Privacy Information Protection of Video Streams based on Codeword Substitution

Yeluru Rajitha
Department of Electronics and Communication Engineering
Narayana Engineering College, Nellore, Andhra Pradesh, India

M. Praveen Kumar
Department of Electronics and Communication Engineering
Narayana Engineering College, Nellore, Andhra Pradesh, India

Abstract— Digital videos are compressed, encrypted and then embedded with secret data for privacy protection during transmission or cloud storage. This can also be used to detect tampering in videos. In this proposal, data is hidden directly in encrypted version of H.264 stream. The three major processes involved in this methodology are encryption of the H.264/AVC video, embedding the data and extraction of the original data. Depending upon the codec's property, the codewords are encrypted with the stream ciphers. The data-to-be-embedded into the video is encrypted using chao's encryption technique and then it is hidden into the video by means of bit replacement method or simply binary text substitution technique. The extraction of the original data can be done either in the encrypted domain or decrypted domain. The experimental results conclude that the size of the video file is strictly preserved and the degradation in video quality caused by data embedding is very less.

Index Terms— Chao's encryption, Codewords, Data hiding, H.264 stream.

I. INTRODUCTION

Due to the rapid advancement of the internet and multimedia, information security has become a major challenge to communication and information technology. Cloud computing is one of the major technology trends that provides large storage and high computation for video data. But cloud storage is prone to many undesirable attacks. So, the data is encrypted before accessing it and to avoid the leakage of the content in videos, data hiding [1] is performed which assures information privacy of the content owner. This technology can be used to verify the data integrity, can be adopted in various applications like medical videos, surveillance videos, multimedia security etc, and can be employed in applications related to video transmission, gray scale mapping and noisy image.

So far, many data hiding techniques in the encrypted domain are proposed. But only few successful schemes have been reported in the literature. Out of them, the most popular schemes are watermarking technique based on paillier cryptosystem [2] and Walsh-Hadamard transform based image watermarking in the encrypted domain using paillier cryptosystem [3]. Both the works focus only on the images but not on the videos. With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will surely become popular in the near future.

In the proposed methodology, the gray scale videos are encoded and decoded using codec of H.264/AVC. Instead of grayscale videos, the proposed method can be extended to color videos, which makes it more useful for real time applications.

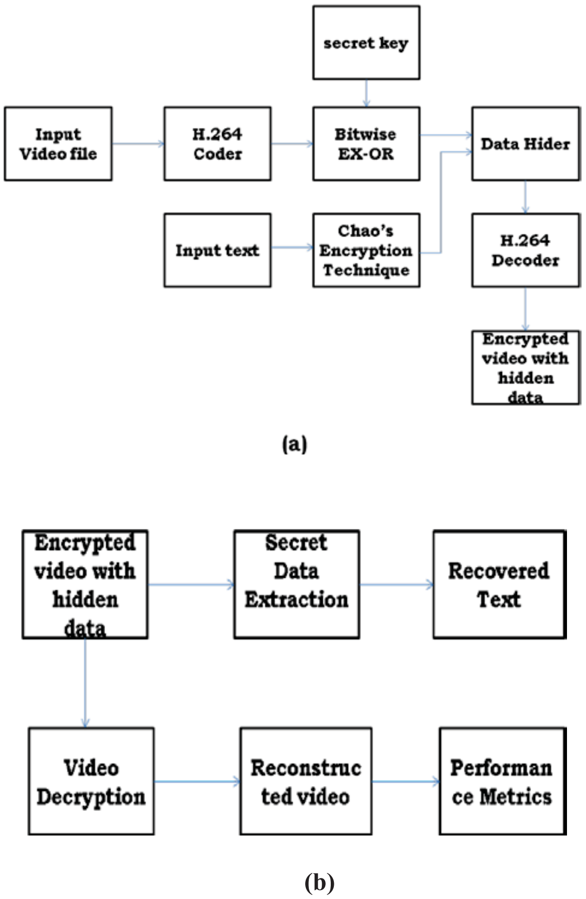
II. LITERATURE SURVEY

In order to maintain the secrecy of a message, many number of encryption and decryption techniques are used. Cryptography and steganography [4] are very well known techniques that are used in communication for the purpose of protecting the privacy information of the content owner. Sometimes, keeping the message secret is not enough, it is very much important to keep the existence of the secret message. The main purpose of cryptography is to make communication unintelligible to those who are not intended for the communication. On the other hand, steganography is the art of hiding the information in other information to provide invisible communication. The strength of steganography can be improved by combining it with cryptography.

