International Conference On Emerging Trends in Engineering and Management Research
NGSPM's Brahma Valley College of Engineering & Research Institute, Anjaneri, Nashik(MS) (ICETEMR-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-7-5

# SECURED DATA HIDING IN ENCRYPTED H.264/AVC VIDEO STREAM

**A.S. Korde[1], A.P.Hatkar[2]**

*[1,2]Electronic and Telecommunication Department, SPP University*
*SVIT, Chincholi, Nashik, (India)*

**ABSTRACT**

*In daily life, there is increase in use of multimedia applications such video conferencing, video telephony, stream video/audio online etc. Such type of applications requires the large storage and high bandwidth to send through the network. For the purpose of highly secure data transmission and privacy, there is need of encryption of digital video. During the encryption of video, the data hiding can be performed and provide the authentication form different servers. In this paper proposed scheme is the secure data transmission with directly hiding data in the encrypted version of H.264/AVC video is presented, which includes three parts are H.264/AVC video encryption, data embedding and data extraction. The content owner can encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce encrypted video stream and the code word substitution for the data embedding purposes, that it eligible codewords can be substituted. Without knowledge of the content original video, a data hider may embedded extra data with the encrypted domain by using codeword substitution technique. Data extraction can be done either in the encrypted domain or in the decrypted domain, in order to adapt to different application. Furthermore, video file size is strictly preserved even after encryption and data embedding.*

***Keywords: Codeword substituting, Data hiding, Encryption, H.264/AVC***

## I. INTRODUCTION

The security of data in a cloud networking is critical and it is very important to maintain the security like confidentially, integrity and the availability over the cloud network as well as the other networks. In recent years there is exponential increase of size of multimedia files and because of the substantial increase of affordable memory storage on the wide spread of World Wide Web (www). Also there is need for the efficient tool to retrieve the images from the large data base becomes crucial. However with the substantial increase of the size of images as well as size of image database, the task of user-based notation becomes very complex and at some extent subjective and thereby, incomplete as the text often fails to convey the rich structure of images. To overcome these difficulties this motivates the research into what is referred as data hiding and compress the image using vector quantization so that small database is required. The different available technologies which provide thehighly efficient computation and large-scale storage solution for video data is cloud computing [1]. The security of data in a cloud networking is critical and it is very important to maintain the security like confidentially, integrity andthe availability over the cloud network as well as the othernetworks. The most popular used standard for video isH.264/AVC (Advanced Video Coding), gives the higher efficiency in video

encoding [2]. To address the security and privacy concerns with cloud computing, the capabilityof performing data hiding directly in encrypted H.264/AVCvideo streams would avoid the leakage of video content.The additional information into an encrypted version of anH.264/AVC video by using data hiding technique, a cloudserver can be embedded. The security and privacy can be protected, with the hidden information without knowledge of the original content which may design for the efficient compression performance and in the rate-distortion efficiency in comparison with the existing standards. This technology can be used for many important applications such as the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people.This chapter reviews the all existing approaches for data hiding.

## II. RELATED WORK

According to [2], H.264/AVC is newest video coding standardof the ITU-T Video Coding Experts Group and theISO/IEC Moving Picture Experts Group. The main goals of theH.264/AVC standardization effort have been enhanced compression performance H.264/AVC has achieved a significant improvement in rate-distortion efficiency relative to existingstandards. In paper [3], most watermarking schemes for copyright protection, a seller usually embeds a watermark in multimedia content toidentify a buyer. When an unauthorized copy is found by theseller, the traitor's identity can be traced by the embedded watermark. In paper [4], Digital asset management systems (DAMS) generally handle media data in a compressed and encrypted form. In this paper, author proposes a robust watermarking algorithmto watermark JPEG2000 compressed and encrypted images. In [5], A scheme is proposed to implement commutative videoencryption and watermarking during advanced video codingprocess. In H.264/AVC compression, the intra-predictionmode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients'amplitudes is watermarked adaptively. According to paper [6], the protection of this multimedia data can be done with encryption or data hiding algorithms.To decrease the transmission time, the data compression is necessary. In [7] this paper, author firstly discuss the implementation of Walsh-Hadamard transform (WHT) and its fast algorithm inthe encrypted domain, which is particularly suitable for the applications in the encrypted domain for its transform matrix consists of only integers. In [8], the paper presents a combined scheme of encryption and watermarking to provide the access right and the authentication of the video content simultaneously. This scheme protects contents more secure because the encrypted contentis decrypted when the watermark is exactly detected.

