ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 10, October 2021

Encryption – JPEG - LS for Medical Image Reliability Control in Encrypted and Compressed Domains

[1] Mahamuthunesha K, [2] Dr. Arunachala Perumal C, [3] Dr. G. Kavya
[1] PG Student, Department of ECE, SA Engineering College, Chennai (India)
[2] Professor, Department of ECE, SA Engineering College, Chennai (India)
[3] Head of Department, Department of ECE, SA Engineering College, Chennai (India)

***Abstract*--- Image data security is the essential portion in communication and multimedia world as part of sharing and storing information to avoid third party access. In this paper, the first joint encryption-compression scheme for the purpose of protecting the medical images has been proposed. The main originality of this scheme stands on its ability to give access to security services from both encrypted and compressed image bit streams without having to decrypt or to decompress them, even partially. A second contribution is that it combines in a single algorithm the bit substitution modulation with JPEG-LS and the AES block cipher algorithm in its CBC mode. On the other side, decompression, decryption and message extraction are conducted separately. Doing so makes the proposed scheme compliant to the medical image standard DICOM. This scheme allows tracing images and controlling their reliability (i.e. based on proofs of image integrity and authenticity) either from the encrypted domain or from the compressed domain. The experiments conducted on broad set of medical images like Retina and ultrasound images demonstrate the capability of our system to securely make available a message in both encrypted and compressed domains while minimizing image distortion.**

***Index Terms*— Image Encryption & Decryption, Advanced Encryption Standard, Cipher, Medical Image**

I. INTRODUCTION

Security of image data has become increasingly important for many applications like video conferencing secure facsimile, medical, military applications etc. It is hard to prevent unauthorized people from eavesdropping in any communication system including internet. Cryptography provides a method for security and authenticating the transmission of information over insecure channels. Images are generally the collection of pixels. Encryption (sometimes called as Encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm to make it unreadable(known as cipher)to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called a decipherment). With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission.

II. LITERATURE SURVEY

P.Prasithsangaree et al (2003) have presented and analyzed the Energy Consumption of RC4 and AES Algorithms in Wireless LANs. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RC4 is fast and energy efficient for encrypting large packets and AES was more efficient than RC4 for a smaller packet size. From the results, it appears that we can save energy by using a combination of RC4 and AES to provide encryption for any packet size. [8]

Iqtadar Hussain and Tariq Shah et al (2011) have presented and analyzed on the complexity of encryption essentially depends on the strength of S-box. It is observed that several properties like non linearity, strict avalanche criterion (SAC), bit independence criterion (BIC), differential approximation probability (DP), and linear approximation probability (LP) of these boxes are similar. These properties enable the user to determine the strength of an S-box. It appears that AES S-box and S8 AES S-box have identical properties and parameters. [10]

III. AES ALGORITHM

The AES (advanced encryption standard) [3] is an encryption standard as a symmetric block cipher. It was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26,2001. The Rijndael algorithm was developed by Joan Daemen of Proton World International and Vincent Fijmen of Katholieke University at Leuven. Generally, Rijndael will implement 9 processing rounds in case both the key length as well as the block key is 128 bit,

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 10, October 2021

but if either the block or the key is 192 bit, Rijndael will implement 11 processing rounds, while Rijndael implements 13 processing rounds if it's 256 bit [11]. Basically, algorithm would act rather different as a result to each encryption key size, accordingly, when the key size increases, it will have a double facet function: the number of the bits increases for rushing data, and the complication of the cipher algorithm increases [7].

A. AES Encryption and Decryption

For each round of AES, 128 bit input data and 128 bit key is required i.e., it needs 4 words of key in one round thus the input key must be expanded to the required number of words depending upon the number of rounds. The output of each round serves as input to the next stage. In AES system, same secret key is used for both encryption and decryption, thus simplifies the design. For both its cipher and inverse cipher, the AES algorithm uses a round function i.e. composed from four different byte-oriented transformations:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The above four transformations are looped Nr-1 times. In the last round Mix column is not performed.[4]