In this regard, knowing the research issues [5] for applying data hiding and encryption techniques to videos is necessary. Firstly, the encryption and modified watermarking scheme [6] provides confidentiality and ownership. The main drawback of this scheme is it does not operate on the compressed bit. In order to overcome this drawback, a reversible watermarking [7] has been proposed. In this scheme, the watermark is embedded into the encrypted domain. It provides right access and authentication of the content but the watermarked stream is not fully format complaint. The Selective Encryption Algorithm [8], based on the partial encryption algorithm, meets the requirement of real time and format compliance. Selective data is encrypted in this approach. Lastly, the Enhanced Selective Encryption [9] that operates in compressed domain that is based on CABAC [10] is not suitable for streaming over heterogeneous networks. To overcome the drawbacks of these encryption techniques, a new technique based on chao's data encryption has been proposed, that ensures preservation of file size and format compliance.

III. PROPOSED METHOD

In this proposal, a novel technique for hiding data in encrypted compressed video streams which is based on codeword substitution technique is presented. The three major steps involved in this scheme are H.264/AVC video encryption, data embedding and data extraction . At the sender end, the input video stream is compressed and then encrypted using the standard stream ciphers with encryption keys. Even without knowing the original video content, the data hider can embed additional data into encrypted video stream using bit replacement or codeword substitution method. At the receiver end, the secret data can be extracted either from the encrypted or decrypted domain. Fig 1, represents the block diagram of the proposed scheme, where video encryption and data hiding are shown in part (a), and data extraction and video decryption are depicted in part (b). The methodology which is addressed above involves the following processes:



(a)

(b)

Fig 1: Block Diagram of the Proposed Scheme, Part (a): Video Encryption and Data Hiding, Part (b): Extraction of Data and Video Display.

i. **H.264/AVC:** H.264 is one of the latest video compression standards that convert digital video into a format which requires less storage capacity. H.264 encoder converts the video into a compressed format [11] and the H.264 decoder converts back the compressed one into an uncompressed format. H.264 coder takes the video file as input and divides it into several frames called Group Of Pictures (GOP's). At the sender side, each frame is divided into non uniform blocks of same size called macro blocks. These macro blocks are subjected to Wavelet transform, Quantization and Entropy coding. Then video bit streams are encrypted by carrying out the ex-or operation between the selected bits and a random sequence. This process is repeated until all the frames are encrypted. All the encrypted frames are reconstructed to form the encrypted video.

ii. **Data Encryption:** Chao's data encryption [12] is one of the advanced data encryption standards that provide secure transmission even through unsecure channels. The equation that generates the chaotic sequence is Xn+1=u*x (1-x) where u=3.999 and x=0.0000565. Using the threshold function (I/255) <Xn+1< (I/1)/255, the encryption key value is generated. Bitwise EX-OR operation is carried out between the ASCII values of the input text and the encryption key value.

iii. **Data Embedding:** After chao's data encryption, data hiding is performed to facilitate higher degree of data security during transmission or cloud storage. The bitwise exclusive-or operation is carried out between the bits of the video streams and the sequence generated by the chaotic process using some threshold function. After embedding the data, the encrypted frames are reconstructed to form an encrypted video with hidden data.

iv. **Data Extraction:** The hidden text data is recovered using the bitwise logical operators. Finally, all the recovered text characters are subjected to chao's decryption module to decrypt the data with symmetric keys. Then the video bit streams are decoded using the H.264 decoder to reconstruct each encoded frame. All the frames are concatenated to form the recovered original video. The quality of the video is measures in terms of performance metrics like PSNR, MSE etc.

