INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue3)

Available online at www.ijariit.com

Hiding Information in Encrypted Video Stream by Using Codeword Technique

Gote Yogita Ram
Computer Engineering Department.
K.S.I.E.T Hingoli, India
yogitagote45@gmail.com

Prof. Ashruba Korde
Computer Engineering Department.
K.S.I.E.T Hingoli, India

Abstract: To preserving the privacy as well as maintain the security of video it needs to be stored in an encrypted format. For copyright protection, access control and transaction tracking we use information hiding techniques, that can be embedded a secret message and secret image into a video bit stream. The quality of video in the absence of the original reference assesses by information hiding techniques. The edge quality information and the no of the bit streams processed in an encrypted format to maintain security as well as privacy. In this paper hiding information directly in the encrypted version of H.264/AVC video stream is proposed. The proposed scheme contains the three main parts, i.e. encryption of video, embedding secret message and extraction of secret message and video.

After analyzing the H.264/AVC codec property, the code words of inter prediction modes (IPM), the code words of motion vector differences (MVD), and the code words of residual coefficients are encrypted. The data hider embeds additional data in the encrypted domain, they use the code word substitution technique. The code word substitution technique gives information without knowing the original video content. After decryption of video secret message remains hidden, it's invisible to a human observer. The extraction of data can be done either in the encrypted or in the decrypted domain.

Keywords: Information Hiding, Encrypted Domain, Codeword Substituting, Decrypted Domain.

INTRODUCTION

Today Cloud computing it is a very important technology, which gives a highly efficient computation and provides large storage video data. For maintaining the security the cloud services are used for the hiding that original video content or access that video content is in encrypted form. There are one information hiding techniques can be used to embed a secret and secret image into a video bit stream for copyright protection, access control, and transaction tracking. The avoiding the leakage of video content the information hiding directly into H.264/AVC encrypted video streams, which can help address the security and privacy concerns with cloud computing [1]. For example, a cloud server can embed information into an encrypted version of an H.264/AVC video by using the information hiding technique. By using that hidden information, the cloud server can manage the video or verify its integrity without knowing the original content, and thus it preserves the security as well as privacy. In the reversible data hiding scheme for the encrypted image after encryption of entire data, the additional data can be embedded into the image and it modifies in small parts of encrypted data [6].At the time of the embedding, the data into the encrypted video the data hider does not know that the original video contents. After encryption when we decrypt the video then the information remains hidden it not observed by the human observer for that we used the codeword technique. Further, providing data security, privacy, and protection, information hiding in encrypted videos will become popular in the future. Information hiding in encrypted videos is a very difficult task, but in the proposed scheme achieved a better performance for that.

I. LITERATURE SURVEY

The secure video processing is an emerging technology used for preserving the privacy. In this paper mainly focus on video data and problem, challenges in securely managing secret video online. There are three aspects for evaluating a secure video processing i.e. security, performance, and complexity [1]. Insecure video processing, the users store their secret videos in encrypted form. There are two parts in the system, the user who owns secret information and server who stores the encrypted videos and performs processing tasks.

In this paper contains processing tasks, video search, classification, and summarization. Video summarization is a task of extracting a set of images called as video frames to represent the original video contents. Video classification means that the classify that video into a different category.

The reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain [4].There are two keys encryption and data hider key. In this paper, it used an improved Zhang's version for reversible data hiding method in encrypted images. The zhang proposed the image encryption and decryption parts. In that, the content owner encrypts the original image using the encryption key and passes that encrypted image and embed the data or additional data to the encrypted image by using data hider key to the receiver side. In the receiver side first, decrypt that image by using an encryption key and then extract the data and image recovery using data hider key. Here uses the LSB method. The embedded additional data is not secure it is the disadvantage of that.