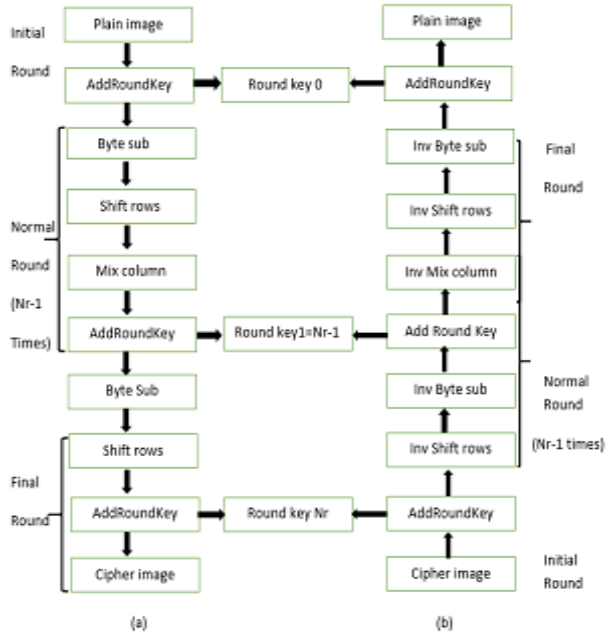


Figure 1: Design flow of AES algorithm (a) Encryption Process (b) Decryption process

The tenth round Mix columns stage is not included. The nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

B. AES Transformation

B.1. Substitute Bytes:

It is a nonlinear byte substitution, using a substation table (S-box) each byte from the input state is replaced by another byte.[5] The substitution is invertible and is constructed by the composition of two transformations as described below. The substitute bytes operation is as shown in Figure 2.

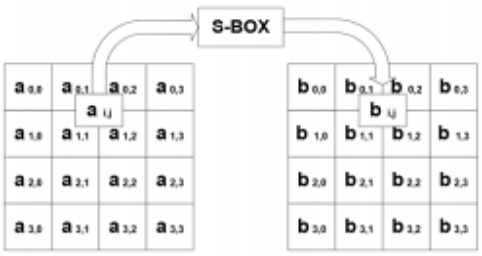


Figure.2: Substitution Bytes

B.1.1. Inverse Substitute Bytes:

It is the reverse operation of the Substitute Bytes transformation, in which the inverse S-box is applied to each byte of the state. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (28).

B. 2. Shift rows:

Shift rows operate on individual rows of the state. It provides diffusion throughout the AES algorithm. In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the left, respectively as shown in Figure 3.

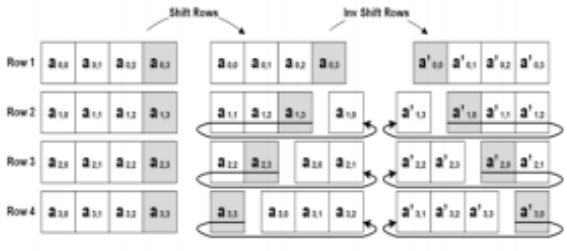


Figure 3: Shift row operation

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 10, October 2021

B.2.1 Inverse Shift rows:

It is the inverse of the shift rows; the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the right, respectively.[1]

B.3. Mix columns:

In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial a(x), the operation of Mix Column is as shown in Figure 4.

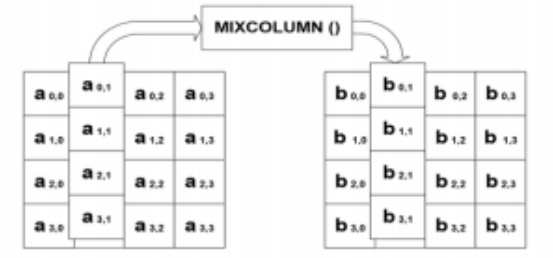


Figure 4: Mix column operation

B.3.1. Inverse Mix columns:

In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial b(x),

$$b(x) = 0B*x3 + 0D*x2 + 09*x + 0E$$

The result is the corresponding column of the output state. As it is not so straightforward hardware implementation as Mix column, so if we compare both, Inverse Mix Col requires more logic resources for implementation.[6]

B.4. Add round key:

The Add Round Key operation is as shown in Figure, which is a simple XOR operation between the State and the Round Key. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element:

$$b(i, j) = a(i, j)\ k(i, j)$$

Where a is the current State, b the next State and k is the round key.