IV. SIMULATION RESULTS

The implementation of the proposed scheme is done using the MATLAB software. The following are the results of implementation. Figure 2, represents the separated original frames from a man in motion video. Figure 3, is the encrypted frames of the compressed man in motion video. Figure 4, shows the recovered or the video.

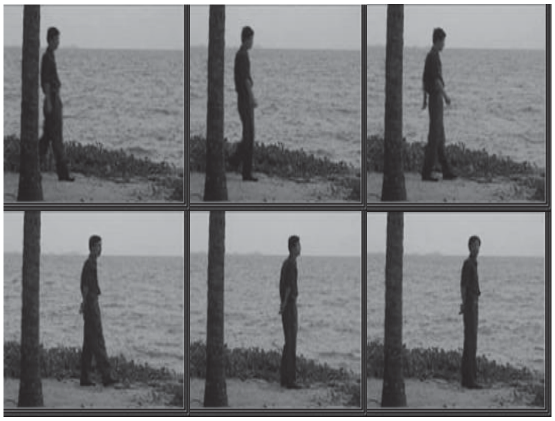


Fig 2: Original Frames of Man in motion video

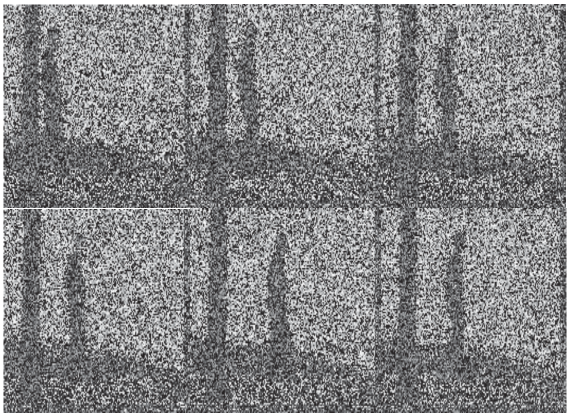


Fig 3: Encrypted compressed frames of Man in motion video

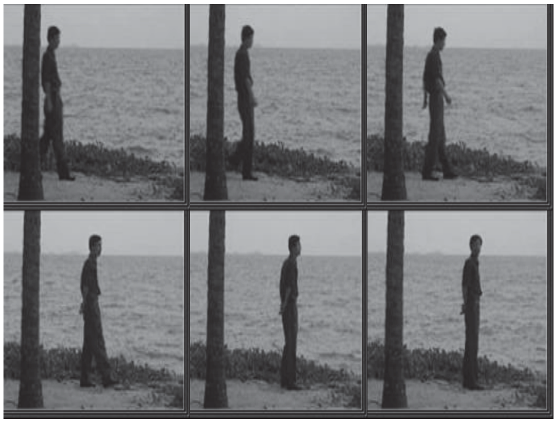


Fig 4: Recovered Original Frames of Man in motion video

The performance metrics like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) talks about the Quality of the video. MSE is calculated using the following equation,

$$\text{MSE}=\sigma_q^2=\frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2 \qquad (1)$$

where 'f' is the original image and 'g' is the reconstructed image. The PSNR between two images in terms of decibels is given by

$$\text{PSNR}=10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (2)$$

Table 1: MSE and PSNR values of Aircraft Video

Video 1 (Aircraft Video)		
Performance Metrics	Without Data Encryption	With Chao's Encryption
MSE	0.3232	0.125
PSNR	53.0357	57.1617

Table 2: MSE and PSNR values of Man in Motion Video

Video 2 (Man in Motion Video)		
Performance Metrics	Without Data Encryption	With Chao's Encryption
MSE	0.4002	0.1548
PSNR	52.1079	56.2339

The graphical representation of the results of comparison of the performance metrics values of MSE & PSNR for without data encryption and with chao's data encryption are shown in the figures 5 & 6 respectively.