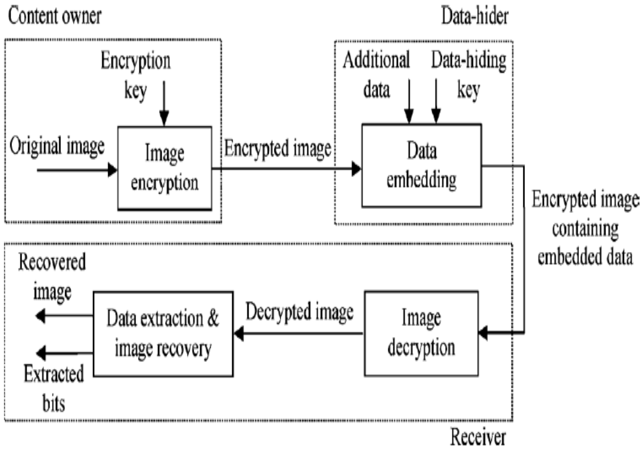

Fig. 1. **Reversible data hiding in encrypted image.**

The selective encryption is performed by using pseudo-random inverting sign. The H.264/AVC contains two types of entropy coding modules, CAVLC supports video baseline profile and CABAC supports video main profile. A selective encryption scheme based on H.264/AVC has been presented in context-adaptive variable length coding (CAVLC) and context-adaptive binary arithmetic coding (CABAC). The CAVLC and CABAC are used for I and P frames [11]. Selective encryption (SE) performed by using advanced encryption standard(AES) with the cipher feedback mode. The AES algorithm can support different cipher modes i.e. electronic code block, cipher block chaining, output feedback, cipher feedback, here it used cipher feedback mode.

The separable reversible information hiding contains content owner encrypts original image using an encryption key. By using the data hiding key data hider compress least significant bits of the encrypted image [10]. In that, the content owner encrypts the original image using the encryption key and embed the data or additional data to the encrypted image by using data hider key. For embedding the data uses the LSB (Least significant bit). Embed the secret data to the each bit pixel of that encrypted image. In the receiver side first, decrypt that image by using an encryption key and then extract the data and image recovery using data hider key. If the receiver knows the encryption key then they only decrypt the image, or if the receiver knows only data hider key then they only decrypt the secret information. Here uses the lossless compression method that contains additional information can be extracted and also the original content of the image is also recovered this is a limitation of this paper. So use lossy compression, it is compatible with the encrypted image.

It is necessary to watermark the compressed encrypted media items in the compressed-encrypted domain itself for tampering detection and ownership declaration or copyright purposes [7]. There is a challenge to watermark these encrypted streams as the compression process embed the information into the encrypted bit stream. It is necessary to choose an encryption scheme very secure and watermarking in an encrypted format. In this paper, there propose a robust watermarking algorithm to watermark JPEG2000 image compressed and encrypted images. The encryption algorithm we propose to use is a stream cipher. The proposed technique embeds a watermark in the encrypted domain, the extraction of the watermark can be done in the decrypted domain.

In this paper, it contains the overview for H264 AVC/SVC video encryption. In this paper summarizes the latest research on video encryption. Here achieved the scalability and security, compression efficiency. In the H264 encryption contains the four parts, encryption before compression, integrated encryption, the bit stream (oriented encryption), svc encryption. The integrated encryption contains inter prediction mode, inter prediction mode, motion vector difference, secret transform [13].The video encryption scheme depends on the application context. This paper is mainly focused on interoperability of video encryption. In this paper contains format compliance, packetization, fast forward and extraction of subsequences, robust watermarking.
For preserving the privacy the video encryption is the main task. Here a secure approach to encrypting H264 is to encrypt the entire H 264-bit stream using the AES algorithm with the cipher block. This paper is structured in following parts, briefly summarization of H264, application scenario of video encryption and their corresponding different notations. The encryption of video scheme preserves the functionality of video bit stream.

A scheme is proposed to implement commutative video encryption and watermarking during advanced video coding process. In that, the intra-prediction mode, motion vector difference, and discrete cosine transform (DCT) coefficients signs are encrypted [8]. The encryption and watermarking operations are commutative. The watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked. In the proposed scheme contains the embedding the watermark data into the encrypted images and then it decrypts the watermarked data. It also contains secure transformation and secure communication.

