MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

INFORMATION HIDING IN THE ENCRYPTED VIDEO STREAM BY CODE WORD

Jakhalekar Priyanka R, Prof. Pankaj Agarkar

Department of Computer Engineering
Dr. D. Y. Patil School of Engineering Pune, Maharashtra, India

Abstract: *To maintain 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. 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. The extraction of data can be done either in the encrypted or in the decrypted domain.*

Keywords*: Information hiding, encrypted domain, H.264/AVC, codeword substituting.*

1. INTRODUCTION

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.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.In the reversible data hiding schema for encrypted image

after encryption of entire data the additional data can be embedded into the image and it modify in a small parts of encrypted data [6].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.

2. LITERATURE SURVEY

- The reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain [7].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.

- In the field of video, selective encryption (SE) of H.264 video is proposed by doing frequency domain selective scrambling, DCT block shuffling and rotation. 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].

- 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.

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

- The information hiding is performed directly in encrypted video bitstream.
- The proposed scheme can ensure both the format compliance and the strict file size preservation.
- This scheme can be applied by extracting the hidden data either from encrypted video stream or the decrypted video stream

3. MODULE DESCRIPTION

The module includes three main parts i.e Encryption of H.264/AVC Video Stream, Data Embedding, Data Extraction.

1. Encryption of H.264/AVC Video Stream

In this H.264/AVC video encryption scheme, it contains better performance, security, efficiency. After analyzing the H.264/AVC codec property, three parts are there i.e., IPMs, MVDs, and residual coefficients.They are encrypted with stream ciphers.

***a. Intra-Prediction Mode (IPM) Encryption*:** There are four different types of intra coding are supported, which are Intra_4×4, Intra_16×16, Intra_chroma, and I_PCM according to H.264/AVC standard.The Intra_4×4, Intra_16×16, Intra_chroma, and I_PCM that four intra prediction modes (IPMs) are available in the Intra_16 ×16.

***b. Motion Vector Difference (MVD) Encryption*:** The IPMs and the motion vectors should be encrypted for protecting both texture information and motion information. The motion vector prediction is carried out on the motion vectors in H.264/AVC codec, which gives MVD.

***c. Residual Data Encryption*:** The frames I-frames and P-frames should be encrypted to keep high security. In H.264/AVC CAVLC entropy coding is used to encode the quantized coefficients. Each CAVLC codeword can be expressed as the supporters form and size: {Coeff_token, Sign_of_Trailing Ones, Level, Total_zeros, Run_before}

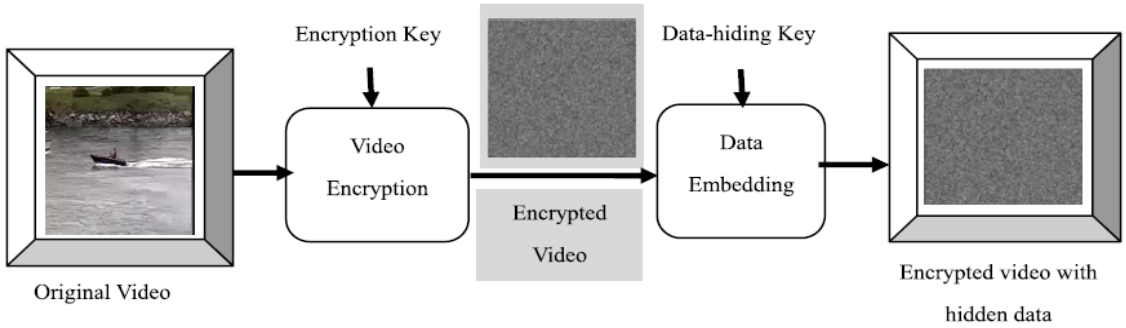


Figure. 1 Video encryption and data embedding at the sender end.

