Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

NOVEL IMAGE ENCRYPTION METHOD BY APPLYING AES MODIFICATION: A REVIEW ARTICLE

Dr. P. Pradeepa
Associate Professor, Department of EEE, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: p.pradeepa@jainuniversity.ac.in.

Abstract

In this article, based on the updated advanced encryption standard (AES) algorithm, a high-speed and highly restricted encryption algorithm is proposed to encrypt high-definition (HD) images. AES is a well-known block cypher algorithm and has many benefits, such as the ability to enforce high-level protection and deployment. AES, however, has some disadvantages, including high costs of computation, pattern appearance, and high specifications for hardware. When the AES algorithm cyphers an image, especially HD images, the aforementioned issues become more complex. In this paper, three improvements are suggested to improve the efficiency of the AES algorithm by reducing the cost of computing, reducing hardware requirements, and increasing the level of security. First, modification was carried out in 5 rounds using Mix Column transformation instead of 10 rounds in the original AES-128 to reduce the time of encryption. By introducing Mix Column transformation to this operation as a second change, security is improved by enhancing the main schedule operation.

Keywords: *Encryption, Image, Internet, Multimedia, Data compression, Protection, Transformation.*

I. INTRODUCTION

The rapid growth in communication techniques, such as satellite, mobile, Internet and ground communications, has resulted in an urgent need to safeguard important individual, general and universal devices and their respective data against attackers, illegal copying and allocation [1]. By translating the data into an incomprehensible form, encryption algorithms are used as the best way to preserve the security of transmitted data [2].

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

Figure 1: Illustrates the real and encrypted images.

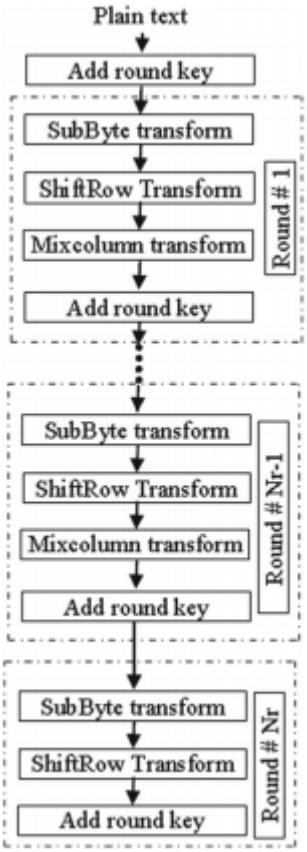

Figure 2: Illustrates the modified AES algorithm structure [3]

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

$$MAE = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}|p(i,j) - E(i,j)|$$

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y)$, $D(x)$ and $D(y)$ can be evaluated by using the following equations [5].

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

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

II. LITERATURE REVIEW

Chai et al. investigated a color image cryptosystem based on dynamic DNA encryption and chaos. This paper introduces a cryptosystem of color images based on complex DNA encryption and chaos. First, the plain color image is decomposed into red, green and blue elements, and then a plain-text-dependent simultaneous intra-inter-component permutation mechanism (SCPMDP) is introduced to shuffle them. Secondly, a DNA encoding rule transforms the recombined permutable components into a DNA matrix.

III. DISCUSSION AND CONCLUSION

Some attempts to change the AES algorithm have been made. Both of these changes, however, did not concentrate on the execution time. Therefore, with image encryption,

particularly HD images, the original and previously updated versions of the AES algorithm take more time. In the MC transformation, the largest number of computations in the AES algorithm was reduced. Therefore, the first change was based on the reduction of the MC transformation execution times from 10 to 5. (Executed only in the first, third, fifth, seventh, and ninth rounds). The cost of computing and encryption/decryption time will therefore be decreased, making the changed AES more compatible with image ciphering, especially HD images

IV. REFERENCES

[1] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[2] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Optics and Lasers in Engineering, 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[3] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," Signal Processing, 2012, doi: 10.1016/j.sigpro.2011.10.023.

[4] 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.

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