This paper describes the efficient selective encryption scheme for video. In this paper, the proposed scheme contains the mainly three parts, intra prediction mode, motion vector difference and residual encryption data. The proposed scheme achieves the computational efficiency, the time efficiency, security. But the limitation of this is that the encryption and embedding the data can be done in the encoding process and the extraction and decryption of video done in the decoding process. Compression and decompression did simultaneously. So it is very time consuming and effects on real-time applications [8] [14].

The existing system contains data hiding is performed directly in encrypted H.264/AVC video bit stream. The scheme can be both the format compliance and the strict file size preservation. The scheme can be decrypted either in encrypted or in decrypted domain. Encryption and data hiding happen at the time of H.264/AVC encoding process. The disadvantages of the existing system are it a degradation of video quality.

After analyzing the above papers the proposed schema can achieve better performance in the following different aspects:

- The JPEG2000 images works have been focused on image. With the increasing demands of g video data security and privacy protection is the main task.
- Data hiding in encrypted H.264/AVC videos will become popular in the near future. For avoiding degradation quality of video we use H265/HEVC video format.
- An H.264/AVC video encryption scheme with good performance including security
- After analyzing the property of H.264/AVC video codec, there are three parts IPMs, MVDs, and residual encryption data that are also supported for H265/HEVC are encrypted with stream ciphers

The following is the advantages of proposed schema:

- Data hiding: Data hiding is one technique used for security purpose. It hides data into the image, video.
- Encrypted Domain**:** It is done by using the encryption algorithm. Plaintext is converted into ciphertext.
- codeword: a code word is an element of a standardized code, used for embedding the data.
- Substituting**:** Substitution allows for recursive evaluation through macro templates
- Here also uses the H265/HEVC video format for improving the quality of the video.

A. Existing System

The existing system contains hiding data is performed directly in encrypted H.264/AVC video bit stream. The scheme can ensure both the format compliance and the strict file size preservation. The scheme can be applied to two different application scenarios by extracting the hidden data either from the encrypted video stream or from the decrypted video stream. In the existing system after the encryption of the video the quality of video get degrade, so for achieving this, we use the proposed scheme.

II. PROPOSED APPROACH FRAMEWORK AND DESIGN

We proposed the information hiding technique in H265/HEVC encrypted video stream by using codeword substitution technique. The H265/HEVC contains the faster data compression than the H264/AVC. That includes the three main parts, video encryption, data embedding, data extraction. The content owner encrypts the original video stream using a standard cipher with the help of encryption keys and then produce the encrypted video. In the video encryption, there is encryption key is generated by using the AES algorithm.

The data hider embeds the additional data into the encrypted video stream by using the codeword method, that all process get happened in the sender side. In the receiver side, hidden data get extracted either in encrypted domain otherwise in decrypted domain shown in fig.

A. Problem Definition

Information hiding in encrypted media is a new topic of privacy-preserving requirements of cloud data management. The encrypted H.264/AVC bitstream, which consists of encryption of videos, data embedding, and data extraction phases. In the information hiding it follows the without decrypting the data, the data hiding and re-encryption takes place. The bit stream preserves exactly after encryption and data embedding. For the data embedding, we use the code word substitution technique, even though it does not know the original video content.

B. Mathematical Model

S={IV, F,A, SF, D, EK, DK,OV, C}
Here, S represents system with several parameters as follows:
IV= input video
F={F1, F2....Fn} set of frames
F ϵ IV
SF=selected frame
SF ϵ F
SF= F/(Data size (in KB))

A=Audio file
EK ={EK1,EK2……EKn} encryption keys
DK={DK1, DK2…..DKn} decryption keys

C is codeword
C={Coeff_token, Sign_of_TrailingOnes, Level, Total zeros, Run before}
OV=Original video.

