Triple-AES Secure Video Steganography System

Gadha M M

Student, Computer Science and Engineering, Calicut University
Malabar College of Engineering and Technology, India

Abstract— *Need for digital video communication is increasing day by day. In the very near future itself, video may become the dominant type of traffic over the Internet. A Secure scheme of digital video communication is presented in this paper using a combination of both cryptography and steganography. Multiple encryptions at the transmitter side followed by data hiding and corresponding decryptions and the data retrieval at the receiver side is proposed here for preserving security. Triple-AES encryption standard is used here for doing encryption. H.264/ Advanced Video Coding (AVC) standard being one of the most commonly used formats for the distribution of video content; it has been selected for the transmission. At the receiver side, embedded data can be extracted both from the encrypted and decrypted version of the digital video. This combinational system will satisfy security, file size preservation and format compliance of the video data in transmission over an open channel.*

Keywords— *H.264/AVC Video Coding, LSB, Spread Spectrum, Triple-AES.*

I. INTRODUCTION

The emergence of internet has brought so many exciting facilities to human. Digital communication systems' using video and voice is an example. But in such cases security of the data being communicated is an important issue. Cryptography, steganography etc. are some techniques which are meant to bring security of the information used in various applications. Cryptography or secret writing is a method of securing data in a particular form so that only those for whom it is intended can read and process it. Whereas, Steganography is a practice of concealing messages or information either textual, image etc. within other known (non-secret) text or data. Ideally, anyone scanning the data will fail to know it contains some hidden information within it. Even though these techniques can preserve security to some extent, loopholes are there. Both techniques are sometimes vulnerable. Attacks can be possible if it is not used efficiently. In this paper, a combination of these two techniques is suggested in which the cryptographic part is much more secure than the previous efforts till date. A secure video communication system in which multiple encryptions at the transmitter side and the corresponding decryptions at the receiver side is proposed here. In the cipher form of video data, image hiding is also proposed for better security. Since multiple encryptions bring a number of times greater security, the encrypted video itself is much more secure. Here, data hiding brings additional security. So the system as a whole can be used for secure transmission of digital videos.

Triple-AES encryption method is used here for doing multiple encryptions at the sender side. It was developed to address the obvious flaws in Advanced Encryption Standard without designing a whole new cryptosystem. And then embedding of the secret data is done by using the LSB and spread spectrum concepts. And at the receiver side, triple-AES decryptions and data extraction can be done producing the original video and the secret image sent. Here, the data extraction can be possible from encrypted as well as decrypted versions of the video data sent from the transmitter. The video transmission system proposed here can be made use in various applications like medical, social media communication and road offence handling systems.

II. BACKGROUND STUDY

Cryptographic techniques began thousands of years ago. Cryptography in earlier systems was solely concerned with converting messages into unreadable formats to protect the message's content during its transmission. Cryptography and also cryptanalysis - "breaking" of codes and ciphers, had its parallel development. In this era, cryptography has grown from basic message confidentiality to include message integrity checking, identity authentication of transmitter or receiver and digital signatures etc. Selective encryption approaches are for doing encryption only on certain, carefully selected bits of the video leaving the rest of the bits unencrypted. Selective encryption using Triple-AES encryption standard is used in this paper. The Triple Advanced Encryption Standard (triple-AES), the symmetric block cipher which was ratified as a standard by the same organization of Advanced Encryption Standard ie., the National Institute of Standards and Technology of the United States (NIST), was chosen using a process that was markedly more open and transparent than its predecessor standard, the AES.

The first description of the use of steganography dates back to the Greeks. A very common steganographic scheme in history was the use of chemical substances to conceal information. Today, steganography is researched both for legal and illegal reasons. Steganography is not the same as

cryptography. Even though both methods provide security, to add multiple layers of security, it is always a good practice to use Cryptography and Steganography together. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. Till now, few successful hybrid implementations of cryptographic and steganographic techniques have been reported in open literature. Among them, most of the works are focused on images. Efforts focusing on video are very few. H.264/AVC being one of the most popularly used format, researches are going on based on this standard and feasibility of its applications. It is a block-oriented motion-compensation-based video compression standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC JTC1 Moving Picture Experts Group (MPEG). The project partnership effort is known as the Joint Video Team (**JVT**). The ITU-T **H.264** standard and the ISO/IEC **MPEG-4 AVC** standard (formally, ISO/IEC 14496-10 – MPEG-4 Part 10, Advanced Video Coding) are jointly maintained so that they have identical technical content.

