IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution

Gauri Gajanan Bathe[1], Prof. Rahul Patil[2]

PG Student, Computer Engineering, BVCOE, Navi Mumbai, India[1]

Professor, Computer Engineering, BVCOE, Navi Mumbai, India [2]

Abstract: Due to increasing security requirements, digital videos need to be encrypted to maintain confidentially, integrity and availability. This paper proposes data embedding in H.264/AVC video where the embedded data is restored without knowing the original video content. In this manner, confidentially is preserved. The property of H.264/AVC code, the codeword of the intra-prediction modes, motion vector differences and residual coefficients are encrypted with the stream ciphers. User may hide additional data in the encrypted domain by using code word substitution method. Data can be restored in encrypted domain or in the decrypted domain.

Keywords: Data hiding, encrypted domain, H.264/AVC, codeword substitution.

I. INTRODUCTION

With the existence of internet service and ubiquitous network coverage through cellular data plan, video can be conveniently downloaded and broadcasted through social networking. Digital media has become very vulnerable to various attacks like data modification, virus, worm etc. Therefore, there are various needs to protect the vast number of digital videos. The capability of performing data hiding directly in encrypted H.264/AVC video streams avoid the leakage of video content, which can help address the security concerns with cloud computing [1]. For example, when some official videos are encrypted to maintain the privacy of important data, one may hide or embed more information which will be retrieved by the intended person only.

II. LITERATURE SURVEY

There are various methods used for data encryption and data hiding/embedding. Different research work is being performed by many institutions. The below gives detail review on various methods of video encryption and data embedding.

A. watermarking scheme

In the year, September 2011 Dawen Xu Rangding Wang [6] proposed Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping, During the data embedding process, the desirable Exp-Golomb code words of reference frames are first recognized, after that rules are mapped between these code words and the watermark bits are established. Watermark embedding is executed by modulating the corresponding Exp-Golomb code words that is based on the established mapping rules. The watermark information can be restored directly from the encoded stream without resorting to the original host video, and just requires parsing the Exp-Golomb code from bit stream rather than decoding the encrypted host video. Proposed scheme is fragile and re-encoding at alternate bit rates or transcoding removes the watermark.

B. Conventional LSB replacement scheme

In June 2009, Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas [3]proposed a data hiding and extraction procedure for high resolution AVI (Audio Video Interleave) videos. They represented two different procedures, which are used at the sender's end and receiver's end respectively. The procedures are used as the key of Data Hiding and Extraction. Initially stream the video and collect all the frames in bitmap format, and collect the information like starting frame, starting macro block, number of macro blocks and frame period. Then author have used conventional LSB replacement with multiple bit planes.

C. Motion estimation process scheme

In the year 2007, Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras [2] proposed method which takes advantages of various block sizes used by the H.264 encoder during the inter prediction stage to hide the desirable data. It is blind data hiding scheme that means data can be reconstructed directly from encoded stream. The most Important part of inter prediction is motion estimation process. Which aims at finding closest macroblock of current frame. Then each macroblock, within the current frame, is motion compensated i.e. its best match is subtracted from it, and the residual macroblock is coded. To increase the efficiency of coding H.264 standard have adopted 7 different block types (4*4,4*8,4*16,16*4,16*8,16*16,8*8) and to each of the block type motion estimation is applied. The best resulted block type is then selected. So, the basic idea behind this scheme is to let the encoder select the block type

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

according to the data hiding requirement rather than the coding efficiency.

D. Data Hiding in Video Streams Without Intra-Frame Distortion Drif scheme

In October 2010, Xiaojing Ma, Zhitang Li, Hao Tu, and Bochao Zhang [4] proposed a novel readable data-hiding algorithm, which can embed data into the quantized discrete cosine transform, coefficients of I frames without bringing any intra-frame distortion drift into the H.264/(AVC) host video, Intra-frame distortion drift is a huge problem of data hiding in H.264/AVC video streams. Based on a thorough inspection of this problem, they have exploit few paired-coefficients of a 4 × 4 DCT block to gather the embedding induced distortion. The directions of intraframe prediction are used to prevent the distortion drift. The original host video is entropy decoded to get the intra-frame prediction modes and quantized DCT coefficients. After that, the 4 × 4 luminance DCT blocks with large residuals and the suitable paired-coefficients for embedding are selected. The encrypted message is embedded into suitable paired-coefficients depending upon on modulo modulation. Then, all the remaining quantized DCT coefficients are entropy encoded to get the desired embedded video.