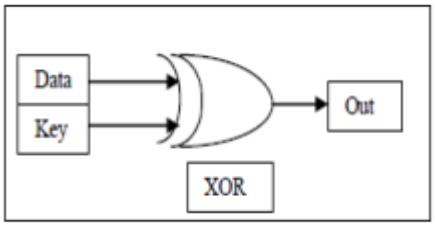


Figure 5: Hardware Implementation of Add Round Key

IV. STATISTICAL ANALYSIS

Performance Metrics

Table 1: Analytical Comparison of Encryption Algorithms

Encryption Algorithms	Histogram analysis	Correlation analysis	Entropy	PSNR
Vigenère	Very poor	Very poor	Moderate	Moderate
AES	Good	Moderate	Good	Good
ECC	Moderate	Moderate	Poor	Excellent
DES	Moderate	Moderate	Good	Good
3-DES	Moderate	Moderate	Good	Good

Security & Breakable Analysis

The professional cryptography industry and the NSA consider AES to be unbreakable and hence chosen as the universal cryptography standard. Key management techniques can be implemented and keys can be often rotated as a countermeasure to the classic attack (Brute force attack). AES would take billions of years to break using current computing technology like brute force attack whereas a 56-bit DES key can be cracked in less than a day.[9]

Computational Analysis

Table 2: Features of Encryption Algorithms

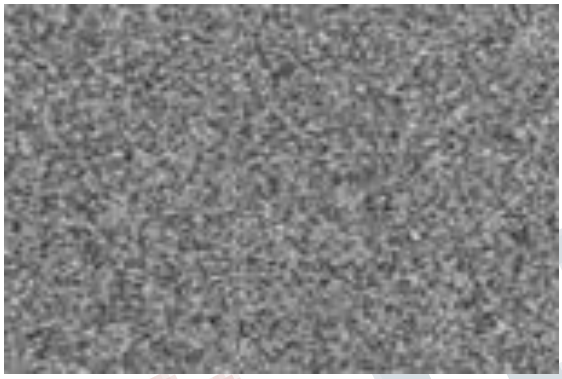
Encryption Algorithms	Key Size	Speed	Security Level
BF	128-448	Fast	Belived Secure
AES	128,192,256	Fast	Secure
DES	56	Slow	Insecure
Triple DES	112,168	Very Slow	Moderately Secure

From Table 2, it is shown that AES is fast, and secure compared to other mentioned encryption techniques.[2]

V. RESULTS

AES algorithm is implemented using the MATLAB platform. Here image is taken as input, applying the AES encryption algorithm creates a cipher mage and this cipher image is input to the decryption algorithm which reconstructs the original image back. This paper presents the literature survey and study of AES algorithm for high speed and wireless communication applications. Also the process of sub byte transformation, shift row transformation, mix column transformation, add round key, S-box and key expansion is studied. The existing AES algorithm is studied and analysed to promote the performance of the encryption methods also to ensure the security proceedings.

Input Image



Encrypted Image

Output Image

REFERENCES

[1] Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors.

[2] Biham, Eli and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.

[3] Debnath, R., Agrawal, P., &Vaishnav, G. (2014). DES, AES And Triple DES: Symmetric Key Cryptography Algorithm. International Journal of Science, Engineering and Technology Research, 3(3) 652–654.

[4] Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI "An FPGA Design of AES Encryption Circuit with 128-bit Keys" GLSVLSI'05, ACM 2005.

[5] Jin Gong ,Wenyi Liu, Huixin Zhang "Multiple Lookup Table- Based AES Encryption Algorithm Implementation" Elseveir- 2012 vol.25 pg no.842 – 847.

[6] Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. International Journal for Light and Electron Optics, 127(4), 2341-2345.

[7] Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaosbased image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, 90, 238-246.

[8] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM, pp. 1445-1449, 2003.

[9] Singhal, N., & Raina, J. P. S. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. International Journal of Computer Trends and Technology, 2(6), 177-181.

[10] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion", International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011.

[11] Xinmiao Zhang and Keshab K. Parhi "Implementation Approaches for the Advanced Encryption Standard Algorithm"IEEE 2002.