Middle-East Journal of Scientific Research 24 (S2): 06-09, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S2.102

Codeword Substitution Technique for Hiding Data in Encrypted H.264/AVC Video

F. Melisha Sharon and M Baritha Begum

Department of ECE, Saranathan College of Engineering, Trichy, India

Abstract: Video of today's world is widely secured in the storage environment by the encryption process. To maintain privacy, content notation and tamper detection it is essential to perform data hiding in encrypted videos. The preservation of confidentiality is done in encrypted domain. This paper proposes an efficient method for hiding data directly in the encrypted domain of H.264/AVC video stream. It has three sections i.e., H.264/AVC video encryption, data embedding and data extraction. From the property of H.264/AVC codec, the intraprediction mode code words, the motion vector difference codeword and the residual coefficients codeword are encrypted with stream ciphers. Then data embedder adds the required data in the encrypted version. Then a data embedder adds the required data by codeword substitution without knowing the original video content. Video file size is strictly preserved even after encryption and data embedding.

Key words: Substitution · Motion vector · Intra prediction mode

INTRODUCTION

Today's trend of technology depends mainly on cloud computing. Even in this service the content are vulnerable to unauthorized servers. Moreover H.264 is the most commonly used format for video content. Security and privacy requirements get fulfilled by the method of data hiding in the encrypted domain. Encryption deals with the masking or manipulation of data. So the video is encrypted by the user. The additional information is hidden by a server who does not have the knowledge of the video encryption process. Security and integrity are the basic requirement, which means the cost of breaking the encryption algorithm is not lesser to buying the video's authorization. The data hiding methodology gives the integrity that the original content has not been altered. So a combination of encryption and data embedding meets out the need of today's users not only in cloud computing but also for medical videos, surveillance etc. A video has to be encrypted before the data hiding method comes on screen. The video encryption process mainly can be classified into four classes on their unique way of encrypting the data. Firstly, fully layered Encryption compresses and then encrypts the whole content by encrypting every byte using standard tradition algorithms. Unfortunately this technique involves heavy computation and hence the speed is slow. Secondly, permutation based encryption uses different permutation algorithms to scramble the video contents. It is not necessary to scramble every byte. Some algorithms use permutation list as secret key to encrypt video contents. The next method is selective encryption which encrypts only the selective features of each video. Finally, the perceptual encryption which is used in areas like pay-per-view video, pay TV and video on demand. This kind of encryption requires that quality of audio and visual data is only partially degraded by encryption i.e. from the encrypted multimedia data one can perceive the content in it.

Related Work: In the field of video, S.G.Lian, Z.X.Liu and Z.Ren [1] have proposed a scheme to implement both the commutative video encryption and watermarking. This can be done in the advanced video coding process. The intra-prediction mode, motion vector difference and discrete cosine transform coefficients' signs are in the encrypted form normally in the H.264 standard. But the DCT coefficients' amplitudes are watermarked prominently. Therefore the watermark that was done before can be extracted from the encrypted videos consequently the encrypted videos can be re-watermarked for the next data. This method hides the watermark without exposing the original video content.

Corresponding Author: F. Melisha Sharon, Department of ECE, Saranathan College of Engineering, Trichy, India.

