iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** X **Month of publication:** October 2017

**DOI:** http://doi.org/10.22214/ijraset.2017.10296

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887*
*Volume 5 Issue X, October 2017- Available at www.ijraset.com*

# Image Encryption

Abass Hassan[1]
[1]*Asst, Professor, Department of Computer Sciences, SRMIET Bhurewala, Ambala, Haryana Affliated to Kurukshetra University, Kurukshetra, Haryana, India.*

***Abstract: Security in transmission of digital images has its importance in today's image communications, due to the increase use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, image security has become a critical issue in the present world. The difficulties in ensuring individuals privacy has become an increasingly challenging. Various techniques have been developed to protect the data and personal privacy. Encryption is probably the most obvious one. In order to protect valuable information from unauthorized access image encryption is must. This paper describes a design of effective security for communication by AES algorithm for encryption and decryption.***
***Keywords: Image Encryption, Symmetric key, Asymmetric key, Cryptography, Encryption, Decryption, Advanced Encryption Standard (AES).***

## I. INTRODUCTION

PC has turned into a key gadget now a days. The fundamental utilization of PC is to store information and to send information from one area to other. The data that is shared must be transported in a protected way. So to keep away from such circumstance information might be scrambled to some organization that is indiscernible by an unapproved individual. In the previous couple of years the security and trustworthiness of information is the primary concern. In the present situation every one of the information is exchanged over PC systems because of which it is defenseless against different sorts of assaults. To make the information secure from different assaults and for the trustworthiness of information we encode the information before it is transmitted or put away.Cryptography is a strategy for putting away and transmitting information in a structure that exclusive those it is planned for can read and process. It is an exploration of securing data by encoding it into an incoherent configuration. It is a successful method for ensuring delicate data as it is put away on media or transmitted through system correspondence ways.

## II. PURPOSE OF CRYPTOGRAPHY

*A. The following are the purpose of cryptography*

1) *Authentication:* The way towards giving one's character. It is another piece of information security that we experience with regular PC utilization.
2) *Integrity:* Numerous a times information should be overhauled however this must be finished by validated Individuals.
3) *Privacy/confidentiality*: Guaranteeing that nobody can read the message aside from the proposed recipient. Encryption is the way toward clouding data to make it confused without exceptional information. Encryption has been utilized to ensure correspondence for quite a long time.

