IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 13-18
www.iosrjournals.org

Effective Data Hiding Scheme For Video in Encrypted Domain with Tampering Detection

R. Aparna[1], Ajish S[2]
[1]*(Guest Lecturer, Sree Narayana Polytechnic College , Kottiyam, Kerala, India)*
[2]*(Assistant Professor, College of Engineering Perumon, Kerala, India)*

Abstract: *Usually encrypted videos when tampered by a third party can be easily detected at the receiver side as the decoder may crash. But there can be instances where the tampering is done such that the compression parameters alone are changed. The paper proposes a novel scheme of tamper detection using the data hidden in encrypted video. The video is first encrypted to ensure perceptual security and then data is embedded into the encrypted video for tamper detection. Two sensitive parameters namely IPM and MVD are selected for encryption . The codewords of levels are used for data hiding. The data embedded is used for tamper detection. Both the encryption and data hiding is done such that the file size is preserved and format compliance is achieved after encryption and data hiding.*

Keywords: *Data Hiding, Encryption, Codeword Substitution, Tampering Detection, Video Security*

I. Introduction

Information security i.e., InfoSec is the art of securing the data or some confidential information from an unauthorised or an unwanted user. The properties of information security includes confidentiality, integrity and availability. Confidentiality is the property which ensures the information is hidden from a third party. Integrity is act of assuring the completeness and accuracy and that it is maintained over time. For the InfoSec to perform its intended functions, it should be available at the time of need.

Video security finds its major applications in the area of cloud computing, military purposes , medical purposes, video surveillance and as such. Cloud computing is an important technology which provides large-scale storage for video data. 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]. The easiest way to provide security is to process or store the video in an encrypted format. Inorder to provide integrity(video notation , or authentication data) , data hiding techniques can be implemented. Suppose that the data hiding process is done by a data hider from which the video content should be hidden. In such cases , data hiding in encrypted domain seems a necessary. Data hiding in encrypted video helps to avoid the leakage of video content which addresses the privacy. With the hidden information, the server can verify the integrity without an idea of the original content. Another major application is in the area of medicine. Medical videos or surveillance videos need to be encrypted for protecting the privacy of the video. As in the case of cloud computing, there can be instances where data has to be embedded into the video say, to provide data management capabilities, personal information can be embedded into the video. In military applications, highly confidential videos need to be transmitted with hidden data. Data hiding is necessary for military applications to provide authentication. To provide video security, encryption schemes are used which helps to bring out perceptual security. Though perceptual security hides the video data from a third party, it won’t assure that the video remains untouched i.e., it won’t rescue the video from tampering efforts. Tampering detection techniques can be implemented using data hiding schemes.

This paper deals with the video security. The security for multimedia should satisfy the above mentioned characteristics. The paper proposes a novel scheme for highly secure video transmission and/or storage. The characteristics of information security is satisfied by:

Confidentiality: The method brings out confidentiality by means of encryption scheme. The method focuses on increasing the perceptual security of the video.

Integrity: The integrity is assured by having a tampering detection technique using a data hiding scheme.

Availability: The method can be easily implemented and it strictly preserve file size and format compliance is achieved.

With the above mentioned applications, it is very important to have a data hiding scheme in an encrypted domain. In order to have a data hiding scheme directly in compressed and then encrypted video, some significant challenges has to be faced. To bring about encryption, it is very difficult and time consuming to encrypt whole video. So selective encryption is used . Selective encryption is the way by which encryption is brought out by encrypting only sensitive parts. So the first challenge is to find the sensitive portion of the bitstream video which when encrypted will result in high perceptual security and such that the encrypted video with hidden data is still a compliant compressed bit stream. The second challenge is to insure that decrypted video with hidden data should be of high visual quality, i.e., the data hiding technique should not affect the visual quality of the video. The third challenge is to preserve the file size even after encryption and data embedding process.

The remainder of the paper is organised as follows. In Section 2, a presentation of the related work is given, while section 3 describes the requirements of a data hiding scheme used for tampering detection from a security perspective, as well as the proposed scheme. Section 4 presents the experimental results and Section 5 evaluates the scheme, before concluding the paper in Section 6.

