THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

An Novel Encryption Method For Videos Using Quantum Key Distribution

Sahil Sharma
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India
Sahil.24886@lpu.co.in

JebaNegaCheltha
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India
Jeba.25111@lpu.co.in

ABSTRACT

In contemporary world we are transferring lot of information through internet. Security is veryessential in modern scenario. Cryptography acts an essential task in contemporary world. Cryptography helps to protects private data. It is preferred to secure informationwhile transmitting through telecommunications set-up also in addition to files and databases. This proposed work presents regarding the security of videos. Advanced Encryption Standard concept is in favor ofenciphers as well as decryption of video. Advanced Encryption Standard employs symmetric key. Symmetric key means both the dispatcher and recipient uses the identical key. So the key should be transmitted securely to both the dispatcher and recipient using Quantum key Distribution is used.

Keywords:*AES, Encryption, Decryption, Quantum key Distribution*

I. INTRODUCTION

In symmetric key encryption technique both the dispatcher and recipient uses the same key. So key should be distributed securely. Quantum Key Distribution (QKD) concentrates on these security issues through the use of quantum key distribution that could subsequently be capable touse scramble messages. The protection QKD is based on important suggestions of character, which might be taking proof towards expanding computational control, and innovativecomputationusing quantum PCs. QKD fruitfullytackles the problems towards classic answer dispersion strategies. Quantum Key Distribution helps to share the key to both the end users in a secure way. This quantum cryptography uses quantum communication to share the keys securely. Cryptography helps to protects private data. It is preferred to secure information while transmitting through telecommunications set-up also in addition to files and databases. This paper explains regarding the security of videos using AES. In AES both the sender and collector makes use

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

of identical key. This identical key securely transmitted with the help of Quantum Key Distribution.

II.LITERATURE SURVEY

Shujun Li et.Al, communicates the plan of perceptual MPEG – Video Encryption calculations, particularlysecurity imperfections of proposed MPEG video perceptual encryption plans [9]. A less complicated and greater securityis recommended in this paper, which specially scrambles length code in MPEG-video [10].

The paper by K.Brindha, Ritika Sharma, SapannaSain used DES algorithm for encryption of videos[11]. The Key length of DES is fifty six , where as in proposed work key length of AES is 128, 196 or 256 bits. So safety of proposed work is greater than this paper.

The paperby Sanjay Kumar Anup&Suchithra used 3DES algorithm for video encryption.The key length of 3DES is 128 or 192 bits which is lesser than that of AES [6,7]. Hence the proposed work is much secured.

II. PROPOSED WORK

A.AES

Advanced Encryption Standard is a coherence key calculation, where, both thedispatcher with the beneficiary formulates the use of a solitary input. AES uses 128 bit keys, along with the inputkeylength of 256, 192 or 128 bits[1]. The number of round in AES is 14, 12 and 10 while the key length is 256, 192 and 128.AES, apart from the final round, comprises of four modifications [5]: ShiftRows ,MixColumns, SubBytes, and AddRound Key. The ultimateround does no longer have the MixColumns . AES is shown inthe following Fig.1

By utilizing AES calculation the video is encoded. The receiveragain decodes the video and gets the originalvideo [8].

