ISSN: 2277-5528
Impact Factor: 3.145

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

A NOVEL, PRIVACY PRESERVING SECRET INFORMATION EMBEDDING TECHNIQUE INTO ENCRYPTED VIDEO STREAM

Meghana N M*, Mr. Santhosh B
* M.Tech Student, Assistant Professor
Department of Telecommunication, DSCE, Bangalore, India

ABSTRACT

Transmission of video over internet is prone to attacks from untrustworthy system administrators. Hence it is necessary to perform encryption of video content for maintaining privacy and security. For authentication and damage detection, it is necessary to embed secret information in these encrypted videos. A novel method is proposed where the secret information is embedded directly into encrypted video stream, thereby maintaining confidentiality of video content. The input video is compressed using H.264/AVC encoder, and selectively encrypted. The codewords of residual coefficients, motion vector differences and intra-prediction modes are encrypted using a stream cipher. The data hider then embeds secret information in this encrypted video using a novel codeword substitution technique, and is unaware of the content of video. Thus confidentiality of video content is protected. The authenticated receiver can then extract the hidden data either in encrypted or decrypted domain. We compute PSNR, SSIM and VQM to validate the feasibility and efficiency of the proposed work.

KEYWORDS: encryption, authentication, H.264/AVC, codeword substitution..

INTRODUCTION

With the ever growing popular usage of internet, multimedia data that is transmitted over the internet is prone to attacks from intruders and untrustworthy system administrators. Thus it is necessary to safeguard the data by performing encryption over the multimedia data. Video finds its applications in many fields like medical surveillance, military etc. For protecting the ownership rights and content notation, it is necessary to embed secret information into this video. In medical videos or surveillance videos, in order to protect the privacy of the people, the videos are encrypted. It is then required that a database manager embed personal information like name or age of the person directly into the encrypted video. This act of performing data hiding directly into encrypted video streams avoids the leakage of the video content, since the data hider can embed the additional information into video without knowing the content of the video. By extracting the hidden data from the video, the authenticated receiver may then verify the integrity of the video.

In this work, the video is compressed using H.264/AVC compression format, which is the most widely used video compression format in Blu-ray, DVDs and for transmission of video streams over internet. It is found from the H.264/AVC baseline profile that the sensitive information of video is contained in 3 parts- Intra-prediction mode(IPMs), motion vector differences(MVDs) and residual coefficients. The IPMs and MVDs are encoded using Exp-Golomb code, the residual coefficients are encoded using Context Adaptive Variable length coding(CAVLC). The encryption scheme is then combined with these two algorithms, where in a standard stream cipher is used for encrypting the codewords.

Selective encryption is performed in H.264/AVC compressed domain, where in bit streams are operated directly. The codewords of IPMs, MVDs and residual coefficients are encrypted using a stream cipher. Data is then hidden directly into this H.264/AVC compressed bit stream. This poses few challenges as we should find out where and how to modify the bit stream so that the encrypted video with the hidden data is still a compliant compressed bitstream. Secondly, we must ensure that the decrypted videos containing hidden data will still appear to be of high visual fidelity. Thirdly the file size after encryption and information embedding must be maintained. To meet the aforementioned requirements, we employ a novel codeword substitution technique, which ensures both format compliance and strict file size preservation. The authenticated receiver can then, according to the application, retrieve the secret data either in the encrypted domain or in decrypted domain. To validate the feasibility of the proposed work, we compute PSNR, SSIM and VQM, which have shown that the degradation in video quality caused by embedding is very small.

RELATED WORKS

In the open literature, a few successful data hiding schemes in encrypted domain have been reported. In [2], a water marking scheme using Paillier cryptosystems is carried out in encrypted domain. But due to the constraints of Paillier cryptosystem, encryption of the image resulted in a high overhead in storage and computation. There has been several works on reversible data hiding in encrypted images recently [4]-[8].However in these images, the host image is in uncompressed format. A robust watermarking algorithm is proposed in [9], to insert watermark directly into compressed and encrypted JPEG2000 images.