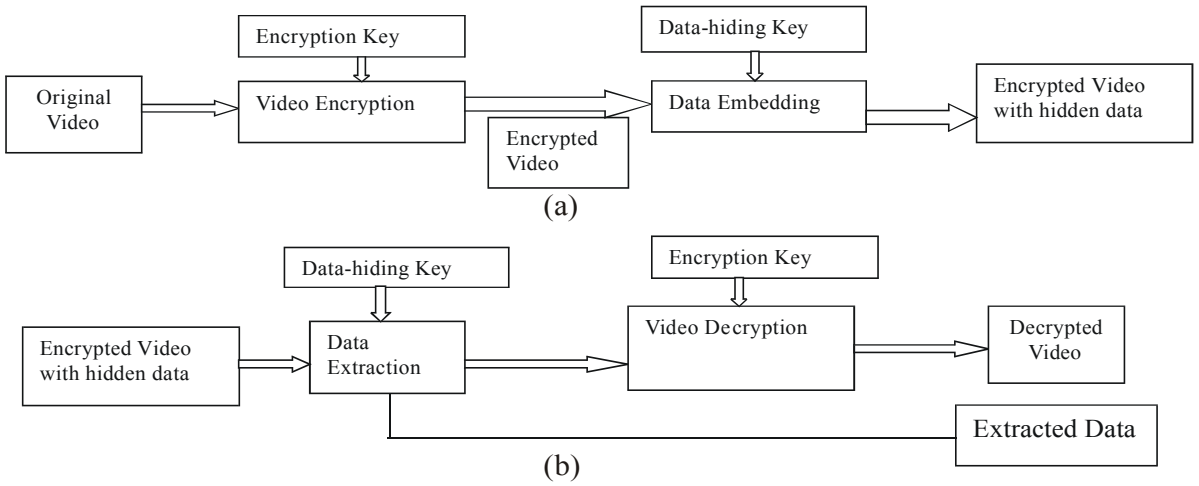

Fig. 1: Block diagram of the proposed methodology

Dawen Xu, Rangding and Jicheng Wang [2] have proposed a method of data hiding in H.264/AVC not in encrypted domain. In this method by the modulation of the prediction modes of 4×4 luminance blocks, the information is hidden. Firstly, the secret information is encrypted by a chaotic sequence and then a small number of luminance blocks that is used for data embedding are randomly selected in each macro block based on another chaotic sequence due to the limitation of easy reproducibility. In the field of image, Peijia Zheng and Jiwu Huang [3] have proposed an scheme of hiding information in the encrypted video. Firstly the Walsh-Hadamard transform has been implemented in the encrypted domain, as it aptly matches the applications in the encrypted domain since its transform matrix consists of only integers. It is then followed by alteration of the relations between the adjacent transform coefficients. Finally watermark extraction is performed both in the decrypted domain and the encrypted domain.

Proposed Methodology: An efficient way of hiding the data in the encrypted domain of H.264/AVC video is introduced here that comprises three sections. Firstly, the video is encrypted using some standard encryption methodology.Secondly, the data that has been selected to be hidden in the encrypted domain is embedded into the video by the proposed codeword substitution method. Here the data embedder may or may not be the video sender. That is the knowledge of video content is not essential for the one who is hiding the data. Finally, the data is extracted at the receiver side from the encrypted domain itself. Fig 1 gives the block diagram of our method. Fig 1. (a) Gives the block at the sender side and Fig 1. (b) Gives the block at receiver side.

Encryption: Encryption is efficient when it satisfies two most important criteria. They are the method has to utilize the time in an efficient manner and the other is it has to be format compliant. So to satisfy the criteria we have chosen to encrypt three most important parts in the video. They are the intra prediction mode, moving vector difference and the residual coefficients. To add a layer of improvement, the encryption is done after the encoding process.

Encryption of IPM: As per the standard of H.264/AVC the Intra_4 × 4, Intra_16×16, Intra_chroma and I_PCM are supported. Inorder to make it an time efficient and also format compliant we choose to encrypt Intra_4 × 4, Intra_16×16.Based on the four modes available for the Intra_16×16 the corresponding code word is being encoded from the standard code book pattern [4].After this encoding process the encryption follows which includes bitwise XOR operation on codeword and pseudorandom sequence obtained by a standard stream cipher. It uses the first encryption key E_key1. Considering the next element Intra_4×4, the preference of prediction mode among the nine available modes for each block must be signaled to the decoder. Let the most probable mode be represented as MPME for the presently considered block. Here the prediction mode of the presently considered block is ModeE. if ModeE is equal to MPME, the codeword is kept unchanged. If not, the three bit code in each of the codeword is encrypted with the pseudo random sequence that is created by a standard secure cipher decided by an encryption key E_Key2.

Encryption of MVD: To preserve the motion information along with the texture information the encryption of

moving vector becomes an important aspect. The MVD is obtained by the prediction on motion vector. The so obtained MVD is encoded by exp-golomb entropy coding. Thus encoding is first done and then the encryption process is done as that of IPM and the cipher is determined by the key E_Key3.