## III. SYSTEM ANALYSIS

The most use of the Internet offers great convenience to the transmission of a large amount of data over networks, which are open but insecure channels, exposing many private and secret data to dangerous situations. Today, ensuring that information transmission over the Internet remains safe and secure has become extremely important. To keep the unauthorized user away from the transmission information, a variety of techniques have been proposed; data hiding is one of the protective techniques in data security. All the methods existing till now try from the encrypted images directly.

**A] System Overview/Flow Chart:**

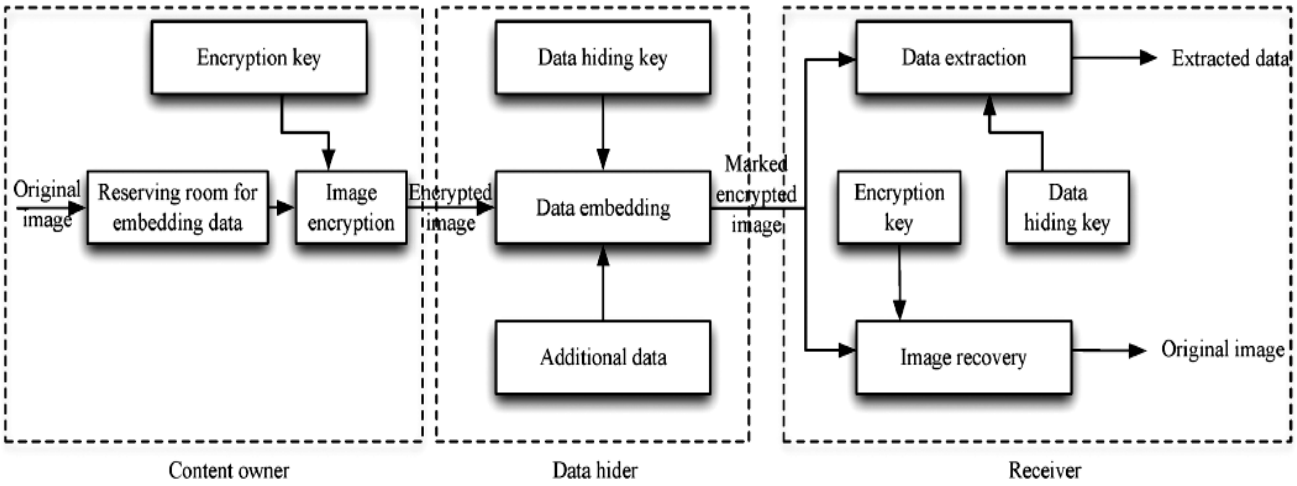



**Fig. 1 Overview of System**

The Fig. 1 shows the content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE (vacating room after encryption). Next, a practical method based on the Frame work "RRBE" (reserving room before encryption), which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery.

**B] Generation of Encrypted Image and Data Hiding In Encrypted Image**

Actually, to construct the encrypted image, the first stage can be divided into three steps: image partition, self reversible embedding followed by image encryption.