II. Related Work

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. There were researches which resulted in embedding into encrypted images. 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]. Here too the Paillier cryptosystem is used to bring out encryption. The main drawback of these two proposals was that they use Paillier cryptosystem which results in high storage overhead and computation. This does not meet the challenges described before. There were papers which satisfied the problem of size and succeeded in performing data hiding task in an encrypted background, but all those methods had their encryption scheme on uncompressed domain which again increased the computational cost[4]-[7]. All these methods worked on images . They failed to act on videos efficiently. As tomorrow's most common compression format is H.264, many works were focused on utilizing the compression parameters of H.264. A successful tampering detection technique was explained in [8]. Here, the watermarking scheme was introduced in the compressed but non-encrypted domain. In [9], data hiding technique is described were the motion vectors were chosen based on their associated macroblock prediction error was proposed. Another successful work was presented in [10] where the data was embedded using the phase angle of the motion vector. A different approach was presented in [11] where the method took advantage of different block sizes used by H.264 encoder during interprediction stage.

There have been works which dealt with joint data-hiding and encryption scheme . as in [10], the compression parameters namely IPM,MVD and DCT coefficient signs are encrypted, while the DCT coefficients amplitudes are watermarked at the same time. In [12] another combined scheme of watermarking and encryption scheme is presented but the method resulted in crashing of a standard decoder as the decoded watermarked bitstream was not fully format-compliant. The main problem with combined watermarking and encryption scheme was the increased computational cost as the compression/ decompression cycle is time consuming and the encryption schemes led to increasing bitrate of H.264/AVC bitstream.

III. Proposed Scheme

3.1 RC4 Encryption

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is XORed with the generated key sequence[13]. RC4 generates a pseudorandom sequence of bits (a keystream). The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key- scheduling algorithm(KSA). Once this has been completed, the stream of bits is generated using the pseudorandom generation algorithm(PRGA)[14].

3.2 Encryption of H.264 Video Stream

The encryption makes use of compression parameters. Inorder to perform selective encryption(SE), sensitive parts has to be identified. The research work for the identification of sensitive parts resulted in finding parameters from both temporal and as well as spatial data. The main aim of encryption was to bring out perceptual security to the video. So two sensitive parts namely IPM-Intra Prediction Mode(spatial information) and MVD, Motion Vector Difference are used. Another challenge faced by encryption schemes for video is of file size preservation. Inorder to maintain strict file size preservation, the codewords formed during encoding are used for encryption. For encryption and data hiding , the encoder is set to work in UVLC mode for encoding rather than CABAC encoding. The detailed encryption procedure is given below:

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. Among the four, only Intra_4x4 and Intra_16x16 modes are used here for encryption.

The encryption is done in CAVLC encoding of the IPM modes[15].For IPM for Intra_4x4 ,predictive coding mode[16] is used. The encoder sends a flag '1' to denote most probable mode or '0' to denote a change of mode[16] . If flag is equal to 1, the codeword consist of only 1 bit namely '1'. But if a change of mode is needed, the codeword if formed by '0' followed by 3 bits. Least significant bit of the codeword is encrypted by using stream cipher RC4 with the key set to Key1.

MVD Encryption

MVD is the offset between the current bock and the position of the candidate region for motion compensation[16]. The MVD is encoded by Exp-Golomb entropy coding. The LSB of the MVD codeword is encrypted by having an XOR operation by a stream of bits generated using RC4 stream cipher with key Key2[16]. Encrypting the LSB of the motion vector does not increase the size of the bitstream and produces format compliant bitstream.

3.3 Tampering Detection

For tampering detection, we make use of a data hiding technique where codewords of levels are substituted depending upon the data bit to be embedded. The main aim of the project is to bring out security to video without an increase in file size and with format compliance. The tampering detection scheme is designed in such a way that both of the challenges are satisfied. For tampering detection, a bitstream is generated by a key Key3. The generated bitstream is embedded into the video using codeword substitution technique. The very same bitstream is generated at the receiver side is he has an access to the key Key3. The data embedded is extracted from the video and is compared with the bitstream generated. If it matches, the integrity if the video is assured. The tampering detection procedure in detail is given below:

Bitstream Generation

The bitstream is generated by the same bitstream generator used for encryption, RC4. Rather than using the bitstream for XOR-ing, the bitstream here is used for data embedding for tampering detection. The bitstream is generated by key Key3.

Data Embedding

The data embedding is based on a codeword substitution technique where the Levels in P-frame are used[17].

Levels : CAVLC entropy coding method is used to encode residual, zig-zag ordered 4x4 blocks of transform coefficient. The format of CAVLC codeword is given below:

{Coeff_Token, Trailing_ones_sign_flag, Levels, Total_zeros, Run_before}

The levels are coded by its prefix and suffix. The level(sign and magnitude) of each non-zero coefficient is coded in reverse order starting with the highest frequency. The length of the suffix(suffixlength) is determined context adaptively[16].

