ISSN 2395-1621

Information Hiding in Advance Video Coding Using Residual Data

[#1]Mr. Makawane Sanjay R., [#2]Mr. Virkar Mayuresh A., [#3]Mr. Shinde Rohit S.,
[#4]Mr. Shinde Prashant B., [#5]Prof. Pawar Asha M.

[1]sanjay.makawane@gmail.com
[2]veer.mayur@gmail.com
[3]rohit.shinde777@gmail.com
[4]shindep2792@gmail.com
[5]asha.pawar@zealeducation.com

[#12345]Computer Engineering Department, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

To maintain security and privacy of digital video is one of the challenge. Sometimes they needs to be stored and processed in an encrypted format to maintain security and privacy. It is necessary to perform data hiding in these encrypted videos, for content notation and tampering detection. In this way, it preserves the confidentiality of the content by data hiding in encrypted domain without decryption. There are three parts of secret data hiding in encrypted version of AVC video streams that is AVC video encryption, data embedding and data extraction. In AVC have three sensitive parts Intra-Prediction Mode, Motion Vector Difference and Residual coefficients then, those parts code words select and encrypted with stream cipher. Data Hider hide encrypted secret data or confidential information into encrypted AVC video streams by code words without knowing original video content, data extraction from decryption domain or video. After Embedding and extraction Secret data preserve File size of Video. In order to evolve to different program circumstances, secret data extraction is from the decrypted format of AVC streams. Furthermore, video quality or file size also totally preserved even after encryption and secret data embedding or extraction.

ARTICLE INFO

Article History

Received :24th May 2016

Received in revised form :

26th May 2016

Accepted : 28th May 2016

Published online :

31st May 2016

Keywords—Embedding, Encryption, Data Hiding, Video Streams, Intra-Prediction.

I. INTRODUCTION

A. Problem Statement

Now a days, Rapidly development of communication, transmission and storage using digital media via network or internet. When we are trying to transfer any secret data or private information through the internet or transmission channel there may be possibility that this information can be hacked or accessed by unauthorized person. Sometimes, transfer the most secret data is not securely reach to destination. To overcome from all this issue trying to embed encrypted secret data into encrypted AVC video streams to make it very securely, Efficiently and Format compliance to reach destination.

B. Objective

Encrypt the secret data before hiding for Confidentiality.

The Encrypted Secret data hiding in encrypted AVC video bit streams. Embed the encrypted Secret data into encrypted video for two way security. The scheme can ensure both the format compliance and the strict video file size preservation. Propose the method to providing the privacy and security to both the video and secret data.

C. Introduction of Topic

Traditionally people world use letters for communication with each other but now a days we are using internet, Skype for communication and transfer and storage the all multimedia data anywhere in the world. But increasing popularity of digital media has concern over the security related issues. Data hiding useful for security purpose. As the internet technology is developing with a

great speed the information media like images, videos are used more and more in day to day life. Internet technology made possible easy to transfer and copy of such data through media. Thus the protection of media is the main issue of discussion. Data hiding or Stenography is process of piece of critical data embeds into noncritical data or media to distract the opponents attention.

