International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

H.264/AVC Video Encoding with Simultaneous Encryption and Data Hiding Based on Histogram Shifting

Kripa Antony[1], Savitha T. P.[2]

[1]M. Tech (ECE) Student, MEA Engineering College

[2]Assistant Professor, MEA Engineering College

Abstract: ***Protecting data from intruders is very important in this present scenario .In this work, a method for encoding and encryption of H.264/AVC video and then to embed data in the encryptedH.264/AVC video stream is proposed. Encoding and encryption of the video is done simultaneously. The main 3 stages are video encryption stage, data hiding stage, and data extraction /video decryption stage .In Encryption stage intra prediction mode encryption and Motion vector difference encryption are done. Video encryption is done by using an encryption key. Since the encryption and encoding is done simultaneously computational time can be reduced .Data hiding is the processing of hiding the data in the encrypted video. Data extraction/video decryption step will give the hidden data that have been sending through the video streams and the original video. According to the different applications it can be done in two domain i.e., in the encrypted domain or in the decrypted domain .Data hiding by XOR based method used in previous work is having problem with visual quality after data removal. Hence a method called histogram shifting is used to improve the visual quality after data removal.***

Keywords: H.264/AVC ,Intra Prediction Mode encryption, Motion Vector Difference encryption, Data hiding, Histogram shifting

1. Introduction

Nowadays we are using internet as a fast medium for communication. A lot of information is transmitting through internet. The information includes images, texts, audio and video. Even though it is a fast method for transmission it is more exposed to attacks. Anyone can access and modify our private information. Hence there is need for multimedia security. It can be done with encryption or data hiding algorithms. And in order to reduce the size and for fast transmission of data it is compressed. Now we are trying to combine all the three i.e., data encryption, data compression and data hiding.

Cryptography is the art and science of protecting our information from unauthorized attacks by converting it into a non readable format by the attackers. The process of converting the information called plaintext into the coded information called cipher text is called encryption. And the process which converts back the information is called decryption. Data compression is done to reduce the size. Data hiding is the process to hide the information into a cover media. Data hiding can be done in images, texts audio and videos. Many works are done in data hiding in images.

Video can be considered as a sequence of images followed by audio information. The video processing techniques are adapted from image processing and audio processing techniques. But due to large volume and high data content encryption and hiding data in videos are more complicated. Through this project proposal we are trying to find a suitable method for simultaneous encoding and encryption of H.264/AVC video streams and for data hiding in encrypted H.264/AVC video streams that provides maximum video quality after the data extraction. H.264/AVC is an advance video coding standard.

2. Literature Survey

Authors, S. G. Lian, Z. X. Liu, and Z. Ren,in 2007[1]proposed a method in which watermarking and encryption techniques are combined to enhance to provide ownership and confidentiality.MVD (Motion Vector Difference) encryption and IPM (Intra Prediction Mode) encryption are used.MVD is used to encrypt the motion encryption and IPM is used to encrypt the texture information. Watermarking is performed after encryption. The main draw back with the traditional water marking is that without decryption of the content the data extraction is impossible. This paper provides an improved method so that the water mark can be extracted from the encrypted domain itself. It is unable to embed the watermark in the encrypted content .It is the main disadvantage of this method.

In order to overcome the above said problem S. W. Park and S. U. Shin in 2008[2] proposed a reversible watermarking scheme and encryption scheme. The original content is first encrypted and then perform the reversible watermarking i.e., it embeds the watermark into the encrypted domain. The draw backs are it is not fully format compliant and has little bit overhead, it do not operate in the compressed domain.

Video encryption must meet the requirements of real time and format compliance. Since the video has high volume data encrypting each and every bit of video bit streams is practically impossible. Only selected bit streams which can provide the adequate security are to be encrypted. Here comes the problem of how to select the bit streams that are to be encrypted. The encrypting algorithm like IDEA, RSA, DES or AES that are used with text and binary data that are difficult to directly apply to the video streams. Hence the selective encryption becomes partial encryption.

G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, in 2006 [3]introduced selective encryption method for video applications .Here the motion vectors difference, intra prediction mode and residual co-efficient which are the sensitive part of the AVC video streams are partially encrypted to make it time efficient secure and format compliant data. The drawback of this method is that the selective encryption is performed during AVC encoding, not on compressed domain.