Data Hiding : Data Embedding is done by level codeword substitution. The codewords of levels with same length are used for substitution. Observations have found out that level codewords where suffixlength greater than or equal to 2 will have replicable codewords (level codewords which can be replaced with codewords of same length). The substitution procedure is governed by the data to be embedded. The codewords with suffixlength 2 or 3 are used in the scheme. The levels of P-frame are used as I frame will result in error in the subsequent frames also. The algorithm is as follows:

```
if(P-frame)
    if(suffixlength equal to 2 or 3)
        if(data to be embedded is 1)
            if(level is odd)
                if(level <0)
                    level=level-1
                else
                    level=level+1
            else
                if(level is even)
                    if(level<0)
                        level=level+1
                    else
                        level=level-1
        end if
    end if
```

Data Extraction

The same bitstream which is generated at the sender side is generated at the receiver side using the data hiding key Key3. The generated bitstream and the bitstream extracted are compared. If there is a change in the order of 0s and 1s, tampering is said to be detected, else the video's integrity is assured.

The data extraction is given in the algorithm:

```
if(P-frame)
    if(suffixlength equal to 2 or 3)
            if(level is even)
                    Data extracted is 1
                    if(Change in bit)
                            Tampering Detected!
            If(level is odd)
                    Data extracted is 0
                    If(Change in bit)
                            Tampering Detected!
    end if
end if
```

3.4 Video Decryption

The codewords of IPM (Intra_4x4 mode) and MVD are identified. The codewords are XOR-ed with the same bitstream generated at the sender side using key Key1 and Key2 to generate the decrypted video.

IV. Experimental Results

The project is implemented in the H.264/AVC reference software version JM-12.2 . Standard video sequences namely, forman, akiyo, carphone, clarie and costguard in QCIF format (176x144) at frame rate 30 frames/s are used for simulation. The first 5 frames in each video sequences are used in the experiments.

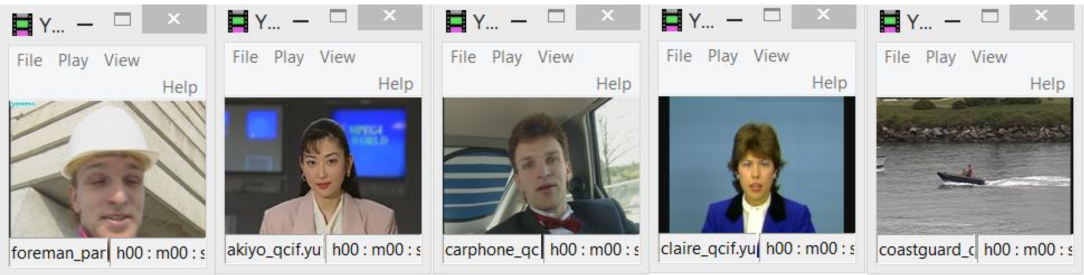

Figure 1 . Original video sequences

The result of encryption of the video sequences is given below in Fig. 2

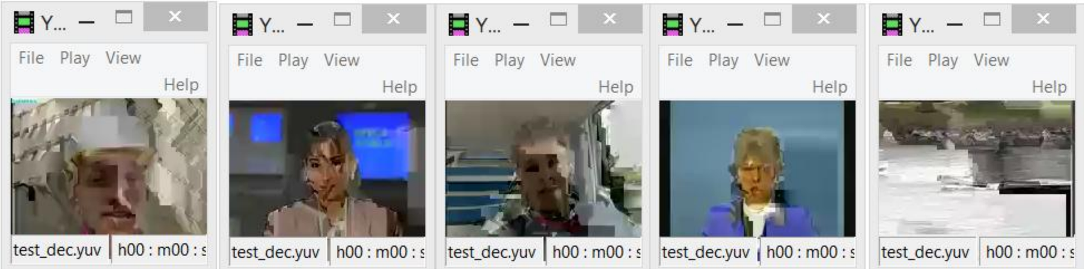

Figure 2. Encrypted video sequences

The result of data embedding on encrypted video is given below

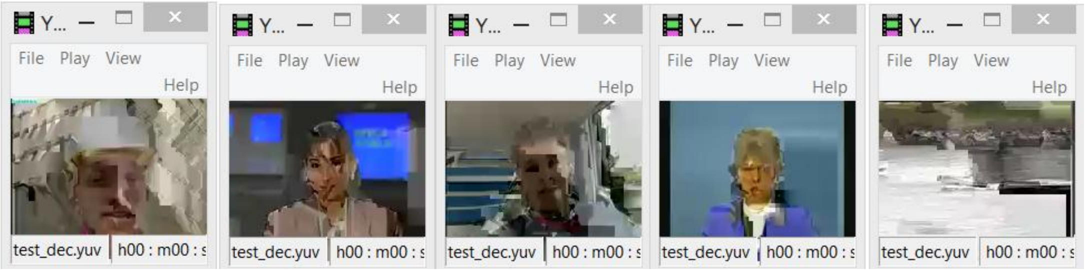

Figure 3. Stego video

Decrypted videos with hidden data is shown in the Fig. 4.