The above mentioned works have been proposed on image. There have been very less or no reports on secret information embedding in compressed, encrypted video streams. Only few joint data hiding and encryption approaches on video have been proposed. I n [10], during H.264/AVC compression, the signs of IPMs, MVDs and DCT coefficients are encrypted while DCT coefficients amplitudes are watermarked. In [11], combination of encryption and watermarking is presented. The IPMs of 4X4 luminance block, sign bits of texture and sign bits of MVDs are encrypted, while IPM is used for watermarking. But the watermarked bitstream is not fully format compliant, so the standard decoder may crash as it cannot parse a watermarked bitstream.In existing technologies, [10]-[11], encryption and data hiding are implemented almost simultaneously during H.264/AVC compression process. But for certain applications, it is necessary to perform data embedding directly in encrypted domain. Besides, these works led to increase in bit-rate of H.264/AVC bitstream.

Therefore it is highly desirable to develop data hiding algorithm that works entirely on encoded bitstream in encrypted domain.

PROPOSED SCHEME

Figure 1(a) and (b) shows the block diagram of the proposed scheme of hiding data directly in encrypted video streams.

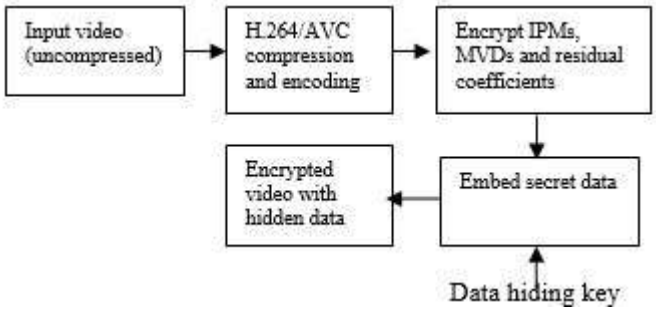


Fig.1 (a) Video encryption and data embedding at the sender end.

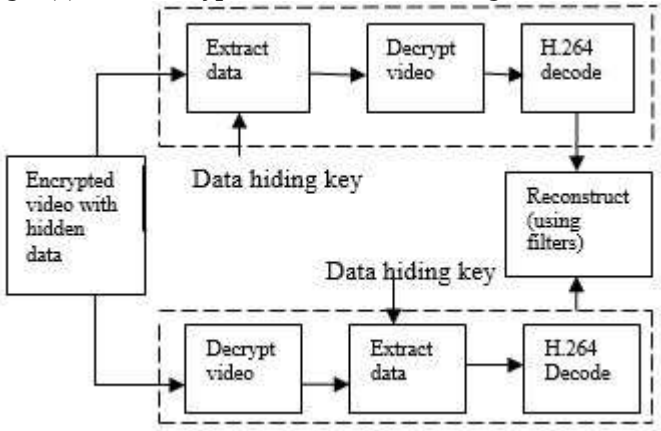


Fig.1 (b) Data extraction and video display at the receiver end in two scenarios.

The input video is fed to H.264/AVC encoder and selectively encrypted. Selective encryption considerably reduces the key size and computation time. This work makes use of symmetric encryption where the sender and the receiver are aware of the encryption key in prior. Using codeword substitution technique, data is embedded directly into encrypted video streams. At the receiver end, data can be extracted either in encrypted domain or in decrypted domain.

A. Encryption of H.264 Video stream

1)Intra Prediction Mode Encryption

For IPM, the prediction is set by the previously encoded data of the same frame, this prediction is subtracted from the current frame. This is called Intra-Prediction Mode. Four types of Intra coding are supported-Intra 4X4, Intra16X16, Intra_chroma and I_PCM. Here IPMs in Intra_4X4 and Intra_16X16 are chosen to encrypt.

The IPMs for Intra_16X16 is specified in mb_type. The mb_type is encoded using Exp-Golomb code[17] which is as follows-

Step 1: Let X= mb_type
Step 2: Compute X+1
Step 3: Represent X+1 in binary.
Step 4: Calculate the number of bits required to represent X+1 in binary. Represent this as N.
Step 5: Append N-1 zeros to binary representation of X+1.