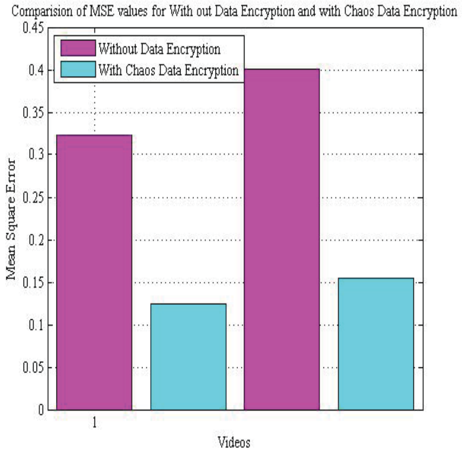


Fig 5: Comparison of MSE values for without data encryption and with chao's data encryption.

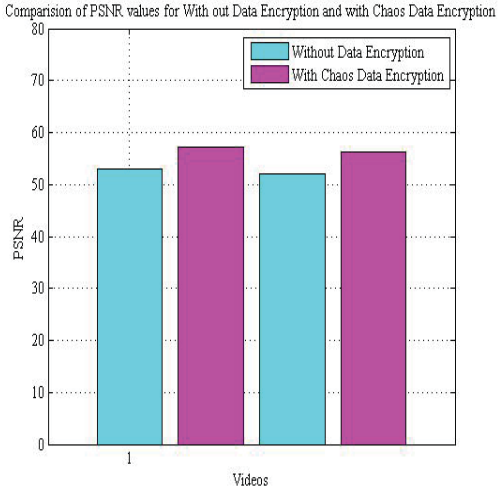


Fig 6: Comparision of PSNR values for without data encryption and with chao's data encryption.

V. CONCLUSION

The encryption of the compressed video bit streams followed by the data hiding technique helps in the protection of videos during transmission or cloud storage. At the sender end, H.264 standard is used for the video compression. Chao's encryption is to encrypt secret text before data embedding. Bit replacement method is used to embed secret text. At the receiver end, the secret text is recovered using the chao's encryption key. The video frames are decrypted and reconstructed to form the original video. Finally, the results show that the proposed methodology gives better bit rates and high PSNR.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, "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] 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, pp. 1–15, 2012.

[4] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: when cryptography meets signal processing," EURASIP Journal on Information Security, Vol. 7, No. 2, pp. 1–20, 2007.

[5] Yogita A Pawar, Prof. Shrilekha Mankhair, "Data Hiding by Code word Substitution (Encrypted H.264/AVC Video Stream)," IJETR, ISSN: 2321-0869, Vol - 3, Issue-3, March 2015.

[6] Shruthi. N, "Enhanced Data Hiding in Encrypted Video Streams," IJTRE, ISSN: 2347 – 4718, Vol 2, Issue 10, June 2015.

[7] A. Sonali Chaudhari and D. Manoj Bagde, "Review on Secret Data Hiding in Encrypted Compressed Video Bit Streams," IJCST – Volume 3, Issue 2, April 2015.

[8] P. Venkateswara Rao (2015), "Data Hiding in Video Streaming by Code Word Substitution," IJRITCC- Volume 3, Issue 3, March 2015.

[9] S. Chandra Mohan and M. Manasa, "Data Hiding in Encrypted Compressed Videos for Privacy Information Protection," i-Manager's Journal on Image Processing, Volume 2 , Issue 2, June 2015.

[10] D. K. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," Proceedings of IEEE ICME, Singapore, pp. 117–121,2010.

[11] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview Of The H.264/AVC Video Coding Standard," IEEE Transaction on Circuits Systems Video Technology, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[12] Sangeeta Mishra, Sanjeev Ghosh Payel Saha, "Chaos Based Encryption Technique for Digital Images" Kandivali (E), Mumbai-400101, 2010.