Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

An Efficient Codeword Substitution Method For Data Embedding Technique in Encrypted H.264/AVC Video Streams

Anisha Jose[1], Anu K Kuriakose[2]

Post-Graduate Scholar, Department of Electronics and Communication, FISAT, Ernakulam, India [1]
Assistant Professor, Department of Electronics and Communication, FISAT, Ernakulam, India [2]

***Abstract*— As technology advances, the use of multimedia applications are increases in day-to-day life. These applications require large bandwidth, high storage, and high latency time to send on network. To conserve these resources, it is required to compress the video data before sending them to the network. Also multimedia contents from different servers may attract more attacks. So the security of multimedia components are important. In this paper, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed. Encryption will provide the security and data hiding will provide the authentication of videos from different servers. By using the property of H.264/AVC codec, the codewords of intraprediction modes, the codewords of motion vector differences, and the codewords of residual coefficients are encrypted with stream ciphers like RC4. Then, a data hider may embed data in the encrypted domain by using codeword substitution technique, without knowing the original video content.**

***Index Terms*— H.264 codec, Context adaptive variable length coding (CAVLC), RC4, Codeword Substitution.**

I. Introduction

In recent years, the security over the Internet is becomes more important because of wide spread of the multimedia and network in different applications. Demand of video applications such as video telephony, video conferencing, online stream video, mobile streaming, TV, 24 hours surveillance system and many others are increasing exponentially because of the evolution of video compression technology. Bandwidth and storage space are the crucial parameters in video communication. Their requirements are also increased exponentially with increasing demand of video applications. So the video compression play an important role in multimedia systems. In order to reduce storage requirement, video compression is very much needed. H.264/AVC is the latest video coding standard jointly developed by Joint video team in 2003,which is organized by two international standards bodies ie the International Telecommunication Union-Telecommunications sector video coding experts group and International Organization for Standardization/ International Electro-technical Commission moving picture experts group. H.264 offers a significant performance improvement over previous video coding standards in terms of better peak signal to noise ratio and visual quality of variable block sizes for motion compensation, multiple reference frames, Integer Transform and Context Adaptive Variable Length Coding (CAVLC).

But the different multimedia applications may attract more attacks and are vulnerable to untrustworthy system administrators. So the security and privacy of multimedia content are becoming more prominent. For example, commercial multimedia content stolen or tampered will cause huge economic losses to the supplier, medical information in telemedicine leaked will threat the personal privacy of the patients. Particularly, the leaking of multimedia content intended for military or national defense always imposes negative impact on the important departments. Security can be provided by encrypting the data with particular stream cipher. Authentication to the encrypted file is given by the process of data hiding. Information can be embedded into digital media by making tiny changes which cause little notice to the human perception. Such data hiding techniques have many applications such as tamper proofing, watermarking, copyright protection, hidden annotations, authentication, secure and invisible communication, etc. The secret message might be a serial number, a copyright logo, a caption data, a covert message, a plain text, another image, or anything that can be represented in bit stream form.

The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help to address the security and privacy concerns for different applications. A cloud server can embed the additional information like authentication data into an encrypted version of an H.264/AVC video by using data hiding technique. With the hidden information, the server can manage the video or verify its integrity without knowing the original content, and thus the security and privacy can be protected. One of the most widely accepted data hiding technique in H.264 video is codeword substitution. Here codewords of video are replaced by another set of codewords without knowing the original video content. For example, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain.

This paper has the following structure: section II explains about the related works, the proposed method is given in section III. Section IV shows the results and analysis of the proposed method, and section V concluded the paper.

II. RELATED WORKS

As the use of multimedia is widely increased, it is very important to provide security to these multimedia contents. So that in recent years, many image and video encryption algorithms have been proposed to provide security and some data hiding methods are used to provide authentication in the presence of attackers. The paper [3] explains a MPEG video encryption mechanism that supports multiple levels of security. The MPEG uses DCT compression with 64 DCT coefficients. Then divided the coefficients into 3 partitions called the base layer, middle layer and enhancement layer. A breakpoint is an integer from 0 to 63 and determines the boundary between partitions. In their approach the base layer and middle layer are encrypted while the enhancement layer is not encrypted. By encrypting only the base and middle layers, the cost of encryption is deceased. So it can provide security by encrypting only a fraction of the data depending on the level of security the user requires. This scheme provides multiple levels of security by letting the user determine the breakpoint group. Here the compression method used is MPEG and does not provide encryption to enhancement layer.