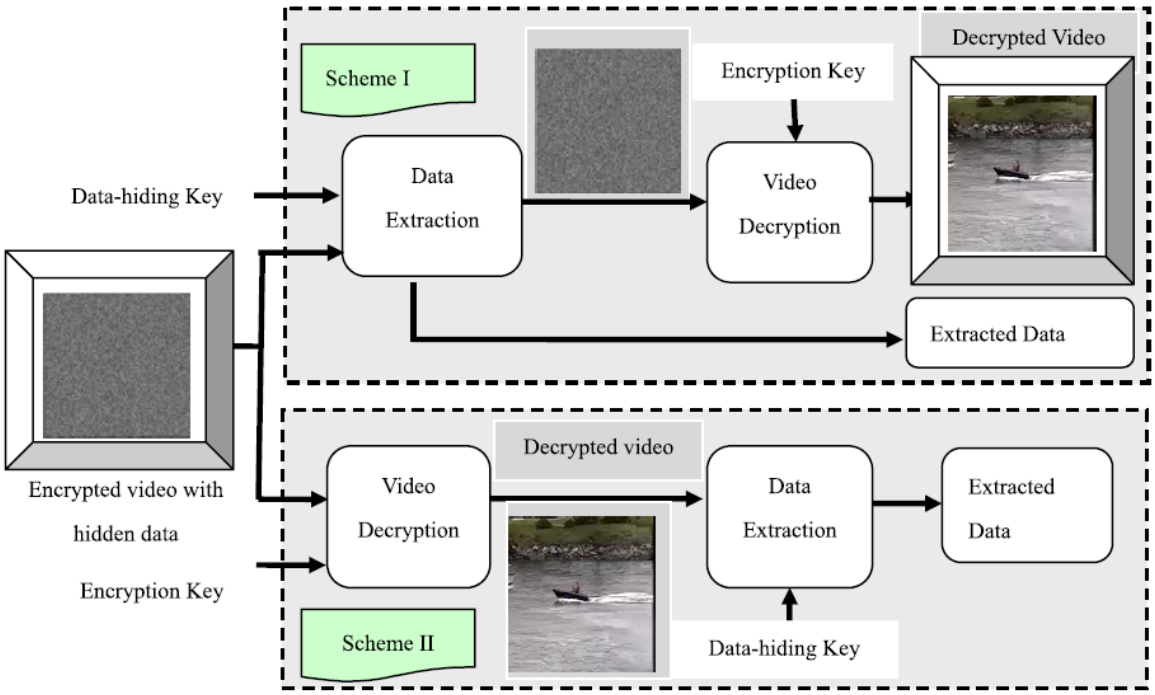
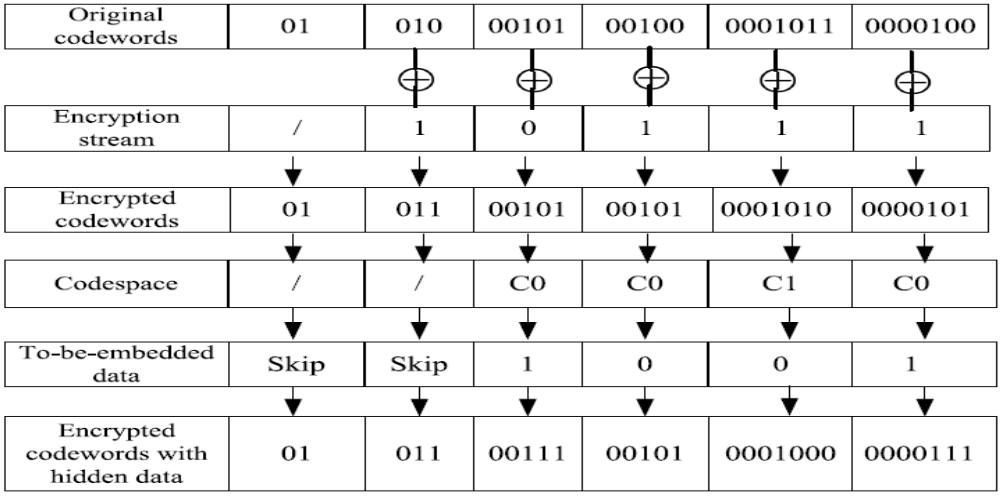


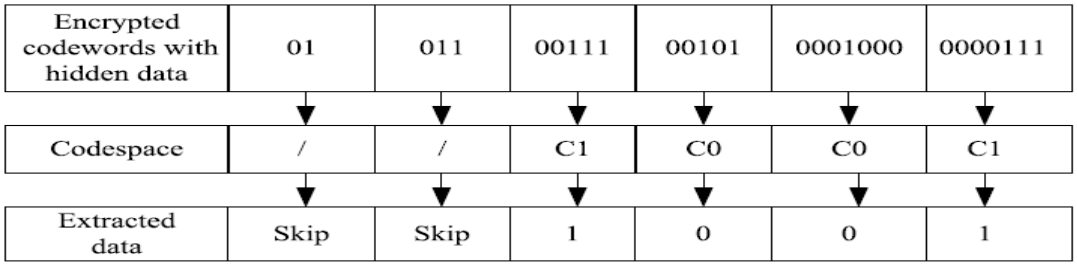
Figure.2 Data extraction and video display at the receiving end in two scenarios.