C. Software Architecture

Software architecture for hiding the information in the encrypted video using codeword, defining the work assignments that must be carried out by design and execution. That architecture contains the 2 parts, sender side, and receiver side. In the sender side original video is encrypted using an encryption key and then embeds the data into that encrypted video using data hider key.

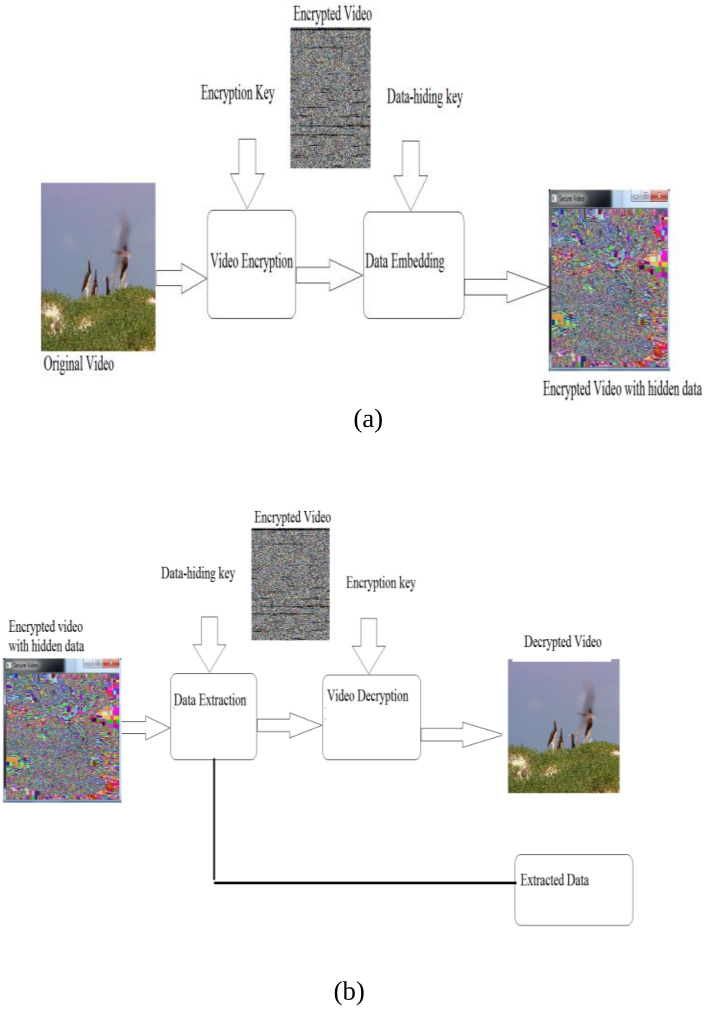

Fig. 2. **Proposed scheme diagram.(a) Video encryption and embedding data at the sender side (b)Data extraction and video decryption at the receiver side.**

Fig. 3.
In the receiver side, the encrypted video and data get extracted by using the encryption key and data hider key. The video is decrypted first and then the data get extracted called the decrypted domain extraction. The data is first extracted and then the video is decrypted called as encryption domain extraction.

D. System Modules

System module having three main parts video encryption, data embedding, data extraction.

1. Video encryption

Video encryption requires time efficient scheme to meet the requirement of real-time. The scheme proposed security, efficiency and format compliance. After analyzing the property of video codec they contain three parts Intra prediction mode (IPM), Motion vector difference (MVD), Residual data encryption. In this encrypted video, it is decoded by the standard decoder, but the encrypted video is completely different compared to the plaintext video data.