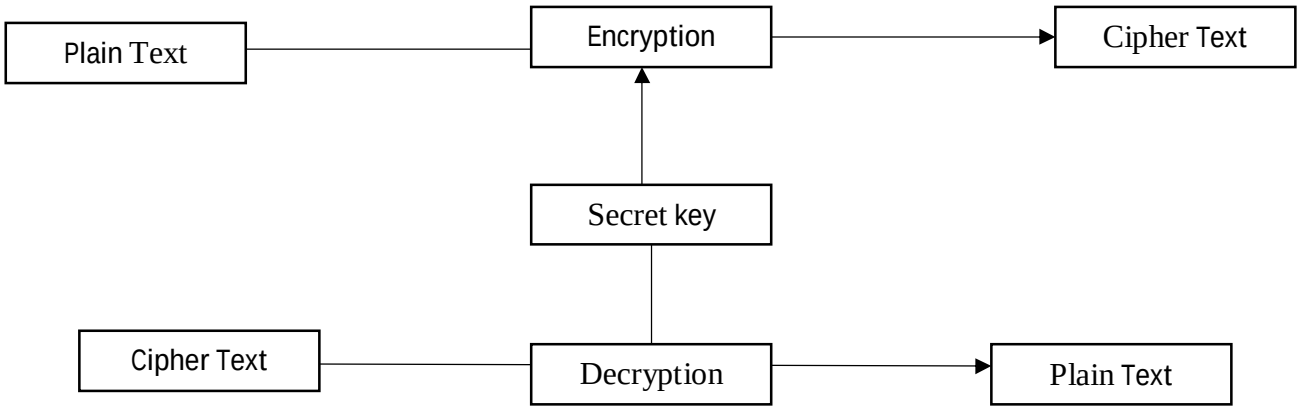



Fig.1.1 Diagram for Encryption and Decryption of Text

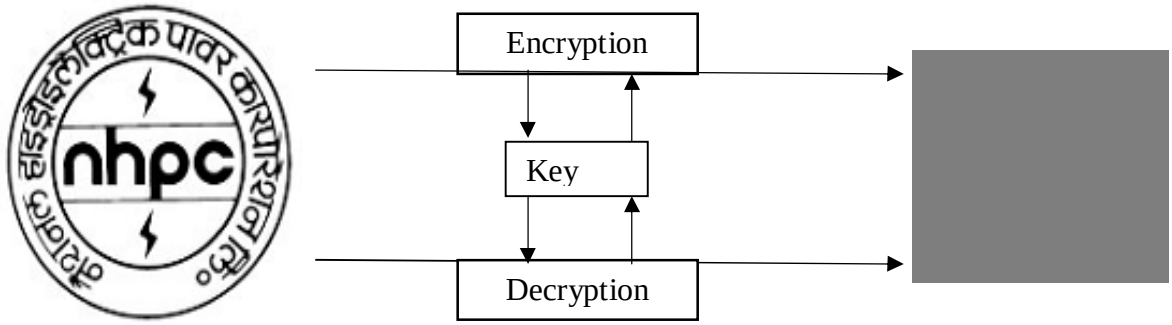



Fig 1.2 Diagram for Encryption and Decryption of an image

## III. IMAGE ENCRYPTION TECHNIQUES

### *A. Classic Image Encryption*

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for substance encryption by Rijmen and Daemen in 1999 [1] besides known as Rijndael calculation, however a couple of researchers made utilitarian utilization of this calculation for picture encryption in like manner with a couple changes in key era and different prerequisites. Zeghid et al. [2] proposed an enhanced AES based calculation by including a key stream generator (A5/1, W7) to AES to ensure upgrading the encryption execution for picture encryption process. A substitute calculation proposed by Subramanyan et al. [3] centered on AES Key Expansion in which the encryption approach is somewhat keen XOR operation of an arrangement of picture pixels other than a 128 piece key that changes for every arrangement of pixels. The keys to be used are delivered uninhibitedly at the sender and beneficiary side centered around AES Key augmentation change subsequently the preparatory key is far off from other people granted as opposed to offering the whole arrangement of keys.Data encryption standard, a predominant square figure calculation uses 64 bit key, which is a substitute printed cryptosystem that used for picture encryption by Qian Gong-canister et al. In [4] another picture encryption arrangement centered around DES combined with a riotous guide acquainted with upgrade the security and build up the key space. The outcomes show that mix of word-based cryptosystems with various techniques or revealing a couple of upgrades, improve the security and against hostile to assault limit of those calculations satisfactorily

### *B. Public Key Image Encryption*

The vast majority of use does not give an office of a protected channel to exchange the private key or longing to keep the unscrambling key in mystery, so we have to use open key cryptography. In any case open key was coursed by Diffie and Hellman in 1976 [5]. It was a key exchange sensible procedure for making bestowed mystery key over a checked correspondence channel without using a previous conferred mystery. Most of ordinary open key cryptosystems planned to encode printed data. A couple works have been dispersed on open key picture encryption, one is proposed by Shuihua et al. [6].

In this arrangement, the plain picture disengaged into pieces using a specific system change and all pixels in every one square traded to DCT field. Open key, private key, encryption strategy and unscrambling technique are described centered around change system of DCT coefficients. The outcomes demonstrate that this framework is vivacious in inconsistency of JPEG lossy clasping and other general strikes. Another open key framework centered around Chebyshev bedlam map depicted by K. Ganesan et al. [1] for shading pictures encryption and elements continuously applications. In any case they endeavored to cryptanalysis the encryption centered aroundChebyshev polynomial guide and results show that it is not effective on a couple assaults, so they endeavored to enhance the security by using a non-Xoring hash capacity to secure it against assault of picked plaintext. They do capability check and some testing for cryptanalysis, for instance, key affectability, association, mono piece, long run test and time examination for both picture and video and decided from the outcome that their prescribed cryptosystem is more secure and solid to any intruder assault and the time examination shows the adequacy of encryption for 64x64 128x128 video encryption.

