SECURE IMAGE ENCRYPTION USING AES

P. Radhadevi[1], P. Kalpana[2]

[1, 2] *Assistant Professor, Computer Application, SNIST, AP, India*
radhajitender@gmail.com*, *ParsiKalpana@sreenidhi.edu.in

Abstract

Security in transmission of digital images has its importance in today's image communications, due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue. The difficulties in ensuring individuals privacy become increasingly challenging. Various methods have been investigated and developed to protect data and personal privacy. Encryption is probably the most obvious one. In order to protect valuable information from undesirable readers, image encryption is essential. This paper presents an application of AES (Advanced Encryption Standard) operations in image encryption and decryption. The encrypted cipher images always display the uniformly distributed RGB pixels.

Index Terms: *Security, Image Processing, AES, Encryption and Decryption*

----------***----------

1. INTRODUCTION

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

Digital images, accounting for 70% of the information transmission on the internet, is an important parts of network exchanges. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Traditional encryption algorithms such as DES, IDES, are against the text messages to be proposed, which are not suitable for digital image encryption, therefore, an reliable digital image with characteristics is in urgent need of the encryption scheme AES is suitable for image encryption, and decryption with is closely related to some dynamics of its own characteristics.

2. DESCRIPTION

The AES algorithm gains wide application in our daily life, such as smart cards, cell phones, automated teller machines and WWW servers. AES encrypts a plaintext to become a ciphertext, which can be decrypted back to the original plaintext by using common private key, an example is shown in Figure 1a, It can be seen the ciphertext is very different from and gives no clue to the original plaintext. Figure 1a shows the Encryption of AES operation using cipher key

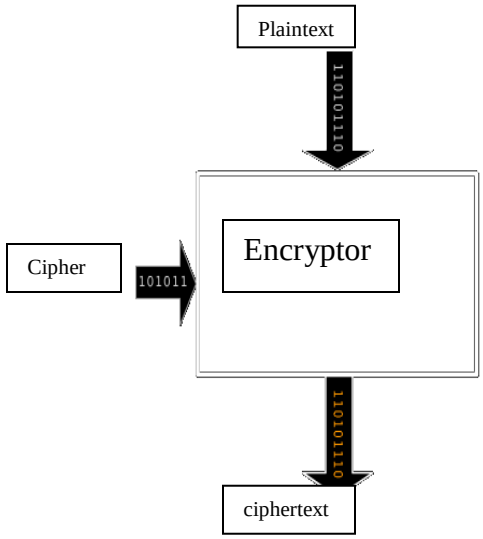

Fig -1a: Encryption of AES operation

For the applications of AES image encryption and decryption, the encrypted image should be different from and give no clue to the original one, an example figure1b is shows the encrypted image and that encrypted image to original image.

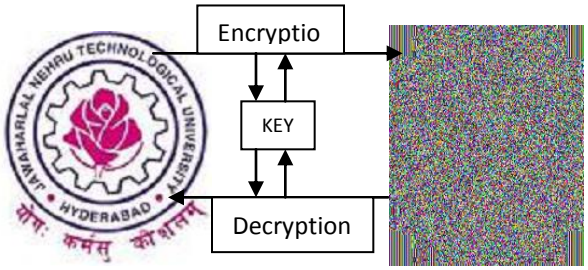

Fig -1b: Example for AES Encryption and Decryption

3. AES ALGORITHM

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state[3]. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) .These rounds are governed by the following transformations:

Subbyte Transformation: Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and Affine Transformation.

Shift rows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

Mix columns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

Add round key transformation: Is a simple XOR between the working state and the round key. This transformation is its own inverse.

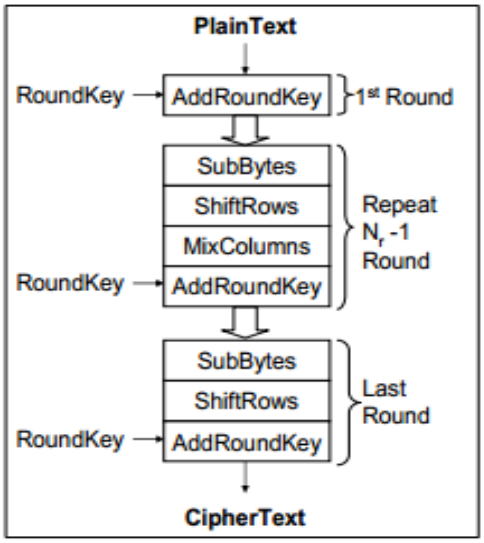

Fig-2a : diagram of AES encryption algorithm

Expansion key: With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm. This key expansion routine can be performed all at once or 'on the fly' calculating words as they are needed.

Strengths:

- AES is extremely fast compared to other block ciphers. (Though there are tradeoff between size and speed)
- The round transformation is parallel by design. This is important in dedicated hardware as it allows even faster execution.
- AES was designed to be amenable to pipelining.
- The cipher does not use arithmetic operations so has no bias towards big or little endian architectures.
- AES is fully self-supporting. Does not use SBoxes of other ciphers, bits from Rand tables, digits of or any other such jokes.
- AES is not based on obscure or not well understood processes.
- The tight cipher and simple design does not leave enough room to hide a trap door.

Cryptanalysis of AES:

So far, the only successful attacks against AES implementations have been side channel attacks. Side channel attacks do not attack the underlying cipher and so have nothing to do with its security as described here, but attack implementations of the cipher on systems which inadvertently leak data. There are several such known attacks on certain implementations of AES.

In April 2005, D.J. Bernstein announced a cache timing attack that he used to break a custom server that used Open SSL's AES encryption. The custom server was designed to give out, as much timing information as possible, and the attack required over 200 million chosen plaintexts. In October 2005, Dag Arne Osvik, Adi Shamir and EranTromer presented a paper demonstrating several cache timing attacks against AES. One attack was able to obtain an entire AES key after only 800 operations triggering encryptions, in a total of 65 milliseconds. This attack requires the attacker to be able to run programs on the same system that is performing AES.

CONCLUSIONS

The above approach offers enhanced security, it aims to provide user satisfaction by transmitting personal and sensitive image data securely. The Advanced Encryption Standard offers the flexibility of allowing different key sizes 128 bit, 192 bit and 256-bit key and the security is based on the various random key selections, different S-box and strong transformations. Thus the algorithm provides many different flexible implementations. Lastly, this intends to give an insight in understanding the concepts of image cryptography along with the importance of secure image transmission. Apart from that, the paper can be used to be developed further by researchers or programmers and acts as a template for ensuring the protection of image using encryption.

REFERENCES

[1]. B. Schneier, Applied Cryptography. NY: John Wiley & Sons, 1996.
[2]. Burr, W.E., Selecting the Advanced Encryption Standard: Security & Privacy Magazine, IEEE Volume 1, Issue 2, Mar-Apr 2003 Page(s):43 – 52.
[3]. Chi-Feng Lu , Fast implementation of AES cryptographic algorithms in smart cards; Yan-Shun Kao; Hsia-Ling Chiang; Chung-Huang Yang; Security Technology, 2003.
[4]. FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of standards and Technology.
[5]. A.Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997, p. 81-83.
[6] Daniel J Bernstein Preliminary version of report "Cache-Timing attacks on AES " to National Science Foundation, grant CCR-9983950.
[7] W.Stallings, Cryptography and Network Security. NJ: Prentice Hall, 2003.
[8] Wikipedia, Page Title: Block cipher modes of operation http://en.wikipedia.org/ wiki/Cipher_block_chaining.
[9] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition.

BIOGRAPHIES:

P. Radha Devi is working as Assistant Professor, in the Dept of CA**,** Sreenidhi Institute of Science and Technology, Hyderabad. She has completed MTech (CSE) from JNTU, Hyderabad. She is having around 3 years of teaching experience. She is interested in Information Security and Web Technologies.

P. Kalpana has completed her M.Tech (CSE) from JNTU, Hyderabad. She is having around 10 years of teaching experience . She is working as Assistant Professor in Sreenidhi Institute of Science and Technology, Hyderabad. She received a gold model from Nishitha Degree and PG college. She is especially interested in Cloud Computing, Information Security and Network Security. She has already some papers to her credit in various international journals.