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

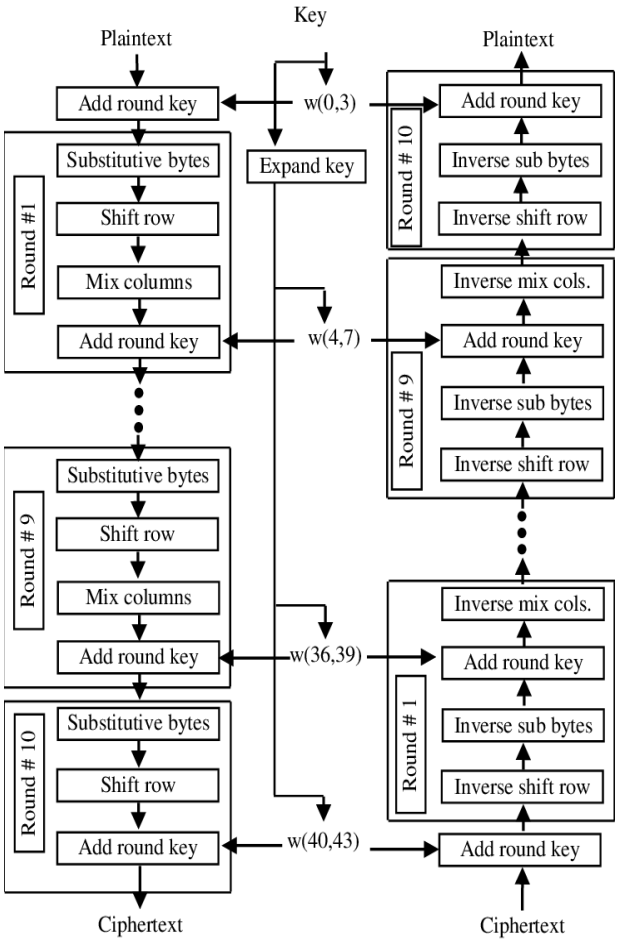

Fig.1 Block Diagram of AES Encryption and Decryption

B. Quantum Key Distribution

Quantum key distribution is simply used to supply suitable input [2]. In QKD photons are used for secure communication of identical keys. In this paper QKD is usedthroughhieroglyphics using symmetric key calculations just like the Advanced Encryption Standard calculation [3]. Quantum correspondence consists of encoding facts in quantum states, in place of conventional correspondence's usage of bits. Typically, photons are applied for those quantum states[4].*E91 protocol:* ArturEkert's plan makes use of units of photons. The photons are appropriated so sender and Receiver use one photon from each pair.

III.IMPLEMENTATION

In this proposed work, I took frame of video and transformed to hexadecimal frame and then transformed the hexadecimal frame to pixel frame with the aid of AES. In decryption method, pixel frame is transformed to hexadecimal layout after which hexadecimal frame is

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

converted to unique frame by AES. Same steps repeated for all the frames in the video. Sample output for singleframe is given in the following Figure. Figure 2 denotes Original frame, Figure 3 denotes Encrypted frame and Figure 4 denotes decrypted frame. As we know AES makes use of symmetric key cryptography. So each the correspondent and the beneficiary uses identical key. Hence Quantum Key Encryption method is used, to send the important thing securely on this projected work.

Fig 2: Original Frame

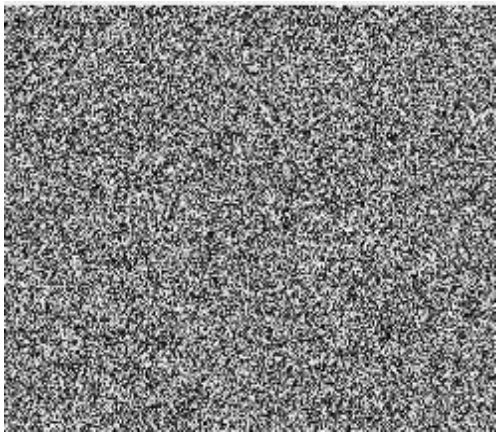

Fig 3: Encrypted Frame

Fig 4: Decrypted Frame

IV CONCLUSION

In this paper I have anticipated a novel loom for video encryption and unscrambling, AES is used. AES is a symmetric key cryptography,in which the sender and receiver makes use of same key. While transferring the secure key must be safe. So in my proposed work I used Quantum

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Key Encryption Technique. Hence motion pictures securely converted by the use of AES and the secret key securely transmitted to different consumer through the usage of Quantum Key encryption Technique.

REFERENCE

[1]. Daemen, J., and Rijmen, R. "The Design of Rijndael: AES–TheAdvanced Encryption Standard",Springer, 2006.

[2] C. H. Bennett and G. Brassard,"Quantum cryptography: Public key distribution and coin tossing", In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol.175, pp.8,2014

[3]. Ekert, ArturKonrad,"Correlations in quantum optics", University of Oxford , 1991

[4] Ekert, Artur,"Quantum cryptography based on Bell's theorem", Physical Review Letters. American Physical Society, pp.661–663, 5 August 1991.

[5] Daemen, Joan; Rijmen, Vincent "AES Proposal: Rijndael" ,National Institute of Standards and Technology, pp.1, 5 March 2013

[6] Sanjay Kumar, "Video Encryption using Simplified Data Encryption Standard" ,International Journal of Computer Applications",Vol.104, pp.2, October 2014

[7] Anup&Suchithra, "Video Encryption using Triple DES Algorithm", IJIR, Vol.3-5, 2017

[8] Biclique,"Cryptanalysis of the Full AES", Archived from the original ,March 6, 2016

[9] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno, "The Twofish Team's Final Comments on AESSelection", May 2000.

[10]Vinayak P , P, Nahala M A, "Avoiding Brute Force attack in MANET using Honey Encryption", IJSR, Vol.4-3, March 2015.

[11] K.Brindha, Ritika Sharma, SapannaSain ,"Use of Symmetric Algorithm for Image Encryption", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3-4, April 2017