An image encryption strategy utilizing ECC is proposed by K. Gupta et al. [8] by transforming every pixel into the elliptic arc point to transform the plain image to encrypted image. They only suggested a framework and experiments done with a simple elliptic arc function with few points, so it is not an appropriate system, but as an innovative idea, results demonstrate the adequate encryption time in contrast with other public key techniques like RSA because of key size, and furthermore gives the key affectability yet needs to be upgraded as future works. Visual cryptography (VC) is a simple and safe technique proposed by Naor and Shamir [9] in 1994.

In [10] A. Jaafar and A. Samsudin proposed another public key plan with straightforward and low processing by consolidation of VC and Boolean AND operation comes about a quick running time for encryption and decoding.

## IV. AES ALGORITHM

The Advanced Encryption Standard specifies a Federal Information Processing Standard (FIPS) approved cryptographic algorithm that can be used to protect sensitive data. The advanced Encryption Standard (AES) algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called Ciphertext. Decrypting the Ciphertext converts the data back into its original form called plaintext.

The Advanced Encryption standard (AES) algorithm is a symmetric-key cipher in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the length can be 128, 192 or 256 bits. In addition, the advanced encryption standard algorithm is an iterative algorithm. Each iteration can be called a round and the total number of rounds is 10, 12, or 14, when key length is 128,192 or 256, respectively. The 128 data block is divided into 16 bytes. These bytes are mapped to a 4X4 array called the state. For full encryption, the data is passed through number of rounds ($N_r$=10, 12, 14). The round consists of the following stages for image encryption shown in fig4. 1.

*A.* Substitute Bytes
*B.* Shift Row
*C.* . Mix Columns
*D.* AddRoundKey

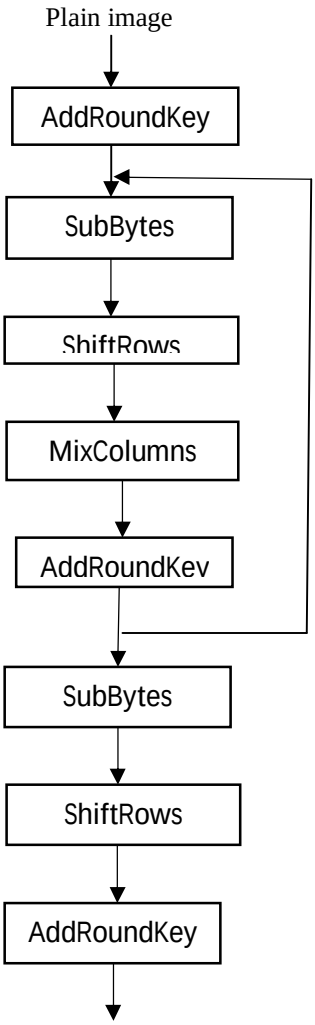



Fig 4.1.AES Image Encryption

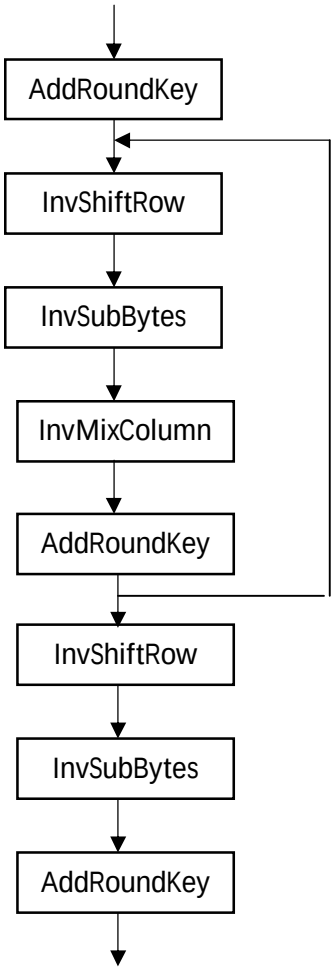
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887*
*Volume 5 Issue X, October 2017- Available at www.ijraset.com*

## V. AES IMAGE DECRYPTION

Conversion of cipher image to plain image or the reverse of encryption is known as decryption.
The round consists of the following stage for image decryption shown in fig 4.2.