III. Proposed System

The triple-AES secure video steganography system is a safer mode of video communication system. That is, the product has video transmission capability which is much more efficient than previous attempts. In this system, the sender can encrypt selective parts of the h.264/AVC video, which is to be transmitted, multiple times ensuring multiple level of security. And this multiple level encryption is followed by image hiding by using the spread spectrum technique.

Here spreading is done at the LSB position of the encrypted video, which brings confidentiality. Fig.1 shows architecture for the transmitter.

At the receiver side, there are two options for obtaining the original video and the image which is hidden in it. Using the first option, data extraction from the encrypted domain is done. Here, first data extraction is performed by the reverse spread spectrum using LSB concept to obtain the hidden image and then triple-AES Decryption is done for getting the Original video from the cipher video output.

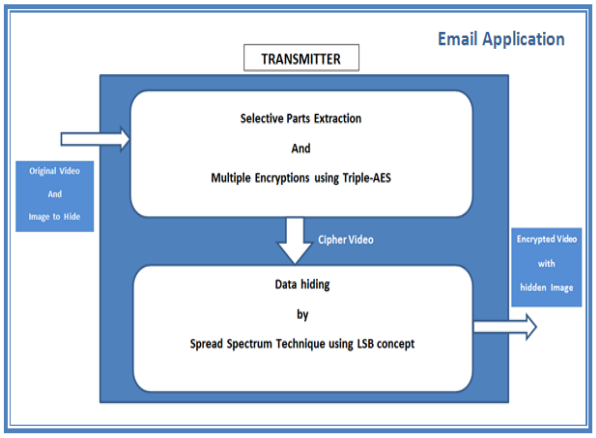

Fig. 1 Architecture of Transmitter

And in the second option, data extraction is done from the decrypted domain. Here, first triple-AES decryption followed by the reverse spread spectrum using LSB concept is applied for getting the image hidden in it. Fig. 2 shows architecture for the receiver with two different schemes.

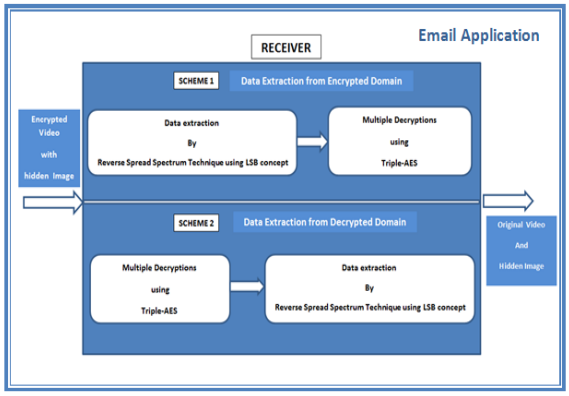

Fig. 2 Architecture of Receiver

IV. Major Module Description

Triple-AES secure video steganography system is divided into five main modules. The basic modules of this project include:

- Admin login and socket creation.
- Client login and secure transmission of encrypted video attachments to receiver.
- Multiple encryptions on the selective data of the video using triple-AES Encryption.
- Embedding of the secret data by spread spectrum techniques using LSB insertion.
- Receiver login and loading email inbox
  - Data extraction from the encrypted domain.
  - Data extraction from decrypted domain.

A. *Admin Login And Socket Creation*

The admin login is the first step. Admin connects the database to check the login credentials. If

username and password is authenticated, then admin creates a socket and waits for a client message. Any client messages can be caught and displayed through the admin. If there is an admin process is running, then admin instance already running message is also displayed.

B. *Client Login and Secure Transmission of Encrypted Video Attachments to Receiver.*

Then client or user login can be possible by connecting with the database. In the user panel, there is a provision to set the server IP and also the email settings needed. In that panel, user can also be able to set his email username and password. The client can send email using the setting entered.

C. *Multiple Encryptions on Selective Parts of the Video using triple-AES Encryption Standard.*

Selective encryption is a technique of encrypting some parts of a compressed data file. Instead of encrypting the whole file bit by bit, only highly sensitive bits are changed here. We propose a technique that selectively encrypts some parts of compressed video file multiple times while guarantee the security of the original file. We reduce the time for encrypting video file, but also system complexity. The idea of this scheme is to encrypt different levels of selective parts of H.264/AVC stream by triple-AES encryption standard.

D. *Data Embedding using Spread Spectrum using LSB Concept*

Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is deliberately varied. This result in a much greater bandwidth than the signal would have if its frequency were not varied.