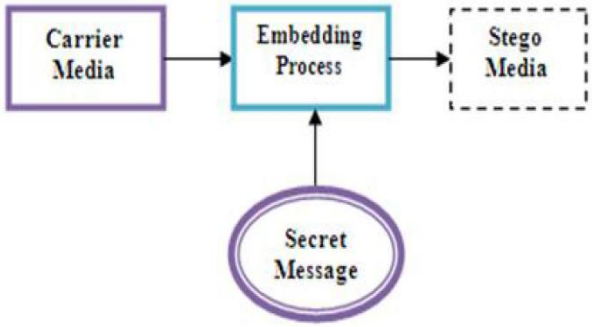

Fig1. Data Hiding Method

Multimedia is very central topic in the world especially for IT industries, telecommunication and internet. To exchange the large amount of multimedia data such as Images, audio, video across the internet required proper Reliability and confidentiality. it is desired that the video content is accessible in encrypted form. The capability of performing data hiding in encrypted AVC video streams would avoid the leakage of video content, which can help address the security and privacy. For example, a cloud server can embed the additional information for example video notation, or authentication data into an encrypted version of an AVC video by using data hiding technique. Without knowing the original content, with the hidden information, the server can manage the video or verify its integrity, and thus the security and privacy can be protected. For example, to guarantee the confidentiality of patients healthcare video, the medical video must be encrypted prior to transmitting over networks and decrypted in a way of preserving near-lossless quality. a medical video encryption method by AVC with near-lossless compression.

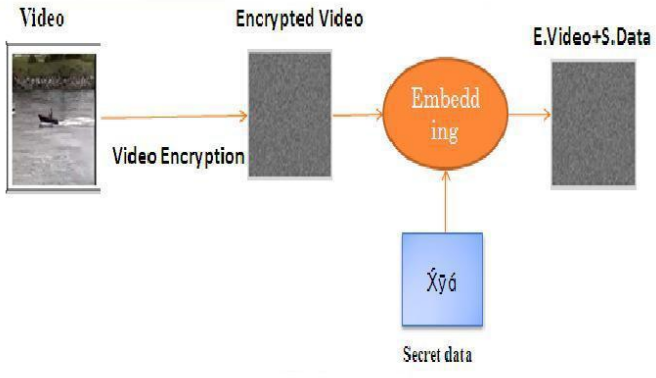

Fig 2. Data hiding in Encrypted Video

II. LITERATURE SURVEY

A. B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol"

In this paper we studied Watermarking process. The Watermarking process embeds data called watermark or tag or label into multimedia object may be an image ,audio, video such that to make an assertion about the object watermark can be detected or extracted later. Watermarking technique is developed for authentication copyright protection and multimedia distribution. A seller normally add a watermark in host multimedia content as a uniquely identify a buyer. The added watermark traces the traitor as identity, If the seller finds an unauthorized copy. But there is sometimes repudiation issue. watermark image is encrypted by a buyer as public key, and it is not exposed to the seller. This scheme increases effective watermarking capacity, removes the additional overhead, an inherent flaw that watermarking capacity depends on the probability distribution of input watermark sequence..

B. W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images"

In this paper we studied a reversible data hiding algorithm for encrypted image. This method firstly host image encrypt using secret key then data hider can hide data into encrypted host image using data hiding key, after decrypt an marked image rebuild the host image with visual quality by extraction of hidden data. The main analysis is during decryption step extraction of hidden data done from marked encrypted image. The data hiding algorithms are mostly used for protection of multimedia data. To decrease the transmission time the data compression is necessary. A research is on going to combine the three steps compression, encryption and data hiding. In this method use Advanced Encryption Standard algorithm(AESA) for encrypt the Host image .There is one important challenge is to embed data in encrypted images. Embedding data capacity for 16pixels is 1 bit only. Recent reversible data hiding methods with high capacity but these methods are not compatible with encrypted images.

C. X. P. Zhang, "Reversible data hiding in encrypted image"

In this paper we studied a novel data hiding technique. An additional data can be embedded into the image by modifying a small proportion of encrypted data. Using encryption key, an encrypted image containing additional data is decrypted. Now this decrypted version is similar to the original image. With the help of spatial correlation in natural image the embedded data can be properly extracted and the original image can be perfectly recovered by using the data-hiding key. A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then the data hider embeds additional data into the encrypted image using a data-hiding key.

D. P. Berenbrink, C. Cooper, T. Friedetzky, T. Friedrichand T. Sauerwald, "

Randomized diffusion for indivisible loads" For balancing indivisible tasks (tokens) on a network a new randomized diffusion-based algorithm is presented. Minimize the discrepancy between the maximum and minimum load is the aim. The working of algorithm as follows. Every vertex distributes its tokens among its neighbors and itself as evenly as possible. The vertex redistributes its excess tokens among all its neighbors randomly without replacement, if this is not possible without splitting some tokens.

