International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Secure Video Encryption Technique Using Rijndael Algorithm

N. Geetha[1], K. Mahesh[2]

[1]M. Phil Research Scholar, Department of Science & Engineering, Alagappa University, Karaikudi, India

[2]Associate Professor, Department of Science & Engineering, Alagappa University, Karaikudi, India

Abstract: ***The transmission of digital content using the images increased consequently in past decades. Secure transmission of data through multimedia has increased much more. Hence, to ensure the security of the data to be transmitted, encryption techniques were used to convert the data into unintelligible format. Encryption takes place almost within every format, with many techniques and algorithms. In this paper, a method for encryption in video is taken place by using the AES Rijndael encryption algorithm. Instead of using the text or the images, the video encoding is taken place here. The video is converted into number of frames, which in turn converted to blocks used for encryption. The division of video resulted in images in turn this image is followed by encryption. The block cipher algorithm is used for converting frames to blocks. The Rijndael algorithm is used, because of its simplicity, efficient working syntax. Since, Rijndael algorithm is specified substitution ciphers were used to encrypt the given frames.***

Keywords: Multimedia formats, Encryption, Video encryption, Frames, Block Cipher

1. Introduction

Security of the digital media becomes major issue in networked infrastructure. The secluded transmission of data between the sender and the receiver becomes more important, so that the unauthorized users cannot intrude it. Cryptography is one of the techniques, which provide security to the data. It comprises of transmission of data into unreadable format. Various algorithms were in use for encryption and reverse process decryption.

Emerging distributed multimedia applications such as Video-on-Demand, video broadcast, multimedia mail and video conferencing must be provided with secure transmission [4]. Multimedia content is a combination of the text, still images, audio, animation, and video. Multimedia security deals with ways of protecting such content. Basically the symmetric key algorithms are best suited for the encryption technique for multimedia content. They also enable transmission security, protection to data etc. Many different encryption algorithms have been proposed in recent years as possible solutions to the protection of digital images and videos, among which MPEG videos attract most attention due to its prominent prevalence [9].

Encryption on video is harder to take place. It involves difficultly in separation of moving videos to split into images and then encryption technique to apply. It involves a careful analysis to determine and identify the optimal encryption method when dealing with audio and video content. Current research is focused on modifying and optimizing the existing cryptosystems for real-time audio and video content. It is also oriented towards exploiting the specific properties of many standard video and audio formats, in order to achieve desired speed and enable real-time streaming.

This is referred to as selective encryption [5].There are two main classes of encryption solutions: those which act on fully encoded MPEG streams and those which work on partially decoded MPEG streams .In general, two basic research methodologies for digital video encryption are used to provide support to aforementioned application requirements. Selective encryption algorithms perform conventional or nonconventional encryption only on certain selected parts of the video bit stream. The second type of algorithms uses a nonconventional full encryption methodology, where the encryption is performed on the entire bit stream using a nonconventional encryption algorithm. Most of these algorithms are targeted for speed [3].

The rest of the paper is organized as follows. Section 2 describes various related works has been put on the same area. Section 3 embraces various existing methods and techniques for the video encryption process and their merits. Section 4 discusses the proposed method for the encryption done on video. It is then followed, by the experimental results and their Conclusions. Finally, the section 5 concludes and justifies the outcome of the experimental results.

2. Literature Review

Arvind Kumar and KM.Pooja, discussed about the data hiding techniques in their paper. Here, digital images can be used as a carrier to hide messages [1]. Neil F. Johnson and Sushil Jajodia in discuss three popular methods for message concealment in digital images [7]. These methods are LSB insertion, masking and filtering and algorithmic transformations.

Daniel Socek et.al, presents a novel encryption model for digital videos [3]. The model relies on the encryption-compression duality of certain types of permutations acting on video frames. In essence, the proposed encryption process preserves the spatial correlation and, as such can be applied prior to the compression stage of a spatial-only video encoder. Several algorithmic modes of the proposed model targeted for different application requirements are presented and analyzed in terms of security and performance, in

addition to providing confidentiality, preserves or improves the compression ratio.

