A Survey on Video Encryption Techniques

Yogita Negi*

Abstract

Various video encryption techniques are proposed to encrypt the videos and used for obtaining highly encrypted videos

The paper focuses on different existing methods for video techniques. It focuses on the full or selective encryption techniques & various schemes under it.
This survey provides information about the existing methods and their improvements, hence providing a platform for new researchers for innovating new Techniques for further research.

Keywords: Deformation & formation Algorithm, I-frames, Chaos, VEA

Introduction

Due to rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important. The main goal of cryptography is keeping data secure form unauthorized attackers. Therefore data is encrypted through process of Encryption. The reverse of data encryption is data decryption.

With digital video transmission, encryption technologies are needed that can protect digital video from attacks during transmission. Due to the huge size of digital videos, they are usually transmitted in compressed formats such as MPEG, or H.264/AVC (standard used for video compression).

Need of Video Encryption

Encryption of images and videos are important due to following reasons:

1. For preventing unwanted viewing of transmitted video, for example from law enforcement video surveillance being

**Asstt. Professor, B.C.I.I.T, Delhi, India. Email: yogita.negi053@gmail.com*

Authors are grateful to the anonymous referees for comments and suggestions for improving the text and contents of the paper. Authors alone are responsible for any errors/mistakes still remaining in the paper.

relayed back to a central viewing centre.
2. To protect the private multimedia messages that is exchanged over the wireless or wired Networks.
3. Video Encryption is helpful in securing videos used in services like video on demand (VOD), Video conferencing-learning.
4. For protecting medical videos which may contain private information of a patient from unauthorized access by malicious users.

This study is based on video encryption based on study of Deformation/Formation Algorithm which is useful in protecting various medical videos that contain private information of patients and requires sharing among various doctors that belongs to different department of hospital. In first part of study I have focused on various prevailing algorithms used for video encryption. Deformation/formation algorithms based on concept of I-frames is discussed.

In second part of study, I have mentioned literature reviews of various research papers.

Basic Concept of Video Encryption:
The encryption and decryption of a plain text or a video stream can be done in two ways:

A. Secret Key Encryption:
A single secret key can be used to encrypt and decrypt the video streams. Only the sender and the receiver have this key. Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted. Most common algorithms in these categories are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

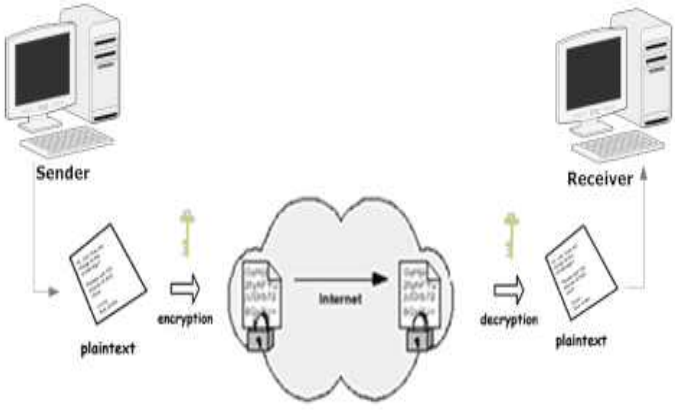

Figure 1: Symmetric key Algorithms [Ref. 1]

Public key encryption:
There are two keys, one for encryption and the other for decryption. The public key, which is known for all senders, is used for encryption. While the private key, which is owned only by the receivers, is used for decryption. [Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey"]

It is based on a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and solves the problem of secret key distribution by using two keys instead of a single key .

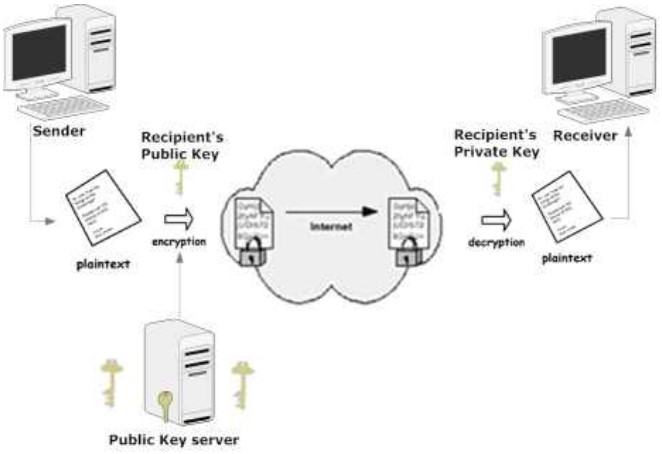

Figure 2: Asymmetric key Algorithms [Ref. 1]

Various approaches used for encryption

Full-encryption:
A video encryption algorithm that performs encryption on the entire video bit stream belongs to this class of algorithms. It suitable for real time video as requires heavy computation and has slow speed.