Encryption of Residual Data: As high security is essential, another sensitive data, which is the residual data, must be encrypted in both I-frames and P-frames. On analyzing the standard of H.264/AVC baseline profile, CAVLC entropy coding is used to encode the quantized coefficients of a residual block [5]. Each CAVLC codeword can be expressed as the following format:

{Coeff_token, Sign_of_TrailingOnes, Level, Total_zeros, Run_before}

Encryption of the Sign_of_TrailingOnes also will be similar to that of MVD and IPM which is determined by the key E_Key4.Then the level codeword will be encrypted by bitwise xor which occurs on the basis of E_Key5.

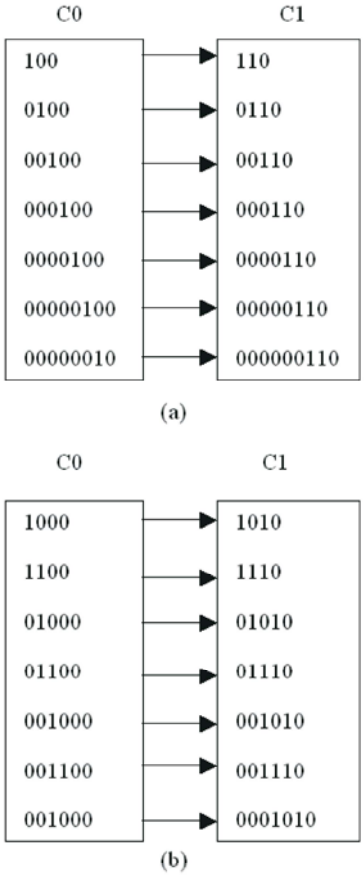

Fig. 2: CALVC codeword mapping (a) suffix length=2 and level >0 (b)suffix length=3 and level >0

Data Embedding: The data embedding process is done by substituting the codeword in the encrypted domain of H.264/AVC. At the same time the codeword that has been substituted must satisfy the following conditions. Firstly, the codeword has to be syntax compliant after the data hiding by codeword substitution. Secondly, the codeword size must be same as that of before substitution. The codewords of the levels of residual data in the P frames are used for hiding the data whereas the I frames are kept unchanged.As the substitution will change the sign of level, codeword substitution is not preferred when suffixlength of the codeword is 1. The codewords belonging to suffixlength 2 and 3 is divided into codespaces as c0 and c1.The codewords for c0 and c1 are connected to binary 0 and 1. So the text has to be in binary.The data hiding is done in four main steps.

- The security is improved by encrypting the data to be hidden with chaotic pseudo random sequence.
- The codewords of Levels are acquired by resolving the encrypted H.264/AVC bitstream.
- If codeword belongs to C0 and data to be embedded is 0 then the codeword is not modified.At the same time if it belongs to C1 it is replaced by the equivalent in C0.But if the data is 1 the codeword will be altered only if it belongs to C0.
- The next codeword is selected and the data is hidden to it.This is repeated until all data is hidden.

Data Extraction: Here, the hidden data is extracted in encrypted domain. The process of data extraction is simple and fast. To maintain the privacy, a database manager may only get approach to the data hiding key and have the influence to the data in encrypted domain. The extraction of hidden data in encrypted domain guarantees the workability of our scheme. In encrypted domain, encrypted video with hidden data is sent directly to the data extraction module.The extraction process will be in three steps.

- The codewords of *Levels* are identified firstly by parsing the encrypted bitstream.
- If the codeword belongs to codespace *C*0, the extracted data bit is “0”.Whereas when the codeword belongs to codespace *C*1, then the hidden data bit is “1”.
- According to the data hiding key, the same chaotic pseudo-random sequence *P* that was used in the embedding process can be generated. Then the extracted bit sequence could be decrypted by using

P to get the original additional information. Since the whole process is entirely operated in encrypted domain, it effectively avoids the leakage of original video content.

Experimental Results: The given data hiding algorithm is implemented in H.264/AVC video.The video is of the 30frames per second.The first 30 frames has been used in experiment.The GOP structure is IPPPP-one I frame followed by four P frames.This data hiding in encrypted video is implemented in MATLAB software with version 2013a.