III. SYSTEM ARCHITECTURE

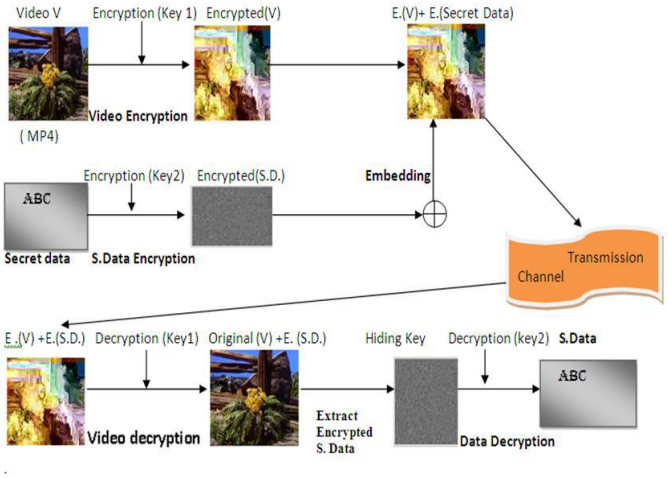

Fig 3. System Architecture

Step 1: Firstly convert video Format into AVC video streams.
Step 2: Encrypt video using Advanced Encryption Standard (AES) algorithm.
Step 3: Form secret data. Encrypt secret data using RC4 algorithm.
Step 4: Encrypted secret data embeds into encrypted video Streams.
Step 5: Then, at the receiver side Firstly decrypt the encrypted video streams.
Step 6: AVC video stream have Encrypted secret data.
Step 7: Extract encrypted secret data, and then decrypt those data.
Step 8: Securely get AVC video streams and secret data.

A. Advanced Encryption Standard(AES) For Video Encryption & Decryption Algorithm

Step 1: Input- The input is Original Video (V).
Output- The output is Encrypted AVC Video Streams (T).
Step 2: Read input video file(V Th).
Step 3: Check compression format of input video. If formatis AVC then go to step 5.
Step4: Convert input video to AVC video streams (M) Using compression format (Converter C).
Step 5: Parse AVC video stream and get three sensitive parts which are Intra-prediction Mode, MVD and Residual Coefficient codeword's.
Step 6: Read Intra keywords, Set C0= get new IV parameter for all codeword in intra Cipher text for current codeword (plaintext) = Encrypt (cipher text (O) of previous codeword) XOR Current codeword (Bi=Ek (Bi-1) XOR Oi).
Step 7: Substitute encrypted codeword to video stream Follow step 6 and 7 similarly for MVD and Residual data codeword's.
Step 9: After completed all rounds of encryption then get Encrypted Video streams.
Step 10: T is cipher-text (video streams encrypted) of plaintext M with XOR operation.
At a time of Video decryption same process as Encryption.

B. RC4 Algorithm: For Secret Data Encryption & Decryption.

Step 1: Input: Confidential Data (P).
Output: Encrypted Confidential Data (U).
Step 2: Given P is Confidential data bytes or (KB) as a plaintext.
Step 3: Shuffling array using to make it a permutation array.
Step 4: Generate key stream by pseudorandom generator of RC4 of length equal to length of Confidential data P
Step 5: Then, Perform XOR operation between Confidential data (P) and Key stream for encryption.
Step 6: Get, Encrypted message U of Confidential data as cipher text.At a time of decryption same process as an encryption time.

