Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 3, Issue 1, 2017, pp 8-12
ISSN: 2395-0196

Development of new framework for secure live video streaming over p2p network using randomize algorithm

Richa Singh[1] Gajanand Sharma[2]
[1]Research Scholar, Dept.of Computer Science & IT ,SGVU,jaipur
[2]Assistant Professor,Dept.of Computer Science & IT,SGVU,Jaipur

Abstract-An important concern in multimedia technology is security and privacy issue of the transmitted data. The encryption of information helps to secure the data from any attack so, there is a need of developing a video encryption algorithm which can provide a confidentiality, integrity and authentication in video. This paper mainly focuses on security for the transmission of data through the encryption technique and the digital signature. For the video encryption, AES-128 is used and then digital signature is used for the watermarking. AES has been adopted by the U.S. Govt. and now widely used.

Keywords: AES-128, digital signature, Encryption, security, confidential

INTRODUCTION

Modern era is fully dependent on the network. We are using the internet for many purposes. With the increase of multimedia data are transmitted in the various fields like business, video conferencing, medical images system and military communication etc. which include some sensitive data. Video- on – demand, video broadcast, multimedia mail and video conferencing are the most promising distributed multimedia applications. Therefore, there is a need of for secured data transmission techniques. For the digital video transmission, there are the various encryption techniques which are needed to protect the digital video from the various attackers. Information security has been confirmed with data encryption techniques.

The cryptography is a basis of security improvement used to ensure data on both crystal clear systems. The main elementary objective of cryptography is keeping information secure from the unauthorized users or attackers. The digital videos are large in size so they are usually transmit in compressed format such as MPEG, H.264. Accordingly information is encoded through process of encryption. The reverse of encryption is information sorting out i.e., decryption. Through the process of encryption, data is changed into the scribbled form and then transmitted. At the receiver end, the encrypted data is decrypted to convert it into readable form. This process is known as decryption.

An algorithm is used to encrypt the data at the sender side and a decryption algorithm is used to disclose the data at the receiving end. The AES (Advanced Encryption Standard) is an encryption/decryption algorithm defined by the US Government. The standard is explained in the Federal Information Processing Standard 197 (AES, 2001) and was request due to the security issues found in DES (Data Encryption Standard) and the undesirable speed of 3DES. The replacement for DES had to support: symmetric encryption, various size encryption keys (128, 192 and 256 bits) and, maybe most important, both hardware and software implementation.

The Encryption mainly focuses on encrypt the data on the basis of algorithms. The algorithms having a basic idea of public key and private key encryption. Both techniques having some advantages and some disadvantages and also have different methods of

Algorithms. Loss of data either by interloper or an hacker is more, so only if security is compulsory and discretionary over the network.

The Encryption is classified into lossless and lossy encryption. The studies on image encryption using the keys with digital signatures, chaos theory and vector quantization. These methods/ techniques have some limitations like key size, cost estimation and the issue of security. To overcome on the limitations the concept of VC was given in which the secret sharing of images is involved by dividing into multiple shares. An intruder cannot recognize any hints about a secret image from individual random share images. In this method, the splitting of image is done at the pixel level so an individual shares transmit no information but the qualified set of these shares will help to redevelop the real image.

In real application like a video encryption, security is the basic necessity. There are the various reasons for the need of video encryption as if we want to send a personal multimedia message, video conferencing learning and video on demand.For this purpose of security, cryptography, stenography, and water marking techniques can be used to obtain the security and privacy of data. All of these provide confidentiality, authentication and integrity to the transmitted data.

Another method is digital watermarking employs visual encryption method to increase security without decreasing the data payload. The digital signature provides the authentication & non-repudiation feature to the data transmission on the network. Watermarking is a major application which is used to validate user documents during the transmission. It is the process of embedding information into a digital signal in a way i.e. is difficult to remove. It is providing copyright protection for the intellectual method that is in digital format.

LITERATURE REVIEW

Qiao, Li et al "A New Algo for MPEG Video Encryption" represent the different statistical behavior of compressed video media in contrast to real time efficient algorithm. They gave an algorithm named as Video Encryption Algorithm [VEA] in which showed the statistical behavior of MPEG video streams and the experimental results on various video verify the goal for providing a fast encryption algorithm and also means that VEA can be a part of retrieval & playback process in video-on-demand.

Negi,Y [2013] "A Survey on Video Encryption Techniques" gives information about the existing methods and their improvements and hence providing a platform for new researchers for innovating new techniques for further research. She mainly focuses on the full or selective encryption techniques. She drawn a conclusion as selective encryption takes less time as compared to full encryption. An encryption algorithm is based on the I-frames & XOR has been defined.