E. Enhanced selective encryption scheme

Z. Shahid, M. Chaumont and W. Puech [5] proposed novel scheme for the integrity of copyrighted multimedia content. H.264/AVC. SE (selected encryption) is performed in the context-based adaptive binary arithmetic coding (CABAC) module of host video. The encryption is performed on entropy coding phase of H.264/AVC utilizing AES encryption, this scheme Owns to no escalation in bit rate of H.264/AVC video, this scheme is fit for heterogeneous multimedia streaming scenarios in real-time environment.

III. SYSTEM ARCHITECTURE

Encryption and data embedding are performed almost simultaneously during H.264/AVC video compression process and not on compressed domain in the previous data hiding schemes. Therefor the compression and decompression cycle is tedious and hampers real time implementation.so to adopt various real time application scenario, data extraction can be performed on either from encrypted domain or from decrypted domain [7]

Fig.1 Video encryption and data embedding at the sender end

A. Encryption of H.264/AVC Video Stream

In this scheme, only fraction of video is compressed rather than compressing whole host video to avoid extra computational cost and to make it format compliance, so key issue will be how to select desired sensitive information, spatial information and motion information is encoded during the H.264/AVC encoding. Fig.1 shows the video encryption and data embedding process. Original video is encrypted with the encryption key using bit- XOR (exclusive-OR) operation. After that data is hidden by using codeword substitution technique. Result of which is encrypted video with hidden data. Below are the codewords of H.264/AVC video which are encrypted with stream ciphers

1) Intra-Prediction Mode (IPM) Encryption:

Here IPM's in Intra_4×4 & Intra_16×16 are chosen to encrypt.

2) Motion Vector Difference (MVD) Encryption:

To protect the texture and motion information MVD should also be encrypted, encryption of MVD is performed using Exp-golomb entropy coding.

3) Residual Data Encryption:

CAVLC (context-adaptive variable length coding) entropy coding is used, to encrypt residual data in both I-frames and P-frames, and it is expressed as follows

{Coeff_token, Sign_of_Trailing Ones, Level,Total_zeros, Run_before }

B. Data Embedding

Proposed data embedding is accomplished by substituting eligible codewords. besides,codewords substitution should satisfy the following. First, the bitstream after codeword substituting must remain syntax compliance. Second, to keep the bit-rate unchanged, third, data hiding does cause visual degradation but the impact should be kept to minimum.

Steps for embedding

Step 1: for the security purpose, additional data is encrypted with the chaotic pseudo-random sequence i.e $P=\{p(i)|i=1,2,\cdots,L,p(i)\in\{0,1\}\}$[8] where P(i) is generated using data hiding key

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Step2: By parsing the encrypted H.264/AVC bitstream, codewords of Levels are obtained, suffix length and levels are used to identify the codewords as shown in TABLE 1.
Step3: The to-be-embedded data bit can be embedded by codeword substituting, if current codeword belongs to codespaces C0 or C1 as shown in fig.2
Step4:Choose the next codeword and then go to Step3 for data hiding.

TABLE1. LEVELS AND CORRESPONDING CODEWORDS

Suffix length	level (>0)	Codeword	Level (<0)	Codeword
0	1	1	-1	01
	2	001	-2	0001
	3	00001	-3	000001
	4	0000001	-4	00000001
1	1	10	-1	11
	2	010	-2	011
	3	0010	-3	0011
	4	00010	-4	00011
	5	000010	-5	000011
	6	0000010	-6	0000011
	7	00000010	-7	00000011
	8	000000010	-8	000000011
2	1	100	-1	101
	2	110	-2	111
	3	0100	-3	0101
	4	0110	-4	0111
	5	00100	-5	00101
	6	00110	-6	00111
	7	000100	-7	000101
	8	000110	-8	000111
	9	0000110	-9	0000101
	10	0000110	-10	0000111
	11	00000100	-11	00000101
	12	00000110	-12	00000111
	13	000000100	-13	000000101
	14	000000110	-14	000000111
3	1	1000	-1	1001
	2	1010	-2	1011
	3	1100	-3	1101
	4	1110	-4	1111
	5	01000	-5	01001
	6	01010	-6	00011
	7	01100	-7	01101
	8	01110	-8	01111
	9	001000	-9	001001
	10	0010100	-10	001011
	11	001100	-11	001101
	12	001110	-12	001111
	13	0001000	-13	0001001
	14	0001010	-14	0001011

