Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

IMAGE ENCRYPTION BY USING ENHANCED AES ALGORITHM: A REVIEW PAPER

Dr. S. Kaushik
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: s.kaushik@jainuniversity.ac.in

Abstract

AES (Advanced Encryption Algorithm) is a block cypher, which is worldwide implemented for encryption of data. Since 2001, it has been recognized as a standard for data protection. AES is a substitution and permutation cypher that generates uncertainty in the algorithm by using the substitution box (S-Box). The key downside of AES is that in the algorithm, it uses static S-Box, which undermines AES security and may be exposed to various algebraic attacks. The new Dynamic AES algorithm developed by key based dynamic S-Box uses dynamic irreducible polynomial and affine constant to solve this problem. The research is carried out on grey scale images and colour images. Using regular AES and Dynamic AES, both images are encrypted and decrypted. Algorithm quality and level of protection are evaluated based on parameters such as Image Histogram Analysis, Adjacent Pixel Correlation Analysis, Image Entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Quality of Encryption.

Keywords: *Communication, Digital Image, Image Encryption, Image Data, Models, Algorithms.*

I. INTRODUCTION

In recent years, with the rapid growth of computer technology, digital image processing technology has also rapidly developed and penetrated into all areas of life, such as remote sensing, industrial detection, medicine, meteorology, communication, science, intelligent robots, etc. Image knowledge has, thus, attracted widespread interest. Image data protection is very important, especially in special military, commercial and medical areas [1]. Picture encryption has been one of the ways of securing the transmission of digital files [2]. However, image data has the features of large data volumes, strong correlation and high redundancy, resulting in low encryption efficiency and low security, so conventional encryption algorithms such as the Data Encryption

Standard (DES) and the Advanced Encryption Standard (AES) do not meet the needs of image encryption [3].

Fig.1: Illustrates the Real Images and Encrypted Images.

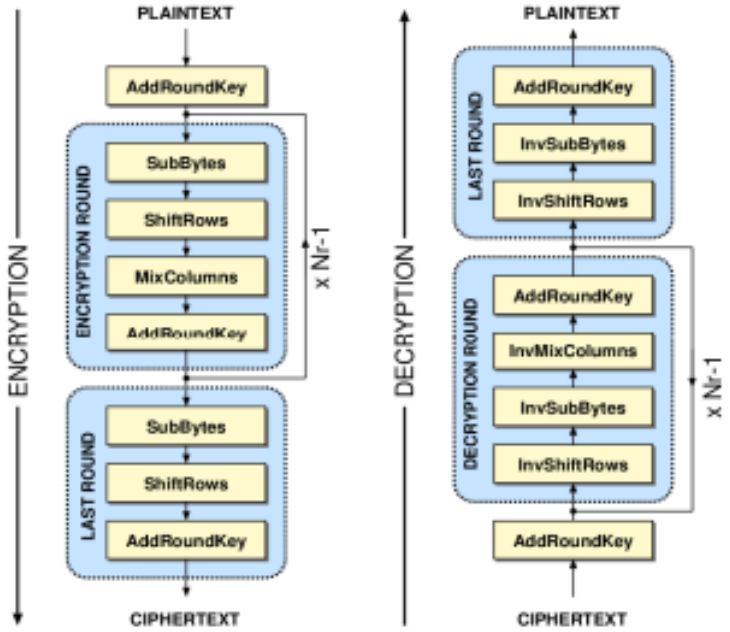

Fig. 2: Illustrates the AES algorithm [4]

