ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 2, March – April - 2019, Page No. 120 - 126

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

Sudhanshu Vashistha, Karuna Soni, Vivek Jethani

Assistant Professor, Department of CSE, Arya College of Engineering and Research Centre, Jaipur

Abstract

An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm is proposed in this paper. Due to increasing use of image in various fields, it is very important to protect the confidential image data from unauthorized access. The design uses the iterative approach with block size of 128 bit and key size of 256 bit. The numbers of round for key size of 256 bits is 14. As secret key increases the security as well as the complexity of the cryptography algorithms. This paper presents an algorithm in which the image is an input to AES encryption to get the encrypted image and the encrypted image is the input to AES Decryption to get the original image.

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

Introduction

In the technological age, images are used very widely for the transmission of confidential information. Security of confidential data and other multimedia such as images becomes an important problem due to its transmission over an insecure network, to prevent unauthorized access. Encryption is the most common method used to secure data against piracy. It is the process of converting information / data into random data to prevent unauthorized access. Photo and video encryption finds applications in a variety of areas, including online communications, multimedia systems, medical imaging, telemedicine and military communication, video on demand, video conferencing, data transmission, etc.

[5]. Various data encryption algorithms such as AES, RSA, or IDEA have been proposed so far, most of which are used in text or binary format [1]. In terms of data security, we have different encryption algorithms, but to secure multimedia data such as images, we face many challenges because images have a very high relationship between pixels and repetitions and a high transfer rate with bandwidth capacity and limited data collected [3]. Due to the above multimedia data features, it is difficult to use these data encryption algorithms directly for multimedia data. Taking into account the above limitations and working for real-time applications, designing new algorithms that require less computing power without affecting data security has always been a topic of concern for design engineers.

In order to have reliable security in storing and transmitting digital images, while communicating via an insecure channel such as the Internet, waves, GSM and Wi-Fi, the Advanced Encryption Standard (AES) algorithm is used worldwide since it is very safe with high productivity High speed and used against various attack techniques So far, a lot of work has been done to implement AES applications. Syed Hussain Kamali [1] designed a new modified version of AES, and set the transformation of the transformation line. The change provides the best security crypto results against statistical attacks compared to traditional AES. Here, the adjustment part reduces the number of calculations and thus increases the speed. Neha Dalakoti [2] used the parallel management of key expansion technology and productivity improvement. It also reduces the hardware requirements for AES implementation. In another research work, the key changes to each set of

pixels. The keys are created using the regular key expansion process independently of the sender and recipient, and only the primary key is shared instead of all the keys [3]. It shows better coding results and shows great resistance against different known attacks, but since a new key is created for each set of pixels, it is not suitable for some real-time applications, as there should be a lot of information shared in less time. The main drawback of this document is that the recipient must know the accuracy of each image the sender sends to generate the keys. Qi Zhang [4] introduced digital image encryption technology based on AES algorithm and showed that this technology could better understand the effect of encoding and decoding. In [5], they proposed an AES-based MPES video coding algorithm with modulation of shifting shift lines. The algorithm does not require additional operations or devices, only the original AES. Chaos Theory was first used as part of cryptography by Edward Lawrence in 1963. In the past decade, chaos-based cryptography has gained more attention due to noise as a sign of a person who cannot be linked, allowed, ergodicity, confused, create confusion in pixel images, and sensitivity For initial conditions, for those in the encoded image, such as mixing and spreading [8]. In the chaotic AES image encryption algorithm of Mr. Shahzad Hussain Shah [6], the key is generated by chaotic cards and encryption is performed by AES. Parallel RAM is used to perform the operation of byte bytes and optimization is also implemented in internal constellations. To improve speed, they synchronized the key extension unit that generates a circular key in each round the clock;

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 128 bits 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 keysis rotate, which performs a one byte circular left shift on a word i.e. RotWord [b0,b1,b2,b3] = [b1,b2,b3,b0].