2. Data Embedding

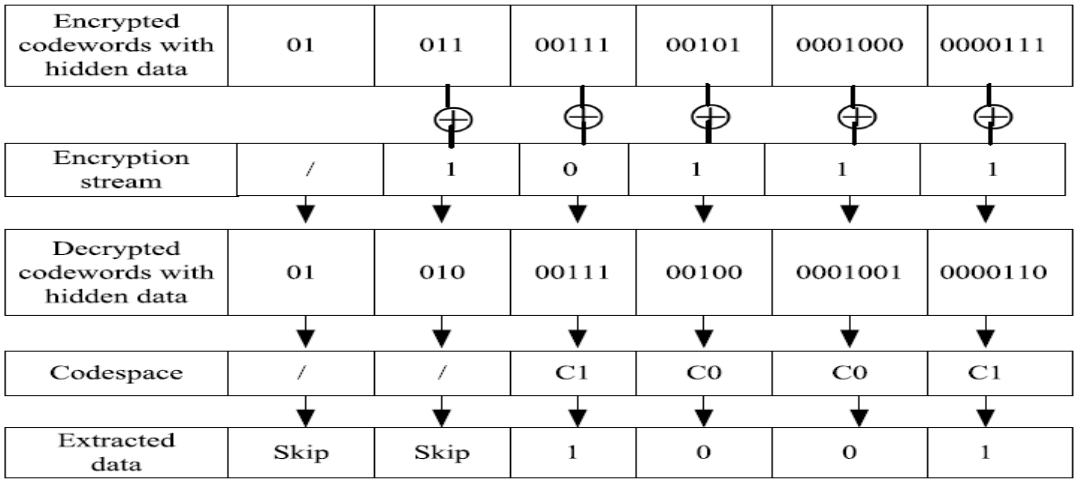
The substituting eligible code word is the one of the technique for data embedding, but the code word substitution should fulfill the limitations. First limitation is after code word substitution the bit stream must remain syntax, compliance so that it can be decoded by the standard decoder. The substituted codeword should have the same size as the original codeword so to keep the bit-rate unchanged it is the second limitation. The data embedding is done by the code word mapping procedure.



(a)



(b)



(c)

Figure.3: An example of data embedding and extraction, (a) Embedding of data.(b) Data extraction in encrypted case (c) Data extraction in decrypted case.

3. Data Extraction

In the extracting process, we extract the received data send by the sender, in that process extracted data should be decrypted and extracted Image received was noisy. The hidden information can be extracted either in encrypted domain or decrypted domain.

a. Image Decryption:

When having an encrypted frame containing embedded data, a receiver initially generates $r_{i,j,k}$ based on the encryption key, and calculates the exclusive-or of the $r_{i,j,k}$ and the received data to decrypt the image. The decrypted bits is denoted as $b'_{i,j,k}$. Clearly, the original five most significant bits (MSB) are obtained correctly. For a certain pixel, if the hidden bit in the block including the pixel is zero and the pixel belongs to S1, or the hidden bit is 1 and the pixel belongs to S0, hiding the data does not affect any encrypted bits of the pixel. So, the three LSB that is decrypted must be same as the original LSB, Which implies that the decrypted gray value of the pixel is similar. On the other hand, if the pixel belongs to S0 then the embedded bit in the pixel's block is 0 , or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB.

b. Data Extraction:

If the receiver has both the data-hiding, then it is possible to extract the embedded data. According to the data-hiding key, the values of L,M and S, the original LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can be extracted from the encrypted image containing embedded data. By putting the LSB of the Np into their original positions, the encrypted hidden data of the Np selected pixels are recovered, and their original gray values can be decrypted correctly using the encryption keys.

a. Encrypted image with data embeded

b. Decrypted version

Figure.4 Encryption and decryption

4. CONCLUSION AND FUTURE WORK

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.For the data embedding we use the code word substitution technique, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain and the data extraction part is either in encrypted or decrypted domain, here we can preserve the confidentiality of the original video content completely. It can be further enhanced by considering the different types of video file format.

ACKNOWLEGEMENT

We thank our guide Prof. Pankaj Agarkar ME coordinator of Computer Engineering for his inspiration and guidance and also thank the Head of Computer Engineering 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] *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*

[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/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.*