Using Codeword Substitution to Hide Data in Encrypted MPEG-4 Videos

Juhi Rohara[1], V.B. Gaikwad[2]

[1]*Student, Dept of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India*
[2]*Professor, Dept of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India*

---***---

Abstract - *The paper proposes data hiding with codeword substitution in encrypted MPEG-4 videos. In this, scheme of data hiding in encrypted version of videos is presented which includes four parts video encryption, data embedding, data extraction and video compression. The sender encrypts the original video using standard stream ciphers with encryption keys to produce encrypted video. After that additional data can be added in encrypted video using codeword substitution. Now video is compressed using arithmetic compression. At the receiver end, after video decompression hidden data can be extracted either in encrypted or decrypted version of video.*

***Key Words*: Data hiding, encrypted domain, MPEG-4 video, codeword substituting.**

1. INTRODUCTION

MPEG-4 [1] video coding standard has been developed and standardized collaboratively by both the ITUT VCEG and ISO/IEC MPEG organization. H.264/AVC or MPEG-4 is a video compression format [2] i.e. standard for high definition digital video. MPEG-4 video streams generally avoids leakage of video content which can help to address the security and privacy concerns with cloud computing. Similarly when medical videos or surveillance videos are encrypted for protecting the privacy of the people, a database manager can embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. With the increasing demands of providing video data security and privacy protection data hiding in encrypted these videos are becoming popular.

1.1 Objective

The main objective is to enhance compression performance and provides a provision of a network friendly video. These videos has achieved a significant improvements in rate distortion efficiency relative to existing standards MPEG-4 covers all common video conferencing and high definition (HD) video storage. To address the need for flexibility and customizability, the design covers a video coding layer (VCL), which is designed to efficiently represent the video content, and a network subtraction layer (NAL) which formats the VCL representation in a manner appropriate for conveyance by a variety of transport layer or storage media. Relative to prior video coding methods, as exemplified by MPEG-2 video, some highlighted features of the design that enable enhanced coding efficiency include the following enhancement of the ability to predict the values of the content of a pictures to be encoded.

1. Variable block size motion compensation with small block sizes.
2. Quarter sample accurate motion compensation.
3. Motion vectors over picture boundaries.
4. Multiple reference picture motion compensation.
5. Decoupling of reference order from display order.
6. Decoupling of picture representation methods from picture referencing capability.
7. Weighted prediction
8. Improved skipped and direct motion inference.
9. Directional spatial prediction for intra coding.
10. In the loop de-blocking filtering.

2. RELATED WORK

There are several methods used to encrypt video and data embedding in video stream. Several research works are being performed by many institutions throughout the world to offer the best scheme in terms of cost effectiveness. This section gives a brief review on various methods of video encryption and embedding.

2.1 Encryption & Modified Watermarking Scheme

In the year 2007, the authors S. G. Lian, Z. X. Liu, and Z. Ren [3] proposed the commutative encryption watermarking schemes for video streams compression. The paper proposed the combine approach of encryption and watermarking to provide confidentiality & ownership. Proposed Encryption Scheme performs the encryption of both motion and texture information, by considering MVD encryption (Motion Vector direction) and IPM encryption (Intra Prediction mode). During MPEG-4 compression the intra-prediction mode, motion vector difference & discrete cosine transform coefficients are encrypted. After encryption watermarking takes place on DCT coefficients. As the traditional watermarking operation affects the decryption operation, means the watermark cannot be extracted without decryption of the content. Hence paper proposed modified watermarking algorithm which makes the modification of traditional watermarking algorithm. The watermark can be extracted from the encrypted domain, thus it preserves the confidentiality of the content. The drawback of this paper is that the original content is first watermarked & then watermarked content is encrypted. It means watermark cannot be embedded on encrypted content. The other drawback is the approaches do not operate on the compressed bit stream.

2.2 Encryption & Reversible Watermarking Scheme

To overcome the drawback of previous scheme mentioned in last paragraph the authors S. W. Park and S. U. Shin [4] in the year 2008 proposed reversible watermarking scheme and encryption scheme which was used to provide the access right and the authentication of the video content simultaneously. The scheme proposes the schemes to perform the encryption of original content and then perform reversible watermarking simultaneously during compression process. This scheme also proposed the efficient selective encryption scheme which encrypts the IPM of 4x4 blocks, the sign bits of texture & the sign bits of motion vector difference values. The Reversible watermarking scheme embeds the watermark into the encrypted domain. The drawback of this scheme is, the proposed watermarking scheme has little bit overhead. The watermarked bit stream is not fully format compliant as a result a standard decoder may crash since it cannot parse watermarked stream.