Authors named ,Z. Shahid, M. Chaumont, and W. Puech[4] uses the two coding algorithm namely context adaptive variable length condign(CAVLC) and context adaptive binary arithmetic coding (CABAC), for enhanced section encryption which overcome the drawback of previous methd encryption algorithm used is the AES encryption algorithm in CFB mode and is performed in the entropy coding stage of H.264/AVC .Since it does not affect the bit rate, it is suitable for streaming over heterogeneous networks- main advantage of this method. Reversible data hiding is used for data hiding in a distortion intolerable cover media such as medical images and for the perfect retrieval of the original image after data extraction. There are a lot of methods are developed for this reversible data hiding in recent years. Xinpeng Zhang[5] proposes a new RDH scheme for encrypted images. The main phases are image encryption phase, data embedding phase and data extraction/image recovery phase. Complete encryption of cover image is done and a part of encrypted data is modified to embed the message. With the aid of spatial correlation in natural images extraction of the embedded data is performed and the original image is acquired perfectly. Encryption key, data hiding key are required for encryption and data hiding phase respectively. And decryption key and data hiding key is needed for the data extraction/image recovery phase. The advantage of this method is that one having the encryption key can decrypt the image and detect the presence of hidden data. Unless he is having the data hiding key he is unable to extract the hidden message embedded in the cover image. RDH method is attracted by researchers because of its excellent property that gives lossless recovery of original cover media after the extraction of embedded data as well as protecting the confidentiality of the cover media. Data embedding process in all previous methods are performed by reversibly vacating room from the encrypted images, which causes errors in the image retrieval/extraction stage. Authors. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li[6] proposes a method by reserving room before encryption. Compare with the vacating room after encryption only difference occurred at the encryption stage, i.e., content owner reserves enough room/space on the original image and encrypted. And there is no need for vacating room for data embedding like VRAE method .Instead data hider can accommodate the data to the space already emptied out. Data extraction/image recovery is same in both cases the method can take advantages of all conventional RDH techniques for images, and achieve excellent performance and preserving perfect secrecy.

In the above said methods the data hiding in videos are performed not on the compressed domain but during the AVC compression process. It affects the real time implementation because it is very time consuming due to the compression and decompression cycle. So there is a need for a method to hide the data in the compressed and encrypted domain. Coming section will explain a new work in which simultaneous encoding and encryption of video and data hiding is done.

3. H.264/AVC Video Encoding And Simulataneous Encryption and Data Hiding Using bit XOR

A new method for simultaneous H.264/AVC video encoding and encryption and data hiding in encrypted video is presented here. The different stages are video encryption, data embedding and data extraction/Video decryption. Using an encryption key the encryption of the video is performed. Then the data hider sometimes may not know any idea about the original video can embed the additional information by bit XOR operation. Extraction can be performed in encrypted domain itself or in decrypted domain depends on the application.

A. Encryption

Encryption method should meet the constraints of format compliance and computational cost .So it is practically impossible to encrypt each and every bit stream of compressed video. And hence only a small portion of data is encrypted while keeping the adequate security .This is called selective encryption. Key problem is then how to select the appropriate data to encrypt. And the most appropriate /sensitive data is identified in AVC as IPM, MVD ,and residual co efficient .Here only IPM and MVDs are taken for encryption. These are encrypted using an encryption key.

1) IPM(Intra prediction Mode) Encryption

Among many features Intra Prediction Mode is considered as the main significant feature of H.264/AVC video streams. The first frame is encrypted with IPM encryption. And this frame is considered as the reference frame for the rest P frames.

2) MVD(Motion Vector Difference) Encryption

For protecting the texture as well as the motion information, along with the IPM, motion vectors are also encrypted

B. Data embedding

Even though many methods are developed for data hiding in H264/AVC streams they were failed to apply the technique into the encrypted domain. The proposed data embedding is done by bit XOR operation.

C. Data Extraction/Video Decryption

Depending on the different application, the decryption of video and extraction of hidden data can be done either in encrypted or in decrypted domain. Extraction is simple and fast.

1) Encrypted Domain Extraction(Scheme 1)

Let's see an example that guarantees the feasibility of this scheme. Consider a data base manager (cloud computing) to enhance the privacy of the data in the cloud computing ,he may get access only to the data hiding and have to work on data in the encrypted domain. Here comes the important of this algorithm.

2) Decrypted Domain extraction(Scheme 2)

In scheme 1 both the embedding and extraction is performed at the encryption domain. Some cases are there where one need to encrypt the video and later perform the data extraction to get the hidden data. Consider an authorized user having the decryption key he received the encrypted video with hidden data. Since he is having the decryption key the video can be decrypted. The decrypted video still contain the hidden data that can be used to trace the source of data. Scheme 2 is suitable in this case. Here in this scheme first using the decryption key the video is encrypted .And the decrypted video with hidden data inside is obtained. Data extraction can be done later to get the data.

