The Video Encryption Scheme Based on Perceptual Encryption Algorithm in H.264 Standards

XueYan Zhang[1, a],HuChao Deng[2,b] ,LiangWei Chen[1, c]

[1]computer engineering department, Chengdu Aeronautic and Vocational and Technical College, Chengdu, China

[2]Jiangsu Posts & Telecommunications Planning and Designing Institute CO.LTD, Nanjing, China

[a]sxzz520110@126.com, [b]denghuchao2008@163.com, [c]clw206064@163.com

Keywords: Video-encrypting; H.264 coding standards; Perception encryption algorithm; FLC; Safety

Abstract. To meet the requirement of multimedia video transmission's safety and real-time, this paper provides a conclusion based on video encryption schemes of the encryption algorithm. The solution sorts video data into VLC(variable length code) and FLC(fix-length code) ,only choose to reconstruction images FLC compared to encrypt the important element of the operation. The analysis and the simulation results show that the encryption scheme is not only high safety but also low cost system.

Introduction

H.264 is the latest video coding standard released in March 2003 currently. It adopts new technologies of motion estimation of 1/8 precision, 4×4 integer commutation, CAVLC and CABAC, etc. These new technologies can significant elevate the compression efficiency and the playback quality of the image. Compared with the former standard, its coding efficiency increases approximately 50% under the condition of the same distortion. Its range of application is very broad, which includes the instantaneous communications aspects of video session, video phone, video conference and others. It also includes digital video cast, digital storage, and streaming media, etc.

With the increasingly extensive application of video, the security of video is becoming more and more significant. Based on the former standard, people studied a lot of encryption algorithm: some process the method of whole encryption by the use of traditional code technique, such as DES algorithm, CSC algorithm, VEA algorithm. Although these algorithms have higher security and do not change the compression ratio, their calculation complexity is very high; some process the encryption method to the DCT coefficient, such as subsection scrambling algorithm. Although this kind of algorithm has lower calculation complexity, its security is lower than the whole encryption algorithm and the compression ratio changes to some extent. Now， the video encryption program of the CAVLC entropy coding based on H.264 is presented, which has a high safety and low complexity. This paper is based on this program be improved to further reduce the computational complexity and lower system overhead, which puts forward a perceptual encryption algorithm based on H.264.

Analysis and Selection of Encryption Data Elements

According to the analysis of the H.264 encryption macro block semantic layer, we determine to process the encryption operation by extracting three kinds of fix-length code, which are intra prediction mode, motion vector difference, and residual coefficient[1].

Intra Prediction Mode

According to the different video group in each macro block, every macro block has several coding prediction mode. However, the intra prediction coding is supported by all of the video coding types. In terms of lightness pixel block, there are three prediction modes, which are Intra_4×4, Intra_8×8, and Intra_16×16. There are nine prediction modes under the Intra_4×4, which is applicable to process coding to the image detail section. The Intra_16×16 has four kinds of prediction modes, which applies to process image coding to the plain area[2].

Published by Atlantis Press, Paris, France.

It adopts the coding mode of Intra_4×4 to process encryption operation. Each 4×4 block is predicted by the above and left pixel, as shown in "Fig. 1". a-p is the waiting prediction pixel, and it adopts the A-Q pixel which has been decoded in the adjacent blocks to process prediction. For every 4×4 block, there are nine modes for selection, among which, except DC mode, the orientations of the other eight prediction modes are shown in the following "Fig. 1":

The coding prediction mode of Intra_4×4 has nine prediction modes in total, and it needs four bits to process coding. In the standard of H.264, it utilizes a "prev_ Intra_4×4_pred _mode" field to exclude a prediction mode, and makes use of the other three bits to represent the rest eight prediction modes. Consequently, we only process encryption disarrangement to the three back bits. This kind of encryption process will not influence the other fields and wound not produce extra bit stream.

