International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Securely Hiding Information in Compressed Video Streams

Ms. Priyanka R Jakhalekar[1], Prof. Pankaj Agarkar[2]

[1]*PG Student, Computer Engineering, Dr.D.Y.Patil School of Engineering,Lohgaon,Pune,India*
[2]*Assistant Professor, Computer Engineering, Dr.D.Y.Patil School of Engineering,Lohgaon,Pune,India*

Abstract – *For maintaining security as well as privacy of video it needs to be stored in an encrypted format. For copyright protection, access control and transaction tracking we use data 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 data 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, that proposed scheme includes the three main parts, i.e. encryption of video, embedding and extraction of data. After analyzing the H.264/AVC codec property, the code words of intra prediction modes (IPM), the code words of motion vector differences (MVD), and the code words of residual coefficients are encrypted. For hiding data into video in existing system used codeword substitution technique and in proposed system used Qr code.*

Key Words: Information hiding, encrypted domain, H.264/AVC, codeword substituting.

1. INTRODUCTION

The cloud computing it is an important technology, which gives a highly efficient computation and large-scale storage video data. The cloud services are used for the hiding that original video content or access that video content is in encrypted form for the security purpose. 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 crucial parameters in video communication. Their requirements are also increased exponentially with increasing demand of video applications. But these services 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 treat 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.

There is 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. For 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 i.e. video notation, or authentication of data 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 and privacy. 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.

2. LITERATURE SURVEY

Secure signal processing is an emerging technology to enable signal processing tasks in a secure and privacy-preserving fashion. It has attracted a great amount of research attention due to the increasing demand to enable rich functionalities for private data stored online. Desirable functionalities may include search, analysis, clustering, etc. [1] In this paper, we discuss the research issues and challenges in secure video processing with focus on the application of secure online video management. Video is different from text due to its large data volume and rich content diversity.

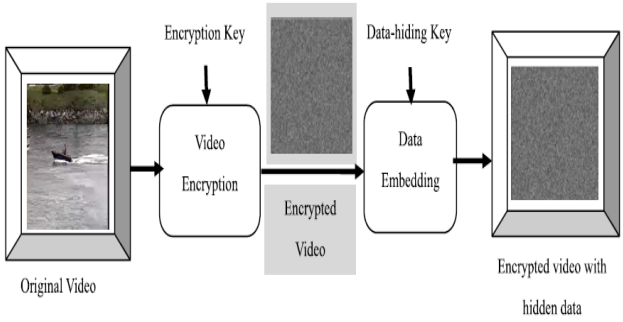
The reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain [6].In this paper it used an improved Zhang's version for reversible data hiding method in encrypted images. By using the data-hiding key, it is easy to reversibly embed data in the encrypted image. Thus the data hider can benefit from the extra space Emptied out in the previous stage to make information hiding process effortless. This work proposes a novel reversible data hiding scheme for 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 is used for I and P frames [10]. SE is performed by using the advanced encryption standard (AES) algorithm with the cipher feedback mode on a subset of codewords / binstrings.

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 encrypted image [8]. The encryption key is very useful in that technique. With the help of the encryption key receiver decrypt the received data. This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. The existing system approaches contains data hiding 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. Encryption and data hiding are accomplished almost simultaneously during H.264/AVC encoding process. The disadvantages of existing system is JPEG2000 images works have been focused on image, IPM (Intra-Prediction Mode) does not exist in the actual standard, it not support advance concepts stenography.

3. SYSTEM ARCHITECTURE

System architecture for hiding the information in encrypted video. They having the 2 parts, sender side and receiver side. In the sender side original video is encrypted using encryption key and then embeds the data into that encrypted video using data hider key. In the receiver side the encrypted video and data get extracted by using the encryption key and data hider key.



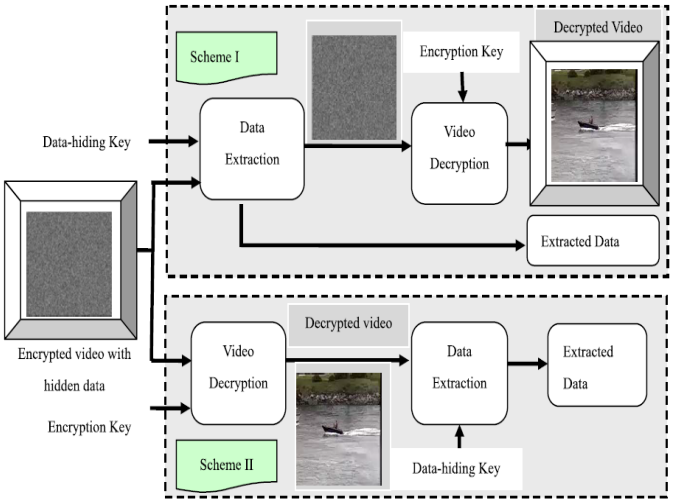


Fig 1 Block Diagram of proposed scheme, Video encryption and data embedding and data extraction

It is a graphical representation of the flow of data through an information system,modeling its process aspects. Flow chart can also be used for the visualization of data processing. The actual flow of system is shown in Fig 2.

