ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

# Implementation of Advanced Encryption Standard (AES) Algorithm for Image Encryption

Abhijeet Patil[1], Palhavi kerkar [2]
ME Student[1], Assistant Professor[2]
Department of Electronics and Telecommunication Engineering
Goa College of Engineering, Ponda Goa, India

**Abstract:**
Hacking of confidential data is increasing at alarming rate. Transmission of confidential data in the form of images is growing drastically all over the world. Therefore the subject of securing this data against the unauthorized attack is a study of utmost importance. In order to secure image transmission, various cryptographic algorithms are used. This paper proposes AES Encryption Algorithm with modification in Shift Row Transformation to reduce the number of calculations without harming its security. Here, in addition, the Key Expansion Technique is processed in a parallel manner which boosts the execution time reduction. Paper also aims at reducing the time required for encrypting and decrypting the image by keeping its security intact. Proposed modification technique takes lesser execution time and is highly secured as it is highly sensitive to its key and also immune to other known attacks. The results prove that with a comparison to conventional AES encryption algorithm, the proposed algorithm gives better encryption and decryption results in terms of security against unauthorized access. A program is executed using Eclipse Java Neon.2 software tool and security analysis is done using MATLAB 2012.

**Keywords:** Advanced Encryption Standard (AES), Decryption, Encryption, Shift Row Transformation, Key Expansion Technique.

## I. INTRODUCTION

In this technological era, images are used at a very large scale for transmission of confidential information. Security of the confidential data and other multimedia such as images is becoming an important issue because of their transmission over an unsecured network, to prevent unauthorized access. Encryption is a most widely used technique used for securing the data from hacking. It is a process of converting information/data into a random data to prevent it from unauthorized access. Encryption of images and videos finds applications in various fields including internet communication, multimedia systems, medical imaging, Telemedicine and military communication, video-on-demand, video conferencing, data broadcasting etc. [5]. Various data encryption algorithms such as AES, RSA, or IDEA have been proposed until now most of which are used in the text or binary data format [1]. For data security, we have various cryptographic algorithms, but to secure multimedia data such as images, we face lots of challenges as images have a very high correlation among pixels, redundancy, high transmission rate with limited bandwidth and bulk data capacity [3]. Considering the previously mentioned properties of the multimedia data it is hard to utilize these data encryption algorithms directly for multimedia data. Taking above constraints in thought and to work for real-time applications, a design of new algorithms that require less computational power without affecting the security of the data has always been a subject of interest for design engineers [3]. In order to achieve reliable security in storage and during transmission of digital images, while communicating over the insecure channel like internet, airwaves, GSM and Wi-Fi, Advanced Encryption Standard (AES) algorithm is used all over the world as it is highly secured having high throughput, high speed and is used against various attacking techniques  Till date, a ton of work has been accomplished for the AES implementations. Seyed Hossein Kamali [1] designed a new modified version of AES, by adjusting the shift row transformation. The modification gives the better encryption results in terms of security against statistical attacks when compared with conventional AES. Here, the modification part reduces the number of calculations and thus increases the speed. Neha Dalakoti [2] utilized the parallel handling of key expansion technique and accomplished an improvement in the throughput. It additionally reduces the hardware requirement for implementation of AES. In another research work, key changes for every set of pixels. The keys are generated using the normal key expansion process independently at the sender and recipient, only the initial key is shared rather than sharing whole set of keys [3]. It indicates better encryption results and shows great resistance against different known attacks but since new key is generated for every set of pixel makes it unsuitable for few real time application where a lot of information must be shared inside less measure of time. And major disadvantage of this paper is that receiver must know the resolution of each image that sender is sending for key generation. Qi Zhang [4], has presented a digital image encryption technology based upon AES algorithm and demonstrated that the technique can better understand the impact of encryption and decryption. In [5], they have proposed MPEG video encryption algorithm based on AES with modification in shift row transformation. The algorithm does not require any additional operation or hardware just the original AES. Chaos theory was firstly utilized as a part of the encryption framework by Edward Lorenz in 1963. During the last few decade chaos based cryptography has receive more attention due to noise like signal for unauthorized person, ergodicity, mixing, making confusion in the pixels of images ,sensitivity to initial conditions, can be connected with those of coded image, such as confusion and diffusion [8]. In chaotic based AES image encryption algorithm by Syed Shahzad Hussain Shah [6], has generated the key by chaotic maps and encryption is done by AES. Parallel RAMs are used to implement Sub-Bytes operation and also optimization is done in internal rounds. For further improvement in the speed, they have synchronized the key expansion unit which generates round key in each clock cycle; keys are stored and read from the key RAM in same clock cycle. Mr. Atul M. Borkar [7] proposed an efficient FPGA implementation of 128 bit block and 128 bit key AES cryptosystem and all the transformations of algorithm are simulated using an iterative design approach in order to minimize the hardware consumption. Pradeep H Kharat [8] determined the procedure in which the first image is encrypted using an encryption key and the extra information is hided into the encrypted image using a data-hiding key. The additional information is embedded with an encrypted image using LSB algorithm. In our paper, we have executed the AES algorithm for image encryption with modification in shift row transformation with keeping its security intake. Change diminishes the number of calculations and enhances the encryption performance. For further speedup, the key expansion technique is processed in a parallel manner. The paper is further organized as follows: Section 2, explains the AES algorithm. The proposed algorithm is talked about in Section 3 while the security and performance analysis results are analyzed in Section 4. Finally, the conclusion is drawn in Section 5 and Section 6 is acknowledgments.

