International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

An Enhanced Approach for Video Encryption using Multilayer and Scrambling through AES Algorithm

Vinay Kumar Soni[1], Prashant Puri Goswami[2]

[1, 2]Central College of Engineering and Management, Raipur, Chhattisgarh, India

Abstract: ***Due to rapid increase in the field of internet and multimedia technology the digital data transmission has increased very fast. The security of data transmission from unauthorised access proved a big issue in this regard. Several papers focused this problem and different methods are also given to protect the data from unauthorised access. As several standard symmetric encryption algorithms provide good security for the multimedia data, but these encryption algorithms for video having larger size have the delay problem of computation. Transmission of video is a very common in multimedia application and its encryption requires a complex computation. To protect the digital data during last few years, several encryption algorithms have developed to secure image or video transmission. Video encryption has application in several fields including medical systems, internet communications and military communication. The Advanced Encryption Standard (AES) algorithm can be used for video encryption and it can be modified too, to reduce the calculation of the algorithm and for improving the encryption performance. This paper presents different video encryption methods and some possible techniques to enhance the security of video data transmission.***

Keywords: MPEG video frame, AES algorithm, Scrambling, Multilayer encryption

1. Introduction

Encryption is the process of applying some algorithm along with a key to convert the data into a format which cannot be understood by unauthorised receivers. As the developments in multimedia technologies resulted increase in the applications like video conferencing, Video On Demand (VOD), video broadcasting etc. and such applications need confidentiality of the video data during transmission which necessitated secure video encryption algorithms.

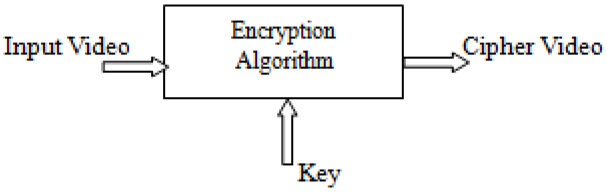

Figure 1: Basic concept of video encryption.

Figure 1 shows the concept of encrypting any video file through any algorithm and a key to convert the input video into an encrypted video known as cipher video.

As a basic approach for video encryption, the MPEG stream having bit sequences can be treated as text data, and encrypted using any encryption algorithms like DES (Data Encryption Standard), or AES (Advanced Encryption Standard). Although this approach will be the high secure method for video encryption, it will be too complex for real-time applications having larger video size files. If the full content of the video is not too important, selective encryption algorithms can be adopted.

A video encryption scheme should take care of encryption efficiency, high security etc into account to prove its importance as compared to the others. An efficient algorithm must not cause larger time delays during the encryption and decryption process.

As the video files have generally a large amount of data and require real-time operations. Also in the case of the wireless communication systems, there is an issue of limited power, memory and channel bandwidth. Therefore these systems do not have capacity to handle the large encryption processing loads. So the consideration of specific characteristics for such resource-limited systems, very efficient video encryption algorithms are needed to be developed. But in most of these methods, computational efficiency can be achieved at the cost of security.

2. Classification of video encryption techniques

The video encryption algorithms are categorised as below:

A) Completely Layered Encryption

In completely layered encryption method, the entire video is first compressed and it is then encrypted using any algorithm like RSA, DES, or AES. This technique takes very much time and therefore not applicable in real time video applications.

B) Encryption Using Permutation

In this method the video content is scrambled using a permutation algorithm. The complete content of video may be scrambled or only a particular part can be used for scrambling. This method gives a more secure way for encryption.

C) Selective Encryption

To minimize the computational complexity and to increase the efficiency only particular video bytes maybe encrypted.

D) Perceptual Encryption

In this Method after encryption the video will still be perceptible. Through this method video quality can be controlled.

3. A New Scheme for Enhanced Security

The basic video encryption scheme involves the following steps:

a) Take input video file.
b) Extract image frames from video file.
c) Apply the encryption algorithm using key.
d) Collect all the cipher images obtained through encryption.
e) Convert the encrypted image frames back into video to get encrypted video.

AES algorithm involves four steps:

1) Substitution bytes transformation.
2) Shift rows.
3) Mix columns.
4) Add round key.

Number of rounds for AES algorithm will depend upon type of algorithm as given:

1) AES-128:10 Rounds.
2) AES-192:12 Rounds.
3) AES-256:14 Rounds.

The scheme of AES encryption and decryption can be figured as below:

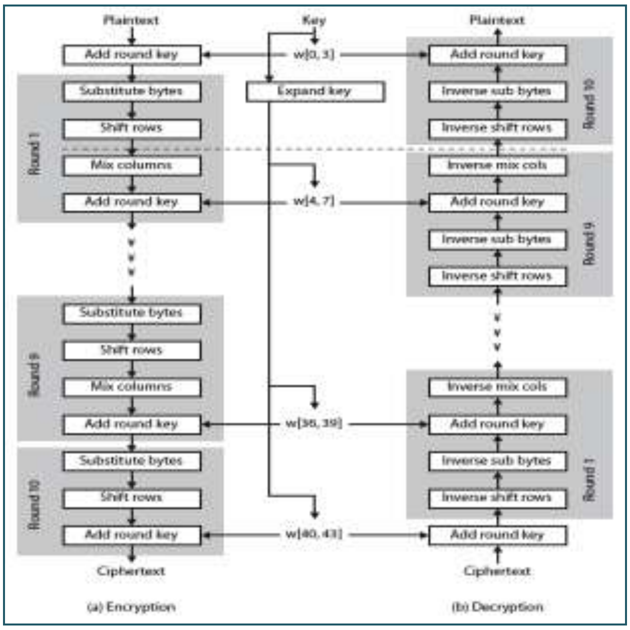

Figure 2: AES Architecture [Stallings, W. (2011)].