Selective Encryption:
Also known as partial encryption & is a subcategory of variable encryption. The algorithms in this class selectively encrypt the bytes within video frames. As these algorithms are not encrypting each and every byte of video data, it reduces computational complexity.

Various Digital video encryption schemes

Naïve Approach:
It is a type of full encryption approach in which a conventional cryptosystem is used in the encryption step. The most straight-forward method to encrypt every byte in the whole Moving Picture Experts Group (MPEG) stream using standard encryption schemes such as DES or AES.

However, this algorithm not applicable for heavy video, because it is very slow especially when we use triple DES. Because of the encryption operation the delay increases therefore it is not suitable for real time video encryption. [M. Abomhara, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques"]

Pure Permutation Algorithm:
It simply scrambles the bytes within a frame of MPEG stream by permutation.[Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey"]

Zig-Zag Permutation Algorithm:
In this method, instead of mapping the 8x8 block to 1x64 vector in "Zig-zag" order, it maps the individual 8x8 block to a 1x64 vector by using a random permutation list (secret key).[M. Abomhara,

Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques"]

Chaos Based Encryption Algorithms:
This is one of the popular algorithms in the field of neural network to perform encryption & decryption as it is a low cost algorithm & is suitable for large amount of data.

Deformation & formation Algorithms:
In this form, encryption using key image is used perform full encryption process. In this new scheme for video encryption which based on encryption of I-frame (video frame).

Deformation Algorithm:

- In this method, a video Vi is divided into I1, I2...In (where n=1, 2…..n) video frames such as frames are collected then take frame one by one.
- Then, select two key Images namely K1, K2 as key frames for encryption and decryption process, so this key images can be send through secure channel.
- Each frame has dimension of "w* h".
- Let αi denotes any sorting permutation like quick sort, heap sort of Ii & α(Ii) is image with sorted pixels from 'Ii'.
- Video stream is collection of still images & these images are refereed as I-frames.
- Here, first frame is not encrypted & is transmitted through secure channel whereas
- Second frame is xored with second key image, K2.Again the output is xored with sorted value of first frame.
- The process is repeated for all frames till encrypted video sequences E1,E2….En are generated.

Formation Algorithm:
For decrypting the obtained sequence of encrypted video following steps are followed [Ref.5]:

- Receive all frames of videos along with key images :K1,K2.
- Each frame E1 is xored with first key image & again the output is xored with its previous frame i.e first frame initially. Then the output is xored with key image K2 to obtain first I-frame of video.
- These steps are repeated for all the encrypted frames E1,E2..En (where n = 1,2…..n.)
- Finally construct the final video (consisting of I1,I2..In frames) by collecting all the frames.

Video Encryption algorithm (VEA):
In this concept, this new encryption will divide the input videos streams into odd chunks (a1, a3, a5, …., a2n-1) and even chunks(a2,a4,….a2n) & then encryption key would be applied to the even list E(a2, a4,a6, … , a2n), where E denotes an encryption function. Finally, cipher text is a concatenation of output of encryption algorithm XOR with the odd list streams.

Literature Review

There are various papers available in journals which are based Video Encryption. Some of them are:

All videos that are needed to be protected from suspicious users require Encryption. To solve this problem of security, a wide variety of encryption techniques have been discussed in this study. This paper description and comparison between encryption methods and representative video algorithms are discussed. With respect not only to their encryption speed but also their security level and stream size. In this research paper relation between quality of video Encrypting and choice of encryption algorithm were shown. [M. Abomhara, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques"]

This study indicates that the classification of encryption algorithm according to two categories:

Namely Full Encryption & Partial or selective encryption. It shows that full encryption requires more computational cost & has less speed due to large data to be encrypted. The classification is also done on the basis of various performance parameters such as Encryption ratio, Cryptographic security, Compression friendliness [Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey"]

In order to perform encryption in video and image contents using chaotic maps , a data (image or video) encryption scheme based on arithmetic coding, which we refer to as Chaotic Arithmetic Coding (CAC) is referred in this research paper. In CAC, a large number of chaotic maps can be used to perform coding, each achieving Shannon optimal compression performance. The exact choice of map is governed by a key. CAC has the effect of scrambling the intervals without making any changes to the width of interval in which the codeword must lie, thereby allowing encryption without sacrificing any coding efficiency. [Amit Pande, Prasant Mohapatra, Joseph Zambreno"]