Shujun Li et.al, expresses the design of perceptual MPEG – Video Encryption algorithms, especially security defects of two recently proposed MPEG video perceptual encryption schemes, are pointed out [9]. Then, a simpler and more effective design is suggested, which selectively encrypts fixed-length code words (FLC) in MPEG-video bit streams under the control of three perceptibility factors. They fit well for size- preservation, encryption and multiple perceptibility. In addition, four different measures are suggested to provide better security against known/chosen-plaintext attack.

Jayshri Nehete et.al proposes video encryption using the AES Algorithm [6]. The algorithm selectively encrypts a fraction of the whole video. It is faster than encrypting the whole video with AES. It can save up to 90% of encryption time compared to the algorithm which encrypts the entire video. It encrypts at most 128 bits, instead of searching what type of frame is used. This considerably reduces encryption computations.

Jolly shah and Dr. Vikas Saxena [8] made a survey on video encryption techniques. Analysis and Comparison of the encryption algorithms with respect to various parameters like visual degradation, encryption ratio, speed, compression friendliness, format compliance and cryptographic security is presented. From their survey, they found Naïve algorithm provides highest level of security but it is very slow in nature and cannot be used in real time. Permutation based algorithms are generally faster but they do not provide sufficient level of security. Selective encryption algorithms reduces computational complexity by selecting only a minimal set of data to encrypt but their security and speed level generally vary based on which and how many parameters they encrypt.

Bharat Bhargava et.al, presents four fast MPEG video encryption algorithms. These algorithms use a secret key to randomly change the sign bits of Discrete Cosine Transform (DCT) coefficients and/or the sign bits of motion vectors [2].The encryption is accomplished by the inverse DCT (IDCT) during the MPEG video decompression processing. These algorithms add a small overhead to MPEG codec. The experimental results show that these algorithms achieve satisfactory results. They can be used to secure video-on-demand, video conferencing, and video email applications.

3. Existing Methods and Algorithms

This section briefly discusses various types of videos exists and encryption algorithms used for the video encryption. The encryption and decryption of a plain text or a video stream can be done in two ways:

3.1 Secret Key Encryption

A single secret key can be used to encrypt and decrypt the video streams. Only the sender and the receiver use this key. Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. Most common algorithms in these categories are Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard.

3.2 Public Key Encryption

For the public key encryption, there exist 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. It is based on a two-key crypto system in which two parties could securely communicate over a non-secure transmission medium.

3.3 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.

3.4 Selective Encryption

It is also called as partial encryption & is a subcategory of variable encryption. The algorithms in this will selectively encrypt the bytes within video frames. As these algorithms are not encrypting each and every byte of video data, it reduces computational complexity.

3.5 MPEG – 1 Video Encoding

In MPEG-1 video coding model [Gall], a video is composed of a sequence of group of pictures (GOPs). Each GOP is a series of I, P and B pictures. I pictures are intra frame coded without any reference to other pictures. P pictures are predictively coded using a previous I or P picture. B pictures are bidirectional interpolated from the previous and following I and/or P pictures. The relative frequency of occurrence of I, P and B pictures can be controlled by the applications. Each picture is divided into macro blocks. A macro block is a 16×16 pixel array. Macro blocks belonging to I pictures are spatially encoded. Those belonging to B and P pictures are temporally interpolated from the corresponding reference picture(s), and the error between the actual and reference values is computed.

4. Proposed Method

The following section shows the proposed methodology with the procedural steps. The AES Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths.