In order to maintain format compliance, we encrypt the IPM codeword with a stream cipher. In order to keep the codeword length unchanged, the last bit of the IPM codeword is XOR-ed with the bits of the standard stream cipher.Table.1 shows the encryption of IPM.

mb_type	Codeword using Exp-Golomb	Stream cipher	Encrypted IPM codeword
1	010	1	011
2	011	0	011
3	00100	0	00100
4	00101	1	00100

Table.1- IPM encryption

2)Motion Vector Difference(MVD)Encryption

IPM encryption is not secure enough, so to protect both texture information and motion information, motion vectors should be encrypted[13]. MVD is obtained by performing motion estimation and motion compensation of current frame and a number of reference frames (Inter Prediction Mode). According to H.264/AVC baseline profile, the same Exp-Golomb code is used to encode the MVDs and the last bit of the codeword is XORed with stream cipher for encryption.Table.2 shows the MVD encoding and encryption.

MVD	code_num	MVD codeword	Stream cipher	Encrypted codewords
1	1	010	1	011
-1	2	011	0	011
2	3	00100	0	00100
-2	4	00101	1	00101

Table.2 MVD encryption

3)Residual Data Encryption

Another type of sensitive data-residual coefficients are also encrypted in both I and P frames. Context Adaptive Variable Length Coding(CAVLC) entropy coding is used encode the residual coefficients. Encryption scheme is then combined with this encoding.

CAVLC works on every macroblock(16X16 pixel block). Each macroblock of a frame is subdivided into sub macroblock of size 4X4. This 4X4 block is read in zig-zag manner.

The Fig.2 shows the steps in CAVLC encoding:

ISSN: 2277-5528
Impact Factor: 3.145

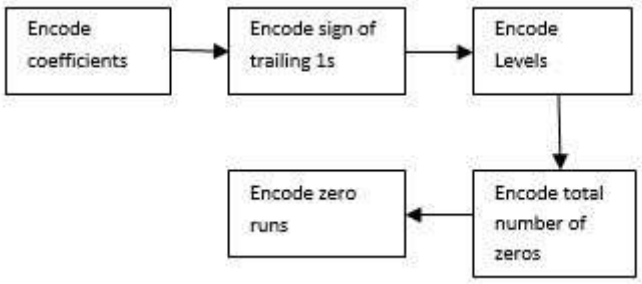


Fig.2- Steps in CAVLC encoding

To maintain bit stream compliant,all syntax elements are not modified during encryption. Residual data encryption is accomplished byb modifying the codewords of Sign_of_Trailing_ones and Levels.Bitwise XOR operation is used with a standard stream cipher for encryption.
Table .3 shows the codeword for each Levels. The codewords are obtained from the look up table with respect to suffix length.

B. Data Hiding

The proposed data embedding is obtained by substituting eligible codewords of Levels in Table.3.The codeword substitution should satisfy the 3 limitations-

1)After codeword substitution, the bitstream must remain syntax compliant to be decoded by the standard decoder.
2)The substituted codweword should have the same length as the original codeword.
3)The data hiding must not damage the visual quality of the video.

The data is embedded only in Levels of P frames and the codewords of Levels in I frames are unmodified. Because the error in I- frame will be propagated to next subsequent frames.

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	0000100	-9	0000101
	10	0000110	-10	0000111
	11	00000100	-11	00000101
	12	00000110	-12	00000111

	13	000000100	-13	000000101
	14	000000110	-14	000000111

Table.3 CAVLC encoding for Levels

The codewords are mapped into two codespaces C0 and C1, in the Table.3. Fig.3 shows the codeword mapping.

