Data Hiding in H.264/AVC Video Streams with Tampering Detection

[1]R.Aparna, [2]Ajish S
[1] PG Scholar, [2] Assistant Professor In CSE
College of Engineering, Perumon, (CUSAT)
[1] raparnamohan92@gmail.com [2] ajishs2014@gmail.com

Abstract- **With the arrival of many sophisticated video editing technologies, it becomes significantly difficult to trust the correctness of the video information. There are many cryptographically secure ways of video transmission. The proposed scheme includes encryption, data hiding and tampering detection using the embedded data. The proposed method includes the following three parts- H.264/AVC video encryption ,data embedding and data extraction for tampering detection. A selective encryption is performed in the compressed domain. Encryption and data hiding make use of the compression parameters. Two sensitive parameters namely intra prediction modes (IPM) and motion vector difference(MVD) are selected for encryption . The data hiding is performed by codeword substitution technique where the codewords of levels are used. The data embedded is used for tamper detection.The scheme ensures both format compliance and strict file size preservation even after encryption and data hiding.**

***Index Terms*— Codeword substitution, data hiding, encryption, H.264/AVC, tampering detection.**

I. INTRODUCTION

In the present world, video security is of a great concern. Video security finds its major applications in cloud computing, military purposes, medical purposes, video surveillance and as such. Since cloud computing has attracted many attacks and unauthorised users ,there is a need to provide high security to the data stored in cloud[1].For secure storing of data, the data must be stored in an encrypted format. For content notation and such purposes, it is important to have some data embedded into it. The main problem with data embedding by a data hider is the revealing of the video content. So the data embedding needs to be carried on an encrypted domain. Another major application is in the medical area. Videos need to be stored in an encrypted format to preserve the security of the video. There may be instances where the details of the patient need to be embedded into the video for content notation purposes. Here too the importance of information hiding in the encrypted video comes into play. In military applications, highly confidential videos need to be transmitted with hidden data. To provide video security various encryption schemes have been introduced to bring out perceptual security. Perceptual security is the process of making a video unintelligible to a third person who does not have an access to the video. Though perceptual security saves a third party from viewing the content, it won’t protect the video from active tampering efforts. To avoid tampering efforts is difficult. The only way to ensure the integrity of the data is through a tampering detection process.

The main challenge faced by every encryption and tamoer detection scheme in video is that the preservation of video size after encryption and data hiding process. There has been much research activity on data embedding in video for authentication and tamper detection. But till now, all the studies were involved in a watermarking or data embedding scheme directly into the compressed or non-compressed video, which will result in revealing of the original content to the data hider which reduces privacy. In [2] a data embedding scheme on encrypted image is proposed, were the encryption is done by using a Paillier cryptosystem. Another watermarking scheme on encrypted image based on Walsh-Hadamard transform is presented in [3]. The main drawback of these two proposals was that they use Paillier cryptosystem which results in high storage overhead and computation. All these methods worked on images . A successful tampering detection technique was explained in [4]. Here, the watermarking scheme was introduced in the compressed but non-encrypted domain.

The paper proposes a novel method of selective encryption and tampering detection in video using the codewords used in encoding. Thus the file size is preserved and strict format compliance is achieved.

The remainder of the paper is organised as follows. Section II describes the proposed encryption and data hiding scheme which is used for tampering detection followed by conclusion.

II. PROPOSED SCHEME

In this section, a novel scheme of data hiding technique in the encrypted domain is presented. The system includes 3 parts- H.264 video encryption, data embedding and data extraction for tampering detection. The encryption is done by encrypting 2 sensitive data elements namely IPM codewords and motion vector codewords. The encryption is done using a standard stream cipher. Data hiding is done in the encrypted domain using a codeword substitution technique. At the receiver side, the data extraction is done in the encrypted domain. The block diagrams are as follows:

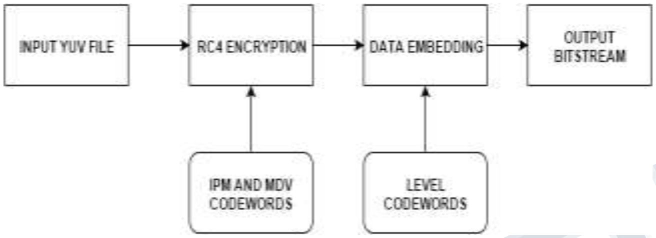

Figure 1. Encoder Block Diagram

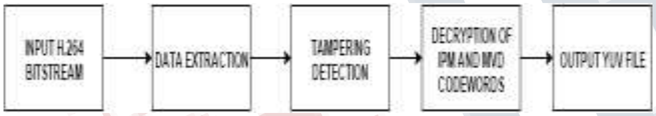

Figure 2. Decoder Block Diagram

A. Overview of H.264

The Moving Picture Experts Group and the Video Coding Experts group (MPEG and VCEG) have developed a new standard entitled 'Advanced Video Coding' (AVC) and is published jointly as Part 10 of MPEG-4.

H.264 does not explicitly define a CODEC(enCOder/DECoder pair) but defines a syntax of an encoding and decoding the bitstream. The encoder consists of two paths- a forward path and a reconstruction path. H.264 defines a set of three profiles namely the Baseline Profile , the Main Profile and the Extended Profile . The encryption is done in the Baseline Profile where the codewords of IPM and motion vectors are encrypted using a stream cipher[5].

B. Encryption of H.264 video stream

In order to bring out perceptual security to the video, sensitive parts should be identified to perform a selective encryption. The sensitive data found were the Intra Prediction Mode(IPM) Codewords and the motion vector difference(MVD) codewords. Both spatial data(IPM) and temporal data (MVD) are encrypted. In order to satisfy the greatest challenge that is file size preservation, the codewords of IPM, MVD formed during the encoding process by CAVLC is used for encryption. The detailed encryption procedure is given in the following subsections.

C. IPM Encryption

Considering H.264 encoder there are 4 types of intra prediction mode formation namely Intra_4x4, Intra_16x16, Intra_chroma and I_PCM. Here only Intra_4x4 mode is used for encryption. The encryption is done in the UVLC format which stands for Universal Variable Length Coding format. The codewords of Intra_4x4 will be a single bit "1" or will be fixed code length of 4 having a bit"0" along with a fixed 3 bit code based on the prediction mode of the currently considered block.[5]. The LSB of the 3 bit code is encrypted with the encryption bitstream produced by the RC4 algorithm with key key_1[6]. The encryption being an XOR operation of the LSB with the encryption stream[7].

D. MVD Encryption

MVD is the offset between the current bock and the position of the candidate region for motion compensation. In H.264 Baseline profile, Exp-Golomb entropy coding[5][8] is used to encode MVD . The INFO field of Exp-Golomb codewords are used to encrypt. The LSB of the MVD codeword is encrypted by performing an XOR operation with bitstream generated by RC4 with key key_2. Since we are encrypting only the last bit, the file size is strictly preserved.

E. Tampering Detection

Tamper detection is the ability of a device to sense that an active attempt to compromise the device integrity or the data associated with the device is in progress; the detection of the threat may enable the device to initiate appropriate defensive actions[9]. Although above mentioned technique brings out perceptual security, it is important that we need to have a tamper detection technique because encryption won't protect the video from active tampering efforts. To bring out tamper detection, we can either add extra bits to the video for authentication or can have a tamper identifier algorithm . In either case, it harms the decoder as the resultant bitstream is not format compliant or it does not preserve the file size. Inorder to satisfy both the problems, it is necessary to have a tamper detection technique through data hiding. The data hiding technique should be such that it results in format compliant bit stream and preserves the file size.

F. Data Selection

The data to be embedded should be such that it denotes a property or a characteristic of the video. In other words, the data selected should be sensitive. In the proposed scheme, the data selected to embed is the codeword of Intra Prediction Modes, specifically the Intra_16x16 mode. The

Intra_16x16 codewords are formed using Exp-Golomb entropy coding and is denoted in mb_type field[8]. Predictive coding is not used here. The prediction mode for luma coded in Intra_16x16 mode or chroma coded in Intra mode is signaled in the macroblock header[5].