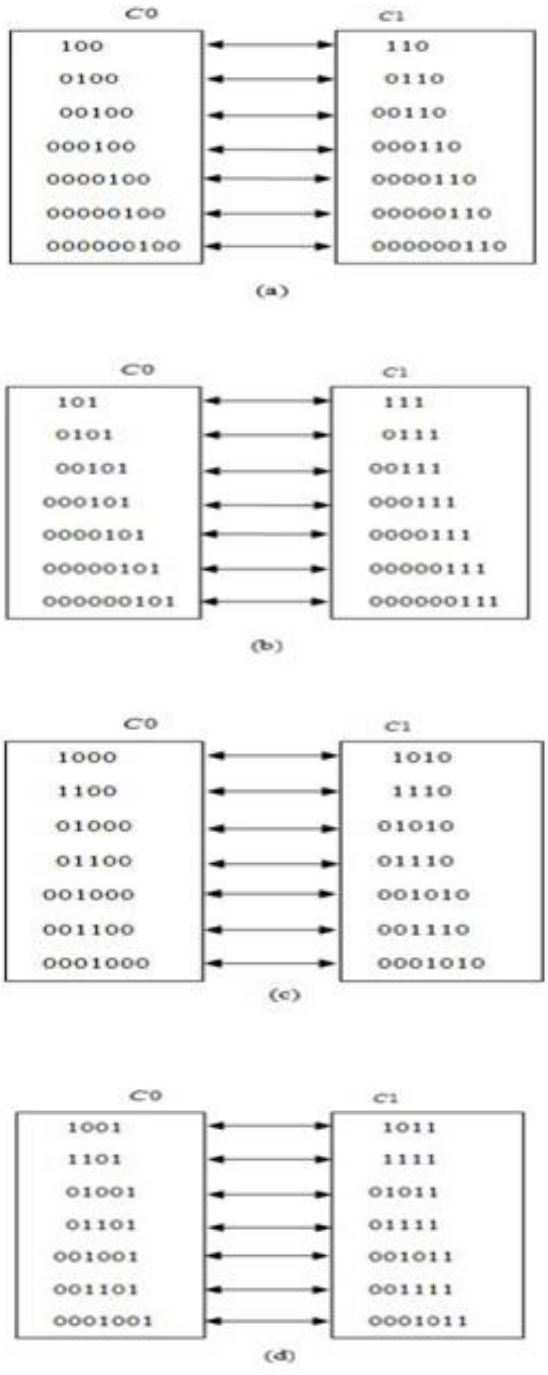

Fig 2. CAVLC codeword mapping.
(a) Suffix Length = 2&Level >0.
(b) Suffix Length = 2&Level >0.
(c) Suffix Length = 3&Level >0.
(d) Suffix Length = 3&Level <0.

C. Data Extraction

In the proposed scheme data can be extracted in two ways either by decrypting the encrypted video streams or without decryption. Fig.2 shows two schemes for data extraction at receiver end.