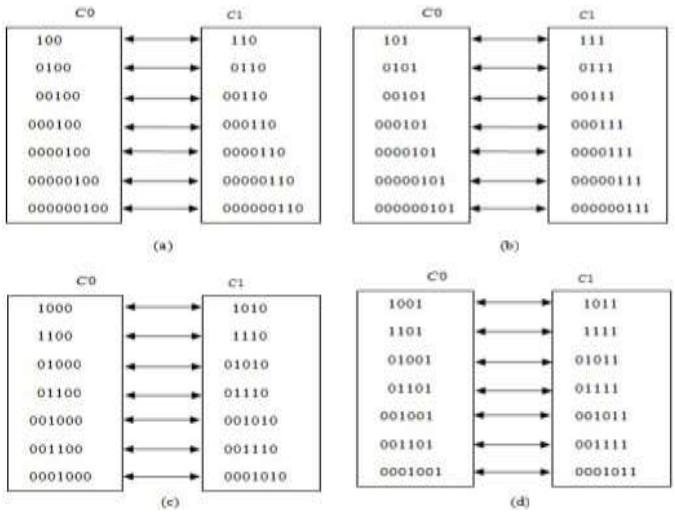
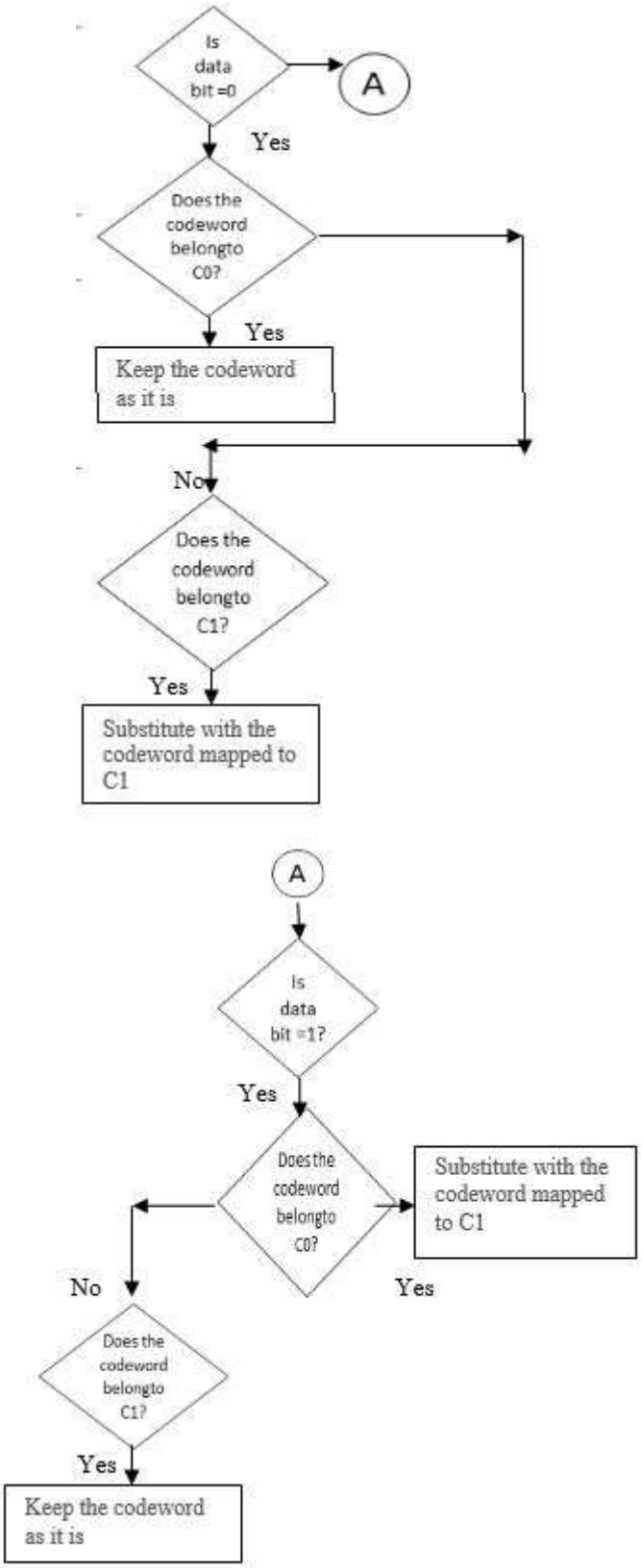


Fig.3 CAVLC codeword mapping. (a) *suffix Length = 2& Level > 0.*
(b) *Suffix Length = 2& Level > 0. (c) suffix Length = 3& Level > 0.*
(d) *suffix Length = 3& Level < 0*

1. *Codeword substitution technique*

The data to be embedded into a binary sequence of 0s and 1s.
Figure below gives the flowchart of the method proposed.