IV. RESULTS

A. Video selected for conversion

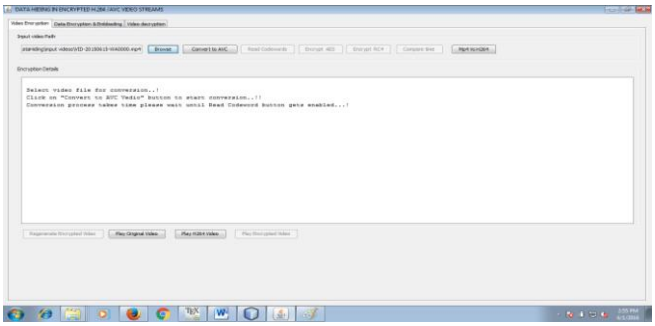

Fig 4. Video selected for conversion

B. Codewords extracted from video successfully

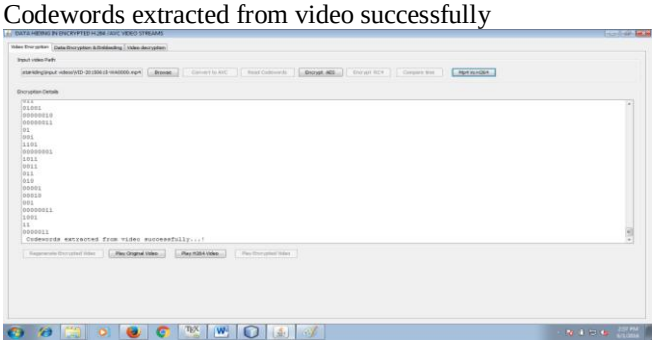

Fig 5. Codeword's extracted from video successfully

C. Codeword's encrypted using AES successfully

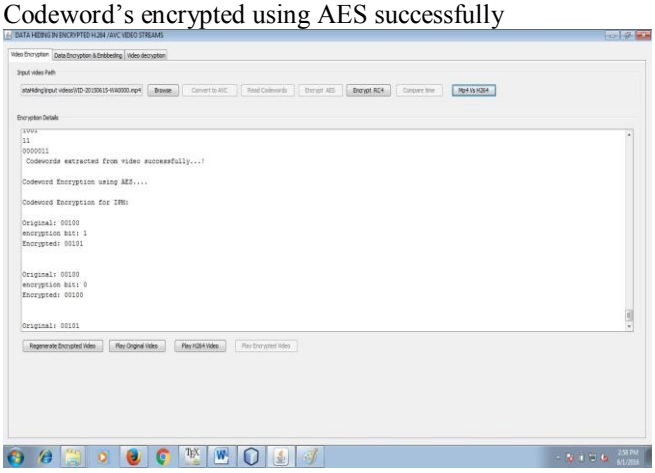

Fig 6. Codeword's encrypted using AES successfully

V. IMPLEMENTATION AND RESULT

A. Experimental Setup

The system is built using Java framework (version jdk 6) on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesnt require any specific hardware to run, any standard machine is capable of running the application.

B. Experimental Results

The system is built using Java framework (version jdk 6) on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesnt require any specific hardware to run, any standard machine is capable of running the application.

In following figure Original Video require convert into AVC video because whole original video required large size to store but this video compress via compression mode is AVC. Then, After compression of original video via AVC reduce the size of video for easily store in minimum space. Compression of video useful to more and more secret data hiding in this remaining space.

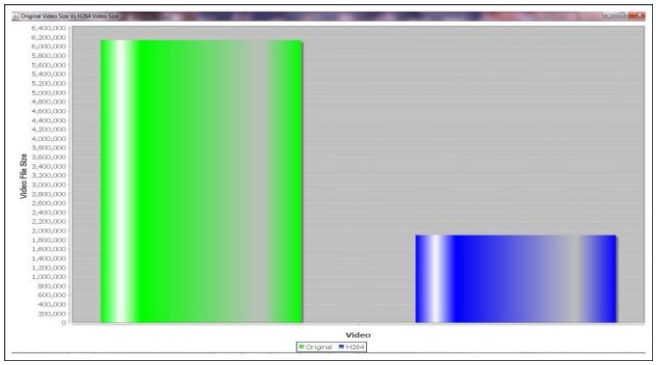

Fig.7:Compression ratio or Size difference between original video VS AVC

Conclude from following figure that time required for video encryption is minimum in proposed system since there is encrypting a part of a video not whole video so it will take less time for encryption.

