IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Ultra Embedder – A Secure Data Transmission By Hiding Data In Audio/Video Files

Litty Mariam Biju[1], Sreelekshmi S Kumar[2], Rakhi R[3] , Rinta Mariam Jose[4], Minu Lalitha Madhavu[5]

[1] littymariambiju18@gmail.com , [2] sreelekshmiskumar246@gmail.com ,
[3] rakhiretnan@gmail.com , [4] rintamariamjose@gmail.com , [5] minulalitha@gmail.com

Abstract

To maintain security and privacy, digital video sometimes needs to be stored and processed in an encrypted format. It is necessary to perform data hiding in these encrypted videos, for the purpose of content notation and/or tampering detection. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. Here, a novel scheme of data hiding directly in the audio/video stream is proposed, which includes the following three parts, encryption, data embedding, and data extraction.

Index Terms-Data hiding, encrypted domain.

1. Introduction

Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for securing data transfer.

Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this paper, a data hiding system based on video/audio steganography and cryptography is proposed to secure data transfer between source and destination.

Audio/video medium is used for the visual cryptography and a Bit Shifting algorithm is employed to encode the message inside the audio file. Thus the objective is to provide security for our data by hiding into encrypted video streams. This paper proposes an authentication algorithm which uses visual cryptography to provide security for data. Visual cryptography scheme is one of the most secure techniques for privacy, that allows the encryption of secret image or data by transferring it into the secure share and the

decryption is done without an computation devices.

The proposed system was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. The system is therefore, recommended to be used by the internet users for establishing a more secure communication.

2. Literature survey

2.1 Secure Video Processing: Problems and Challenges

The application considered in this paper is secure online video management [1], where users store their private videos in encrypted form on remote servers & server performs processing tasks over encrypted videos. There are three key components in the system: pre processing the video to obtain auxiliary information[2], encryption of the video, and computation in the encrypted domain by the server. Obtaining auxiliary information is more often necessary to assist the secure computation by the server, which would otherwise highly computationally intensive or incur large communication difficulty. Videos can be encrypted before or after compression with different computational complexity and different level of protection from full encryption to partial encryption. The security and statistical analysis performed further verify the effectiveness of the proposed security system for H.264/SVC.

2.2 Efficient Security System for CABAC Bin-Strings of H.264/SVC

The distribution of copyrighted scalable video content to differing digital devices requires protection during rendering and transmission. In this paper[3], we propose a complete security system for H.264/ scalable video coding (SVC)[4] video codec and present a solution for the bit rate and the format compliance difficulties by careful selection of entropy coder syntax elements for selective encryption, and problem of managing the multiple layer encryption keys for distribution of scalable video.

A key management protocol, multimedia Internet keying protocol, is implemented for the hierarchical generation of key mechanism, in which the subscriber has only one key for encryption to unlock all scalable layers that have been subscribed to. The proposed system is highly suitable for the video distribution to users who have subscribed to a varying degree of

video quality on the devices with medium to high computational resources.

2.3 Secure Advanced Video Coding Based On Selective Encryption Algorithms

Advanced video coding is recently announced and widely used, although the according protection means have not been developed thoroughly. In this paper [5], a secure AVC coding scheme is presented that is based on partial encryption algorithms.

During AVC encoding, such type of sensitive data as intra-prediction mode, residue data and motion vector are both encrypted partially. Among them, the infra-prediction mode is encrypted based on the exp-Golomb entropy coding, the intra-macro block's DCs are then encrypted based on context based adaptive variable length coding (CAVLC), and infra macro block's ACs and inter-macro block's MVDs are sign-encrypted with the stream cipher followed with variable-length coding.

This encryption scheme is secure in perception that keeps format compliance, and obtains high time efficiency though reducing encrypted data volumes [6]. These properties make this practical to incorporate encryption/ decryption process into compression/ decompression process, and thus it is suitable for secure video transmission or for sharing.

2.4 Overview of the H.264/AVC Video Coding Standard

H.264/AVC is the newest video coding standard of the ITU-T Video Coding Experts Group and ISO/IEC Moving Picture Experts Group[7]. The main goals of H.264/AVC standardization effort have been enhanced performance of compression and provision of a "network-friendly" video representation addressing "conversational" and "non conversational" applications.

H.264/AVC has achieved a significant improvement in efficiency of rate-distortion relative to existing standards. This article [8] provides an overview of technical features of H.264/AVC that describes profiles and applications for the standard, and outlines the history of the process of standardization.

2.5 Watermarking in H.264/AVC Compressed Domain Using CAVLC

A new real-time watermarking technique [9] based on H.264/AVC video standard is proposed. The algorithm works in the compressed domain by embedding watermark bits into quantized DCT coefficients of 4×4 blocks of the I-frame during the Context-based Adaptive Variable Length Coding(CAVLC) process.