This study focuses on a novel scheme to efficiently secure variable length coded (VLC) multimedia bit streams. The proposed scheme employs code word diffusion and content based shuffling techniques to achieve security. Specifically, it is a combination of a highly secure random number generator based on chaotic maps and a low computation complexity block shuffling procedures. The main idea of this encryption scheme is to make the decoding of the VLC codes in the bit streams computational infeasible in the absence of a private key. Here the contents are divided into random size blocks. Within each block, a few bits are flipped such that the correlation present among codeword is diffused. Next the blocks are randomly shuffled. [Sufyan T. Faraj Al-Janabi, Khalida Shaaban Rijab, Ali Makki Sagheer,"]

A brief introduction of AES algorithms is presented in this paper. With the AES algorithm of video encryption, a novel algorithm classification is discussed. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. The study done in this paper is valuable, and will have great utility. This essay brings efficient algorithm for encryption. [M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based for Image Encryption"]

A new scheme for video encryption which based on encryption of video frame. Here researcher has taken an idea from matrix calculation for generating the encrypted I-frame. In this method, we collect the all video frame then take frame one by one form it and select a key Image as key frame for encryption and

decryption process, so this key image is send through secure channel. Other frame encrypted by following algorithm & after applying the encryption algorithm we combine all frame, make video which is in encrypted form, send it from simple channel. [Mayank Arya Chandra, Dr. Ravindra Purwar, Dr. Navin Rajpal, "A Novel Approach of Digital Video Encryption"]

Conclusion

This paper focuses on the various methods for video Encryption .From the above analysis; the following conclusions have been drawn:

- Amongst the two approaches: selective encryption takes less time as compared to full Encryption.
- Zigzag method & chaos based method are hot research topics for encryption of video but takes more time
- Therefore a encryption algorithm based on
- I-frames & xor has been defined.

Future Work:
The results of implementation of various encryption schemes depict that a lot of advancement need to be done to get highly secured video after encryption. A I-frame based method is used that utilizes the concept of xor frames which in future can be used for video steganography.

References

1. *M. Abomhara, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.*
2. *Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.*
3. *Amit Pande, Prasant Mohapatra, Joseph Zambreno," Using Chaotic Maps for Encrypting Image and Video Content", 2011 IEEE International Symposium on Multimedia.*
4. *Sufyan T. Faraj Al-Janabi, Khalida Shaaban Rijab, Ali Makki Sagheer," Video Encryption Based on Special Huffman Coding and Rabbit Stream Cipher", 2011 Developments in E-systems Engineering.*
5. *Mayank Arya Chandra, Dr. Ravindra Purwar, Dr. Navin Rajpal, "A Novel Approach of Digital Video Encryption", International Journal of Computer Applications (0975 - 8887) Volume 49-No.4, July 2012.*
6. *M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based for Image Encryption", World Academy of Science, Engineering and Technology 3 2007.*
7. *Fadi Almasalha, Ashfaq Khokkar, Rogelio Hasimoto beltran, "Scalable Encryption of variable ength Coded video Bit Streams", 35th Annual IEEE conference on Local Com.*
8. *Daniel Soek, Hari Kalva, Syyros S. Magliveras," New Approaches to encryption and steganography for digital videos", Multimedia Systems, 01 1007/s00530-007-0083-,@Springer-Verlag 2007.*
9. *Knuth, D.E.: The art of computer programming, 2nd edn., vol. 3: Sorting and Searching, pp. 113-122. Addison-Wesley, Reading, MA (1998).*
10. *S., Chen, G., Zheng, X.: Multimedia security handbook. Internet and Communications Series, vol. 4, chap. Chaos-Based Encryption for Digital Images and Videos, pp. 133–167. CRC Press, West Palm Beach (2004).*
11. *X., Eskicioglu, A.M.: Selective encryption of multimedia content in distribution networks: Challenges and new directions. In: Proceedings of the Second IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), pp. 527-533. Scottsdale, AZ, USA, IASTED, 17-19 November 2003.*
12. *ISCAS 2004. 2004. 3. Guosheng Gu, g.H. The application of chaos and DWT in image scrambling. in Proceeding of the Fifith Interational Conference on Machine Learning and Cybernetics. 2006.*
13. *Dalian S. Agaian, J.A., K. Egiazarian, P. Kuosmanen, Decompositional methods for stack filtering using Fibonacci pcodes. Signal Processing, 1995.*
14. *David. Gevorkian, K.O.E., Sos S. Agaian, Parallel Algorithms and VLSI Architectures for Stack Filtering Using Fibonacci p-Codes. IEEE Transactions on Signal Processing, 1995.. 286-295.*
15. *Tzouveli Paasikivi, Ntalianis Klimis, Kollias Stefanos "Security of Human Video Objects by Incorporating a Chaos-Based Feedback Cryptographic Scheme".*
16. *MPEG. (1988). The MPEG Home Page. Retrieved Jan 13, 2009, from http://www.chiariglione.org/mpeg/*