Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 3, Issue 6; April-June, 2016, pp. 480-483

http://www.krishisanskriti.org/Publication.html

Efficient and Format Compliant Technique for Securing H.264/AVC Video Streams

Divya A[1] and Kiran Kumar[2]

[1]M.Tech Student, Sahyadri College of Engineering & Management under VTU, Belgaum
[2]Sahyadri College of Engineering & Management, under VTU, Belgaum
E-mail: [1]divis11@gmail.com, [2]kiran.ec@sahyadri.edu.in

Abstract—*To ensure privacy and security digital videos has to be processed and stored in an encrypted form. To further enhance security of these videos from tampering, it becomes necessary to embed data in these videos. Hence embedding data in the encrypted videos preserves the confidentiality of the video content. So a novel scheme of embedding data in the encrypted version of H.264/AVC video stream is proposed which involves encryption of H.264/AVC video, embedding data and extraction of data. In order to achieve format compliance and reduce the computational cost, encryption is not performed on the whole compressed video bit stream but the three sensitive parts of H.264/AVC i.e. IPM's, MVD's and residual co-efficient are encrypted. Additional data is embedded in the encrypted domain by using the technique of code word substitution. Extraction of data can be accomplished before decryption, based on the application.*

1. INTRODUCTION

Cloud computing is the latest technological buzzword doing rounds in the business world. It can provide a powerful and scalable infrastructure for large scale storage, processing and dissemination of video data. Though the benefits of cloud services are multifold, cloud security still remains a major concern as it attracts more attacks and are prone to untrustworthy system administrators. Hence it becomes necessary to encrypt the video data. In addition to encryption if data embedding is performed in these videos, then the security and privacy issues concerned with cloud computing can be resolved. In addition to cloud computing, the proposed method, can also be used in other applications which deals with storage and transmission of videos. It can be used in the field of medicine and surveillance systems to store and transmit video streams.

According to the association of encryption algorithms with the compression of video, it can be classified as joint encryption and compression algorithms and encryption algorithms which are independent of compression. For the first type encryption technique is performed during certain step of the video compression process. In [1]-[3] the algorithms for encryption scramble the coefficients of DCT after transformation .some algorithms encrypt the signs of MVD and coefficients of DCT after quantization[4],[5] and in some techniques [6]-[7],during entropy coding selective encryption is performed on modes of inter prediction, motion vector differences and residual coefficients .In the above works, format compliance is achieved, but all of them require a modified structure of the standard video codec, which makes all the existing codec useless. Also the permuting or scrambling of DCT coefficients results in degradation of compression efficiency.

Encryption done in compressed domain improves efficiency. In [8], encryption of the compressed bit stream is done firstly by encrypting the odd indexed bytes in compressed bit stream with a conventional cryptographic algorithm and then used as keys to XOR with the even indexed bytes.in [9], according to the importance of bit stream for decoding, they are divided into five types. Only the first three are encrypted whereas others remain unchanged. The above mentioned algorithms provide satisfying security but computational efficiency and format compliance is low. In [10], the code words of DCT coefficients and MVDs in compressed bit stream are shuffled. In [11], the code words of intra-prediction modes are encrypted. Both these algorithms maintain format compliance and high computational efficiency but have low security.

The security of videos can be enhanced by including additional data hiding algorithm along with encryption algorithm. In [12] an approach which combines encryption and watermarking techniques to protect the videos from attack is put forth. The encryption technique involves the encryption of motion vector differences and encryption of intra prediction modes. The DCT co-efficient are used for watermarking. Earlier water marking techniques didn't allow the extraction of water marks from the encrypted videos. But here the watermarking techniques Are altered such that watermark can be extracted from the videos in encrypted format. This is an advantage as it protects the privacy of the content. The disadvantage of this work is that watermark cannot be embedded in encrypted domain. In [13] a reversible water marking scheme and encryption techniques which protects the right to access and also the originality of video content is proposed. In this work encryption and watermarking is performed simultaneously during compression process. Here

an efficient selective encryption scheme which encrypts the 4x4 blocks of IPM's, the sign Bits of texture and the sign bits of MVD's is used. The watermark is embedded into the encrypted domain using reversible watermarking scheme. The disadvantage of the proposed scheme is that it has bit overhead. The watermarked bit stream is not fully format compliant, which may result in the crashing of a standard decoder since it cannot parse the watermarked stream. Another drawback is that the approaches do not operate on the compressed bit stream.