## II. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES is most important symmetric algorithm in the world and was developed by Joan Daemon and Vincent Rijmen. It is a 128 bit block cipher with key lengths of 128/192/256 bits. The number of rounds depends upon the key length. For 128 bit key 10 rounds are used and these are sufficient to protect the classified information up to the secret level. Top secret information requires longer keys. For 128 bit key we have $2^{128}$ possible keys thus makes AES highly secured. AES encrypts all 128 bits of data path in one round and is divided into 3 processes Encryption Process, Decryption Process and Key Expansion Process.

### A. Encryption & Decryption Process

Encryption Process is a series of transformation beginning with an initial round and completing with a final round. Each round has four transformations Bytes Substitution Transformation, Shift Rows Transformation, Mix Columns and Round Key Addition. The Bytes Substitution provides the confusion, Shift Rows and Mix Columns provides diffusion. Decryption is just opposite to Encryption process, its four stages include Inverse Bytes Substitution Transformation, Inverse Shift Rows Transformation, Inverse Mix Columns Transformation and Round Key Addition Transformation.

➢ **Bytes Substitution Transformation:** In Bytes Substitution we make utilization of a substitution box (S box) to lookup for a new value. Here selection of row based upon the lower nibble and column by upper nibble. This gives a new hex value for the first byte and the same process is repeated for remaining bytes of the state matrix. S-box is invertible is constructed by first taking the multiplicative inverse in the finite field GF (28) with irreducible polynomial m(x) = x8 + x4+ x3 + x + 1 [8].

➢ **Inverse Bytes Substitution Transformation:** Inverse Bytes Substitution is just opposite to the Bytes Substitution. For the replacement of every byte in the state matrix, we make use of inverse substitution box.

➢ **Shift Rows Transformation:** This is done by progressively shifting the first byte of the row depending upon the row number. First row is not shifted at all, second row is shifted by one byte, third row by two bytes and fourth row by three bytes so on.

➢ **Inverse Shift Rows Transformation:** In the decryption process, the transformation is called Inverse Shift Rows Transformation. The operation is nearly the same in the decryption process except for the fact that the shifting offsets have different values [8].The shifting of bytes is done to the right by one, two and three bytes.

➢ **Mix Columns Transformation:** This transformation operates on the State column-by-column, treating each column as a four-term polynomial [8]. The columns are considered as polynomials over GF (28) and multiplied by modulo x4 + 1 with a fixed polynomial a(x) = {03} x3+ {01} x2+ {01} x+ {02} [8]. Four bytes of each column are combined using an invertible linear transformation such that each input byte effects the 4 output bytes. This is done by taking each column at a time and applying matrix operations.