ISSN: 2277-5528
Impact Factor: 3.145



In order to allow only the authenticated person to embed the secret data, the secret data is encrypted with secret key.

C. Data Extraction

The hidden data can be extracted either in encrypted domain or in decrypted domain. Data extraction in encrypted domain guarantees the feasibility of the proposed work by avoiding the leakage of the original video content.

In encrypted domain:

Step 1: The codewords of Levels are identified by parsing the encrypted bitstream.

Step 2: If the codeword belongs to C0,the extracted data bit is 0, If the codeword belongs to C1, the extracted data bit is 1.

In decrypted domain:

Step 1: Decrypt the video using the stream cipher.

Step 2: Identify the codewords of the Levels.

Step 3: If the codeword belongs to C0,the extracted data bit is 0, If the codeword belongs to C1, the extracted data bit is 1.

The original video is reconstructed using the bilinear filter to remove the noise added during data embedding and to retain the edges. Processing is done in gray scale, while displaying the reconstructed video in color reduces the salt and pepper noise.The contrast is increased.

EXPERIMENTAL RESULTS

The proposed work is implemented in MATLAB version 2013b. The scheme is tested on 3 real time videos which are in uncompressed .avi format. The frames are in QCIF format(176X144).The secret data to be hidden is an image of dimension 64X64.The group pictures structure is "IPPP", one I frame followed by four P frames

This video encryption scheme provides both cryptographic security and perceptual security. PSNR (Peak Signal to Noise ratio),SSIM(Structural Similarity Index) and VQM(Video Quality Measurement) are evaluated to test the perceptual quality.

PSNR is given by-
PSNR= 10log(signal amplitude/noise amplitude) dB

The SSIM deals with the content of the video with regard as to how much identical the reconstructed video is with original video. SSIM index lies in the range between 0 and 1, 0 indicates no similarity and 1 indicates almost similar.

VQM is a measure related to human perception, regarding the visual quality and contrast.0 indicates excellent quality.

Table .4 evaluates the performance of the proposed scheme on 3 videos for a designed QP(quantization parameter) value.

.

Sequence	QP	PSNR(dB)	SSIM	VQM	Embedding Capacity (kb/s)
Video 1	24	36.839	0.9622	1.002	2.25
Video 2	24	32.3976	0.9276	1.043	2.304
Video 3	24	34.7809	0.945	1.008	2.276

Table 4 Results

CONCLUSION

A novel data hiding algorithm is proposed which operates directly on encrypted H.264/AVC video streams, which allows the data hider to embed the secret data without the knowledge of video content, thereby avoiding content leakage. The mentioned scheme finds extensive applications in cloud computing[1]. The data-hider can embed additional data into the encrypted bitstream using codeword substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, our method can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides two different practical applications. Another

advantage is that it is fully compliant with the H.264/AVC syntax. Experimental results have shown that the proposed encryption and data embedding scheme can preserve file-size, whereas the degradation in video quality caused by data hiding is quite small.

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. B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," *Inf. Sci.*, vol. 180, no. 23, pp. 4672-4684, 2010.
3. P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homo- morphic encrypted domain and its application in image watermarking," in *Proc. 14th Inf. Hiding Conf.*, Berkeley, CA, USA, 2012, pp. 1-15.
4. W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE*, vol. 6819, pp. 68191E-1-68191E-9, Jan. 2008.
5. X. P. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255-258, Apr. 2011.
6. W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199-202, Apr. 2012.
7. X. P. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826-832, Apr. 2012.
8. K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553-562, Mar. 2013.
9. A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Trans. Multimedia*, vol. 14, no. 3, pp. 703-716, Jun. 2012.
10. 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.
11. 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.
12. T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560-576, Jul. 2003.
13. S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Trans. Consumer Electron.*, vol. 52, no. 2, pp. 621-629, May 2006. 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.
14. M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 3, pp. 425-437, Mar. 2013.
15. T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryp-tion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325-339, Mar. 2012.
16. *Advanced Video Coding for Generic Audiovisual Services*, ITU, Geneva, Switzerland, Mar. 2005.