The video encryption first contains the Extraction of video into the no of frames. In that first, we extract or divide the video into audio and the number of frames. Then following operations are performed on that selected frames, encrypt that frames and passes it for embedding of data.

a. Intra prediction mode:
There are four types of intra prediction modes. Intra_4*4, intra_16*16, intra_chroma, I_pcm. Intra_4*4 and intra_16*16 chosen for the encryption purpose. They contain the macroblocks. At the time of the encryption, it takes the previously predicted block and the current block can be encrypted. The codeword length remains unchanged means that original codeword and encrypted codeword remains the same size.

b. Motion vector difference:
In this type, it protected the texture information as well as motion information. It is similar to intra prediction mode. It predicts the frames in a video.

c. Residual data encryption:
It keeps the high security there is one type of data called as residual data. That can be encrypted the I frames and P frames.

2. Data embedding

In the embedding of data contains embed the additional data into the encrypted video stream. There are few methods for embedding the data into the videos i.e. LSB, codeword method. LSB means that it embeds the bit of message into the each pixel of that image called LSB technique. Here we used codeword for embedding the data.
There are three limitations that satisfy codeword method.

1. First, the bit stream after codeword substitution decoded by the standard decoder.
2. Second, keep that bit rate remains unchanged, means that the original codeword and substituted codeword should have the same size.
3. Third, after decryption of video the information remains hidden, it cannot visible to a human observer.

For embedding data into the encrypted video there are the following the procedure:

Step 1. The additional data is encrypted with pseudorandom sequence P. Sequence P is generated by using data hiding key. It is difficult to anyone who does not know data hiding key to recover the hidden data.
Step 2. Codeword belongs to codespaces C0 or C1 to embed the data bit. If the data bit is 0 and codeword belong to codespace C0 then codeword unmodified, or if the data bit is 0 and codeword belongs to codespace C1 then replaced with the corresponding codeword in C0.
Step 3. If the data bit is 1 and codeword belong to codespace C1 then codeword unmodified, or if the data bit is 1 and codeword belong to codespace C0 then replaced with the corresponding codeword in C1.
Step 4. Take the next codeword and then go to step2 and step3. If there is no data bit to embed then that embedding process is stopped.

3. Data extraction

Data extraction can be done in the encrypted domain and decrypted domain. In encrypted domain contains first extraction of hidden data and then decryption of video using an encryption key. In decrypted domain contains firstly decryption of video using an encryption key and then extract data using data hider key. If the codeword belongs to codespace C0 then extracted data bit is 0. If the codeword belongs to codespace C1 then extracted data bit is 1.

E. Overview of data hiding

The below architecture contains components of data hiding in the encrypted video.

III. CONCLUSION AND FUTURE ENHANCEMENT

Information hiding in the encrypted video is a new topic for preserving the privacy and requirement into the cloud computing. The proposed scheme contains the three main parts, video encryption, data embedding, and data extraction. This technique follows without decryption the re-encryption takes place. For the embedding the data into the video stream uses the codeword substitution method. At the time of data embedding the data, hider does not know the original video contents. When we can decrypt the video the hidden information remains invisible to a human. Data extraction is done in the encrypted domain and in decrypted domain. Here we preserve the confidentiality of video content and also preserve the privacy and the quality of the video.

ACKNOWLEDGMENT

It gives me a great pleasure and immense satisfaction to present this paper of topic “**Hiding information in encrypted video stream by using codeword technique**” which is the result of unwavering support, expert guidance and focused direction of my guide **Prof. Pankaj Agarkar** to whom I express my deep sense of gratitude and humble thanks, for his valuable guidance and also thank the Head of the computer department **Prof. Soumitra S. Das.**

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] .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] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data hiding algorithm for H.264/AVC," J. Real-Time Image Process., vol. 7, no. 4, pp. 205–214, 2012.

[6] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp.255–258, Apr. 2011.

[7] 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.

[8] 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.

[9] 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

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

[11] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVCby 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.

[12] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving a room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[13] 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.

[14] 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.

[15] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data hiding algorithm for H.264/AVC," *J. Real-Time Image Process.*, vol. 7, no. 4, pp. 205–214, 2012.

[16] J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, "An Improved selective encryption for H.264 video based on intra prediction mode scrambling," *J. Multimedia*, vol. 5, no. 5, pp. 464–472, 2010.