International Journal of Research in Advent Technology, Vol.7, No.5S, May 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Recent Encryption Technique for Images Using AES and Quantum Key Distribution

Jeba Nega Cheltha C
Assistant Professor, Department of CSE, Jaipur Engineering College & Research Centre
Jaipur, India
jebanegacheltha.cse@jecrc.ac.in

Abstract— Data security acts an imperative task while transferring information through internet, whereas, security is awfully vital in the contemporary world. Art of Cryptography endows with an original level of fortification that protects private facts from disclosure to harass. But still, day to day, it's very arduous to safe the data from intruders. This paper presents regarding thetransferring encrypted images over internet using AES and Quantum Key Distribution method,where Advanced Encryption Standard (AES) algorithm is used for encryption as well as decryption of the picture. AES employs Symmetric key that means both the dispatcher and recipient use the identical key. So the key should be transmitted securely to both the dispatcher and recipient using Quantum key Distribution, whereas, using AES and Quantum Key Distribution the Data would be more secure.

Keywords— Encryption, Decryption,AES, Quantum key Distribution

1. INTRODUCTION

The most secured just as widely utilized approach to watch the protection and dependability of data communicate depend on symmetric cryptography. Key distribution is the way toward sharing cryptographic keys between at least two gatherings to enable them to safely share data. Quantum Key Distribution (QKD) addresses these difficulties by utilizing quantum properties to trade mystery data, for example, a cryptographic key, which would then be able to be utilized to scramble messages that are being imparted over a shaky channel. The security of QKD depends on essential laws of nature, which are resistant to expanding computational power, new assault calculations or quantum PCs. It is secure against the most self-assertively incredible busybodies. QKD successfully addresses the difficulties going up against classic key dispersion approaches, by giving a provably secure cryptographic structure obstruct for remote gatherings to share cryptographic keys. For the most elevated security necessities, QKD even empowers the persistent age and sharing of genuinely arbitrary one-time pad keys. The Advanced Encryption Standard (AES), is a symmetric block cipher actualized in programming and hardware all through the world to encode delicate information. In this paper image is scrambled by utilizing AES. In AES both the sender and collector utilizes same key. This key is safely transmitted by utilizing Quantum Key Distribution.

2. LITERATURE SURVEY

The paper entitled "Color Image Encryption and Decryption Using DES Algorithm" by Manjula K G, M N Ravikumar, IRJET used DES algorithm [5]. The Key size of DES is 56 where as the key size of AES is 128, 196 or 256 bits. So security of our proposed work is more than this paper.

The paper "Image Encryption using Simplified Data Encryption Standard (S-DES)" by Sanjay Kumar [6] and the paper entitled " Image Encryption using Triple DES Algorithm" by Anup & Suchithra [7] and the paper entitled "Image Encryption Based on the Modified Triple DES Cryptosystem" by V. M. SILVA-GARCÍA [8] used triple DES. The key has length of 128 or 192 bits in 3DES which is lesser than the size of AES . Also AES is against Brute Force attack. Hence the proposed work is much secured.

3. PROPOSED WORK

A. AES

The AES is a symmetric key calculation, in which both the sender and the beneficiary utilize a solitary key for encryption and decoding. AES characterizes the information square length to 128 bits, and the key lengths to 128, 192, or 256 bits [1]. It is an iterative calculation and every emphasis is known as a round. Number of rounds, is 10, 12, or 14 when the key length is 128, 192, or 256 bits, individually [1]. Each round in AES, aside from the last round, comprises of four changes: SubBytes, ShiftRows, MixColumns, and AddRound Key. The last round does not have the MixColumns . The decoding stream is essentially the turnaround of the encryption stream and every activity is the converse of the relating one in the encryption procedure. Block diagram of AES encryption and decryption is shown in the following Fig.1

The round change of AES and its means work on some middle outcomes, called state. The state can be envisioned as a rectangular framework with four lines. The quantity of sections in the state is equivalent to the block length in bits separated by 32. For a 128 piece information block (16 bytes) the estimation is 4, consequently the state is treated as a 4*4 framework and every component in the network speaks to a byte. For straight forwardness, in the remainder of the paper, both the information block and the key lengths are considered as 128 piece long. Anyway every one of the discourses and the outcomes remain constant for 192 piece and 256 piece keys also. By utilizing AES calculation the shading image is encoded and sends to the recipient side. The beneficiary again decodes the image and gets the first shading picture. The encoded picture by utilizing AES