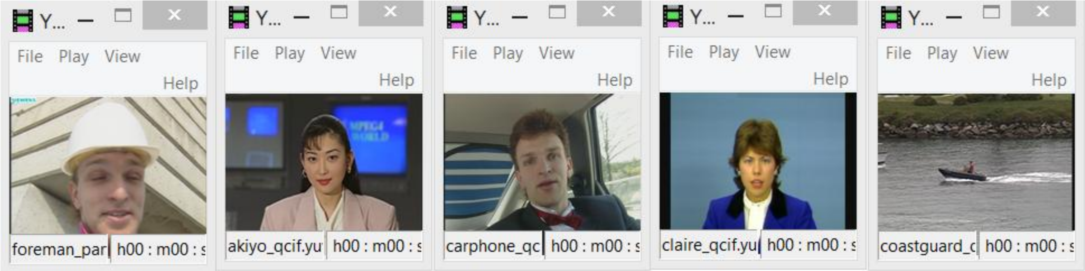

Figure 4. Decrypted videos with hidden data

V. Performance Analysis

5.1 Visual Quality of the Video with Hidden Data

Only the codewords of Levels within P-frames are modified for data hiding. Simulation results have demonstrated that we can embed the additional data with a large capacity into P-frames while preserving high visual quality. PSNR (Peak Signal to Noise Ratio) have been adopted to evaluate the perceptual quality of the video. The observations are tabulated below. The observations are tabulated based on the foreman standard video sequence.

Table 1. QP and PSNR values corresponding to Luminance(Y)

QP	PSNR(dB)	
	Non-Stego	Stego
24	13.13	13.15
28	11.10	11.10
32	10.08	10.08
36	11.74	11.741

Table 2. QP and PSNR values corresponding to Blue Chrominance(Cb)

QP	PSNR(dB)	
	Non-Stego	Stego
24	27.48	27.482
28	28.63	28.63
32	28.37	28.37
36	27.82	27.84

Table 3. QP and PSNR values corresponding to Red Chrominance(Cr)

QP	PSNR(dB)	
	Non-Stego	Stego
24	25.31	25.312
28	25.32	25.32
32	24.44	24.44
36	25.96	25.96

5.2 Decoding Time

The decoding time before and after encryption and data hiding were observed . A graph is plotted by taking decoding time against different QP values. It was observed that the decoding time almost remains the same. The graph is given in the Fig. 5.

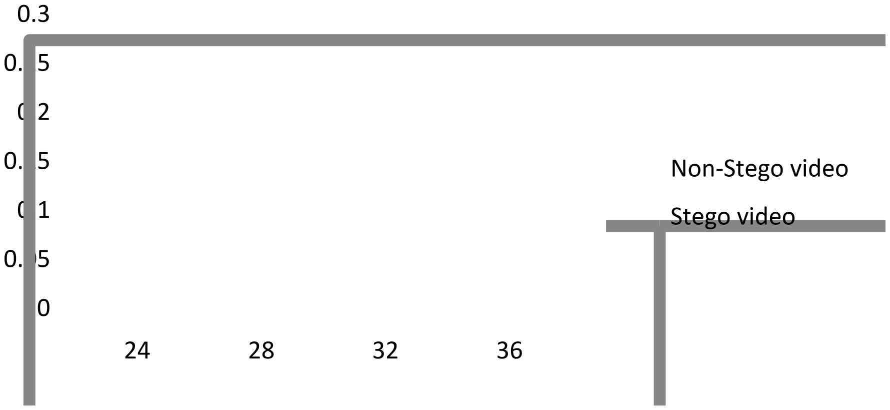

Figure 5: Graph plotted with QP values against decoding time

VI. 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, MVD and residual coefficients , 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. The future work can 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]. X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[5]. 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.

[6]. X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[7]. 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

[8]. 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.

[9]. Hussein A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error", IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, March 2011.

[10]. Ding-Yu Fang, Long-Wen Chang, "Data hiding for digital video with phase of motion vector", IEEE. Proc. ISCAS, 2006

[11]. Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras, "Data hiding in H.264 encoded video sequences",IEEE Proc. MMSP 2007

[12]. 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.

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

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

[15]. 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.

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

[17]. 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.