International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

Efficient Data Embedding and Data Encryption in video Stream

Ms. Rupali D. Wankhade[1], Dr. G.R. Bamnote[2], Ms. S.W. Ahmad[3]

[1]ME FT Final Year, Computer Science & Engineering, P.R.M.T&R, Badnera
[2]Head & Professor, Dept. Computer Science & Engg, PRMIT&R, Badnera, Amravati
[3]Astt. Professor, Dept. Computer Sci. & Engg., PRMIT&R, Badnera

---

Abstract: - *Now day's Digital video needs to be stored and processed in an encrypted format to maintain security and privacy. Data hiding in encrypted data without decryption preserves the confidentiality of the data. In addition, it is more efficient without decryption followed by data hiding and re-encryption. The data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. By analysing the method of H.264/AVC codec, the code words of intraprediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to different technic application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly hide even after encryption and data embedding.*

Keywords*: Data Hiding Encrypted Domain, H.264/AVC, Codeword Substituting*

1. Introduction

The Cloud computing has become a much required technology, which provides efficient computation and large storage of solution for video data. Cloud provide services may more protection to attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content can be accessible in encrypted form. The capacity of performing data hiding directly in encrypted H.264/AVC video streams avoid the leakage of video data, this protects privacy and security concerns with cloud computing.[1] For example, a cloud server can embed the additional information into an encrypted H.264/AVC video by using data hiding technique. The server can manage the video and crosscheck its integrity without knowing the actual content, then helps to protect privacy and security. This technology can be used in other application. For example, when surveillance videos or medical videos have been encrypted for protecting the privacy and security of the people, a database manager can add the personal information into the corresponding encrypted videos is provide to data management capabilities in the encrypted domain.

The increasing demands of providing video data in high security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the future. Due to the constraint of encryption, it is very difficult and sometimes impossible to transplant the existing data hiding algorithms to the encrypted domain. In the paper gives the data hiding, on the implementation of data hiding in encrypted H.264/AVC video streams.

H.264/AVC having various advances in standard video coding innovation, as far as both coding proficiency improvement and adaptability for powerful use over a wide assortment of system sorts and application spaces H.264/AVC is a video pressure design i.e. standard for high definition (HD) advanced video.

2. System Implementation

The Video Encryption and Sharing is an application developed for preventing hacking of videos being shared via users. The source video is uploaded by the user itself which undergoes through various processes. First we take the video undergoes different encryption process separately. We use RSA algorithm for encryption techniques. In this system, video will be saved in encrypted format and saved on the server directly. After video is successfully uploaded, User can then share the video by selecting the users he wants to share with. User will get list of videos uploaded by him and videos shared with him. He can just select the video and send to another user. Encrypted parts of video is decrypted with their respective algorithm and merged together, And Original video is retrieved and view receiver user. Access to the shared video can be withdrawn by the owner itself. The application makes the sharing of video very secure which makes this developed application unique from others.

The security provides of 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 while data online share. There are three factors for evaluating a secure video processing i.e. security, performance, and complexity [1]. In high secure video processing, the users store their secret videos in encrypted form. There are two parts in the system, the user who owns original information and server who stores the encrypted videos and performs processing tasks. In this paper contains processing tasks, video search, classification, and summarization. Video recall is a task of extracting a set of images called as video frames to represent the original

video contents. Video classifications mean that classify the video into a different category.

The reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain [3].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 embeds the data or additional data to the encrypted image by using data hider key to the receiver side.

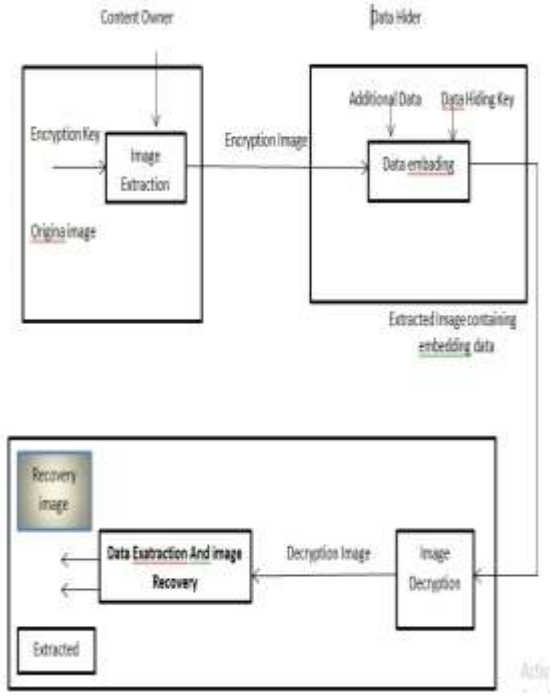


Fig 1: Reversible data hiding in encrypted image.