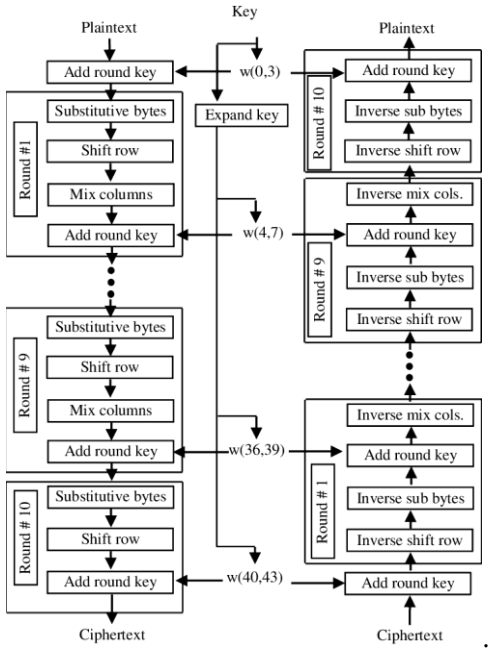

Fig.1 Block Diagram of AES Encryption and Decryption

B. QKD

A critical and extraordinary property of quantum key appropriation is the capacity of the two imparting clients to identify the nearness of any outsider endeavoring to pick up learning of the key [2]. These outcomes from a crucial part of quantum mechanics: the way toward estimating a quantum framework by and large bothers the framework. An outsider attempting to listen in on the key should somehow or another measure it, accordingly presenting noticeable inconsistencies. By utilizing quantum superposition's or quantum snare and transmitting data in quantum expresses, a correspondence framework can be executed that identifies listening in. In the event that the dimension of listening in is underneath a specific edge, a key can be delivered that is destined to be secure, generally no safe key is conceivable and correspondence is prematurely ended. Quantum key distribution is just used to deliver and appropriate a key, not to transmit any message information. This key would then be able to be utilized with any picked encryption calculation to encode and unscramble a message, which would then be able to be transmitted over a standard correspondence channel. In this paper QKD is utilized with encryption utilizing symmetric key calculations like the Advanced Encryption Standard calculation. Quantum correspondence includes encoding data in quantum states, or qubits, instead of traditional correspondence's utilization of bits. Typically, photons are utilized for these quantum states. Quantum key dissemination abuses certain properties of these quantum states to guarantee its security.

C. E91 protocol: Artur Ekert

Artur Ekert's [3,4] plan utilizes ensnared sets of photons. These can be made by sender, by receiver,or by some source separate from them two, including spy Eve. The photons are appropriated so sender and Receiver each end up with one photon from each pair. The plan depends on two properties of entrapment. To begin with, the caught states are impeccably associated as in if Sender and Receiver both measure whether their particles have vertical or level polarizations, they generally find a similar solution with 100% likelihood. The equivalent is valid on the off chance that they both measure some other pair of correlative (symmetrical) polarizations. This requires the two far off gatherings have precise directionality synchronization. Be that as it may, the specific outcomes are totally irregular; it is unimaginable for Sender to anticipate on the off chance that she (and consequently Receiver) will get vertical polarization or level polarization. Second, any endeavor at listening in by Eve demolishes these relationships such that Sender and Receiver can distinguish.

Likewise to BB84, the convention includes a private estimation convention before recognizing the nearness of Eve. The estimation organize includes Sender estimating every photon she gets utilizing some premise from the set while receiver browses where is the premise turned by . They keep their arrangement of premise decisions private until estimations are finished. Two gatherings of photons are made: the main comprises of photons estimated utilizing a similar premise by sender and Receiver while the second contains every single other photon. To recognize listening stealthily, they can process the test measurement utilizing the relationship coefficients between sender bases and receiver like that appeared in the Bell test tests. On the off chance that this were not the situation, at that point Sender and Receiver can finish up Eve has acquainted neighborhood authenticity with the framework, abusing Bell's Theorem. On the off chance that the convention is fruitful, the main gathering can be utilized to produce keys since those photons are totally hostile to adjusted among Sender and Receiver