4.1 AES Rijndael Algorithm

The output of the algorithm consists of sequence of 128 bits with values zeros and ones. These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. On the other hand, the Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. The following is the working model foe AES standard. The AES algorithm works in a two dimensional

way, called as the state array. It consists of four rows and four columns. It is a block cipher algorithm, in which the block means the information to be encrypted is divided into blocks of equal length. It is an iterated block cipher, with a variable block length and variable key length. The function of AES Rijndael is as follows;

(a) SubBytes Transformation: The SubBytes ( ) transformation is a non linear byte substitution that operates independently on each byte of the state using a substitution table.
(b) ShiftRows Transformation: In the ShiftRows ( ) transformation, the bytes in the last three rows of the state are cyclically shifted over different number of bytes. The first row will not get shifted.
(c) MixColumn Transformation: In MixColumn ( ), the columns of the state are considered as polynomial and then multiplied by modulo with fixed polynomial, individually.
(d) AddRoundKey Transformation: In the AddRoundKey () transformation, a round key is added to a state by a simple bitwise XOR operation. Each round key consists of Nb words from the key schedule; those Nb words are each added into the columns of the state.

4.2 Steps to Video Encryption

Step 1: Read the User defined Video
Step 2: Split the video into I - Frame, B- Frame and P – Frame. I-frames fall at low compression ratio. P- Frame consists of difference between the two frames. Finally, B frames are bi directionally interpolated using the previous closest I/P frame.
Step 3: An I frame is encoded as a standard JPEG still image.
Step 4: Convert the provided JPEG Image into Blocks, each of 128 bits.
Step 5: Input the Key value to encrypt the blocks.
Step 6: The original image, divided into blocks is transformed based on the Rijndael encryption algorithm, with the given key size mentioned above.
Step 7: Now, the frame is encrypted. Rearrange each transformed frame, into video again.
Step 8: The output is the encrypted Video.
To retrieve the data, the decryption process should be taken place, in the vice versa order.

5. Conclusion

In this paper a simple and secure method for video encryption using the Rijndael algorithm is proposed. By using the Rijndael each frame can be effectively converted into blocks. After transformation, the encryption of the image taken place efficiently. The Rijndael algorithm is simple to implement, and throughput is high. The entropy as well as the correlation coefficient between the frames also remains the former with high and lower with low ratio, which provide more secure to the data.

References

[1] Arvind Kumar and KM.Pooja, “Steganography – A data Hiding Technique”, in International Journal of computer Applications, Volume 9, Issue 7, November 2010, pp.- 19-23.
[2] Bharat Bhargava , Changgui Shi, Sheng-Yih Wang, “MPEG Video Encryption Algorithms “, in Multimedia Tools and Applications, vol 24, pp:- 57–79, 2004.
[3] Daniel Socek, Spyros Magliveras,Dubravko Culibrk,Oge Marques, Hari Kalva, and Borko Furht, “Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations”, in EURASIP Journal on Information Security , Volume 2007,pp: 1-15.
[4] D.L. Gall, “MPEG: A video compression standard for multimedia applications,” Communications of the ACM, Vol. 34, No. 4, pp. 46–58, 1991.
[5] Meyer, J., - Gadegast., F.: “Security mechanisms for multimedia-data with the example MPEG-1-video”. Proj. description of SECMPEG, Te ch. Univ.of Berlin, Germany , 1995.
[6] Jayshri Nehet K. Bhagyalakshmi, M. B. Manjunath, Shashikant Chaudhari, T . R. Ramamohan, “A Real-time MPEG Video Encryption Algorithm using AES”.
[7] Neil F. Johnson, and Sushil Jajodia, “Exploring Steganography, Seeing the Unseen,” in IEEE Computer Magazine, pp. 26-34, February1998.
[8] Jolly shah and Dr. Vikas Saxena, “Video Encryption: A Survey”, in International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011, pp:- 525 – 534.
[9] Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, , “On the Design of Perceptual MPEG-Video Encryption Algorithms” in Ieee Transactions On Circuits And Systems For Video Technology, Vol. 17, No. 2, Pages 214-223, February 2007.