A image watermarking algorithm in the encrypted domain using Paillier cryptosystem is explained in the paper [4]. The Paillier cryptosystem have both the probabilistic property and the homomorphic property. It use an additive homomorphic property. That is, for any two ciphertexts, one can generate a ciphertext of the sum of the plaintext as long as the public key is known. That is, each addition in the plaintext domain will be mapped to a modular multiplication in the encrypted domain, and each multiplication in the plaintext domain will be mapped to a modular exponentiation in the encrypted domain. As for the subtraction in the plaintext domain, the Paillier cryptosystem will map it to one modular multiplicative inversion and one modular multiplication. The modular multiplicative inversion can be computed by using the Euclidean algorithm. The implementation of the modular inversion is more complex than the modular multiplication. The complexity can be evaluated as the number of modular exponentiations, modular multiplications, and modular inversions. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image results in a high overhead in storage and computation. Because here the host image is in an uncompressed format .

Another paper [5] describes a method to provide a encryption to the intra prediction mode, the intra macroblock's residue data and the inter macroblock's MVDs partially and selectively during AVC encoding, and keeps the format information and other data unencrypted. It obtains high time efficiency through reducing the encrypted data volumes. Both the texture information and motion information are encrypted, which makes the scheme not only secure in perception but also secure against bruteforce and known plaintext attacks. Additionally, the segment-encryption mode makes the scheme of higher robustness to transmission errors. These properties make the scheme suitable for real-time applications .

As these encryption algorithms are all accomplished before the last step of the video compression process, all the encrypted bitstreams could maintain the format-compliance and can be decoded by a standard decoder without decryption, while only obtain the unintelligible video content. However, encrypting or scrambling the DCT coefficients during compression process usually destroys the inherent energy impact capability of the DCT transform, resulted in low compression efficiency. Here full encryption of video is required, which will increase the computational complexity. Furthermore, these algorithms require a modified structure of the standard encoder, leaving all existing encoders unusable.

III. PROPOSED METHODS

The data embedding methods discussed so far has high computational complexity. To reduce the computational complexity, selective video encryption scheme on a compressed domain has been adopted. The proposed system consists of a H.264 encoder to compress the video, encryption block to encrypte the data with stream cipher like RC4 and data embedding block to hide a binary data to the encrypted video by codeword substitution method at the transmitter. At the receiver, a set of reverse operations are performed. Here data is extracted from the received video. After extracting the binary data, video decrypted using the same symmetric cipher used at the transmitter. Then video is decompressed to get the original video content. Fig.1 shows the proposed system.

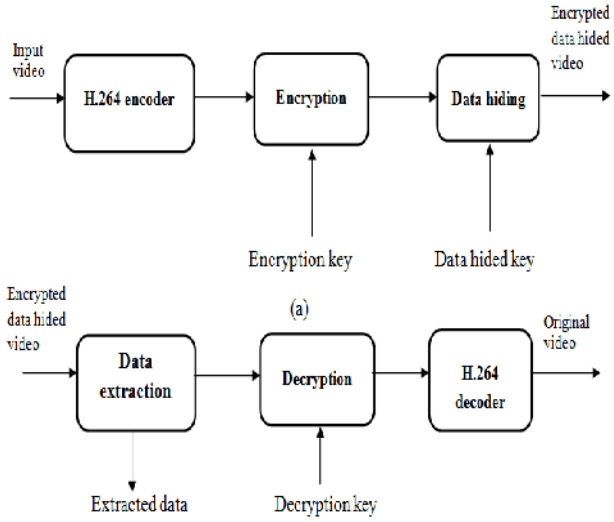

Fig. 1 (a) Block diagram of transmitter, (b) Block diagram of receiver

A . H.264 Encoder

Encoder is used to compress a digital media file. The compression is done by reducing and removing redundant video data so that a digital video file can be effectively sent and stored. An input frame is processed in units of a macroblock. Each macroblock is encoded in intra or inter mode and a prediction macroblock (P) is formed. In Intra mode, P is formed from samples in the current slice that have previously encoded, decoded and reconstructed. In Inter mode, P is formed by motion compensated prediction from reference pictures. The prediction P is subtracted from the current block to produce a residual block that is transformed and quantised to give a set of quantised transform coefficients which are reordered and entropy encoded[7]. Context adaptive variable length coding(CAVLC) and exp golomb coding are used[8]. The entropy encoded coefficients, together with side information required to decode each block within the macroblock form the compressed bitstream which is passed to the receiver. Fig 2 shows the block diagram of H.264 encoder. As well as encoding and transmitting each block in a macroblock, the encoder reconstructs it to provide a reference for further predictions. The coefficients are scaled and inverse transformed to produce a difference block. Then the prediction block is added to this to create a reconstructed block.