*A.* AddRoundKey
*B.* InverseShiftRow
*C.* InverseSubstituteByte
*D.* InverseMixColumns

Cipher image




Plain Image

Figure 4.2 AES Image Decryption

## VI. PARAMETERS

*A. Key Length*

Key Length is the number of bits in a key used by a cryptographic algorithm. Key Length defines the upper bound on an algorithm's security.

*B. Avalanche Effect*

The avalanche effect refers to an attractive property of block ciphers. The avalanche effect is satisfied if: the output changes significantly as a result of a slight change in input.

*C. Security*

The Algorithm provides a very high level of security because of using variable length key that is 128,192 or 256 bits. Different type of attacks tried to crack AES like square attack, key attack, Differential attack and other attacks but none of them is possible to crack this algorithm. So AES is a highly secured encryption technique.

## VI. CONCLUSION

The proposed algorithm offers enhanced security; it aims to provide user satisfaction by transmitting personal and sensitive image data securely. The Advanced Encryption Standard offers the flexibility of allowing different key sizes 128 bit, 192 bit and 256 bit key and security is based on the various random key selection, different S-box and strong transformation. Thus the proposed algorithm offers high encryption quality. There is currentl no evidence that AES has any weakness making any attack.

Also the Advanced Encryption standard algorithm offers high encryption quality. Even AES-128 offers a sufficiently large number of possible keys making an exhaustive search impractical for many decades.

In addition to this the time required for encryption by AES algorithm is less than the time required by DES algorithm. Due to these features the Advanced Encryption Standard (AES) algorithm is suitable for image encryption in real time applications.

## VII. FUTURE WORK

The Advanced Encryption standard algorithm can again be modified to be used for image encryption and decryption. Various algorithms were developed for image encryption like image encryption using combinational permutation technique or combining MATLAB with encoder. But these techniques had its limitations. Also these techniques were not suited for real time applications as it was very fast at the prize of security.

Hence there is a need for an algorithm that in general is applicable for all image security applications in real time. Thus a method that is based on AES key Expansion which overcomes the limitations of above mentioned algorithm is preferred.

## REFERENCES

[1] Shaima A. El-said, Khalid F. A. Hussein, Mohamed M. Fouad, **"**Securing Image Transmission Using In-Compression Encryption", International Journal of Computer Science and Security(IJCSS),volume(4),(pp 466-481),2010.

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption" World Academy of Science, Engineering and Technology( pp 70-75) -2007.

[3] L Krikor,S Baba, T Arif, Z Shabaan, "European Journal of Scientific Research",(pp 89-97),2009.