For video encryption security includes both cryptographic security and perceptual security.So for cryptogenic security the secure stream cipher is used to encrypt the bitstream and chaotic pseudo-random sequence generated by logistic map is used to encrypt the additional data. Perceptual security refers to the impact of encryption on the intelligibility of the video. It is adopted by measuring this PSNR, VQM and SSIM.

Table 1 gives the PSNR,SSIM and VQM values for the video.Though the PSNR value is decreased a little it does not affect the working of the system.Structural similarity index normally lies in the range of 0 to 1.So our method makes only a smaller impact on the similarity after the data has been hidden.Video quality measurement is another approach to find the quality of the video as it agrees more with human visual system.Generally the VQMvalue should be as low as possible.Zero specifies an excellent quality.We obtain values nearer to zero.Fig 2. (a) Gives the 1st and 30th frame of our input video and Fig 2. (b) gives the encrypted frames with hidden data and finally the Fig 2. (c) Gives the retrieved frames after the data has been extracted.

Table 1: PSNR,SSIM,VQM

	PSNR		SSIM		VQM	
Video Sequence	*NON-STEGO*	*STEGO*	*NON-STEGO*	*STEGO*	*NON-STEGO*	*STEGO*
BQMALL	40.7	35.6	0.94	0.82	0.55	0.68

CONCLUSION

The privacy-preserving need from cloud data management has paved way to draw attention into the new topic of data hiding in encrypted media. Here we have proposed a newer algorithm to hide the data into an encrypted H.264/AVC video.This method has only simple stages as video encryption,data embedding,data retrieval and the decryption. The advantage that the data-hider can embed additional data into the encrypted bitstream by codeword substitution, without the knowledge of the original video content adds up to this method. As the data is hidden in the compressed and encrypted realm, it is suitable for real time video application. Experimental results show that it is highly H.264/AVC syntax compliant and that the degradation in quality of video is quite negligible.

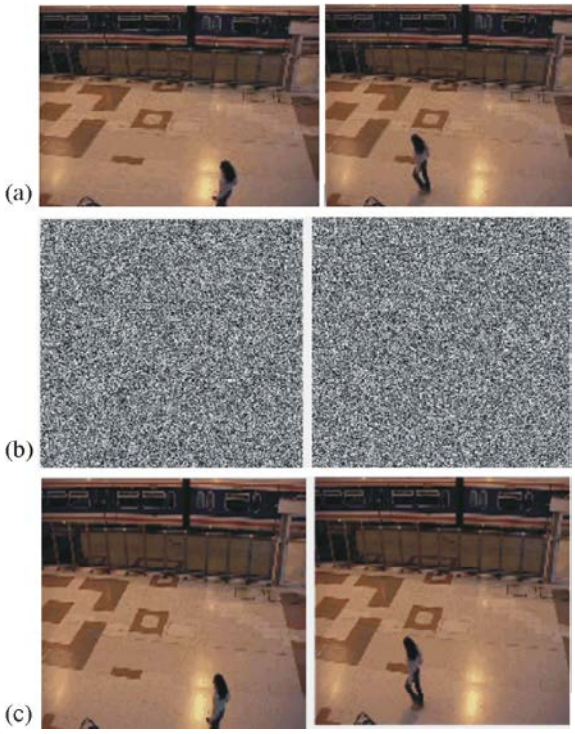

Fig. 3: (a) Input frames (b) Encrypted frames (c) decrypted frames

REFERENCES

1. Lian, S.G., Z.H. Liu and Z. Ren, 2007. Commutative encryption and watermarking in video compression, IEEE Trans. Circuits Syst. Video Technol., 17(6): 774-778.
2. Xu, D.W., R.D. Wang and J.C. Wang, 2012. Prediction mode modulated data-hiding algorithm for H.264/AVC, J. Real-Time Image Process., 7(4): 205-214.
3. Zheng, P.J. and J.W. Huang, 2012. Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking, Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, pp: 1-15.
4. Puech, W., M. Chaumont and O. Strauss, 2008. A reversible data hiding method for encrypted images, Proc. SPIE, 6819: 68191E-1–68191E-9.
5. Stutz, T. and A. Uhl, 2012. A survey of H.264 AVC/SVC encryption, IEEE Trans. Circuits Syst. Video Technol., 22(3): 325-339.