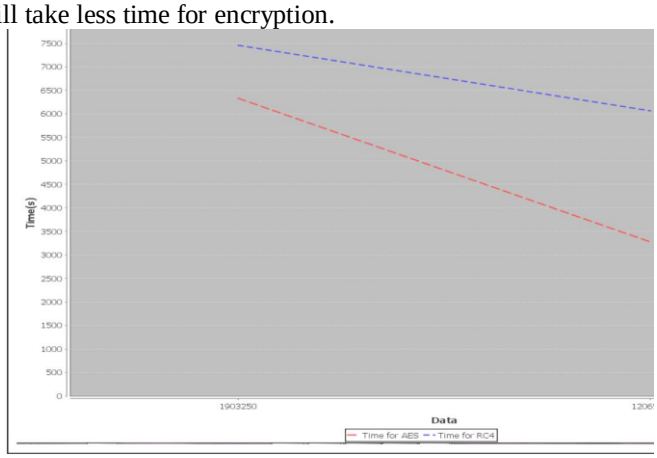

Fig.8. Time required for video Encryption

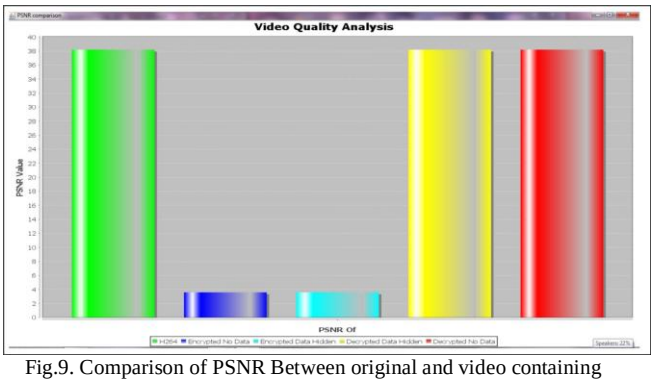

Fig.9. Comparison of PSNR Between original and video containing encrypted data

Conclude from graph shows above the comparison of PSNR(Peak signal to noise ratio) ratio between Original video and video containing encrypted data. It shows that PSNR of video containing encrypted data of proposed system is greater than existing system.

VI. CONCLUSION

Here, an algorithm to embed additional data in encrypted AVC Bit stream is presented, which consists of video encryption, data encryption, encrypted data embedding and video extraction, data extraction and data decryption of data phases. Even after encryption and data embedding, the algorithm can preserve the bit-rate exactly. The data-hider can embed additional data into the encrypted bit stream using codeword substituting, even though he does not know the original video content. It is fully compliant with the AVC syntax. Encryption and data embedding scheme can preserve file size, whereas the degradation in video quality caused by data hiding is quite small.

ACKNOWLEDGEMENT

We take this opportunity to thank our Project guide **Prof. Pawar Asha M.** and Head of the Department **Prof. Sangave S.M.** for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this report.

REFRENCES

[1] 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 to 4684, 2010.

[2] W. Puech, M. Chaumont, and O. Strauss, 'A reversible data hiding method for encrypted images,' Proc. SPIE, vol. 6819,pp. 68191E□1 to 68191E□9, Jan. 2008.

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

[4] 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 to 202, Apr. 2012.

[5] 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. 553ˆa562, Mar. 2013.

[6] T. Shanableh, aData hiding in MPEG video files using multivariate regression and flexible macroblock ordering,ˆa IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 455ˆa464, Apr.2012.

[7] Yiqi Tew, KoKSheik Wong ,ˆa An overview of InformationHiding in H.264/AVC compressed video.ˆa Vol 24,N0.2,Feb2014

[8] White Paper: An Overview of H.264 Advanced Video Coding