In this paper, we propose an efficient and format compliant technique to secure H.264/AVC video streams. In order to achieve high security and reduce computational complexity, only the code words of intra prediction, inter prediction and integer transform coefficients are encrypted and additional data embedding can be done by substituting the code words of levels.

2. PROPOSED METHOD

2.1 Block Diagram

The input video in H.264/AVC compressed form is encrypted. Encrypting the entire bit stream is impractical as the computational cost increases and also format compliance cannot be achieved. So only a part of the video data is encrypted. The video data which is most crucial for decoding the video must be selected. Hence we have selected the spatial information and motion information which is in the form of inter prediction mode, Intra prediction mode and integer transform coefficients to encrypt .additional data is then embedded to the encrypted video by substituting the code words of levels.

At the receiver end, the data can be extracted and then the video can be decrypted to get the original video in H.264/AVC compressed form.

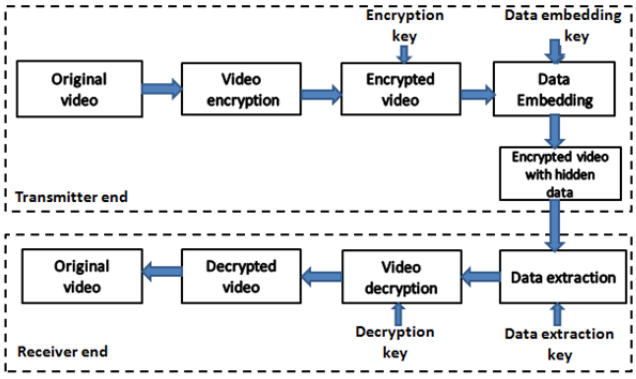

Fig. 1: Block Diagram of proposed system

2.2 Detailed Design

1. Encryption of intra prediction mode:

We choose to encrypt prediction modes in 4x4 and 16x16 intra macro blocks .The prediction modes for 16x16 intra macro blocks are given in macro block type field which also specifies other parameters like coded block pattern. In baseline profile of H.264/AVC, the macro block type field is encoded with the Exp-Golomb code. The coded block pattern indicates the blocks within a macro block containing coefficient of integer transform, hence its values should not be changed. If the value changes, then format compliance cannot be achieved. So it is clear that encrypting the last bit of the code word does not change the value of block pattern which helps to maintain format compliance. thus for 16x16 intra macro blocks, the encryption of intra prediction mode is done by using XOR operation on the last bit of code words and a bit

Of sequence generated using stream cipher determined by encryption key. 4x4_luma blocks of intra macro blocks are similarly encrypted using bitwise XOR operation.

2. Encryption of inter prediction mode:

Exp-Golomb entropy coding is used to encode inter prediction mode. The last bit of the code word is encrypted by applying the bitwise XOR operation with a standard stream cipher determined by an encryption key. Due to last bit encryption the sign of the code word may change but the length will not change thereby maintaining the compliance of format.

3. Encryption of co-efficient of integer transforms:

Context adaptive variable length entropy coding is used to encode quantized co-efficient of integer transform.to maintain compliance of bit stream, we encrypt only the code words of sign of trailing ones and level. The code word of sign of trialing ones and level is encrypted by applying bitwise XOR operation.

4. Data Embedding:

In the encrypted bit stream of H.264/AVC, the Proposed data embedding is accomplished by substituting eligible code words of levels. The code words of levels with suffix length 2 or 3 is divided into two opposite code spaces denoted as C0 and C1.if data bit one needs to be embedded, then code word belongs to C0 else if data bit zero needs to be embedded then code word belongs to C1.

