Increasing Security by Implementing Image Encryption using AES Algorithm

Radhika Desai
CMPN- Thakur college of engineering and technology

Kiran Bhandari
Associate Professor
CMPN- Thakur college of engineering and technology

Veena Kulkarni
Assistant Professor
CMPN- Thakur college of engineering and technology

Abstract—To provide security in image application, encryption is required. In this paper, we analyze AES algorithm and various security measures used for image encryption in AES algorithm. As cryptography helps in hiding the sensitive information or its transmission over an insecure network. Preventing any unidentified or unintended user to read it. Cryptography is the method to protect information from undesirable attackers while transmitted or stored.

Keywords- Security, Image Processing, AES, Encryption and Decryption

I. INTRODUCTION

The use of image and video applications has increased dramatically in recent years. When communication bandwidth or storage is limited, data is often compressed. Especially when wireless network is used, low bit rate compression algorithms are needed because of limited bandwidth. On the other hand, encryption operation is also performed if it is necessary to protect information. Traditionally, an appropriate compression algorithm is applied to multimedia data and its output is encrypted by an independent encryption algorithm. This process must then be reversed by decoder. The processing time for encryption and decryption is a major bottleneck in real time image communication and processing. Along with that processing time required for compression and decompression is also important. The computational overhead incurred by encryption and decryption algorithms makes it impossible to handle tremendous amount of data processed [1] [2]. Encrypting the whole compressed bit stream is very expensive both in delay and processing time, it is proposed in literature to only partially encrypt the compressed bit stream, as a matter of fact, although a large portion of the compressed data is left unencrypted, an adequate choice of bits to encrypt still makes it sufficiently difficult to recover the original data without deciphering the encrypted part so that the security of transmission is achieved [2]

II. LITERATURE REVIEW

1. Performance Parameters

Set of parameters are defined based on which evaluation and comparison of image encryption schemes can be done. Some of the parameters listed below are gathered from literature.

- *Tunability*: It could be very desirable to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications. Tunability factor can have one of the values ‘yes’ or ‘no’.

- *Visual Degradation:* This criterion measures the perceptual distortion of the image data with respect to the plain image. In some applications, it could be desirable to achieve enough visual degradation, so that an attacker would still understand the content but prefer to pay to access the unencrypted content. However, for sensitive data, high visual degradation could be desirable to completely disguise the visual content. Compression

- *Compression Friendliness:* An encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase.

- *Format Compliance :* The encrypted bit stream should be compliant with the compressor. And standard decoder should be able to decode the encrypted bit stream without decryption.

- *Encryption Ratio* : This criterion measures the amount of data to be encrypted. Encryption ratio has to be minimized to reduce computational complexity. Speed (S): In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

- *Cryptographic Security :* Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high.

- *Computational Speed:* The speed of the algorithm should be fast enough to meet the real time requirements.

- *Key Length Value*: In cryptography, key is the most important factor. Asystem should be secure even after it is exposed to public but its should not be available publicaaly.

2. Security using AES

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.

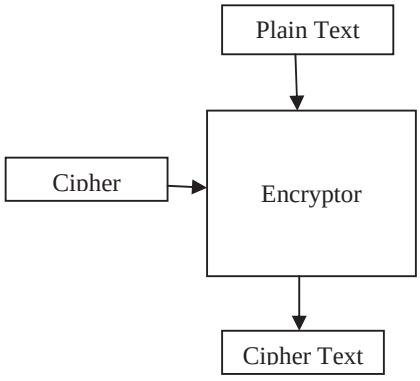

Figure 1: Security overview in AES

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 Figure 2 shows the encrypted image and the encrypted image to original image.

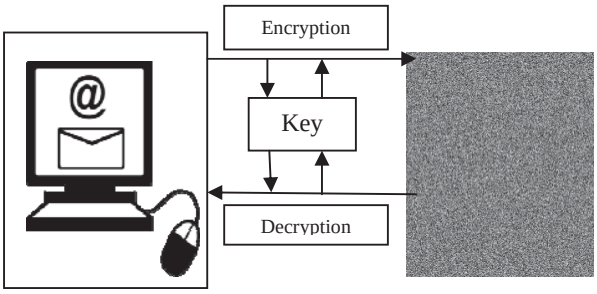

Figure 2: Example of AES encryption

3. The structure of 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 [5]. 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.

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. [3]

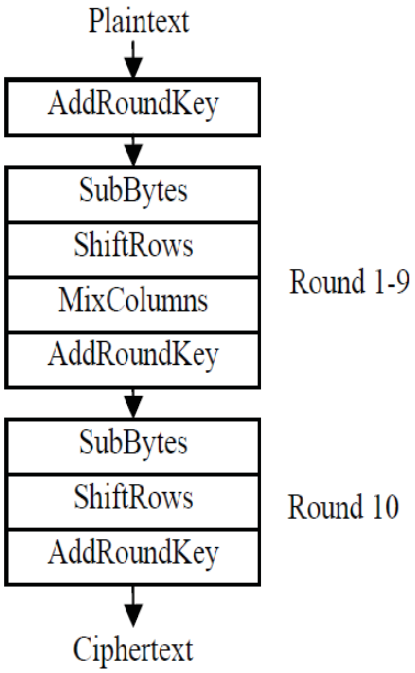

Figure 3: The encrypt process of AES-128 [4]

III. ADVANTAGES

AES is extremely fast compared to other block ciphers. (Though there are tradeoff between size and speed)

- The design of round transformation is parallel. This is important in dedicated hardware as it allows faster execution as compared to others.
- The design of AES is amenable to pipelining.
- Arithmetic operations are not used, so it has no bias towards little or big architectures.
- AES is fully self-supporting. Does not use other , bits from Rand tables, ciphers, digits of any other such sources.
- The process of AES is well defined and not hypothetical.
- It has tight cipher and simple design

IV. CONCLUSION

The AES approach offers enhanced security, User satisfaction is achieved by the level of security provided in the transmission of sensitive data. The AES provides flexibility by allowing different key sizes 128 bit, 192 bit and 256-bit key and the security is given by the various random key selections, different S-box and transformations that are very strong. Thus, many flexible implementations are provided by the algorithm. Lastly, this intends to give an insight in the importance of secure image transmission and understanding the concepts of image cryptography process.

REFERENCES

[1] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, “Recent Advances in Multimedia Information System Security”, International Journal of Computing and Informatics, Vol. 33, No.1, March 2009, pp. 3-24.

[2] S.lian , Multimedia Content Encryption : T echniques and Application, CRC,2008.

[3] P. Radhadevi1 , P. Kalpana2, “SECURE IMAGE ENCRYPTION USING AES”, IJRET: International Journal of Research in Engineering and Technology ISSN: 2319-1163, Volume: 01 Issue: 02 , Oct-2012

[4] Qing-xiang zhu1, lu li1, jing liu2, nan xu1 “The Analysis And Design Of Accounting Information Security System Based On AES Algorithm” *Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding*, 12-15 July 2009

[5] Chi-Feng Lu , Fast implementation of AES cryptographic algorithms in smart cards; Yan-Shun Kao; Hsia-Ling Chiang; Chung-Huang Yang; Security Technology, 2003.