➢ **Inverse Mix Columns Transformation:** Inverse Mix Columns Transformation is reverse of Mix Columns Transformation, where all the mix column operations were done in reverse manner. It requires logic resources more as compared to the mix columns [2].

➢ **Round Key Addition:** In Round Key Addition sub keys are combine with the state matrix. Each sub key is added byte by byte one column at a time to the output of mix columns. For each round different sub keys are utilized. The sub keys are derived from the main key.

### B. Key Expansion Process

This is where the keys are expanded from a short key of 16 bytes into the number of separate round keys also of 16 bytes. The transformations are Rotate, SubBytes and Rcon. Subsequent column for the first key are generated from the key until a new 16 byte sub key has been created. Once this is completed the process is repeated to create the next sub keys.

➢ **Rotate:** The first transformation in creating a sub keys is rotate, which performs a one byte circular left shift on a word i.e. RotWord [b0,b1,b2,b3] = [b1,b2,b3,b0].

- **SubBytes:** Sub Bytes performs a byte substitution on each byte of input word using the S-box.

- **Rcon (Round Constant):** Rcon is performed using Rijndeal finite field. The first column of the state matrix is XOR ed with the last column of the state matrix which is then XOR ed with the Rcon. This process is repeated for the remaining columns of the sub keys.

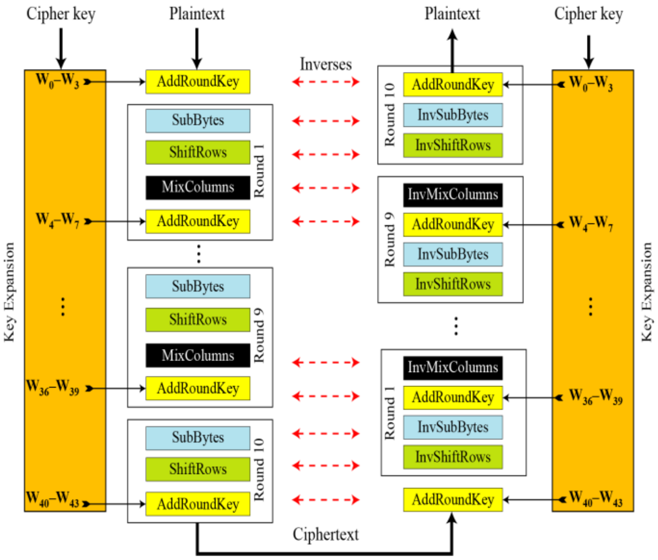
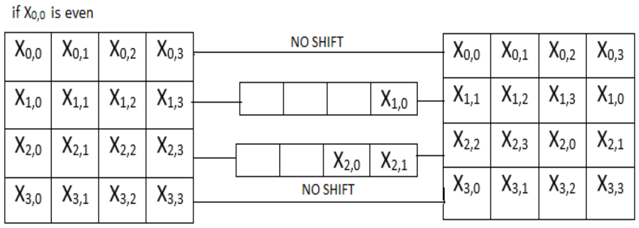


**Figure.1. Structure of AES algorithm for encryption and decryption process.**

## III. PROPOSED AES ALGORITHM

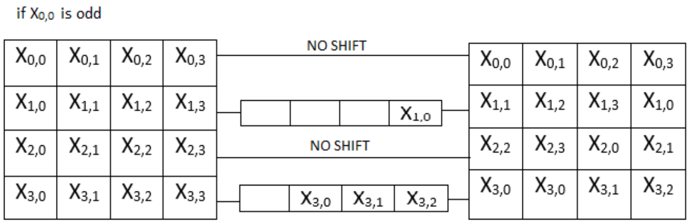
This paper proposes an altered AES Algorithm which lessens the execution time required for encryption and decryption of an image using the modification in the shift row transformations, without influencing the security. For further lift up in speed, the parallel processing of key expansion technique is used. In standard AES algorithm during shift row transformation, the first row of the state matrix remains unchanged and rest all rows are shifted to the left with a subsequent period depending on the row number. In proposed algorithm, the first row of the state matrix remains unchanged but depending upon the value of the state X $_{(0, 0)}$ the row shifting transformation is done. If the value of the state X $_{(0, 0)}$ is even, then the fourth row is kept unchanged along with the first row of the state and the shifting operation is performed on the second and third row of the state matrix. The second row and third row is in row shifted by one position and by two positions to the left respectively. Figure 2 shows the modification in shift row transformations when the value of the state X $_{(0, 0)}$ is even.