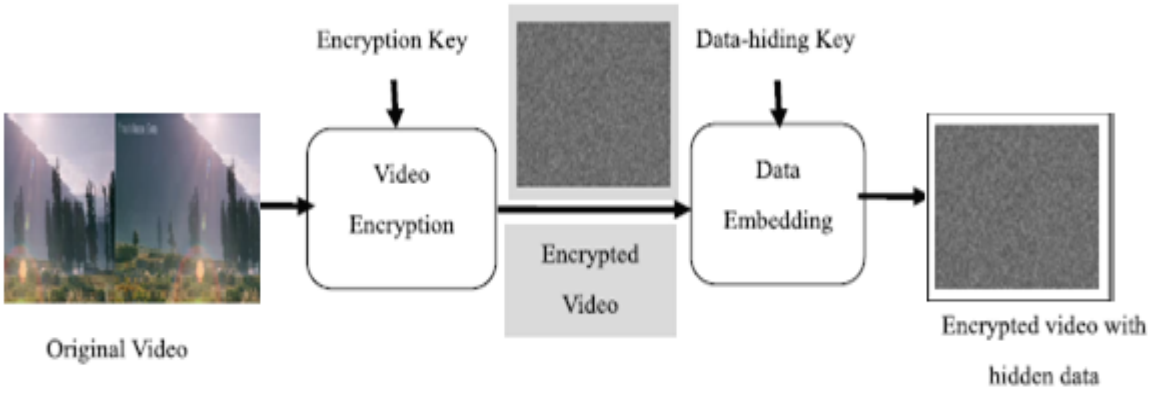
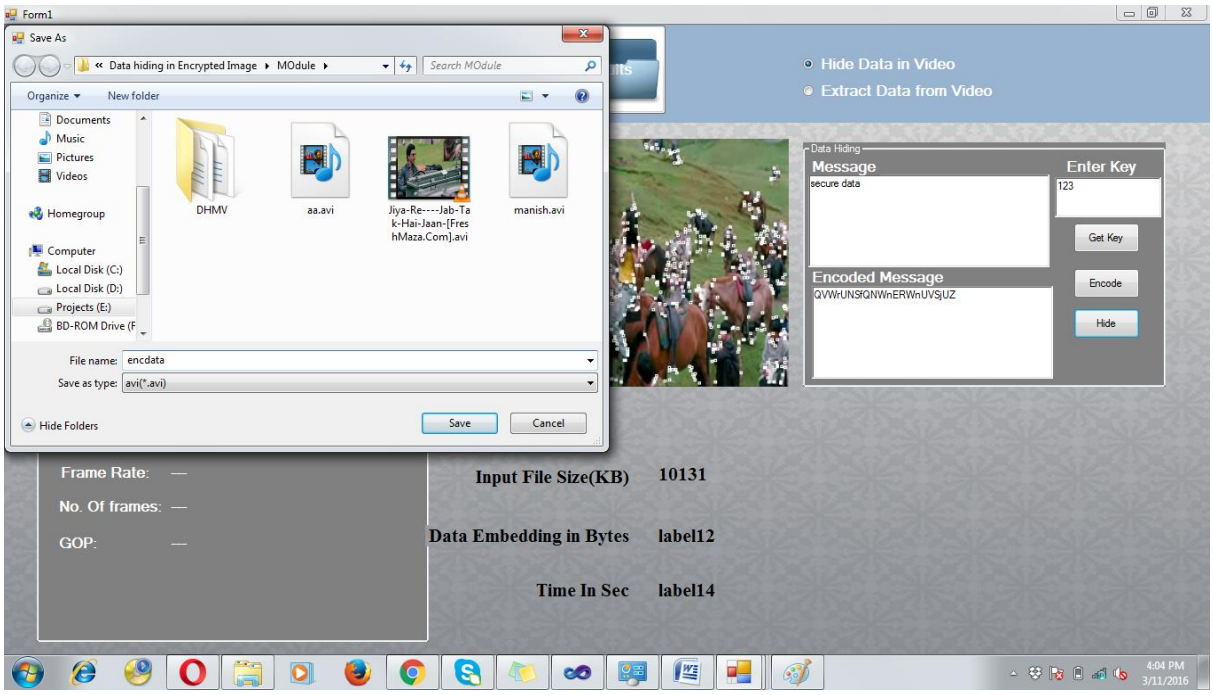



**Fig. 2 Diagram of Video Encryption and Data embedding**


In this scheme of data hiding in the encrypted version of H.264/AVC videos is presented, 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 with encryption keys to produce an encrypted video stream. Then, the data-hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using codeword substituting method, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

A scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes three parts [1] :-

**1] H.264/AVC video encryption:-** The encryption of video requires the scheme to be time efficient to meet the real time requirement . In this paper, an H.264/AVC video encryption scheme provides the

good performance, efficiency, security. The property of H.264/AVC codec analyzing by IPMs, MVDs, and residual coefficients are encrypted. In this proposed scheme encryption of the codewords of IPMs, the codewords of MVDs, and the codewords of residual coefficients.