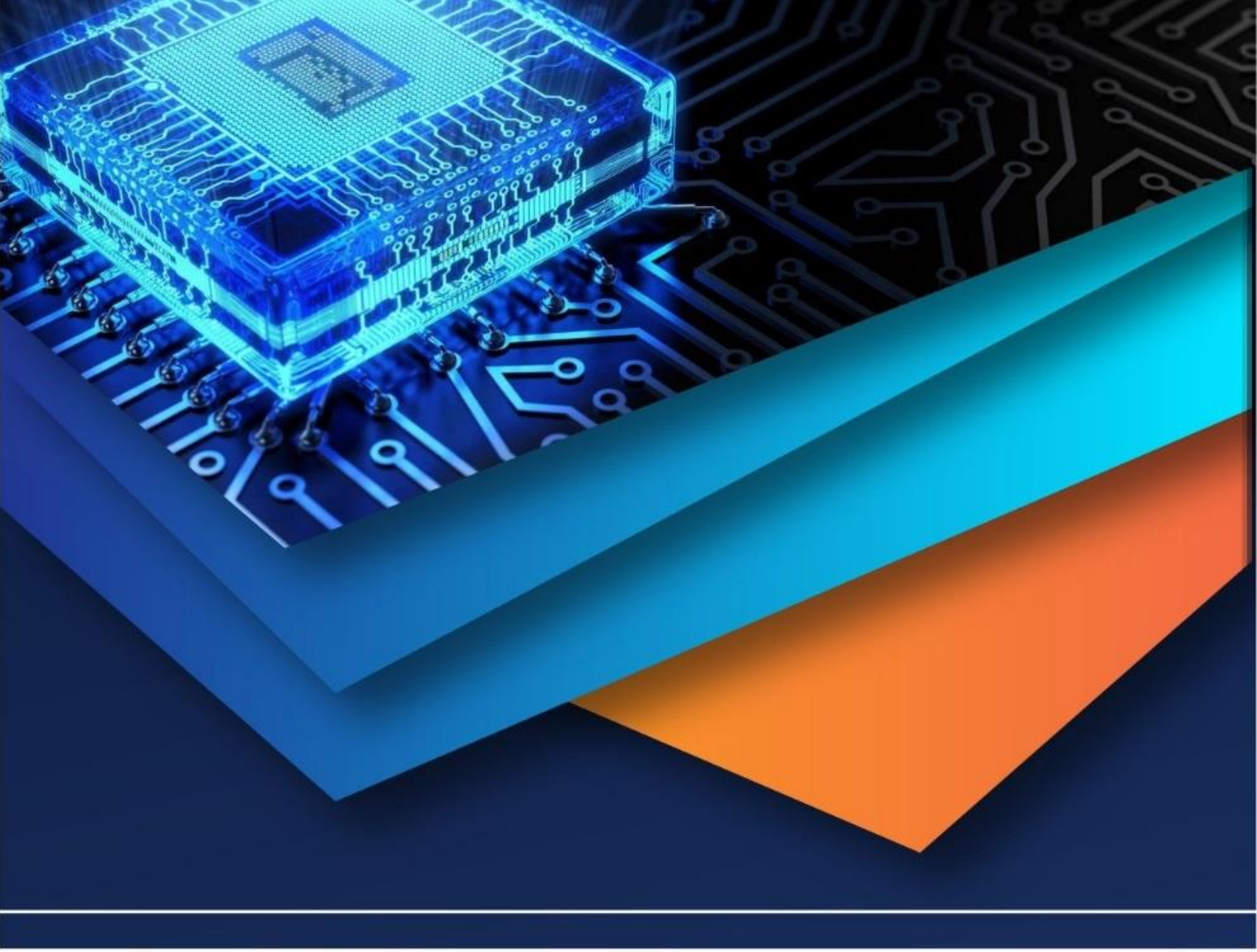
[4] Kamali, S.H., Shakerian, R., Hedayati, M., Rahmani, M., "A new modified version of Advance Encryption Standard based algorithm for image encryption", Electronics and Information Engineering (ICEIE), (vol.1, pp. v1-141)2011 International Conference.

[5] P.Karthigaikumar, SoumiyaRasheed, Simulation of Image Encryption using AES Algorithm, IJCA Special issue on Computational Science-New Dimensions and Perspectives NCCSE, 2011,166-172.

[6] P.Radhadevi,P.kalpana,"secure image Encryption using AES algorithm", International Journal of Research in International Journal of,(pp 115-117).2012

[7] MansoorEbrahim, Shugaat Khan Umer Bin Khalid, "Comparative analysis of Symmetric Algorithms" , International Journal of Computer Applications of pp(12-19).2013

[8] Manoj.B, Manjula N Harihar, "Image Encryption and decryption using AES algorithm" International Journal of International Journal (pp. 290-294) june-2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY