INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET)

ISSN 0976 – 6464(Print)
ISSN 0976 – 6472(Online)
Volume 6, Issue 1, January (2015), pp. 23-29
© IAEME: http://www.iaeme.com/IJECET.asp
Journal Impact Factor (2014): 7.2836 (Calculated by GISI)
www.jifactor.com

IJECET

© I A E M E

IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM

Roshni Padate[1], Aamna Patel[2]

[1]Computer Engineering Department, Fr. Conceicao Rodrigues College of Engineering, Fr. Agnel Ashram, Bandstand, Bandra(West), Mumbai-400050, India

[2]Electronics Department, Fr. Conceicao Rodrigues College of Engineering, Fr. Agnel Ashram, Bandstand, Bandra(West), Mumbai-400050, India,

ABSTRACT

Data Security is primary concern for every communication system. The relentless growth of Internet and communication technologies has made the extensive use of images unavoidable. There are many ways to provide security to data that is being communicated. This Paper describes a design of effective security for communication by AES algorithm for encryption and decryption. It is based on AES Key Expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the a 128 bit key which changes for every set of pixels. The National Institute of Standards and Technology (NIST) has initiated a process to develop a Federal information Processing Standard (FIPS) for the Advanced Encryption Standard (AES), specifying an Advanced Encryption Algorithm to replace the Data Encryption standard (DES) the Expired in 1998. The Advanced Encryption Standard can be programmed in software or built with pure hardware.

Keywords: AES, Block Cipher, Cryptography, DES, NIST

1. INTRODUCTION

In the past few years the security and integrity of data is the main concern. In the present scenario almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored.

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an

unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.
Purpose of cryptography:

1.1 Authentication

The process of proving one's identity. It is another part of data security that we encounter with everyday computer usage. Just think when you log into your email, or blog account. The simple sign-in process is a form of authentication that allows you to log into applications, files, folders and even an entire computer system. Once logged in, you have various given privileges until logging out. Some system will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter.

The simple sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. Non-repudiation: In this, the receiver should know whether the sender is not faking.
For example, if suppose when one purchases something online, one should be sure that the person whom one pays is not faking.

1.2 Integrity

Many a times data needs to be updated but this can only be done by authenticated people.

1.3 Privacy/confidentiality

Ensuring that no one can read the message except the intended receiver. Encryption is the process of obscuring information to make it unreadable without special knowledge. Encryption has been used to protect communications for centuries, but only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now used in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

2. AES ALGORITHM

In January, 1997 NIST began its effort to develop the AES, a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES. The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.

Difference between AES and DES

Factors	DES	AES
Key Length	56 bits	128, 192, 256 bits
Block Size	64 bits	128, 192, 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Possible Keys	2^{56}	2^{128}, 2^{192}, 2^{256}

2.1 The Rijndael Algorithm

For Rijndael, the length of both the block to be encrypted and the encryption key are not fixed. They can be independently specified to 128, 192 or 256 bits. The number of rounds, however, varies according to the key length. It can be equal to 10, 12 and 14 when the key length is 128bits, 192 bits and 256 bits, respectively. The basic components of Rijndael are simple mathematical, logical, and table lookup operations. The latter is actually a composite function of an inversion over Galois Field (GF) with an affine mapping. Such structure makes Rijndael suitable for hardware implementation.

3. IMPLEMENTATION

The algorithm is based on AES Key Expansion technique.

AES Key Expansion technique in detail.

3.1 AES Key Expansion

Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x(Nr+1) words. Where Nr is the number of rounds.
The process is as follows

- The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on.
- The rest of the words (wi for i=4 to 43) are made as follows

If (i mod 4) != 0, wi=wi-1 xor wi-4.
If (i mod 4) = 0, wi=t xor wi-4. Here t is a temporary word result of applying SubByte transformation and rotate word on wi-1 and XORing the result with a round constant.

3.2 Modifications in AES Key Expansion

Certain changes made in the above key expansion process improves the encryption quality, and also increases the avalanche effect. The changes are

a) The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.
b) Both the s-box and Inverse s-box are used for the Key Expansion process which improves non-linearity in the expanded key and also improves the encryption quality.
c) We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

The above changes in the algorithm can be represented as

1) Formation of Rcon values
Rcon [0]=key[12:15]; Rcon [1]=key[4:7];
Rcon [2]=key[0:3]; Rcon [3]=key[8:11];

2) Using Inverse S-Box for key expansion
The ‘temp’ value used in the algorithm is formed as
temp = SubWord(RotWord(temp)) XOR InvSubWord(Rcon[i/4]);
Where InvSubWord: InverseSubByte transformation table value

3) Shifting of S-box and Inverse S-box
Sbox_offset = sum(key[0:15])mod256;
Inv_Sbox_offset = (sum(key[0:15])*mean(key[0:15]))mod256;
The initial key is represented as blocks key[0],key[1],..,key[15]. Where each block is 8bits long (8*16=128 bits).

3.3 Steps Involved

3.3.1 Key Selection

The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).

3.3.2 Generation of Multiple keys

The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

3.3.3 Encryption

Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey.

3.3.4 Decryption

The decryption process is similar as encryption, but we use Inverse SubByte Transformation. The whole AES structure is sketched in Fig 1.

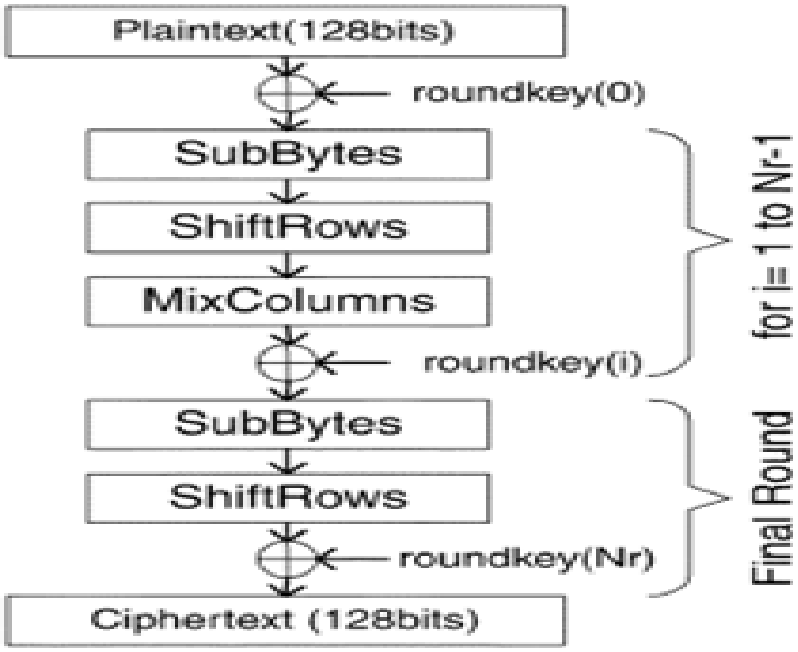

Fig 1: Structure of AES Algorithm

4. RESULTS

4.1 Encryption and Decryption

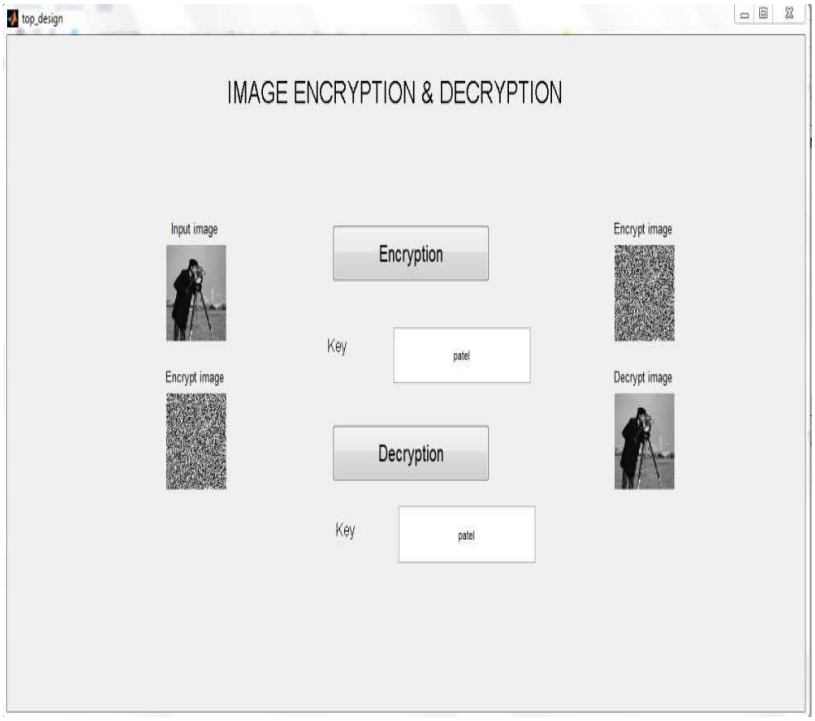

Fig 2: Encryption and Decryption Output

4.2 If key for encryption and decryption is different than the original image is not retrieved.

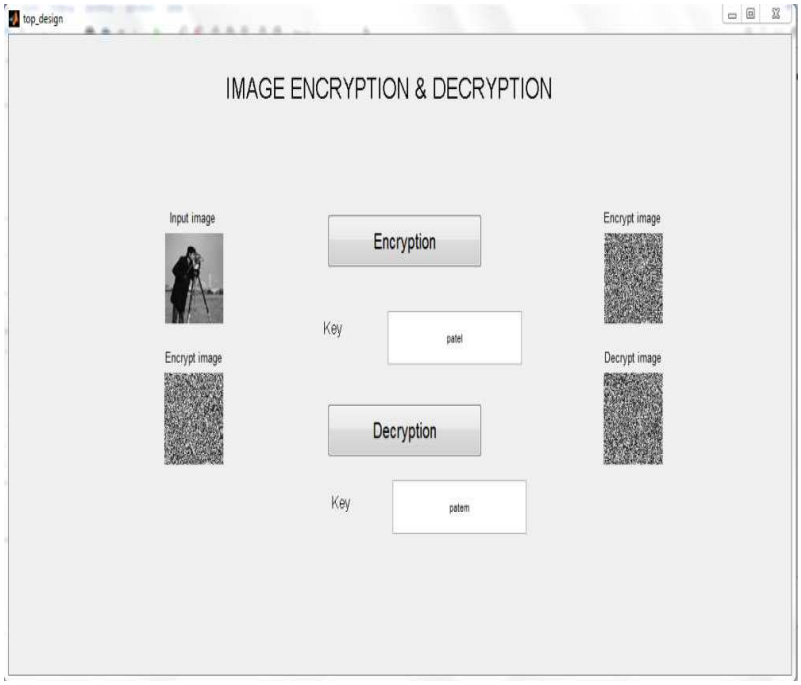

Fig 3: Encryption and Decryption with different keys

4.3 Time required for encryption

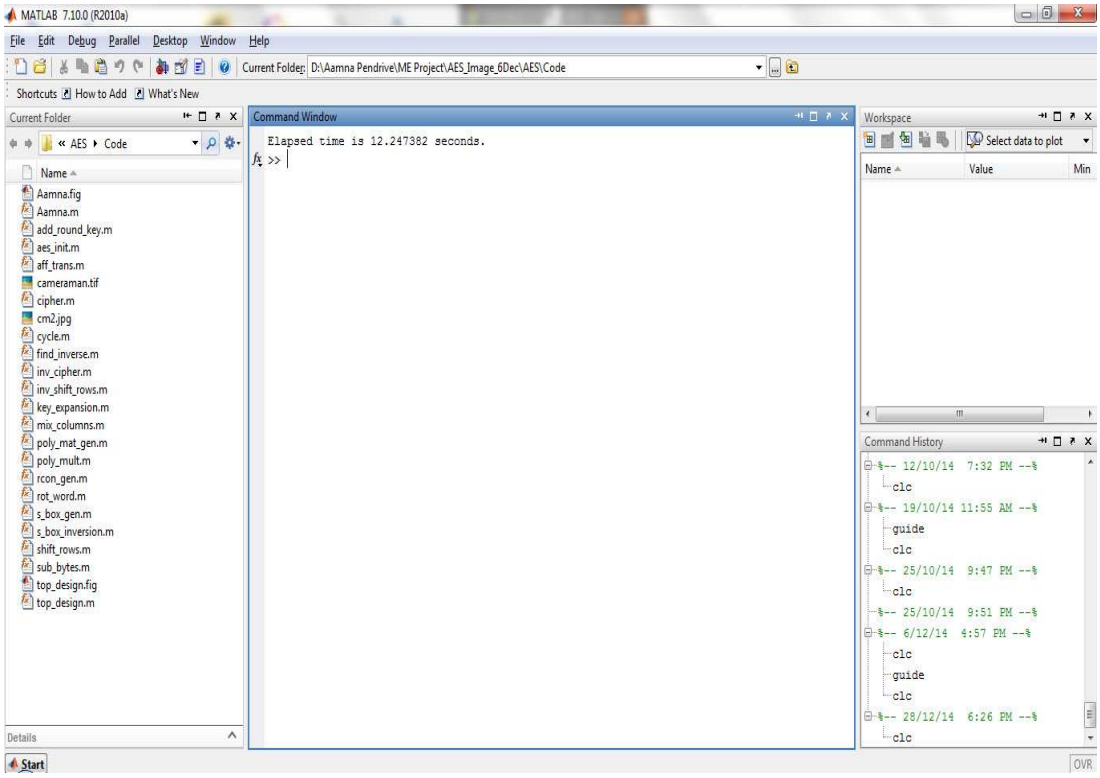

Fig 4: Encryption time

5. CONCLUSION

Image is encrypted and decrypted using AES Algorithm. The proposed algorithm offers high encryption quality. Even AES-128 offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades

Encryption and decryption of image is possible using AES Algorithm. Time required for encryption by AES Algorithm is less than the time required by DES Algorithm. Due to these features the algorithm is suitable for image encryption in real time applications.

6. REFERENCES

1. P.Karthigaikumar, Soumiya Rasheed, Simulation of Image Encryption using AES Algorithm, IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, 2011, 166-172.
2. Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, Analysis and Comparison between AES and DES Cryptographic Algorithm, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012, 362-365
3. The First 10 Years of Advanced Encryption, Copublished by the IEEE Computer and Reliability Societies, 2010 IEEE, 72-74.
4. Irfan AbdulGani Landge, Implementation of AES Encryption and Decryption using VHDL, International J. of Engg. Research & Indu. Appls. (IJERIA). ISSN 0974-1518, Vol. 4, No. III (August 2011), 395-406.

5. B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, Image Encryption Based on AES Key Expansion, 2011 Second International Conference on Emerging Applications of Information Technology 978-0-7695-4329-1/11 $26.00 © 2011 IEEE DOI 10.1109/EAIT.2011.60, 217-220
6. About AES – Advanced Encryption Standard, Copyright 2007 Svante Seleborg Axantum Software AB.
7. Dhanya Pushkaran and Neethu Bhaskar, "AES Encryption Engine For Many Core Processor Arrays For Enhanced Security" International journal of Electronics and Communication Engineering &Technology (IJECET), Volume 5, Issue 12, 2014, pp. 106 - 111, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.
8. Priyanka Chauhan and Girish Chandra Thakur, "Efficient Way of Image Encryption Using Generalized Weighted Fractional Fourier Transform with Double Random Phase Encoding" International Journal of Advanced Research in Engineering & Technology (IJARET), Volume 5, Issue 6, 2014, pp. 45 - 52, ISSN Print: 0976-6480, ISSN Online: 0976-6499.
9. Prof. Maher K. Mahmood and Jinan N. Shehab, "Image Encryption and Compression Based on Compressive Sensing and Chaos" International journal of Computer Engineering & Technology (IJCET), Volume 5, Issue 1, 2014, pp. 68 - 84, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
10. J. V. Gorabal and Manjaiah D. H, "Image Encryption Approach for Security Issues" International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 5, Issue 2, 2010, pp. 59 - 64, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.
11. Ahmad Salameh Abusukhon, "Block Cipher Encryption For Text-To-Image Algorithm" International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 50 - 59, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.