Motion Vector Difference

In the P frame or B frame, each macro block can be divided into four manners, which are 16×16, 16×8, 8×16, 8×8. The figure adopts 8×8 mode, and it can be divided into four son macro blocks (8×8 pixel). Each son macro block can be further divided into 8×8, 4×8, 8×4, and 4×4. As shown in Fig. 2

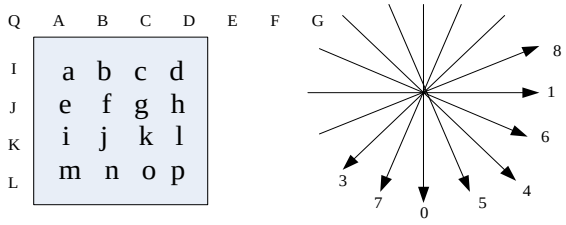


Figure1:The prediction sketch map of Intra_4×4

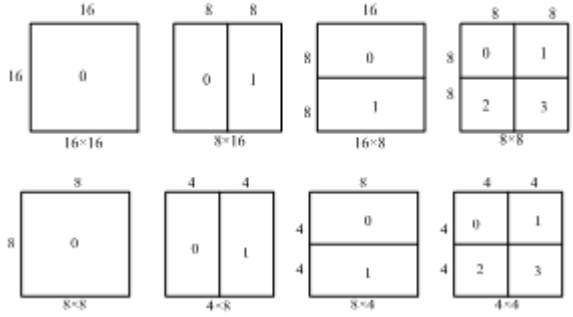


Figure 2: The partition sketch map of macro block

Each subarea or son macro block can have an individual MV (Motion vector), which is used for introducing the corresponding field of the former reference frame to process prediction coding to the present block. All of the MV of each prediction field needs bits of the corresponding number to process coding. In order to further reduce the bits, we can utilize the correlation between the adjacent MV to process prediction coding. The later MV can be predicted by the former coded MV. We only need to process coding to their MVD (motion vector difference). In the H.264, MVD value processes coding by the use of Exp-Golomb, which is a kind of variable length coding[3].

The Exp-Golomb coding consists of prefix and suffix. The prefix is 0 for the number of M and 1 for the number of 1, and the suffix is INFO for the bit of M, and its code shape is [M zero]1 [INFO], among which, M=floor（$\log_2^{(codeNum-1)}$）. If mvd<0, CodeNum=2|mvd| -1, the INFO will be CodeNum- 2^M .

We make use of encryption function to process encryption to INFO: y=Encrypt-(INFO), among which y is the cryptograph fater encryption.

This paper only process encryption to the MVD sign bit. For every MVD value, it only needs to process the encryption operation to one bit.

Residual Coefficient

In H.264, the residual coefficient processes coding by the use of CAVLC and CABAC. During the process of CAVLC coding, it involves the following semantic fields[2]: Total coeffs, Trailing Ones, Level, Total Zero, and Run Before. Through analysis, we find that only the sign bits of Trailing Ones and Level belong to the fixed-length field. Consequently, we extract signs of these two fields to process encryption operation. As shown in "Fig.3":

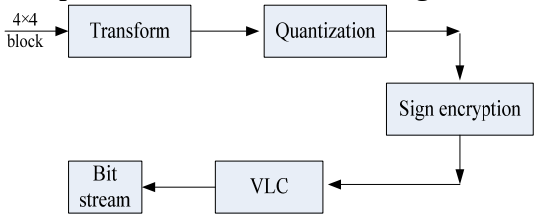


Figure 3: Residual coefficient sign encryption

Algorithm Design

For the three elements above: IPM, MVD, and Residual coefficient, we respectively introduce three different controls parameters to control their encryption strength[1], the concrete scheme is as follows:

We should take the probability of P1, P2, and P3 to respectively process encryption to IPM, MVD, and Residual coefficients. When P1, P2 and P3 vary from 0 to 1, we should correspondingly operate from no encryption to total encryption. The method of realizing probability control is as follows: we should use the random number marker to produce a pseudo random number series r between the ranges of 0 to 1, which corresponds to every element mentioned above. When r<=P, we should process encryption to this element.

The description of the concrete pseudo code of algorithm is as follows:

```
While (syntax element)
{
 Switch(syntax element_type)
    {Case: IPM read 3bits from pseudo random sequence;
     new_mode=original_mode XOR 3_bits;
     break;
      Case: MVD Read 1bits from pseudo random sequence;
     new_sign=original_sign XOR 1_bits;
     break;
      Case: DCT    coefficients for each none zero coefficients
     read 2 bits from pseudo random sequence;
     new_sign=original_sign XOR 2_bits;
     break;}
   scan for next syntax element;
}
```

Simulation Result and Analysis

Experiment Environment

The experiment test conditions are H.264/AVC standard, JM10.2 edition, taking the mode of IPPP……P to process coding, the refresh rate of I frame is 10, frame rate is 30 frame/sec, 2G memory, Intel T5670 processor, and making use of VS2008 to accomplish the debugging of JM10.2 code. The experiment adopts the foreman of 352×288 CIF format as the video sequence.