Kulkani, A., et al.[2013] "Proposed Video Encryption Algorithm Vs. Other Existing Algorithm: A Comparative Study". In this paper, the two methods of encryption were highlighted named as symmetric key and asymmetric key encryption. He evaluated these algorithms with respect to their level of security and the encryption speed.

Singh, S. & Verma N., [2015] "Efficient & Secure Video Encryption & Decryption using Neural Network" focused on that compressing encrypted video still performed efficiently even after the encryption and the compression. They mainly focused on the quality of video after the encryption process.

Kester,Q., [2014] "A Hybrid Cryptography & Digital Watermarking technique for securing digital images based on symmetric key". He said that for securing the images,both pixel displacement and pixel encryption were used for the cryptographic techniques. The digital watermarking is used to authenticate a user, and documents.

Bhandari,L & Wadhe,A. [2013] "Speeding up video encryption using ECC" implemented both ECC & RC5 encryption algorithm and provides the problem happened with the RC5. For encryption process, he uses RC5 for the encoding of DCT.

coefficient and ECC for generating a key of small size.

Kumar,A., et al., [2013] proposed a new technique for the image stenography. They implemented Hash-LSB with RSA algorithm where it provides more security to both data and data hiding method. This method ensures that before hiding a data into a cover image it has been encrypted. If in any case encrypted data is revealed from the cover image then the intruder cannot read or access the data as it is in encrypted form.

Peuch,W et.al[2012] focused on the problems associated with the techniques as the number of images and video are increasing. He gave a brief overview of the approaches and the problems which are exist in applying the techniques.

Munteanu,G et.al[2015] "GPGPU optimized parallel implementation of AES using C++AMP Gabriel" focused on the comparative study on the implementation of AES algorithm on CPU and two different platforms GPGPU and creating a platform independent application and implemented using C++ AMP. The load of the GPGPU was constant, the method was called only once and the resultant value was used for the entire encryption process. However, in case of heavy loaded systems, the method will be called for each step of the encryption. In this way, the best amount of data that can be processed at that instant by the GPGPU without being bothered by the GPGPU will be determined.

Li,S. et.al[2013] "Research on the Performance of Encryption Techniques for HighBandwidth Multicast Video Streaming" studied the performance of AES, DES and RC4 encryption algorithms for encrypting the data stream with the bandwidth of 1~1000Mbps. For testing these three encryption algorithm, considered the MPEG-4 format of multicast streaming. They measured the delay time in an encrypting number of texts, audio and video packets with the three algorithms and concluded that AES and RC4 can be used to encrypt the high bandwidth of 20Mbps streaming data.

Lakshmi ,R et.al[2015]"Efficient Technique for Secure Transmission of Real-Time Video over Internet" focuses on a techniques named as Enhanced Real Time Video Encryption using lossless compression for the encryption of video with a best quality of resultant video. According to result analysis, concluded that the proposed algorithm has lossless compression with a fast speed of transmission and better security. The proposed method is efficient in real time video and the time of encryption depends on the type of encryption method used. In ERTVEL technique, both video and audio are encrypted and therefore, it provides a good security. The lossless compression technique provides a better output video after the decryption of video.

Saraf,K et.al [2014] "Text and Image Encryption Decryption Using Advanced Encryption Standard" presents the text and image encryption using the AES algorithm using java application platform SDK. For the text encryption, Code Composer Studio and DSP processor is used for the implementation and provide a unique solution for the same. For image encryption, AES algorithm in CFB mode and PKCS55 padding is used.

METHODOLOGY

The AES has various modes of operations such as ECB, CBC, OFB, CTR, CFB etc. Here CBC mode of AES is used. It allows three different key size as 128,192,256 bits and here 128 bits key size is used in video encryption and decryption.

Algorithm:

- Take the video of maximum size 4.3 Mb and it must be in the .mov format.
- Divide the video into the frames and number of frames must be 5183.
- Save these frames into the .png format.
- Identify the edges of an object into each frame.
- Read the pixels of edge in each frame and saves these pixels into the matrix variable.
- Apply the AES encryption algorithm and the digital signature on to the edge pixels and save

- Then, these frames are send to the receiver in sequenced manner.
- At the receiver side, apply the reverse algorithm for the decryption of the encrypted video. these encrypted frames into .png format.