To increase the security level through the AES algorithm one possible way is to scramble the frames and increase the encryption layers. This scheme may contain following steps:

a) Take input video file.
b) Extract image frames from video file.
c) Apply frame scrambling.
d) Apply the encryption algorithm using first key.
e) Apply the encryption algorithm using second key.
f) Apply the encryption algorithm using third key.
g) Collect all the cipher images obtained through encryption.
h) Convert the encrypted image frames back into video to get encrypted video.

The decryption scheme will reverse the above sequences to get the input video file.

The frame scrambling involves changing the frame sequences before the encryption algorithm application. This can be depicted as below:

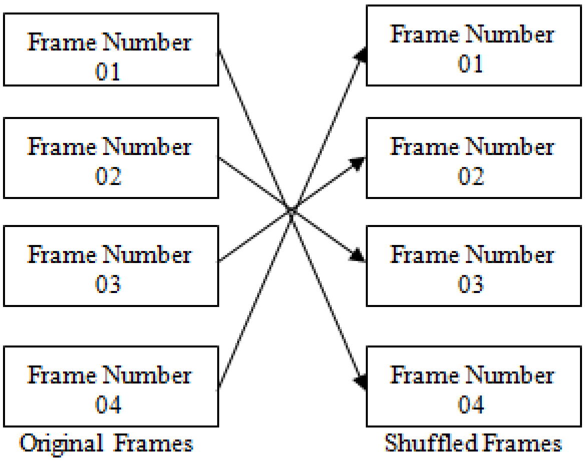

Figure 3: Concept of frames shuffling.

4. Conclusion

This new structure of video encryption will enhance the security of encrypted video which will prove more strength of the encryption scheme against the known attacks. Further this scheme is easy to implement as the AES algorithm is a very popular encryption scheme.

References

[1] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar, “Fast and Secure Real-Time Video Encryption”, Sixth Indian Conference on Computer Vision, Graphics & Image Processing, IEEE, pp 257-264.

[2] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More, “Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study”, International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013, pp 1-5.

[3] Jayshri Nehete , K. Bhagyalakshmi, M. B. Manjunath, Shashikant Chaudhari, T. R. Ramamohan, “A Real-time MPEG Video Encryption Algorithm using AES”, Central Research Laboratory Bharat Electronics Ltd., Bangalore.

[4] Dr. Salim Ali Abaas and Ahmed Kareem Shibeeb, “A New Approach for Video Encryption Based on Modified AES Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 17, Issue 3, Ver. VI (May – Jun. 2015), PP 44-51.

[5] Jayakrishna.P, Chinnam Mahesh, P.Santhosh, “Implementation of AES Algorithm for Video Streaming Security System”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2016, pp 1111-1118.

[6] N. Geetha and K. Mahesh, “A Secure Video Encryption Technique Using Rijndael Algorithm”, International

Journal of Science and Research, Volume 3 Issue 5, May 2014, pp 1732-1734.

[7] T. Pradeep Pai, M.E. Raghu and K. C. Ravishankar, “Video Encryption for Secure Multimedia Transmission - A Layered Approach”, Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference, IEEE.

[8] M Yang, N. Bourbakis and Shujun Li, “Data-image-video encryption”, IEEE Potentials (Volume: 23, Issue: 3, Aug.-Sept. 2004).pp 28-34.

[9] Muhammad Asiml and Varun Jeoti , “On Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme”, IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp.65-69.

[10] B.Subramanyan, Vivek.M.Chhabria, and T.G.Sankar babu, “Image Encryption Based On AES Key Expansion”, IEEE Second International Conference on Emerging Applications of Information Technology, pp 217-220.

[11] Dhananjay M. Dumbere and Nitin J. Janwe, “Video Encryption Using AES Algorithm”, IEEE 2nd International Conference on Current Trends in Engineering and Technology, pp 332-337.

[12] Ms. Pooja Deshmukh and Ms. Vaishali Kolhe, “Modified AES Based Algorithm for MPEG Video Encryption”, IEEE ICICES2014.

[13] Qi Zhang and Qunding, “Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm”, IEEE Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp 1218-1221.

[14] Cuixia Li, Yang Zhou ,Y inghua Shen and Cheng Yang, “A Video Selective Encryption Strategy based on Spark”, IEEE 2016, pp 957-960.

[15] Alvin Mustafa and Hendrawan, “Calculation of Encryption Algorithm Combination for Video Encryption using Two Layers of AHP”, IEEE 2016, pp 1-7.

[16] Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni and Agilandeeswari Loganathan, “A Novel Image Encryption Algorithm using AES and Visual Cryptography”, IEEE 2nd International Conference on Next Generation Computing Technologies, pp 808-813.

[17] www.wikipedia.org/aesalgorithm.