The selective encryption (SE) is performed by using pseudo-random inverting sign. The H.264/AVC contains two types of entropy coding modules, context-adaptive variable length coding (CAVLC) supports video baseline profile and context-adaptive binary arithmetic coding (CABAC) supports video main profile. A selective encryption scheme based on H.264/AVC has been presented in CAVLC and CABAC. The CAVLC and CABAC are used for I and P frames [7]. Selective encryption (SE) performed by using advanced encryption standard(AES) with the cipher feedback mode. The AES algorithm can support different cipher modes means electronic code block, cipher block chaining, output feedback, cipher feedback, here it used cipher feedback mode.

The particular 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 [6]. In that, the content owner encrypts the original image using the encryption key and embeds 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 bit pixel of that each encrypted image. In the receiver side first, decrypt the 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. So use loss 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 [4]. 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 select an encryption of data very secure and watermarking in an encrypted format. It contains the H.264AVC/SVC video encryption, also achieved the scalability, privacy, security, compression efficiency. In the H.264/AVC 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 [8].The video encryption scheme depends on the application context.

For privacy the video encryption is the main task. Here a secure approach to encrypting H.264 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 H.264, application scenario of video encryption and their corresponding different notations. The encryption of video scheme preserves the functionality of video bit stream.

In this paper, 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 [5].

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. Encryption and data hiding completed at the time of H.264/AVC encoding process. The disadvantages of the existing system are it a degradation of video quality.

After analysing 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 video data security and privacy protection is the main task.

•H.264/AVC video encryption scheme with have good performance including security and privacy.

• After analysing 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

3. Result & Discussion

The information hiding technique in H.264/AVC encrypted video stream by using codeword substitution technique. That includes the three main parts, video encryption, data embedding and data extraction. The content owner encrypts the original video stream using a standard cipher with the help of public and private key and then produces the encrypted video. In the video encryption, there is public and private key is generated by using the RSA algorithm. The data hider embeds the additional data into the encrypted video stream by using the codeword method, that all process gets happened in the sender side. Hidden data get extracted form in receiver side.

A. Problem Definition

Information hiding in encrypted of privacy-preserving requirements of cloud data management. The encryption of H.264/AVC bitstream, which consists of encryption of videos, data embedding, and data extraction phases. The information hide in it follows the without decrypting the data, the data hiding and re-encryption takes place. The bit stream stored the information exactly after encryption and data embedding. For the data embedding, the code word substitution technique is used, 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. System Modules

System module having three main parts

1. To generate public key & private key,
2. Data embedding,
3. Data extraction.

1. To generate the public key and private key requires time efficient scheme to meet the requirement of real-time. The scheme proposed security, efficiency and format compliance. After analysing the property of video codec they contain to generate public key and private key with the help of RSA algorithm. In the encrypted video, it decoded by the standard decoder, but in the encryption video is totally different compared to the plaintext video data. The video contain firstly encrypt then Extraction of video contain into the number of frames. Firstly the video data must be extract or divide into audio and the number of frames. Then the operations are performed on that selected frames, encrypt the frames and passes it for embedding of data.

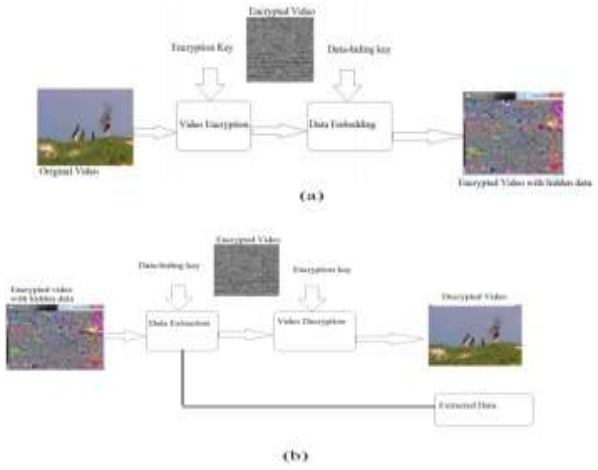


Fig 2: Encrypted & Decrypted scheme diagram. (a) Video encryption and data embedding at the sender side (b) Extraction of data and decrypted video at the receiver side.