G. Data Embedding

In H.264/AVC baseline profile, CAVLC entropy coding is used to encode the quantized coefficients of a residual block[5]. The CAVLC entropy coding follows the following format:

{Coeff token, Sign of TrailingOnes, Level,Totalzeros, Run before}

The codeword for each Level is made up of a prefix (level prefix) and a suffix (level_suffix) as

Level codeword =[level prefix],[level suffix]

The data embedding process is done by substituting eligible codewords of levels. The levels with suffixLength less than 2 are not used for data embedding because there is no corresponding codeword with same length to be substituted. The codewords of P-frame[5] is used for data embedding and I-frame and B-frame level codewords are not changed. The codewords of level with suffixLength 2 or 3 are used. The corresponding pair of codewords are divided into 2 codespaces namely C0 and C1 as shown in the figure below:

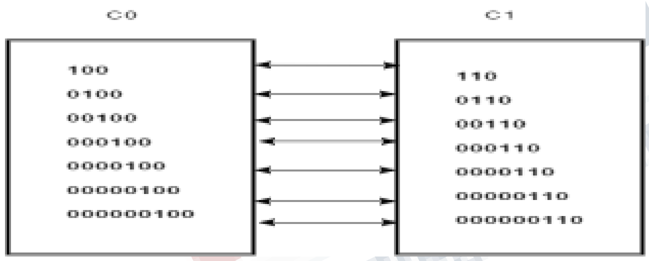

Figure 3. CAVLC codeword mapping

The data to be embedded is first encrypted with a chaotic pseudo-random sequence.[8].

The algorithm for codeword mapped data hiding is given below:

```
if(data bit==0)
{
        If(the codeword belongs to C0)
                The codeword is unmodified;
        Else if(the codeword belongs to C1)
                The codeword is replaced with the corresponding
        codeword in C0.
}
else if(data bit==1)
{
        if(the codeword belongs to C1)
                The codeword is unmodified;
        else if(data bit==1)
{
        if(the codeword belongs to C1)
                the codeword is unmodified;
        else if (the codeword belongs to C0)
                the codeword is repaced with the corresponding
        codeword in C1.
```

H. Data Extraction

The proposed scheme extracts the data from the video for tampering detection.

The steps are as follows:

Step 1:The codewords of Levels are identified.

Step2: If the codeword belongs to C0, the extracted bit is 0, else if the codeword belongs to C1, the extracted bit is 1.

Step3: The same pseudorandom key used for encrypting the sequence is used to decrypt the bits. The bit stream is generated using RC4 stream cipher.

Step4: Parse the bitstream to obtain the set of IPM_16x16 modes.

Step5: Compare the value obtained from the video and the set of IPM_16x16 modes calculated from the video.

Step6: If there is a change in order then the video is tampered. Else the video's integrity is said to be certain

I. Decryption of H.264 video stream

The video bitstream is parsed to identify the set of IPM codewords- Intra_4x4 codewords and motion vector difference codewords. The same bitstream sequence obtained by RC4 using keys is produced at the decoder side. The same XOR operation is performed with the LSB of the codewords. The video is decoded to obtain the YUV format video sequence.

III. CONCLUSION

The main aim of the proposed scheme is to increase the security of video transmission and to detect tamper detection without an increase in the size of the video transmitted. The scheme encrypts IPM and MVD which keeps perceptual security of the video. A large number of data can be embedded into P-frames without degrading the visual quality of the video. Moreover the scheme can ensure both the format compliance and the strict file size preservation.

The current work includes tampering detection using codeword substituted data hiding technique .Future work include finding the exact position where tampering had occurred and its correction.

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 homomorphic encrypted domain and its application in image watermarking," in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.

[4] Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao, "Tampering detection in compressed digital video using watermarking" IEEE Trans. Instrumentation and Measurement, vol. 63, no. 5, May 2014.

[5] I. E. G. Richardson, H.264 and MPEG-4 Video Compression: Video Coding for Next Generation Multimedia. Hoboken, NJ, USA: Wiley, 2003

[6] https://en.wikipedia.org/wiki/RC4

[7] https://staff.najah.edu/sites/default/files/Evaluation_of_the_RC4_Algorithm_for_Data_Encryption.pdf

[8] Dawen Xu, Rangding Wang, and Yun Q.Shi, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", in IEEE Trans., Inf. Security vol. 9, April 2014.

[9] http://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_229