- **Algorithm for AES encryption in matlab**

Algorithm:

```
Cipher(bytein[16], byteout[16], key_array round_key[Nr+1])
  begin
        byte state[16];
        state = in;
        AddRoundKey(state, round_key[0]);
          for i = 1 to Nr-1 stepsize 1 do
      SubBytes(state);
      ShiftRows(state);
MixColumns(state);
      AddRoundKey(state, round_key[i]);
  end for
      SubBytes(state);
      ShiftRows(state);
      AddRoundKey(state, round_key[Nr]);
end
```

- **Method used in AES Algorithum**

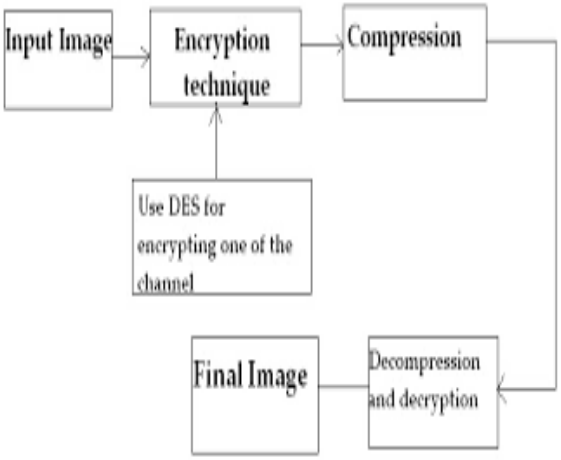


FIG1: Methodology for video encryption

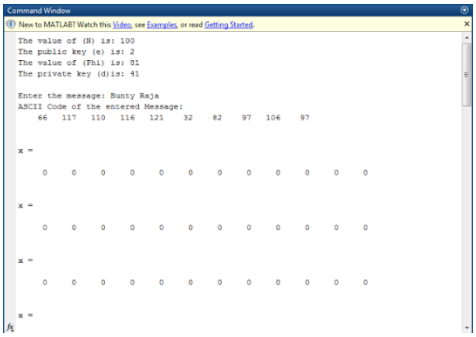
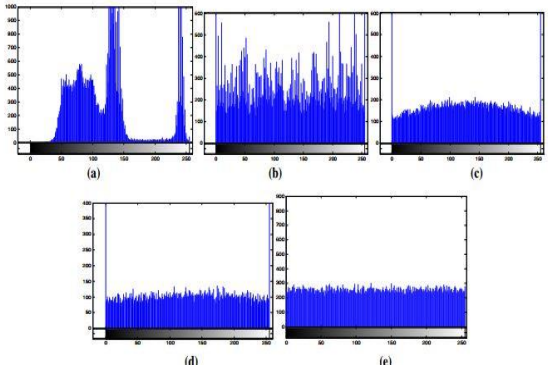


FIG2: Snapshot of encryption algo using MATLAB

The main aim of digital signature is to ensure that message is being not tailoredand it is signed to ensuring the receiving party that message is being sent by the expected party. The encrypted video send to receiver with the digital signature for ensuring the receiver that video is sent by the right person or party. It is better for the quality of video and security purposes.

RESULT &CONCLUSION

The fusion nature of the algorithm involves the cryptographic techniques and digital watermarking. In this paper, a combination of AES and Digital Signature technique is proposed for the video encryption.



Histogram analysis of AES algorithm using Different Frame rate and Different Key Used in matlab .

This is mainly aimed on the security of video when it is transmitted on the open network as internet.It

reduces the overhead processing as encryption is applied only the edge. There is no need of compression of video as on compressed encrypted video, signal noise ratio increases as compared to the original encrypted video.

REFERENCES

[1]Abomhara, M. et al. [2010] "An Overview of Video Encryption Techniques "International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[2]Bhandari ,L. et al [2013]"Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3)

[3]Jaffar , A .et al[2014] "Visual Digital Signature Scheme: A New Approach" IAENG International Journal of Computer Science, 37:4, IJCS_37_4_04

[4]Kester , Q. et al[2014]"A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key" International Journal of Computer Applications (0975 – 8887) Volume 94 – No. 19, May 2014

[5]Kulkarni , A. et al[2013]"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

[6]Kumar , N. et al[2013] "Issues and Challenges in Symmetric Key based Cryptographic Algorithm for Videos and Images" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[7]Li ,S. et al[2007]"On the Design of Perceptual MPEG-Video Encryption Algorithms" IEEE Transactions On Circuits And Systems For Video Technology, Vol. 17, No. 2, Pages 214-223, February 2007

[8]Negi ,Y[2013] "A Survey on Video Encryption Techniques" International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013)

[9]Qiao ,L .et al[2013] "A New Algo for MPEG Video Encryption"

[10]Saraf , K. et al[2014] "Text and Image Encryption Decryption Using Advanced Encryption Standard" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ISSN 2278-6856(vol-3)

[11]Singh ,S. et al [2015] "Efficient and Secure Video Encryption and Decryption using Neural Network" International Journal of Advanced Research in Computer Science ISSN No. 0976-5697

[12]Soni, S.[2015]"A Road Map to Visual Cryptography"International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, 2015 ISSN: 2277 128X