2.3 Selective Encryption Algorithm

The authors S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang proposed selective encryption scheme [5]. Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bit stream, because of the following two reasons, i.e., format compliance and computational cost. Hence, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is, how to select the sensitive data to encrypt. Till now, various encryption algorithms have been proposed and widely used, such as DES, RSA, IDEA or AES, most of which are used for text or binary data. These algorithms are difficult to use directly for video encryption. Thus the Selective encryption scheme works on partial encryption algorithm. During AVC encoding sensitive data as intra-prediction mode, residual data & motion vector difference are partially encrypted. It provides approach for selecting sensitive data to encrypt to make it time efficient, secure & format compliance. The drawback of this paper is that the selective encryption is performed during H.264/AVC encoding & not on compressed domain.

2.4 Enhanced Selective Encryption Scheme

The author Z. Shahid, M. Chaumont, and W. Puech [6] in the year 2011 proposed Selective Encryption scheme which operates in compressed domain based on context adaptive variable length coding & context adaptive binary arithmetic coding. It overcomes the drawback of previous scheme. The selective encryption is performed on the entropy coding stage of H.264/AVC using AES encryption algorithm in CFB mode, Hence it does not affect the bit rates & H.264/AVC bit stream compliance. The proposed method has the advantage of being suitable for streaming over heterogeneous network because of no change in bit rates.

2.5 Encryption scheme and Codeword Substitution Technique

The previous methods perform encryption and data embedding almost simultaneously during MPEG-4 compression process and not on compressed domain, Hence the compression and decompression cycle is time-consuming and hampers real-time implementation. Besides this, the encryption and watermark embedding would lead to increase in the bit- rate of MPEG-4 bit stream. However, to meet the application requirements, it's necessary to perform data hiding directly on compressed bit stream in the encrypted domain. To overcome the drawbacks of previous scheme, The author D. Xu, R. Wang,& Yun Q Shi [7] in the year 2014 proposed Codeword substitution technique, a data hiding algorithm that work entirely in the encrypted domain, & thus preserves confidentiality of the content. The proposed methodology for video encryption is to use standard stream cipher (RC4) with encryption keys. And after video encryption, codeword substitution technique generates pseudo-random sequence as data hiding key & embed the data into the encrypted video stream without knowing the original content. By making the comparative analysis with the previous papers, this paper [7] achieved a better performance in following aspect:

1. Data hiding performed entirely in the encrypted domain
2. Preserves confidentiality of the content.
3. The schemes operate directly on the compressed bit stream.
4. The schemes can ensure both the format compliance & strict file size preservation.
5. In order to adapt to different application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

Here data hiding is in the encrypted version of H.264/AVC videos, which includes three parts i.e. H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers and encryption keys to produce an encrypted video stream. Then, the data hider can embed additional data into encrypted video stream by using the code word substitution method, without knowing original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

3. PROPOSED SYSTEM

The proposed system will encrypt the video after which data will be embedded in the video and video compression will be performed. At the receiver end after video decompression data can be extracted either in encrypted or decrypted version of the video.

3.1 Encryption of Video

It is not practical to encrypt the whole compressed video bit-stream like what the traditional ciphers do because of following two constraints i.e. format compliance and computational cost. Hence, only a fraction of video is encrypted to improve the efficiency of while achieving the adequate security. The key issue is then how to select the sensitive data to encrypt. Here we encode the both spatial information and motion information.