2.3 Flow chart of Data Embedding

Data Extraction Phase:

The extraction of data in the encrypted domain can be done as follows:

STEP 1: Code words of levels are identified

STEP 2: If code word belongs to code space C0, then the bit hidden is 0.

STEP 3: If code word belongs to code space C1, then the bit hidden is 1.

Fig. 2: Flow chart of data embedding

3. EXPERIMENTAL RESULTS:

To evaluate the performance of the proposed algorithm we have implemented H.264/AVC encoder in mat lab and then encrypted and hidden data. The simulations were performed for different image resolutions and different QP values.Table1 shows the results of simulation.

As QP value increases, the compression also increases, but higher the value of QP, degrades the quality of reconstructed picture.

Generally a PSNR value 35 and above implies that the reconstructed frames is indistinguishable from the original.

The SSIM index lies in the range between 0 and 1, where 1 indicates that the reconstructed frames is identical to the original frames.

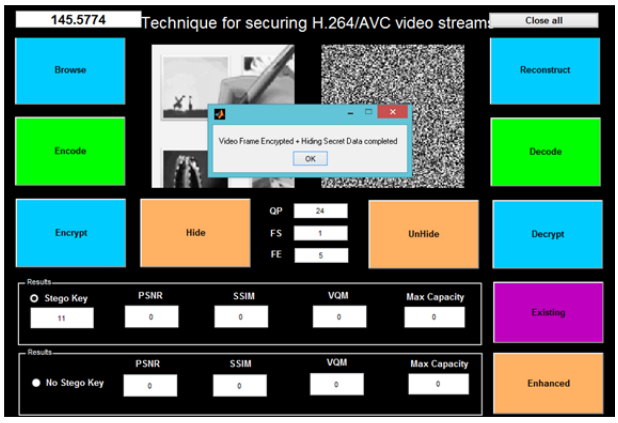

Fig3: GUI showing the process of video encryption and additional data embedding

Another approach to measure video quality is VQM, lower the value of VQM, and higher is the video quality in terms of perception.

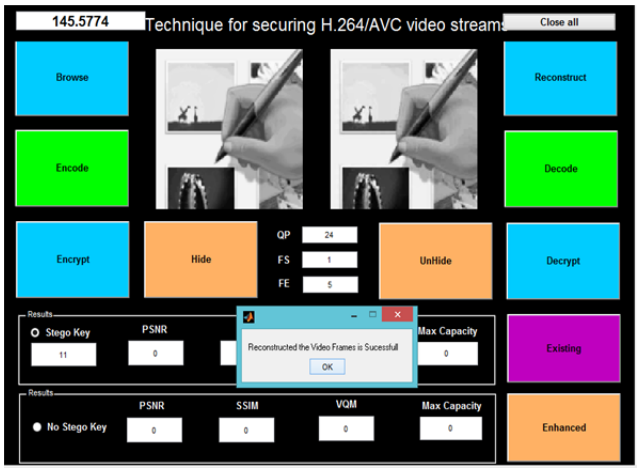

Fig. 4: Shows the GUI of reconstructed frames after data extraction and decryption.

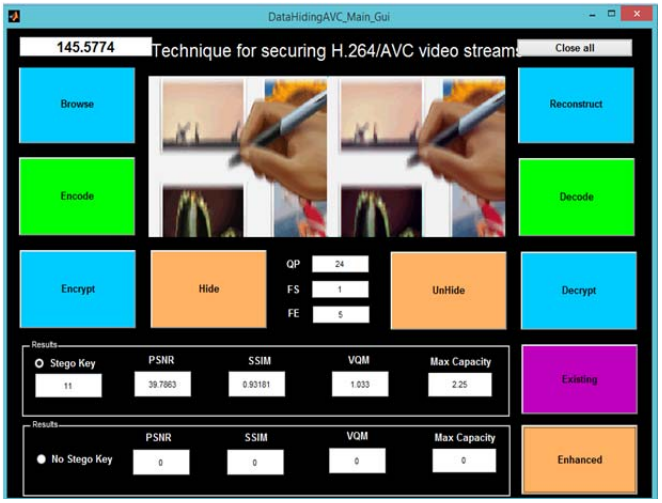

Fig5: Shows the original video at the transmitter end and receiver end.