if $X_{0,0}$ is even
$X_{0,0}$ $X_{0,1}$ $X_{0,2}$ $X_{0,3}$
$X_{1,0}$ $X_{1,1}$ $X_{1,2}$ $X_{1,3}$
$X_{2,0}$ $X_{2,1}$ $X_{2,2}$ $X_{2,3}$
$X_{3,0}$ $X_{3,1}$ $X_{3,2}$ $X_{3,3}$
NO SHIFT
$X_{1,0}$
$X_{2,0}$ $X_{2,1}$
NO SHIFT
$X_{0,0}$ $X_{0,1}$ $X_{0,2}$ $X_{0,3}$
$X_{1,1}$ $X_{1,2}$ $X_{1,3}$ $X_{1,0}$
$X_{2,2}$ $X_{2,3}$ $X_{2,0}$ $X_{2,1}$
$X_{3,0}$ $X_{3,1}$ $X_{3,2}$ $X_{3,3}$

**Figure.2. State X $_{(0, 0)}$ is even.**

If a value of the state X $_{(0, 0)}$ is odd then first and third rows of the state matrix are kept intact while second row and fourth row of the state matrix are respectively shifted by one and three positions to the left. Figure 3 shows the modification in Shift Row transformations when the value of the state X $_{(0, 0)}$ is odd.



if $X_{0,0}$ is odd
$X_{0,0}$ $X_{0,1}$ $X_{0,2}$ $X_{0,3}$
$X_{1,0}$ $X_{1,1}$ $X_{1,2}$ $X_{1,3}$
$X_{2,0}$ $X_{2,1}$ $X_{2,2}$ $X_{2,3}$
$X_{3,0}$ $X_{3,1}$ $X_{3,2}$ $X_{3,3}$
NO SHIFT
$X_{1,0}$
NO SHIFT
$X_{3,0}$ $X_{3,1}$ $X_{3,2}$
$X_{0,0}$ $X_{0,1}$ $X_{0,2}$ $X_{0,3}$
$X_{1,1}$ $X_{1,2}$ $X_{1,3}$ $X_{1,0}$
$X_{2,2}$ $X_{2,3}$ $X_{2,0}$ $X_{2,1}$
$X_{3,0}$ $X_{3,0}$ $X_{3,1}$ $X_{3,2}$

**Figure. 3. State X $_{(0, 0)}$ is odd.**

This modification in AES algorithm accelerate the encryption and decryption process by keeping its security in place. The parallel processing of key expansion technique adds plus points to the proposed algorithm by processing the key expansion technique in parallel manner using JAVA threads. Key is processed in parallel with the execution of the main code which creates the new sub keys in a parallel way. Due to this, required sub keys are made available in advance. This decreases the time required for the processing the keys, as keys are available prior to its requirement.

## IV. EXPERIMENTAL RESULTS SHOWING SECURITY AND PERFORMANCE ANALYSIS

### A. Key Space Analysis

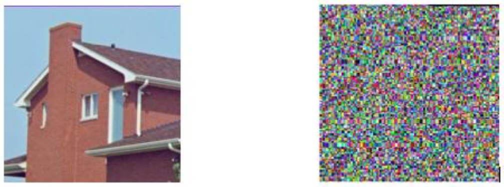
The key length of encryption determines the practical feasibility of performing a brute-force attack. Brute-force attack involves systematically checking all possible key combinations until the right key is found. Longer keys are more difficult to crack than the shorter one. Thus key space of the algorithm should sufficiently large enough to make it immune against brute force attack. The proposed AES algorithm has key space of $2^{128}$ possible keys. If the intruder tries for brute force attack, he would have to try all combinations of keys for the image which is computationally infeasible [3]. Since the key sensitivity of this algorithm is very high.

### B. Key Sensitivity Test

Key is the most sensitive element in the algorithm, and proposed algorithm shouldn't resist even a small change in the key. A little change in the key should make vast change in the output. To check the sensitivity of the algorithm we encrypt the image with one Key and try to decrypt it with other key. We only change 1 bit, between the correct key and wrong key.