CAVLC offers a lower computational complexity which is efficient to the algorithm. During watermark extraction, the

entire video doesn't need to be decoded, which meets the requirement of the real-time processing. The scheme yields tiny bit-rate change after watermarking and the degradation of video quality is negligible.

3. Proposed System

In our system we are not following the regular encryption, decryption techniques. We are using an algorithm called BitShift in Random Cycle Order i.e. totally four different types of BitShift algorithms are used randomly to encrypt the data. This Encryption is embedded into an audio or video file. Again it will be embedded into another media. This double embedding increases the level of security. Password protection of this entire works gives an additional security. When coming to the decrypting section we have two proposed schemes that define decrypting data either from the encrypted source or from the decrypted source.

3.1 Encryption

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 bitstream 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.

3.2 Embedding

In merger inputs are Audio/ video, Image/Text and secret message file with password. Then merge the all requirements and then send to receiver. The target file is encrypted using an algorithm called Bit Shifting and it is embedded into an audio or video or any media file. The original format of resultant media file doesn't change in its original format and it can be run in the player, we can't find any encrypted data inside it.

- **Single Embedding :**

In single embedding source file is embedded with an audio file only. Here the inputs consist of a data to be hided and the audio that the data should be embedded. Now the process consists of both the audio and data is encrypted and the data is embedded within the audio. The output will be a single audio file.

- **Double Embedding :**

In double embedding source file is embedded with both an audio file and a video file. Here the inputs consist of a data to be hided, an audio and a video file that the data should be embedded. Now the process consists of both the audio, video

and data is encrypted and the data is embedded within the video. The output will be a single video file**.**

3.3 Extraction

This module can get the merged file after to give the password. Then extract the merged file and call the result window module for open extracted file. In this scheme, the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple.

• **Scheme I** Encrypted Domain Extraction

Here the hidden data can be extracted without decrypting the video or audio file used for embedding.

• **Scheme II** Decrypted Domain Extraction

Here the hidden data can be extracted only by decrypting the video or audio file used for embedding.

3.4 Advantages

- Two schemes for embedding which enables the user to embed files with the required level of security needed.
- Embedding data with any specified formats such as different formats of Audio/Video and with Image files also.
- Password security for embedded files provides an additional level of security.
- Two schemes for De-embedding which makes the user to decrypt the required files only.

4. Conclusion

The fundamental advantage of this system is to create shield for your secret data. The system is designed as any user with basic knowledge can run the system. Two embedding schemes are provided in order to choose the level of security.

5. Future Enhancement

An online platform for the same system can be developed to share embedded files within the system aswell as via different communication means. In future it can be enhanced to support portable devices like android cell phones.

4. REFERENCES

[1] F. Liu and H. Koenig,“A survey of video encryption algorithms,” Computers & Security, vol. 29, no. 1, pp. 3–15, 2010.

[2] A.Massoudi, C.De Vleeschouwer, F. Lefebvre, B. Macq, and J.-J. Quisquater, “Overview on selective encryption of image & video: challenges & perspectives,” EURASIP Journal Information Security, vol. 2008, pp. 1–18, 2008.

[3] An efficient security system for CABAC bin-strings of H.264/SVC, M. N. Asghar and M. Ghanbari, *IEEE Trans.*

Circuits Syst. VideoTechnol., vol. 23, no. 3, pp. 425–437, Mar. 2013.

[4] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*vol. 53, no.10, pp. 3976–3987, 2005.

[5] Secure advanced video coding based on selective encryption algorithms, S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, *IEEE Trans.Consumer Electron.*, vol. 52, no. 2, pp. 621–629, May 2006.

[6] A. Kudelski, *Method for scrambling & unscrambling a video signal*, December 1994.

[7] "Draft ITU-T recommendation and final draft international standard of joint video specification (ITU-T Rec. H.264/ISO/IEC 14-10 AVC", *Joint Video Team (JVT) of ISO/IEC MPEG and ITU-T VCEG JVT-G050*, 2003.

[8] Overview of the H.264/AVC video coding standard, Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, *IEEE Trans. Circuits Syst.Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[9] Watermarking in H.264/AVC Compressed Domain Using CAVLC Qian Li College of Information Science and Engineering, Ningbo University, Ningbo 315211, China.

About Authors

Litty Mariam Biju pursuing B.Tech. Degree in Computer Science and Engineering from Kerala University, India.

Sreelekshmi S. Kumar pursuing B.Tech degree in Computer Science and Engineering from Kerala University, India
.

Rakhi R pursuing B.Tech degree in Computer Science and Engineering from Kerala University, India.

Rinta Mariam Jose pursuing B.Tech. degree in Computer Science and Engineering from Kerala University, India.

Minu Lalitha Madhavu received B.Tech. degree in Computer Science and Engineering from Rajiv Gandhi Institute of Technology , MG University, India, received M.Tech. degree in Technology Management from Kerala University, India. Currently, she is Assistant Professor at Sree Buddha College of Engineering, Kerala University, India.