**2] Data embedding**:- Tthe proposed data embedding is accomplished by substituting eligible codewords in the encrypted bitstream of H.264/AVC. After video decryption the embedded data has to be invisible to a human observer.

**3] Data extraction:- T**he hidden data can be extracted either in encrypted or decrypted domain, as shown in Fig. 3. Data extraction process is fast and simple.

**C] Data Extraction and Image Recovery**

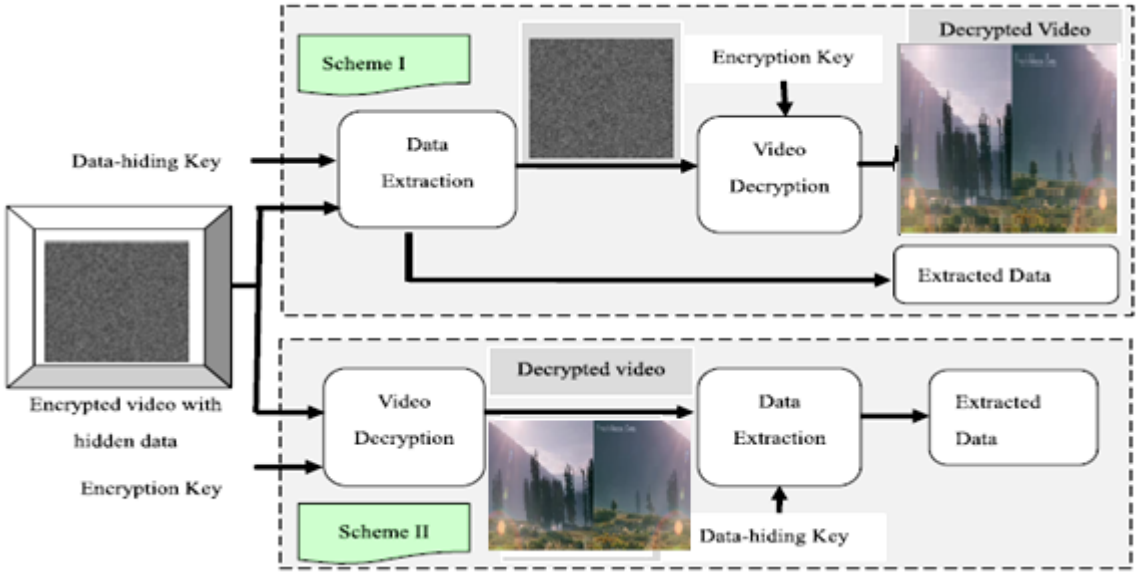
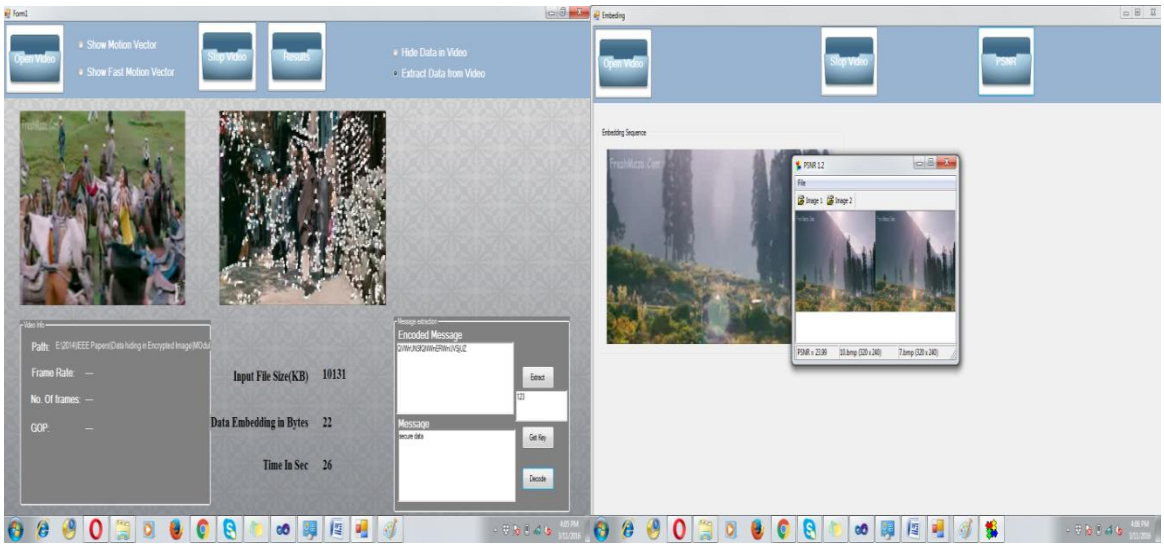