**Correct Key:** "1a25s8fe5dsg65a0"

**Wrong Key:** "1a25s8fe5dsg65a1"



a) The decrypted image with correct key

b) The decrypted image with wrong key

**Figure.4. Key sensitivity analysis**

From results we can easily make out that even with 1 bit change in the key we can't decrypt the original image. This shows that the proposed algorithm is highly sensitive to the key.

### C. Histogram Analysis

The general features of an image can be depicted through gray histogram of the image that is the number of occurrences of different pixel values. If an image with a low contrast, then the histogram is thin and centered around the center of the scale. If the pixel of an image occupies all possible gray scale and it is a uniform distribution, then the image has high contrast and various gray color. Thus it can break down the impact of image encryption through the differentiation of the advanced image histogram. In simple words an image in histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. Encrypted images should have no relation with the original images in-order to prevent leakage of data. A histogram of an encrypted image has to be uniform so that it does not provide any clue about the image information thus preventing any statistical attacks on the encrypted images.

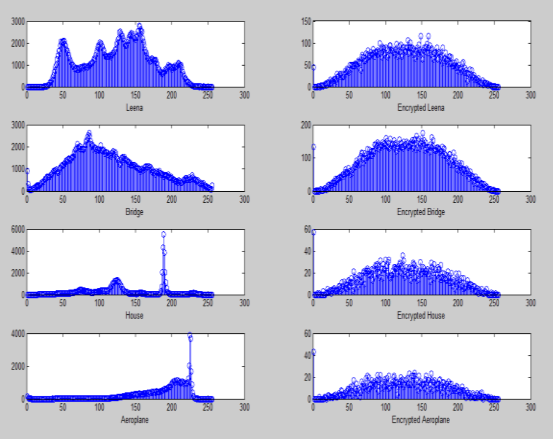


**Figure.5. Histogram analysis of original and encrypted images.**

Fig. 5 shows the histogram analysis of different images. There are incredible changes in the distribution of the pixels. The analysis shows that the histogram of the encrypted image is fairly uniform and is significantly different from the original image. The histogram pixel values of the encrypted image depicts the feature of a random image. From this outcome, we can see that the AES algorithm has a great impact for image encryption. In this process of mage transmission the histogram results shows that the proposed algorithm is highly secured and it will be not susceptible to tampering or eavesdropping [4]. Database is obtained from (http://sipi.use.edu/database/).

### D. Information Entropy Analysis

Information theory is the numerical theory of data communication, storage and is concerned with error-correction, data compression, cryptography, and related topics [5]. A high entropy value of an encrypted image indicates that it is well encrypted and contains truly random bytes. In ideal case the entropy of the encrypted data has to be 8. If entropy value of the encrypted image is less than 8 than there exist certain degree of predictability, which is a risk to its security. TABLE 1 shows entropy values for varies images. From Table 1 we can note that the entropy of the encrypted image of proposed algorithm are very near to 8.

**Table.1. Entropy Values of Encrypted Images.**

| File Name | Size(KB) | Entropy Values of Proposed Algorithm |
|---|---|---|
| Leena.jpg (512 x 512) | 91.4 KB | 7.945 |
| Bridge.jpg (512 x 512) | 131 KB | 7.911 |
| House.jpg (256 x 256) | 22.6 KB | 7.899 |
| Aeroplane.jpg (256 x 256) | 14.7 KB | 7.903 |

### E. Performance Analysis

For real time applications the algorithm has to be very fast, thus along with the security considerations other issues like running speed are also important. TABLE 2 shows the performance of AES encryption on different images. The tests were carried on Intel(R) Pentium(R) CPU N3540 with 2.00GB of RAM and 450GB hard-disk capacity. From obtain results we can conclude that the proposed algorithm shows better performance as compared with conventional AES, Reference [1] and Reference [2]. It takes less time for both encryption and decryption of the image.