The secret data to embed is encoded by using the method of least significant bit modification n-times. Replacement of least-significant bits (LSBs) n-times in digital video will in effect cause Spreading of data for information hiding. For the non-expert steganographer, its ease of embedding, high capacity, and visual imperceptibility may prove attractive.

E. *Receiver Login and Receiving Encrypted Video containing hidden Data*

Then receiver or user login can be possible by connecting with the database. In the user panel, there is a provision to set the server IP and also the email settings needed. In that panel, user can also be able to set his email username and password. Receiver can load email inbox and open mails in it.

- ***Data Extraction From Encrypted Domain***

First Reverse Spread Spectrum technique from the LSB position is applied to get the hidden image from the video. And then this video is decrypted three times using triple-AES decryption to get the original video back.

- ***Data Extraction From Decrypted Domain***

Here Hidden image is obtained from the Decrypted Video. So decryption using triple-AES is done first followed by the hidden image extraction from the decrypted video.

V. PERFORMANCE ANALYSIS

The performance of proposed system compared to the existing system with single level encryption is very different. The number of bytes encrypted versus time was measured. There were measurable difference in encrypting there two versions of the system. The graph plotted for these two systems are given in Figure 3 and 4.

So, multiple encryptions can be used to enhance the security. In short, the System is more secure than the existing approaches.

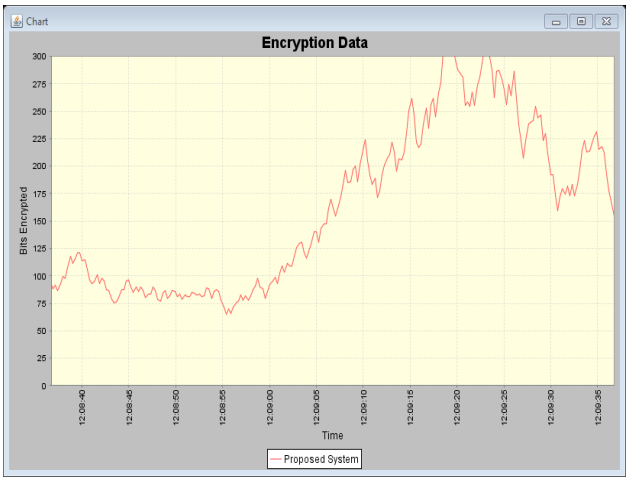

Fig.3 Performance graph of proposed system

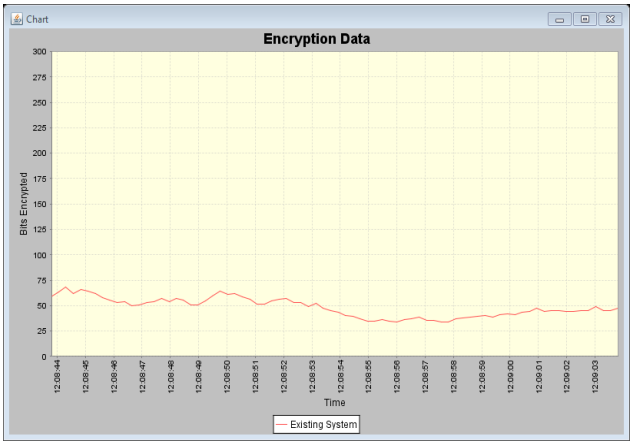

Fig.4 Performance graph of existing system

VI. CONCLUSIONS

This project is an attempt to satisfy the security requirements in the video transmission applications. In this paper, a secure video transmission scheme having

multiple level encryption and data hiding is presented. The system preserves 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 thus making it ideal for real-time video applications. Data embedding is done by using LSB and spread spectrum concepts. LSB Insertion is simple and easy. Spread Spectrum techniques are technologically superior to conventional narrowband modulation techniques in a number of important areas.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, *Fellow, IEEE*, "*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] J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, "*An improved selective encryption for H.264 video based on intra prediction mode scrambling*," J. Multimedia, vol. 5, no. 5, pp. 464–472, 2010.

[3] X. P. Zhang, "*Reversible data hiding in encrypted image*," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon,"*Secure Spread Spectrum Watermarking for Multimedia,"* Ieee Transactions On Image Processing, VOL. 6, NO. 12, December 1997.

[11] N. Keshaveni , S. Ramachandran and K.S. Gurumurthy," *Implementation of Context Adaptive Variable Length Coder for H.264 Video Encoder*," International Journal of Recent Trends in Engineering, Vol 2, No. 5, November 2009.

[12] B.Raja Rao, P.Anil Kumar, M.Nagu and K Rama Mohana Rao "*A Novel Information Security Scheme using Cryptic Steganography* " Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 327-332