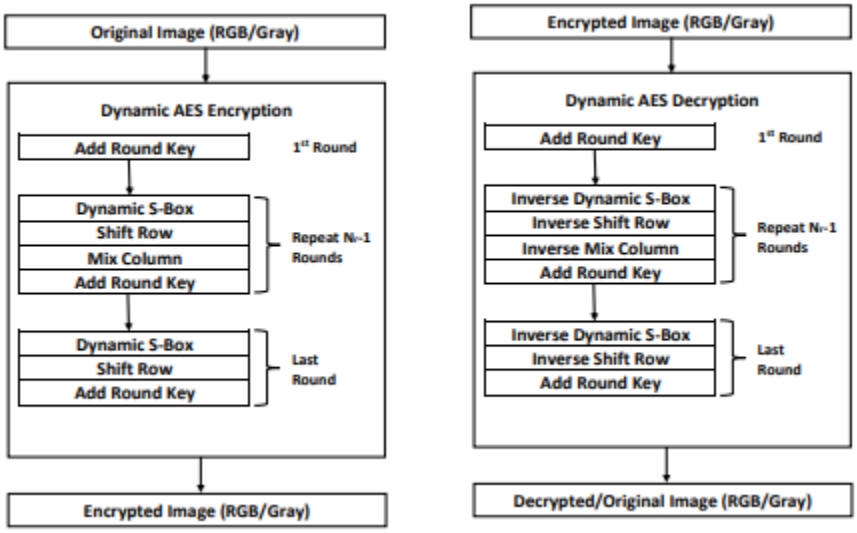

Fig. 3: Illustrates the Enhanced AES Encryption and Decryption algorithm [5]

A hash function is a function which may be utilized in order to map the data of arbitrary size to data of a fixed size. Here, we utilize the SHA-256 to originate the 256-bit hash value V, that can be segregated into 32 blocks with the same size of 8-bit, the i-th block vi ∈ [0, 255], i = 1, 2, . . . , 32, so it can be expressed as V = v1, v2, . . . , v32. Suppose the size of the plain-image P is m × n, obtain an integer k as:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\;(y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)}\; \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

II. LITERATURE REVIEW

A analysis of the image compression and encryption method based on 2D compression sensing and fractional transformation of Mellin was performed by Zhou et al. Most of the latest techniques of image encryption bear security risks for linear transformation or are expanded by encryption data for direct nonlinear transformation adoption. To overcome these difficulties by combining 2D compressive sensing with nonlinear fractional Mellin transformation, a novel image compression-encryption scheme is proposed. In this scheme, the original image is measured in two directions by measurement matrices to simultaneously achieve compression and encryption, and then the nonlinear fractional Mellin transform re-encrypts the resulting image. The measuring matrices are managed by a map of chaos. To obtain the decryption image, the Newton Smoothed l0 Standard (NSL0) algorithm is applied. The results of the simulation verify the validity and reliability of this regime [6].

III. DISCUSSION AND CONCLUSION

A new image encryption method that includes three key components is proposed: inserting image pixels, pixel scrambling, and pixel diffusion. First, the plaintext image hash value is transformed into a pseudo-random sequence, then pseudo-random sequences are applied to the plaintext image field surrounding it. In the permutation and diffusion method, the pseudo-random sequences used are connected to the plaintext image, which can resist the selected plaintext attack. Our algorithm converts the hash value of the plaintext image, unlike previous algorithms, into a pseudo-random sequence, which takes the pseudo-random sequence as part of the encrypted image, whereas the previous algorithm takes the plaintext image's hash value as part of the key. The key of the encryption scheme is just the initial value of the chaotic system in our encryption algorithm, minimizing the complexity of key management.

IV. REFERENCES

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, 2004, doi: 10.1016/j.chaos.2003.12.022.

[2] S. Kumar, A. Gupta, and A. Arya, *Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio*. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-

9801, 2016.

[3] E. N. Kumar and E. S. Kumar, “A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach,” 2013.

[4] Y. Zhou, L. Bao, and C. L. P. Chen, “A new 1D chaotic system for image encryption,” *Signal Processing*, 2014, doi: 10.1016/j.sigpro.2013.10.034.

[5] L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” *Opt. Lasers Eng.*, 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[6] O. Mirzaei, M. Yaghoobi, and H. Irani, “A new image encryption method: Parallel sub-image encryption with hyper chaos,” *Nonlinear Dyn.*, 2012, doi: 10.1007/s11071-011-0006-6.