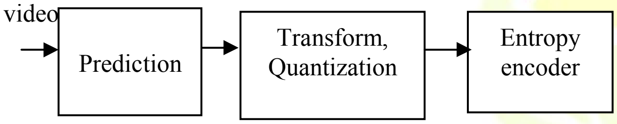

Fig. 2 H.264 encoder

B. Encryption of video

Instead of encrypting all video content, selective encryption is performed. Here three sensitive information like intra prediction mode, motion vector difference and residual coefficients are encrypted. So in this method, both spatial and motion information is encrypted.

1) Intra Prediction Mode Encryption:

It is used to remove the spatial redundancy from individual frame. Nine intra prediction modes (IPMs) are available in the Intra_4 × 4. These modes are used to generate a prediction macroblock for the current macroblock. Based on the mode number different prediction macroblock can be created. So it is very required to give protection to the mode number. Therefore the mode number used in each prediction is encrypted here. A key from RC4 is used for the encryption. The last bit of pseudo random number generated from RC4 is xored with last bit of intra prediction mode number.

2) Motion Vector Difference Encryption:

In order to protect both texture information and motion information, not only the IPMs but also the motion vectors should be encrypted. In H.264/AVC baseline profile, exp golomb entropy coding is used to encode the motion vector difference(MVD). The last bit of the codeword is encrypted by applying the bitwise XOR operation with a standard stream cipher, which is determined from RC4. The last bit encryption may change the sign of MVD, but does not affect the length of the codeword.

3) Residual Coefficients Encryption:

The residual data in both I frames and P frames should be encrypted. In H.264/AVC baseline profile, CAVLC entropy coding is used to encode the quantized coefficients of a residual block. The format of CAVLC is :
{Coeff_token, Sign_of_T1, Level, Total_zeros, Run_before}

Here all syntax elements are not modified during encryption process. Therefore, residual data encryption can be accomplished by modifying the codewords of Level. The last bit of the codeword is encrypted by applying the bitwise XOR operation with a standard stream cipher like RC4. The last bit encryption may change the sign of Levels but does not affect the length of the codeword.

C. Data Embedding

Data hiding deals with the ability of embedding data into digital media with a minimum amount of visible degradation. The method used should satisfy three conditions.

- Bit stream after codeword substituting must remain in same syntax.
- To keep the bit rate unchanged, the substituted codeword should have the same size as the original codeword.
- The embedded data after video encryption has to be invisible to a human observer

The codewords of Levels within P frames are used for data hiding, while the codewords of Levels in I frames are remained unchanged. Because I frame is the first frame in a group of pictures (GOPs), the error occurred in I frame will be propagated to subsequent P frames. The codewords are divided into two code space C0 and C1[1]. Here the data embedded is a binary sequence of 0 and 1. Depend upon the binary information, different codewords from C0 and C1 are substituted. The algorithm used here is:

1. Obtain the codeword of levels used for the substitution by parsing the stream.
2. Check whether the current codeword belongs to C0 or C1.Otherwise, the codeword is left unchanged.
3. If data bit=0 and codeword in C0, then codeword is not modified. Otherwise if codeword in C1, the corresponding codeword in C0 is transmitted.
4. If data bit=1 and codeword in C1, then codeword is not modified. Otherwise if codeword in C0, the corresponding codeword in C1 is transmitted.
5. Choose the next codeword and then go to Step3 for data hiding. If there are no more data bits to be embedded, then the embedding process is stopped.

So if the data to be hided is zero, the codeword in C0 transmitted. Otherwise the codeword in C1 transmitted.

D. Data extraction

Encrypted video with hidden data is directly sent to the data extraction module, where the binary data is tried to extract. Here the data extraction module will check whether the hided data is 0 or 1 by using the property of code space. Here assume that receiver also has the same code space C0 and C1 as in transmitter. To extract the data, receiver will check whether the received codeword belongs to C0 or C1. If codeword in C0, the data bit is zero, else it is one.

E. Decryption

Decryption is the reverse process of encryption. It is the process of decoding the encrypted data so that only authorized user can access it. Here uses a symmetric key algorithm, ie, same key is used at the transmitter and receiver. Here only authorized user has the same key that is used at the transmitter for encryption and user will generate stream cipher using RC4. XOR is the operation used for decryption. Because two XOR operations will cancel out. For that, the codewords of IPMs, MVDs, Levels are identified by parsing the encrypted bitstream and then these encrypted codewords can be decrypted by performing XOR operation.

F. H.264 Decoder

The decoder receives the compressed bitstream and entropy decoder decodes the data elements to produce a set of quantized coefficients. Inverse of exp golomb coding and CAVLC are used here. These are scaled and inverse transformed. Using the header information decoded from the bitstream, the decoder creates a prediction block P, identical to the original prediction P formed in the encoder. P is added to residual macroblock which is then filtered to create original macroblock. The block diagram of H.264 decoder is shown in fig. 3.

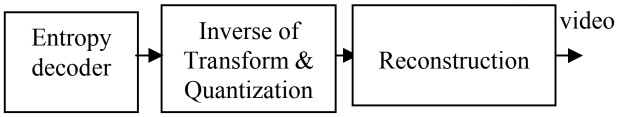

Fig. 3 H.264 decoder

IV. EXPERIMENTAL RESULTS

The proposed data hiding scheme has been simulated on Matlab 2012. Here, the input video used for simulation is “xylophone.mpg” present in matlab software and the last frame of video after each stage is shown in fig. 4. Fig. 4(a) represented the last frame of input video which is then converted into gray scale image. This is shown fig. 4(b). Fig. 4(c), 4(d) and 4(e) shows the effect of intra prediction mode, motion vector differences and residual data encryption respectively on the input video. The combined effect of these three encryptions on video is shown in fig. 4(f). This combined encryption method provide security to the both spatial and motion information. To provide authentication, a binary data is hided into the encrypted video without any visual degradation. This is represented in fig. 4(g). The last frame of video after data extraction is represented in fig. 4(h). The effect of encryption is removed by XORing with RC4. This is shown in fig. 4(i), 4(j) and 4(k) and finally obtains the original video.