**Fig. 3 Diagram of Data extraction and video display**

As the data extraction process is totally independent from image decryption, therefore two different practical applications.

**1) Extracting Data from Encrypted Images**: To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case.

**2) Data Extraction and Image Restoration:** After generating the marked decrypted image, the content owner can further extract the data and recover original image. This process is similar to that of traditional RDH methods.




### D] Data security

In this proposed scheme encryption methods IPM, MVD and residual coefficients are used which keeps perceptual security of the encrypted video. This technique gives both cryptographic security and perceptual security. At the same time for enhanced security purpose we can use the key for encryption and decryption process, so that unauthorized person cannot access the video file or data.

### E] Algorithm Used In our Proposed System

- Security of Encryption Algorithm
- Intra-Prediction Mode (IPM) Encryption
- Motion Vector Difference (MVD) Encryption

## IV. RESULTS

PSNR (Peak Signal to Noise Ratio), is widely used objective video quality metric. So the PSNR are used to evaluate the perceptual quality of the video, which illustrate the video quality between the original video and the video after extraction and encryption process.

**Table-1 Comparison of different existing methods with proposed method based on PSNR values**

| PSNR VALUES | | | | | |
|---|---|---|---|---|---|
| Data Embedded(QP) | | 0.005 | 0.01 | 0.05 | 0.1 |
| Video name | LSB Plane | | | | |
| Table | 1- LSB Plane | 67.88 | 64.25 | 55.25 | 53.23 |
| Mobile | 1- LSB Plane | 65.90 | 63.37 | 57.45 | 55.10 |
| Hall | 1- LSB Plane | 68.22 | 65.32 | 56.33 | 53.12 |
| News | 1- LSB Plane | 67.26 | 64.22 | 56.33 | 53.12 |

**Table-2 Comparison of Different Existing Methods With Proposed Method Based On Time**

| Algorithm/Data | Existing Algorithm | | Proposed scheme | |
|---|---|---|---|---|
| | 256 | 512 | 256 | 512 |
| Data Embedding | 1.20 | 1.05 | 1.01 | 0.89 |
| Data Extraction | 1.15 | 0.96 | 0.89 | 0.85 |

The visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video which is shown in Table that is comparison of PSNR. By modifying the compressed bit stream to embedded additional data, the most important challenge is to maintain perceptual transparency, which refers to the modification of bit stream should not degrade the perceived content quality.

## IV. CONCLUSION

Data hiding in encrypted video is a new technology that has started to cause attention dueto the storage and privacy requirements from cloud server network. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, which includes the video encryption, data embedding and data extraction stages. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e., it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications [1]. The data-hider can embed additional data into the encrypted bitstream using codeword substituting, even though he does not know the original video content. Furthermore the data hiding process is completed entirely in the encrypted domain, so can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides different practical applications. The proposed encryption and data embedding scheme can preserve file-size. Thus there are so many applications by data hiding in encrypted domain such as Content authentication , Copyright Protection, Broadcast monitoring, Finger printing, Metadata binding, Covey communication.

## REFERENCES

[1] DawenXu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE, "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] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard*," IEEE Trans. Circuits Syst. Video Technol.,* vol. 13, no. 7, pp. 560–576, Jul. 2003.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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

[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.