**Table.2. Comparative Analysis of Time with different AES Implementation Approaches**

| File Name | Size | Conventional AES Time (ms) | | Reference [1] Time (ms) | | Reference[2] Time (ms) | | Proposed Algorithm Time (ms) | |
|---|---|---|---|---|---|---|---|---|---|
| | | Encry. | Decry. | Encry. | Decry. | Encry. | Decry. | Encry. | Decry. |
| Leena.jpg (512 x 512) | 91.4 KB | 377.04 | 644.66 | 351.15 | 642.34 | 352.9 | 631.1 | 343.26 | 626.79 |
| Bridge.jpg (512 x 512) | 131 KB | 505.69 | 760.80 | 462.58 | 747.64 | 455.1 | 754.0 | 443.61 | 746.37 |
| House.jpg (256 x 256) | 22.6 KB | 348.76 | 583.64 | 335.26 | 557.29 | 326.3 | 557.3 | 318.03 | 547.21 |
| Aeroplane.jpg (256 x 256) | 14.7 KB | 313.47 | 538.04 | 305.08 | 526.07 | 302.2 | 526.3 | 297.11 | 517.68 |

## IV. CONCLUSION

In this paper we have presented a less complex, high speed algorithm which takes less encryption and decryption time and also gives better encryption results as compared with conventional AES algorithm. The modification is done by adjusting the shit row transformation, which reduces the number of calculations performed during encryption and decryption process. This modification saves the time, and speed up the process. For further improvement in the throughput the key expansion technique is process parallel manner which gives boost up to the system. The experimental results shows the efficiency of the scheme, which include key space analysis, key sensitivity test, histogram, entropy and performance analysis were performed with respect to time. The visual inspection of applying the proposed Modified AES is done in both encryption and decryption. The above features of the proposed algorithm make it suitable for image encryption in real time applications.

## VI. ACKNOWLEDGEMENTS

I would like to express my profound gratitude to my project guide Mrs. Palhavi Kerkar, for her valuable guidance at every step for completion of this work. I would also wish to thank Principal Dr. V. N. Shet, Head E&TC Department Dr. H .G. Virani, Goa College of Engineering for providing me with all the facilities and infrastructure for carrying out this work. Last but never the least I would also like to thank all the members of ETC Department for constant support and encouragement provided throughout the project work.

## VII. REFERENCES

[1]. Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani. (2010). “A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption.” *International Conference on Electronics and Information Engineering (ICEIE)*.

[2]. Neha Dalakoti, Nidhi Gaury, Anu Mehra. (4-5 September 2015). “Hardware Efficient AES for Image Processing with High Throughput.” *1st International Conference on Next Generation Computing Technologies (NGCT-2015).* Dehradun, India.

[3]. B. Subramanyan, Vivek M. Chhabria, T. G. Sankar babu. (2011). “Image Encryption Based on AES Key Expansion.” *Second International Conference on Emerging Applications of Information Technology*.

[4]. Qi Zhang, Qunding. (2015). “Digital Image Encryption Based On Advanced Encryption Standard (AES) Algorithm.” *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control*.

[5]. Ms. Pooja Deshmukh, Ms. Vaishali Kolhe. (2014). "Modified AES Based Algorithm for MPEG Video Encryption." *ICICES - S. A. Engineering College*. Chennai, Tamil Nadu, India.

[6]. Syed Shahzad Hussain Shah, Gulistan Raja. (2015). "FPGA Implementation of Chaotic based AES Image Encryption Algorithm." *IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*.

[7]. Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare. (2011). "FPGA Implementation of AES Algorithm." *IEEE*.

[8]. Pradeep H Kharat, Dr. S. S. Shriramwar. (May 28-30, 2015). "A secured Transmission of data using 3D chaotic map encryption and data hiding technique." *International Conference on Industrial Instrumentation and Control (ICIC), College of Engineering Pune*. India.

[9]. Yuwen Zhu, Hongqi Zhang, Yibao Bao. (2013). "Study of the AES Realization Method on the Reconfigurable Hardware." *IEEE International Conference on Computer Sciences and Applications*.

[10]. N. Sklavos, O. Koufopavlou. (Dec. 2002). “Architectures and VLSI Implementations of the AES-Proposal Rijndael.” *IEEE Transactions on computers*. Vol. 51, NO. 12.