4. IMPLEMENTATION

In this paper, during encryption the image is taken and the image converted to hexadecimal values and then the hexadecimal values is converted to pixel by using AES. Again in the decryption the pixel image is taken and then converted to hexa decimal values and then the hexa decimal values will be converted to original image. It is explained in the following figure 2 and 3

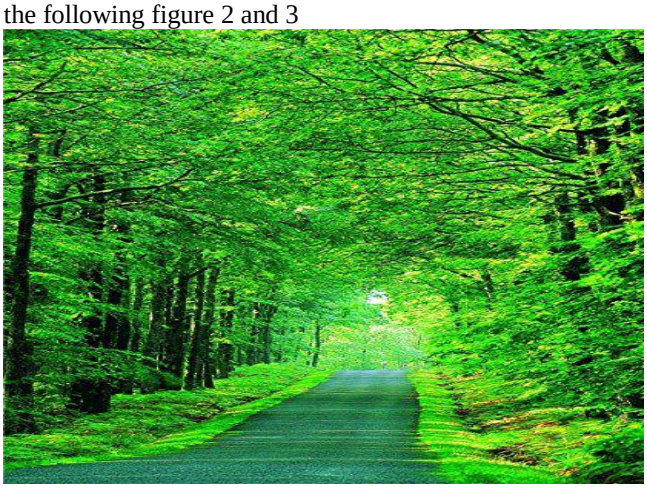

Fig :2 Original Image

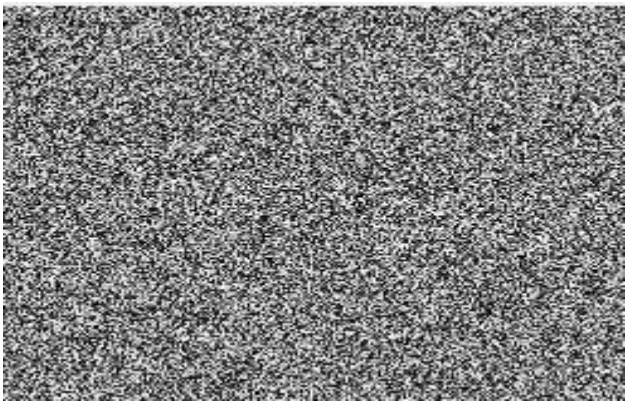

Fig: 3 Decrypted Image

In AES both the sender and receiver uses same key for encryption and decryption. So the key should be shared in secure way. Hence Quantum key Distribution is used in this paper.

5. CONCLUSION

This paper exhibits an encryption strategy for scrambling image utilizing AES algorithm. As of now protection issues are progressively worried in correspondence. So AES is utilized for ie image encryption and unscrambling. Both the sender and beneficiary uses same key for encryption and unscrambling. So the key ought to be exchange safely. Consequently QKD is utilized for exchanging key safely

.

REFERENCES

[1] Daemen, J., and Rijmen, R. The Design of Rijndael: AES–The
Advanced Encryption Standard. New Yrok: Spriger-Verlag, 2002.New York: 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, volume 175, page 8. New York, 1984.

[3] Ekert, Artur Konrad (1991). Correlations in quantum optics *(DPhil thesis). University of Oxford.* OCLC 556450608.

[4] Ekert, Artur (5 August 1991). "Quantum cryptography based on Bell's theorem". Physical Review Letters. American Physical Society. **67**: 661 – 663. Bibcode*:*1991PhRvL..67..661E. doi*:*10.1103/Phys RevLett.67.661. PMID 10044956R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] Color Image Encryption and Decryption Using DES Algorithm Manjula K G1, M N Ravikumar2 International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

[6] Image Encryption using Simplified Data Encryption Standard (S-DES) Sanjay Kumar Department ofComputerScience Engineering Sobhasaria Engineering College, Sikar, India Sandeep Srivastava , International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014

[7] Image Encryption using Triple DES Algorithm Anup R1 & Suchithra R2 , Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-5, 2017 ISSN: 2454-1362

[8] International Mathematical Forum, Vol. 7, 2012, no. 59, 2929 - 2942 Image Encryption Based on the Modified TripleDES Cryptosystem V. M. SILVA-GARCÍA 1 , R. FLORES-CARAPIA 2 , I. LÓPEZ-YAÑEZ 3 and C. RENTERÍA-MÁRQUEZ