1) Intra-prediction mode (IPM) encryption

2) Motion vector difference (MVD) encryption

3) Residual data encryption

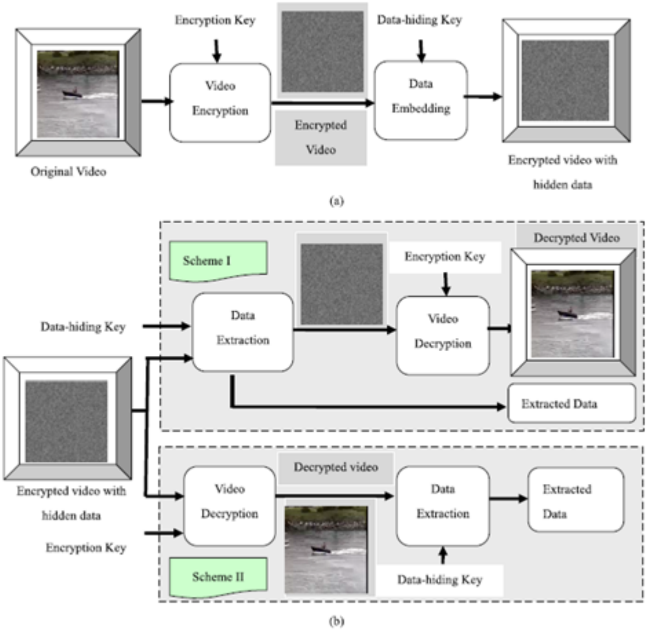

Fig – 1: a) Encryption and data embedding b) Data extraction and video decryption [7]

3.2 Data Embedding

The additional data can be embedded in the encrypted video using codeword substitution technique.

3.3 Arithmetic Coding

The proposed method will compress the video after data embedding process using arithmetic compression. This algorithm is used in both lossless and lossy data compression algorithm. It is an entropy encoding, in which the frequently seen symbols are encoded with fewer bits than lesser seen symbols It is different from the Huffman coding that rather than separating the input into the component symbols and replacing each with a code arithmetic coding encodes the entire message into a single number, a fraction n where ($0 \leq n \leq 1$). Video is compressed to reduce the band width.
Advantages of arithmetic coding -

- Compression ratio is higher.
- Efficiency is greater.
- Redundancy is reduced.

3.4 Data Extraction

At receiver end, video is decompressed first after that the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple.
Fig1 (a) and 1(b) represents the existing method. In fig1(a), the sender is having original video, which user encrypts with the encryption key. After that data is embedded by using codeword substitution technique. Result of which is encrypted video with hidden data. All these process is done at the sender end.

In fig-1(b), process at receiver end is shown, which shows two schemes.

In fig-1(b) Scheme-1, hidden data is extracted first and by using key video is decrypted and result of which is the original video.

In fig-1(b) Scheme-2, video is decrypted first using key and after that hidden data is extracted and after that receiver will get the original video.

In fig-2, video is compressed after embedding the data at the sender side and at the receiver end video is decompressed first after which Scheme-1 or Scheme-2 can be performed illustrated in fig-1.

The main advantage of proposed method is that it will decrease the bandwidth so that it will be easy to transfer the video.

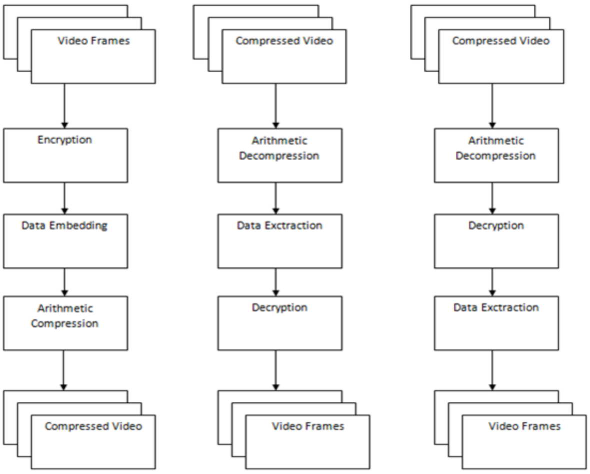

Fig – 2: Proposed method with video compression

4. PERFORMANCE EVALUATION

Following parameters are used to evaluate the performance

4.1 Peak signal to noise ratio (PSNR) -

The mean square error (MSE) and Peak signal to noise ratio [8] are the two error matrices used to compare the image compression quality. The MSE represents the cumulative squared error between the compressed and original image, where as the PSNR represents a measure of peak error.

4.2 Structural Similarity (SSIM) -

The structural similarity (SSIM) [9] index is a method for measuring the similarity between two images. The difference with other techniques such as MSE or PSNR is that these approaches perceived errors, on the other hand SSIM considers image degradation as perceived change in the structural information. For the better result SSIM should be 1.

4.3 Video quality measurement (VQM) -

The objective of VQM [10] is to provide measurement for the perceived video quality. It measures the perceptual effect of the video impairments including blurry, unnatural motion, global noise, block distortion and colour distortion and combine them into single metric.

Fig-3 shows comparison of different videos before and after compression. There is not much degradation in PSNR, SSIM and VQM parameters after compressing the videos. Compression ratio of this system is 0.20.

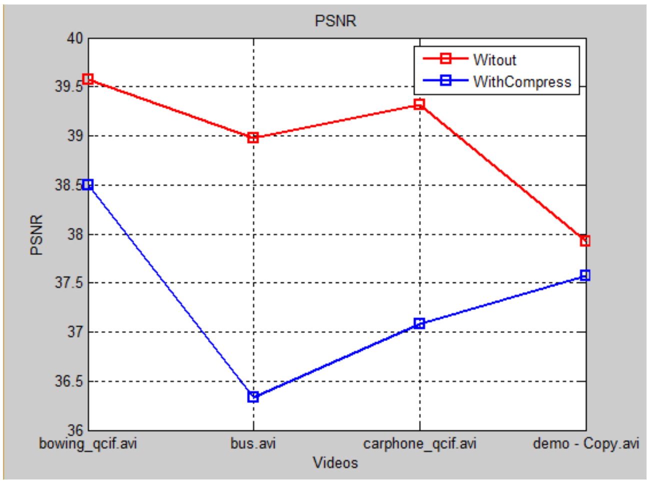

Fig - 3(a): comparison of PSNR between existing and proposed system

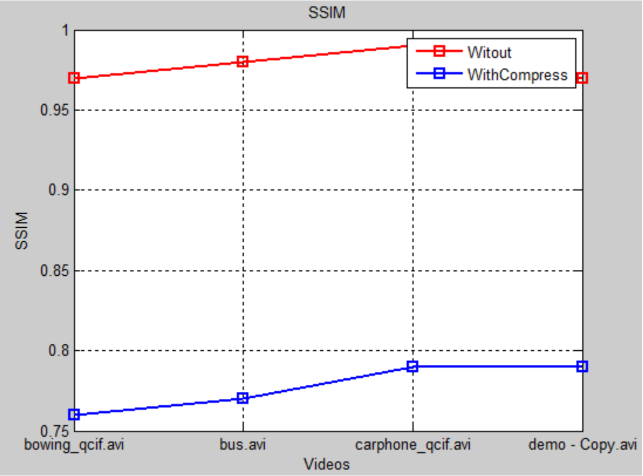

Fig - 3(b) comparison of SSIM between existing and proposed system

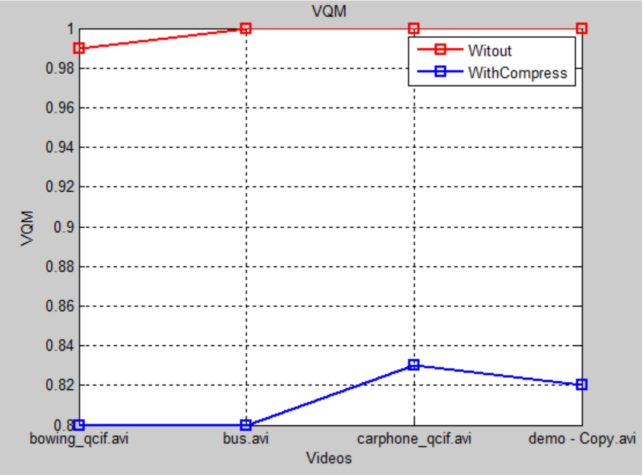

Fig - 3(c): comparison of VQM between existing and proposed system.

5. CONCLUSION

The proposed system shows that after video compression there is not much effect on the performance evaluation parameters. Hence video quality is not degraded. As compression decreases the band width, so it will be easy to transfer the video from one place to another. One more advantage of this system is that at the receiver end data can be extracted either in the encrypted or in the decrypted version of the video.

ACKNOWLEDGEMENT

I would like to acknowledge Prof. V.B. Gaikwad, for guiding me throughout the project development

REFERENCES

[1] Koenen R., “Overview of the MPEG-4 standard,” ISO/IEC JTC1/SC29/WG11 M4030, 2001.

[2] T. Stutz and A. Uhl, “A survey of H.264 AVC/SVC encryption,” IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 3, pp. 325–339, Mar. 2012.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] D. Xu, R. Wang,& Yun Q Shi,” Data hiding in encrypted H.264/AVC video streams by codeword substitution”, IEEE Trans. Inf. Forensics Security,vol.9,No.4, pp.596-606,Apr.2014.

[8] Poynton, C.A.: A Technical Introduction to Digital Video. John Wiley & Sons Ltd., Chichester (1996).

[9] Wang, Z., Bovik, A.C.: A Universal Image Quality Index. IEEE Signal Processing Letters (March 2002).

[10] Xiao, F.: DCT Based Video Quality Evaluation. Final Project for EE392J (2000)