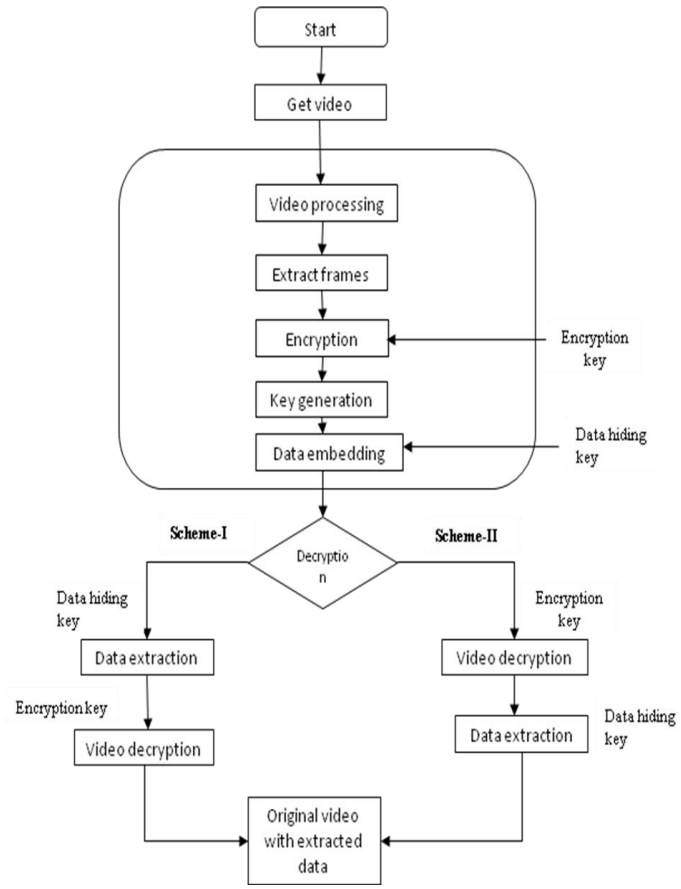


Fig 2 Flow Chart

In the proposed system we used the Qr code for hiding data into the compressed video file.

4. RESULTS

The result of work is the comparison between the existing system and proposed system. In that first we take the original video, here preserved the size means that original video size and after embedding the data into video size remains same. In the existing system after hiding data into video contains the more size than the original video size and the proposed system after embedding data into video contains the same size compare to the original video size.

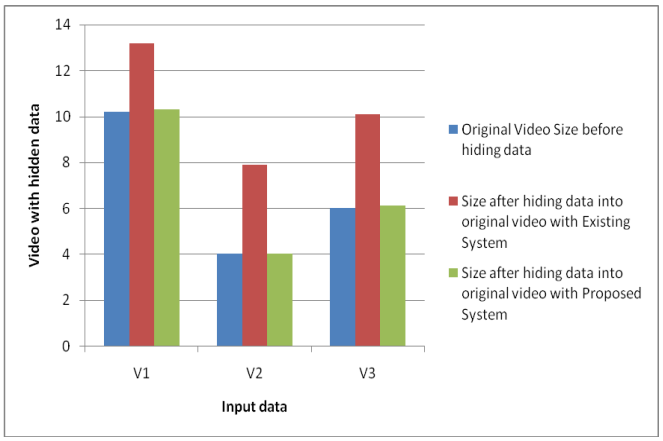


Fig 3 Comparison of existing system and proposed system

PSNR (Peak Signal to noise ratio), is widely used video quality metrics. PSNR are used to measure the perceptual quality of video, which illustrate the video quality between the original video and video after extraction and encryption process.

Therefore, the visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video that is comparison of PSNR. By modifying the compressed bit stream to embed 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.

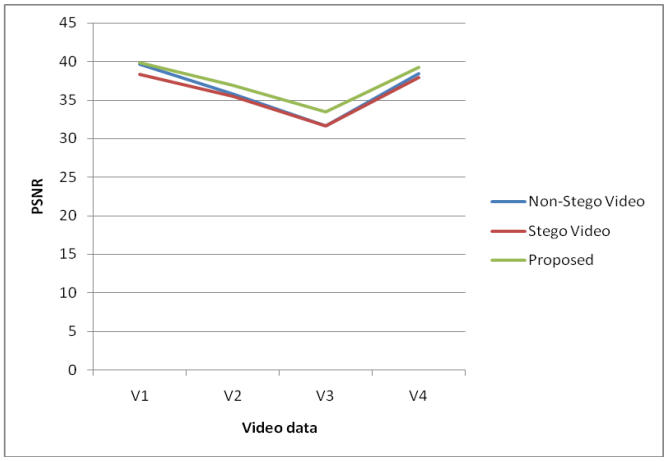


Fig 4 Graph for the comparison of non stego, stego and proposed videos

5. CONCLUSIONS

Information hiding in encrypted media is a new topic of privacy-preserving requirements of cloud data management. The encrypted H.264/AVC bit stream, 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. In proposed system we are used the Qr code, it provides more security. Future work will continue it is supported for all the file formats of video and increase the performance, preserve the quality of video.

ACKNOWLEDGEMENT

I wish to express my sincere thanks to the guide and PG Coordinator Prof. Pankaj Agarkar and Head of Department, Prof. Soumitra Das, as well as our principal Dr.S.S.Sonavne and last but not least, the departmental staff members for their support.

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] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using sidematch," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012
[8] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol.7, no. 2,pp. 826–832, Apr. 2012D.
[9] W. Xu and R. D. Wang, "Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping," Opt. Eng., vol. 50, no. 9, p. 097402, 2011.
[10] 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.

BIOGRAPHIES

Ms. Priyanka R Jakhalekar, PG Student at Dr. D.Y.Patil School of Engineering, Savitribai Phule Pune University.

Email-priyanka.jaklekar@gmail.com

Prof. Pankaj Agarkar, Assistant Professor at Dr.D.Y.Patil School of Engineering, Savitribai Phule Pune University.

Email - pmagarkar@gmail.com