Sub Bytes: Sub Bytes performs a byte substitution oneach byte of input word using the S-box.

Rcon (Round Constant): Rcon is performed usingRijndeal 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.

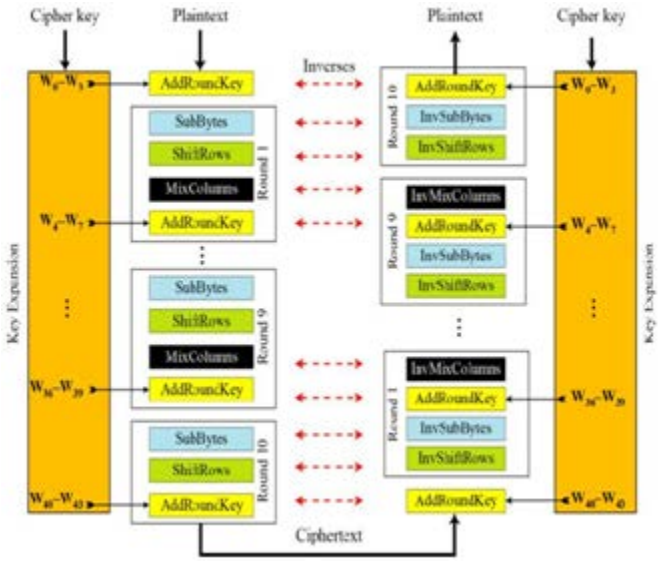

Figure 1: Structure of AES algorithm for encryption and decryption process.

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 keys. We only change 1 bit, between the correct key and wrong key.

Correct Key: "1a25s8fe5dsg65a0"

Wrong Key: "1a25s8fe5dsg65a1"

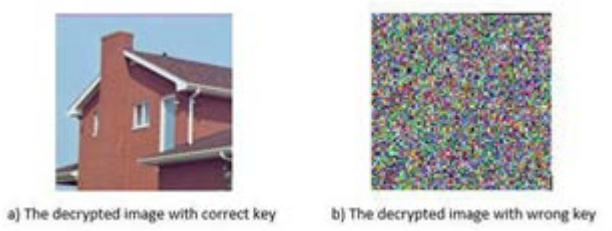

Figure 2: Key sensitivity analysis

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.

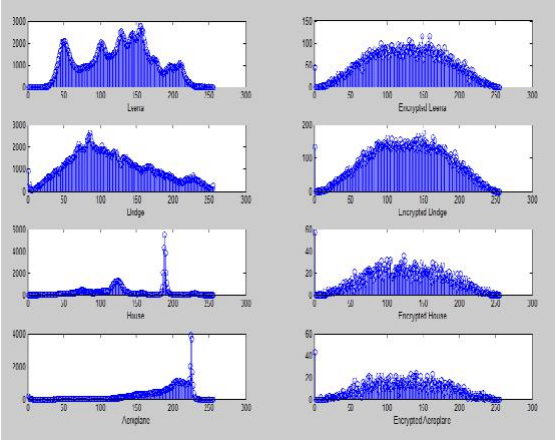

Figure 3: Histogram analysis of original and encrypted images.

Fig. 3 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 depict 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 exists 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.

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.

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 andInformation 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 GenerationComputing 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. Syed Shahzad Hussain Shah, Gulistan Raja. (2015). "FPGA Implementation of Chaotic based AES Image Encryption Algorithm." IEEE International Conference on Signal and ImageProcessing Applications (ICSIPA).
6. Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare. (2011). "FPGA Implementation of AES Algorithm." IEEE.
7. 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 Conferenceon Industrial Instrumentation and Control (ICIC), College of Engineering Pune. India.
8. 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.
9. N. Sklavos, O. Koufopavlou. (Dec. 2002). “Architectures and VLSI Implementations of the AES-Proposal Rijndael.” IEEETransactions on computers. Vol. 51, NO. 12.