Simulation Results for different Quantization Parameter.

Table1: Simulation results of the proposed technique

QUANTIZATION PARAMETER	INPUT VIDEO1.avi 350X250 PIXELS				INPUT VIDEO2.avi 160X120 PIXELS			
	COMPRESSION	PSNR	SSIM	VQM	COMPRESSION	PSNR	SSIM	VQM
24	145.5	39.7863	0.9318	1.033	150.4	38.6374	0.978	1.134
26	125.8	39.7868	0.9311	1.032	120.7	38.6376	0.977	1.133
28	110.9	39.7851	0.9303	1.031	105.7	38.636	0.975	1.135
30	94.4	39.7835	0.9288	1.034	85.6	38.6372	0.973	1.133
32	80.5	39.7887	0.9279	1.034	74.9	38.6389	0.970	1.136

4. CONCLUSION

System presents an algorithm to embed additional data in encrypted H.264/AVC bit streams, which consists of video encryption, data embedding and data extraction phases. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e. it does not requires partial decompression of the video stream thus making it ideal for real-time video applications. It preserve the confidentiality of the content completely.

REFERENCES

[1] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," In Proceeding(s)of the 4th Multimedia Conference (ACM Multimedia 96), pp. 219-229, 1996.

[2] A. S. Tang, W. C. Feng, "Efficient multi-layer coding and encryption of MPEG video streams,"2000 IEEE International Conference on Multimedia and Expo., vol. 1, pp. 119-122, 2000.

[3] W. Zeng, S. Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 118-129, 2003.

[4] C. Shi, B. Bharqava, "An Efficient MPEG video encryption algorithm," In Proceeding(s) of the 17th IEEE Symposium on Reliable Distributed Systems, pp. 381-386, 1998.

[5] C. Shi, S. Wang, B. Bhargava, "MPEG video encryption in real-time using secret key cryptography," In Proceeding(s) of PDPTA'99, pp.2822-2828, 1999.

[6] C. P. Wu, C. J. Kuo, "Design of integrated multimedia compression and encryption systems," IEEE Transactions on Multimedia, vol. 7, no. 5, pp. 828-839, 2005., Z. Liang, Y. Chen, O. C. Au, "Security analysis of multimedia encryption schemes basedon multiple Huffman table," IEEE Signal Processing Letters, vol. 14, no. 3, pp. 201-204, 2007.

[7] L. Qao, K. Nahrstedt, "A new algorithm for MPEG video encryption," In Proceeding(s) of the First International Conference on Imaging Science, Systems and Technology(CISST'97), pp. 21- 29, 1997.

[8] T. Shi, B. King, P. Salama, "Selective encryption for H.264/AVC video coding," In SPIE International Society for Optical Engineering, vol. 6072, pp. 171-179, 2006.

[9] J. Wen, M. Severa, W. Zeng, *et al*, "A format-compliant configurable encryption framework for access control of video," IEEE Trans. Circuits Syst. Video Technol., vol. 12, no. 6, pp. 545-557, 2002.

[10] J. Ahn, H. Shim, B. Jeon, I. Choi, "Digital Video Scrambling Method Using Intra PredictionMode," Advanced in Multimedia Information Processing PCM2004, vol. 3333, pp. 386-393, 2004.

[11] S. Lian, Z. Liu, Z. Ren, H. Wang, "Secure advanced video coding based on selective encryption algorithms," IEEE Transactions on Consumer Electronics, vol. 52, no. 2, pp. 621-629, 2006.

[12] S.W.Park and S.U.Shin,"Combined scheme of encryption and watermarking in H.264/scalable video coding.