.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

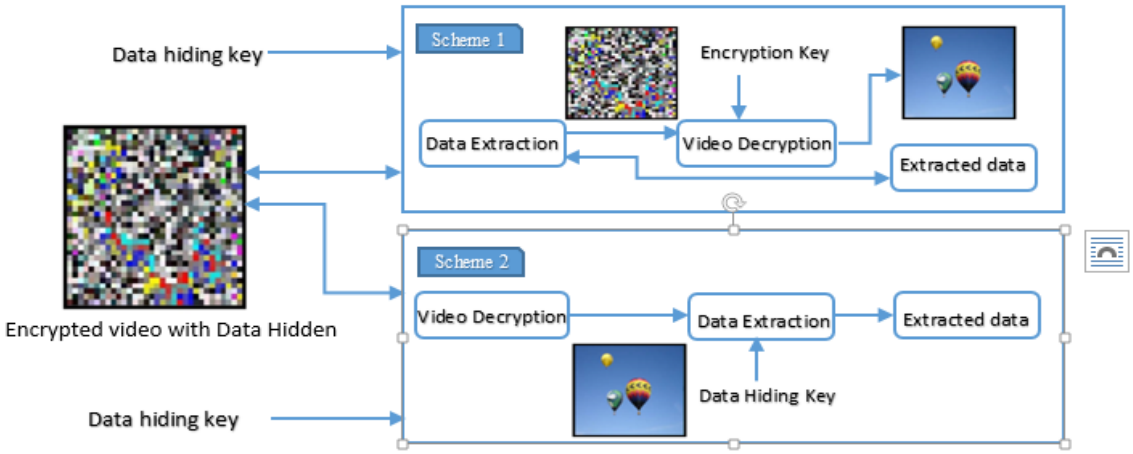

Fig.3. Data extraction and video display at the receiver end

1) Encrypted Domain Extraction.

In Fig.3 scheme 1 at the receiver end data is extracted first without decryption of the video

Step1: By parsing the encrypted bitstream, codewords of Levels are firstly identified.

Step2: extracted data bit is "0" when codeword belongs to codespace C0, and extracted data bit is "1" when codeword belongs to codespace C1.

Step3: As Per the data hiding key, pseudo-random sequence P which was used in embedding process is generated to decrypt the extracted bit sequence.

2) Decrypted Domain Extraction

In Fig.3 scheme 2 first the host video is decrypted then the hidden data is extracted.

Step1: As given by encryption process, Generate encryption streams with the encryption keys.

Step2: The codewords are identified by parsing the encrypted bit stream.

Step3: The encrypted codewords are decrypted by performing XOR operation with generated encryption streams, and then two XOR operations cancel each other out, which renders the original plain-text. Since the encryption streams depend on the encryption keys, the decryption is possible only for the authorized users. After generating the decrypted codewords with hidden data, authorized user may proceed with extraction of the hidden information.

Step4: the sign of Level may change due to last bit encryption. The encrypted codeword and the original codeword remains same code spaces.

Step5: Generate the pseudo-random sequence that was used in embedding process according to the data hiding key. For the additional information, extracted bit sequence should be decrypted.

IV.CONCLUSION

Objective of any data hiding algorithm is to hide the data in such way that it should become difficult to retrieve the hidden data for unintended user. In this paper, code word substitution is used to hide data in host video. Using this scheme file size of the host video is preserved along with the confidentiality.

ACKNOWLEDGMENT

I would like to acknowledge **Prof. Rahul Patil,** for guiding me throughout the project development.

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras “Data Hiding in H.264 Encoded Video Sequences” in IEEE trans, 2007

[3] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas Proposed “Data hiding in video” International Journal of Database Theory and ApplicationVol. 2, No. 2, June 2009

[4] Xiaojing Ma, Zhitang Li, Hao Tu, and Bochao Zhang, “A Data Hiding Algorithm for H.264/AVC Video Streams without Intra-Frame Distortion Drift”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 20, NO. 10, OCTOBER 2010

[5] Z. Shahid, M. Chaumont and W. Puech “FAST PROTECTION OF H.264/AVC BY SELECTIVE ENCRYPTION OF CABAC FOR I & P FRAMES”, 17th European Signal Processing Conference (EUSIPCO 2009) Glasgow, Scotland, August 24-28, 2009

[6] Dawen Xu Rangding Wang “Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping”, Optical Engineering Volume 50, Issue 9, 1 September 2011

[7] Dawen Xu, Rangding Wang, and Yun Q. Shi, “Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014

[8] D. W. Xu, R. D. Wang, and J. C. Wang, “Prediction mode modulated data-hiding algorithm for H.264/AVC,” J. Real-Time Image Process., vol. 7, no. 4, pp. 205–2