM, 1991, 34(4) p.30-44.

[7] Wu C P, Kuo C C J. Fast encryption methods For audiovisual data confidentiality[A].Proceedings of SPIE International Symposia on Information Technologies 2000[C]. Boston, USA: SPIE, 2000.p.284-295.