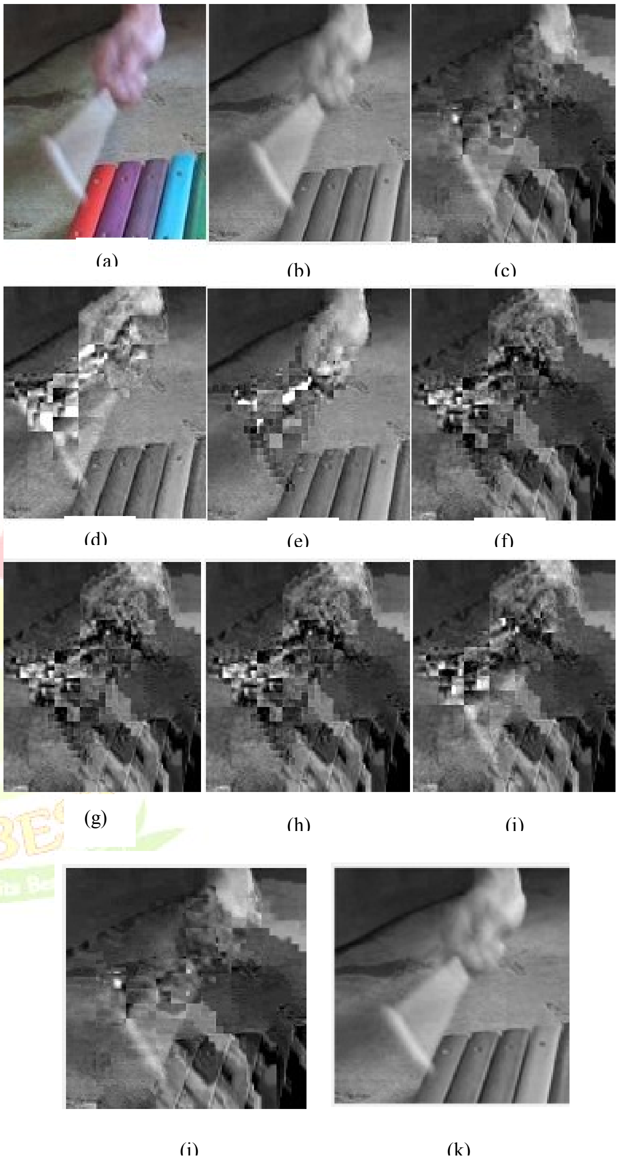

Fig. 4 (a) Input frame, (b) Gray scale frame, (c) IPM encrypted frame, (d) MVD encrypted frame, (e) Residual data encrypted frame, (f) Combined encrypted frame, (g) Data hided frame, (h) Data extracted frame, (i) Residual data decrypted frame, (j) MVD decrypted frame, (k) IPM decrypted frame

A. Security

This techniques gives both cryptographic security and perceptual security. Cryptographic security depends on the ciphers adopted by the scheme. In the proposed scheme, the secure stream cipher like RC4 is used to encrypt the bitstream. The proposed scheme encrypts IPM, MVD and residual coefficients, which keeps perceptual security of the encrypted video.

B. Visual Quality

The visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video. Here the codewords of Levels within P frames are modified such that the visual quality is maintained. The codespace are form such that encrypted codeword and original codeword in the same subspace.

C. Provides savings in bandwidth and storage costs

The video in compressed format is used for encryption and data hiding.

D. Encryption and decryption processes are fast

Here only selective encryption is performed which only encrypte the intra prediction mode, motion vector differences and residual coefficients.

V. CONCLUSION

Here an algorithm to hide a binary data in encrypted H.264/AVC bitstream is presented, which consists of video encryption, data embedding and data extraction phases. 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, this method can preserve the confidentiality of the content completely. Encryption will provide the security and data hiding will provide the authentication of videos from different servers. In this algorithm, the visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video. Here the codewords of Levels within P frames are modified such that the visual quality is maintained. So that the codespace are form such that encrypted codeword and original codeword in the same subspace. Since all the process are in compressed domain , the bandwidth required to transmit the data is very less. Instead of encrypting the whole video content, a selective encryption is used, which only encrypt the sensitive information like intra prediction mode, motion vector difference and residual coefficients. So the computational complexity is very less and encryption and decryption processes are fast compared to other data hiding techniques.

ACKNOWLEDGMENT

This work is supported and guided by my research guide. I am very thankful to my guide Ms Anu K Kuriakose, Assistant Professor, Electronics and Communication Department, Federal Institute of Science and Technology,(FISAT) Mookkannoor for her guide and support.

REFERENCES

[1] 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

[2] 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.

[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] Ali Saman Tosun, Wu-chi Feng, "Efficient multi-layer coding and encryption of MPEG video streams", IEEE International Conference on Multimedia and Expo, vol. 1, pp. 119-122, 2000.

[5] Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang, "Secure advanced video coding based on selective encryption algorithms", IEEE Transactions on Consumer Electronics, vol. 52, no. 2, pp.621-629, 2006

.[6] Chungping Wu, C.-C. Jay Kuo, "Design of integrated multimedia compression and encryption systems", IEEE Transactions on Multimedia, vol. 7, no. 5,pp. 828-839, 2005.

[7] Bharathi S.H.1, K. Nagabhushana Raju2 and S. Ramachandran3," Implementation of Intrapredictions, Transform, Quantization and CAVLC for H.264 Video Encoder", *International Journal of Electronics and Communication Engineering.* ISSN 0974-2166 Volume 4, Number 1 (2011), pp.95-104.

[8] 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.

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

Anisha Jose received the Bachelor's degree degree in Electronics and Communication Engineering from MG University, Kerala, India, in 2013. Currently, she is post graduate student with the Department of Communication Engineering, Federal Institute of Science and Technology (FISAT), Kerala, India. Her current research area includes antenna design and image processing.

Anu K Kuriakose received the Bachelor's degree in Electronics and Communication Engineering and M Tech in Communication Systems from Anna University, Chennai in 2009. Since 2011 she has been working as a Assistant Professor in Federal Institute of Science and Technology (FISAT), Kerala, India.