RESEARCH ARTICLE OPEN ACCESS

Review on Secret Data Hiding in Encrypted Compressed Video Bit Streams

Sonali.A.Chaudhari [1], Prof.Manoj.D.Bagde [2]
Research Student [1][, Assistant Professor [2]
Department of Electronics and Communication
G.H. Raisoni Institute of Engineering & Management
Jalgaon
Maharashtra - India

ABSTRACT
To protect videos during transmission or cloud storage, encryption of compressed video bit streams and hiding privacy information can be done. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. It is also for the purpose of content notation and tampering detection. Here, data hiding directly in the encrypted version of H.264/AVC video stream .It has following three parts, H.264/AVC video encryption, data embedding, and data extraction. In H.264/AVC codec, the code words of intra prediction modes, motion vector differences, and residual coefficients are encrypted with stream ciphers. A data hider may embed additional data in the encrypted domain by using bits replacement technique, without knowing the original video content. Chaos crypto system is used here to encrypt/decrypt secret text data before/after data embedding/extraction.

Keywords:- Bits replacement technique, Chaos crypto system, Encrypted bit streams, H.264/AVC..

I. INTRODUCTION

Cloud computing has become an important technology, which provides efficient computation and large-scale storage solution for video data. Cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content can be accessible in encrypted form. The ability of performing data hiding directly in encrypted H.264/AVC video streams avoid the leakage of video data, this protects privacy and security concerns with cloud computing.[1]

For example, a cloud server can embed the additional information into an encrypted H.264/AVC video by using data hiding technique. With this the server can manage the video and crosscheck its integrity without knowing the actual content, thus helps to protect privacy and security. This technology can be used in other application. For example, when surveillance videos or medical videos have been encrypted for protecting the privacy of the people, a database manager can add the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain.

II. RELATED WORK

Till now, few successful data hiding schemes in the encrypted domain have been found in the open literature.[2] A watermarking scheme using Parlier cryptosystem is proposed based on the security requirements of buyer-seller watermarking protocols[3]. In Walsh-Hadamard transform image watermarking algorithm is used in the encrypted domain using Paillier cryptosystem is presented [4]. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image shows high overhead in storage and computation. Note that, several research on reversible data hiding in encrypted images are found recently. The encryption is performed by using bit-XOR operation. In these methods, the host image is in an uncompressed format.

In [5] a robust watermarking algorithm is proposed to embed watermark into compressed and encrypted JPEG2000 images.

As development of the multimedia and Internet technology, more information including images, audio and other multimedia, are being transmitted over the Internet. Due to some internal features of images, such as large data capacity and high correlation among pixels, early encryption algorithms are not suitable for practical image encryption. Recently, the image encryption technologies based on chaos theory have been developed to overcome the disadvantages present in early encryption techniques.

III. PROPOSED SCHEME

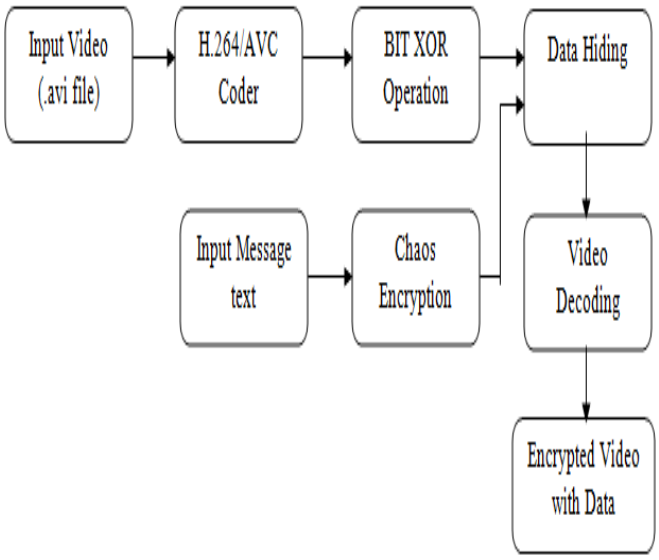

Fig.1 Video Encryption and Data Hiding

In this section, a novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, the processing system involves H.264/AVC Coder, Chaos encryption, and Bits replacement to accomplish better compression performance and efficient data hiding. The content owner encrypts the original H.264/AVC video stream with encryption keys using standard stream ciphers 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 Chaos encryption for text, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

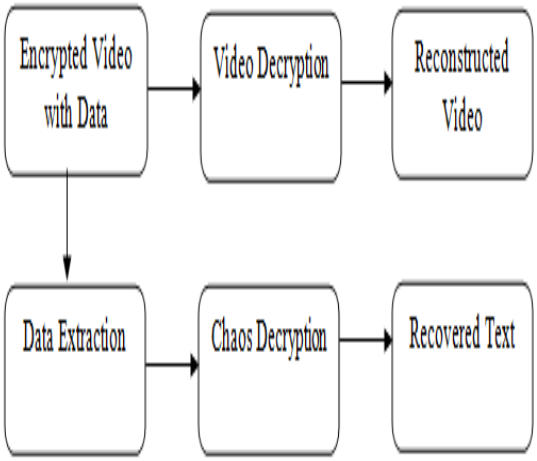

Fig. 2 Data Extraction And Video Decryption

Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bit stream like what the traditional ciphers do because of the following two constraints, i.e., format compliance and computational cost. Alternatively, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt.

A. H.264/AVC Coder

H.264 is a standard used for video compression, It converts digital video into a format that requires less capacity when it is stored or transmitted. Video compression (or video coding) is an important technology for applications such as digital television, DVD-Video, videoconferencing, mobile TV and internet video streaming. In H.264, encoder converts video into a compressed format and a decoder convert's compressed video back into an uncompressed format [8].

B. Chaos Cryptosystem

Chaotic systems are suitable for data message encryption because they have good properties as follows: 1) chaotic motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain. 2) Flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise.

The discrete sequences of the chaotic dynamical system are gained by the following equation.

$Xn+1 = Tn (xk)$.

The basic Logistic-map is formulated as,

$f(x)=\mu x(1-x)$

Where, x (0, 1). The parameter μ and the initial value x_0 can be adopted as the system key (μ, x_0). The research result shows that the system is in chaos on condition that $3.569 < \mu < 4.0$.[6]

C. Bits Replacement Technique

The frequently used steganography method is the technique of LSB substitution. Every pixel of gray-level image consists of 8 bits. One pixel can hence display 28 =256 variations. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.[7]

IV. CONCLUSIONS

System presents an algorithm to embed additional data in encrypted H.264/AVC bit streams, which consists of video encryption, data embedding and data extraction phases. 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 requires partial decompression of the video stream thus making it ideal for real-time video applications. It preserve the confidentiality of the content completely.

ACKNOWLEDGMENT

Authors would like to express sincere thanks and deep gratitude to Prof. H. K. Bhang ale, Head of E&C Department who extended wholehearted co-operation to complete this work successfully.

Authors are also express deep and sincere gratitude to the principal, G.H. Raisoni institute of engineering & management, Jalgaon for being a constant source of inspiration.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution",Vol. 9, No. 4, April 2014.

[2] 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.

[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] 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.

[5]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.

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

[7] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[8] 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.