Analysis of Encryption Effect

The individual encrypted IPM field only process encryption to the luminance information. As shown in “Fig.4”, the information of face and profile are clear and visible. In the process of individual MVD encryption, as shown in “Fig.5”, I frame image is totally not affected by any factors, I bock of B, P frame are totally not affected either. The key information is easily to be given away. We should process encryption to residual coefficient individually. As shown in “Fig.6” and IPM, the profile information of image do not concealed perfectly. Besides, from the aspect of confronting decryption attack ability, the encryption space of individually analyzing one encryption element becomes smaller and more easily to be cracked. Consequently, the vision security demands higher environment, and it should process encryption to all of the three kinds of elements united. We can see in “Fig.7” that the strength of encryption increasingly elevated and the perceptibility of video image constantly declined. Under the strongest encryption strength, the total disarrangement of the whole image has high vision security.

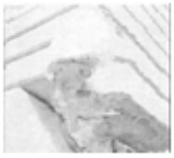
Published by Atlantis Press, Paris, France.



p=0.05 p=0.5 p=1

Figure 4: Image after IPM encryption





P=0.05 p=0.5 p=1

Figure 5: Image after MVD encryption



P=0.05 p=0.5 p=1



P=0.05 p=0.5 p=1

Figure 6: Image after Residual coefficient encryption. Figure 7: Image after associated with encryption of three elements

Security Analysis

In the encryption scheme, it should keep the semantic compatibility of the video format. The encryption operation does not change the length of the corresponding field. The attacker will process Cipher-only Attacks[5] by individually guess the value of each field element. The most easily method is to process ECA attack (error concealment. Based attack), namely, to evaluate all of the value of FLC a fixed value and crack it. Meanwhile, the attacker could guess the value of each FLC through the correlation between the adjacent blocks. Now, I will process analysis and introduction to its complexity. Given that all of the FLC data in the frame data are N and the probability control of encryption is P, then the number of the actual encryption FLC in a frame data is pN. The difficulty of the attack to one frame data should be at least O ((C_{pN}^{N})2^{pN}) in each sigh field, and have at least two values (0 and 1). If it is IPM, then there will be more value possibility. If we assume that P＞100/N, then there will be $2^{pN} > 2^{100}$. Actually, in a data frames, the number of FLC is far more than 100. This encryption scheme is very effective to antagonize the Cipher_Only Attacks.

Performance Analysis

The computation complexity of an encryption algorithm mainly lies on its data volume that needs to be processed. the video encryption program of the CAVLC entropy coding based on H.264, which has encryption data, including Total coeffs, Trailing Ones, Level, Total-Zeros and Run-Before. His paper includes IPM, MVD and Residual coefficient. In a macro block, only the three elements of the sign bit need to encrypt. Therefore, The encryption data has been less than that of the CAVLC encryption program. The encryption operation adopted by us is only the operation to the corresponding bits. The required system spending is extremely small, and it will not bring influences to the codec.

Conclusion

This paper studies a method that can be used to process perceptual encryption under the coding of H.264. Through the research of analysis and coding mode of the grammar elements, it selects three fixed-length fields, which are IPM, MVD and Residual coefficient to process encryption, controls the encryption strength of each kind of field by introducing the probability parameter, and analyzes the video encryption effects brought by encrypting different elements. The experiment result shows that the individual encryption of any kind of element will bring a lot of disturbs to the image. But if you want to obtain excellent security, you must encrypt these three elements united. This kind of encryption scheme possesses excellent security and timeliness, and it would not bring the extra streaming. It can keep the video compression ratio unchanged, and adjust different encryption strength. Therefore, it applies to all kinds of application demands.

References

Published by Atlantis Press, Paris, France.

[1] Liu Xiao. The video encryption research based on H.264 coding [D]. Hangzhou: Computer Science and Technology College of Zhejiang University. 2010:18-29.

[2] Bi Houjie. The video compression coding standard of new generation: H.264/AVC: [M]. Beijing: Renmin post and telecommunications press, 2005.

[3] Li Xiaoju, Feng Zhanshen, Hu Youqing. The video encryption scheme based on H.264 CAVLC entropy coding [J]. Computer engineering and application. 2009, 45(34)114-117.

[4] LIAN S G,LIU Z,REN Z.Secure advanced video coding based on selection algorithms [J].IEEE Transactions on Consumer Electronics,2006,52(2):621~629.

[5] Li Xiaoju, Hu Haina, Li li. A video encryption scheme based on H.264CABAC [J]. Telecommunications Science. 2010, 26(7)80-83.

Published by Atlantis Press, Paris, France.