We are performing the data hiding using bit XOR method. By knowing the No of letters or bits added and the location we can detect the data at the receiver . The bit XOR method will results in a distorted frame.If somehow any noise is added to the video the bits will change. And while performing the bit XOR ing we will get a somewhat distorted video. It will affect the quality of the video. These are the main disadvantage of data hiding using bit XOR method.

4. Data Hiding Using Histogram Shifting Method

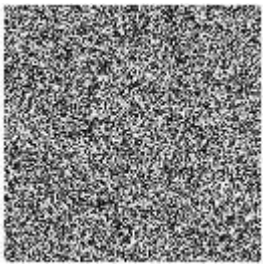
Most of the data hiding techniques are characterized by the permanent distortion of the host image and complete recovery of marked content become impossible. But some applications such as medical and military images degradation is intolerable. So there is need for a method to be introduced which helps the complete recovery of the content after data hiding, i.e., it must be reversible and degradation must be lowered .Solution is histogram based techniques. In this method the data is embedded in the cover media by shifting the image histogram.

In histogram shifting method first the histogram of the image is found. And if the data to be added is one then the pixel count of that block where we want to hide the data is increased by one. If the data is zero no change applies. At the decoder by decreasing the pixel count we can decode the data.

5. Results

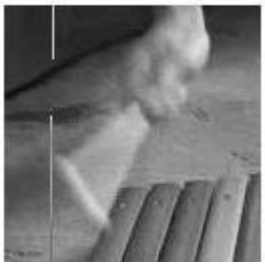
Data hiding in encrypted H.264/AVC video using bit XOR method is having distortion problem. Since we are adding the data using bit XOR ing the frame will modify according to the data hidden. And depending upon the data the distortion may vary. To overcome this problem histogram shifting method is used. It shows better results. A comparison is done by using PSNR , MSE ,Max error and Energy ratio parameters.

(a)Original Frame



(b)Encrypted Frame

(c)Decoded Frame
bit-xor data hiding



(d)Problem with bit Xor method
original image

data hided image

data decoded image

(e) Histogram Shifting Method

In order to see the distortion clearly images taken before encryption is shown here. Figures (a) to (d) shows the result of data hiding using bit XOR method. (e) shows the result of histogram shifting method.

Parameter	Bit XOR method	Histogram Shifting method
PSNR	29.027	38.1488
MSE	0.081354	0.0099587
Max Err	0.29	0.14
L2RAT	0.8267	1.0008

MSE

Mean Squared Error is given by the equation

$$\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(I(i,j)-K(i,j)\right)^2}{mn}$$

Where "m" is the height of the image, "n" is the width of the image, "I" is the original image, "K" is the reconstructed image.

PSNR value

Peak Signal to Noise Ratio in dB is a measure used to find the quality of reconstructed images. PSNR can be calculated by the formula

$10 * \log\frac{MAX^2}{MSE}$ log is taken to the base 10.

Where "MAX" is the maximum possible pixel value, It is 255 if the pixels are represented using 8 bits per sample. MSE is the mean Squared Error .

Max Err

Maximum Error is the maximum absolute squared deviation of the image from the reconstructed image.

L2ARAT

L2RAT is the ratio of the squared norm of the reconstructed image to the original image.

6. Conclusion

In this work a method for simultaneous encoding and encryption of H.264/AVC video streams and data hiding in encrypted H.264/AVC video streams by using histogram shifting is proposed. Since the data hiding is performed in the compressed domain, the time consumption for compression and decompression cycle is avoided. By analyzing the properties of H.264/AVC video the IPM and MVD are chosen as sensitive parts for the selective encryption. IPM encryption is used for texture information and MVD for motion information. The main problem with the XOR method (Bit XOR method will results in distortion of frame, addition of noise will also results in a distorted video ,because we are using XOR method) is solved perfectly by introducing an improved scheme named as histogram shifting. Better results are obtained.

References

[1] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[2] S. W. Park and S. U. Shin, "Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC)," New Directions Intell. Interact. Multimedia ,vol. 142, no. 1, pp. 351–361, 2008.

[3] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 5, pp. 565–576, May 2011.

[4] *Xu, R. Wang,& Yun Q Shi," Data hiding in encrypted H.264/AVC video streams by codeword substitution", IEEE Trans. Inf. Forensics Security, vol.9,No.4, pp.596-606,Apr.2014.*

[5] X. P. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011

[6] X. P. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2,pp. 826–832, Apr. 2012