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 do not changed means that original codeword and encrypted codeword remains the same size.

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

2. Data embedding of data contains embed the additional data into the encrypted video stream. There some methods for embedding the data into the videos which are used i.e. LSB, codeword method. LSB (List Significant Bit) means 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:

Step1. Some additional data is encrypted with pseudorandom sequence P. Sequence P is generated by using public key & private key. It is difficult to anyone who does not know public key & private 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.

Step3. 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.

Step4. Take the next codeword and then go to step2 and step3. If all the data must be embed then stop the embedding process.

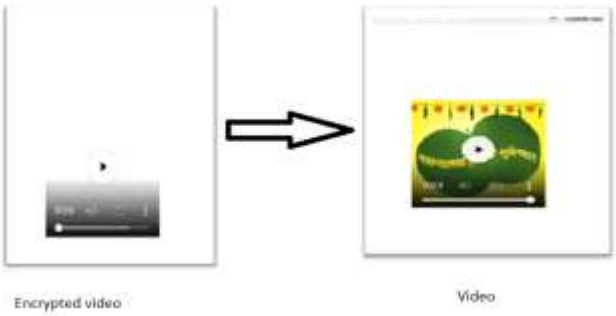
3. Data extraction can be done in the encrypted domain and decrypted domain. In encrypted domain contains extraction of hidden data and then decrypt the data by using encryption key. In decrypted domain, firstly contain decryption of data using an encryption key and then extract data using data hider key means public and private 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. Data hiding architecture contains components of data hiding in the encrypted video and those encrypted video must be decrypted in original bit rate.

Case I: To select the particular video then firstly encrypted the data by generating the public key and private key.

Case II: To uploading the video then those video must be encrypted in two way by using public key and private key by using RSA algorithm.

Case III: Most high secured data must be stored in cloud then hacker do not hack the data.



4. CONCLUSION

The recent technology inData Encrypt in Video Stream by Efficient Data Embedding has started to pay an attention to the storage and privacy requirements from cloud server. An algorithm is used to embed additional information in encrypted H.264/AVC bit stream presented, which have the video encryption, data embedding and data extraction stages. The bit-rate is preserved by an algorithm exactly even after encryption and data embedding, also simple to implement as it is directly performed in the compressed and encrypted domain, that is it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. Additional data is been added by the data hider into the encrypted bitstream using codeword substituting, even though the original information content are not known Information hiding in the encrypted video by using public key & private key for preserving the privacy and security of video which required into the cloud computing .Embedding the data into the video stream uses the codeword substitution method. At the time of data encryption the data, hider does not know the original video contents. Data extraction is done in the encrypted domain and in decrypted domain. This application provides confidentiality of video content and also gives the privacy and security of quality of the video.

5. Future Scope

This Application provides the security as well as keep away the hacker form hacking the video contents because the Application provide first RSA public and private key generate using video encrypt than video framing images. Then the Encrypted files is upload on server ,than server provide decryption of the data at receiver side most of security provided through the application such as important video conference, government video conference, lecture in private sector etc.

This application is enabling to suggest the user to the appropriate video security and size of video as per his/her requirements. In future, to enhance the algorithm to find out the statistical trustworthiness of vender by tracking their behaviour like hacker, user satisfaction for security, etc.

6. References

[1] Johnathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett, Steganography: The Art of Hiding, School Of Computer Science, The University Of Birmingham.

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

[3] 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

[4] Choudry, K.N. and Wanjari, A., 2015. A Survey Paper on Video Steganography.International Journal of Computer Science and Information Technologies, 6(3), pp.2335-2338.

[5] Mukherjee, S. and Sanyal, G., 2015, November. A novel image steganographic technique using Position Power First Mapping (PPFM). In Research in Computational Intelligence and Communication Networks (ICRCICN), 2015 IEEE International Conference on (pp. 406- 410). IEEE.

[6] 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.

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

[8] R. Sridevi, V. L. Paruchuri, and K.S. Rao, "Image steganography combined with cryptography", International Journal of Computers & Technology, Vol.9, pp. 976-984, July2001.