Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Secure Transmission of Images using Encryption

Santhi Mol P.[1], Anjana P. Nair[2]
[1]Computer Science & Engineering, SBCEW
[2]Computer Science & Engineering, SBCEW

Abstract— Nowadays, security is an important factor of internet and network application. Likewise, secure transmission of images is the most challenging aspects. This paper explains the secure end to end transmission of images. Here encryption process is used to ensure the security during the transmission and also hash values of the images are used as verification criteria of the security. Here, to secure the image, calculate the hash value of the image and append this value with the image. Then encrypt the appended image using AES (Advanced Encryption Standard) algorithm, and then send to the receiver. Cryptography is a main category of computer security that converts information from its normal form into an unreadable form. Encryption methods are used to securely transmit data in open networks. Symmetric key algorithms are most suitable for encrypting this multimedia objects. Here AES algorithm is used for encryption and decryption process. Some existing symmetric key algorithms like DES, triple DES with 3 keys and AES have been implemented in different papers. Out of these algorithms DES and Triple DES are not considered as secure algorithms, since some attacks have been found on both algorithms. AES with 128 bit key has proved to be a secure and efficient algorithm.

Keywords— Cryptography, Encryption, Hash value, Security**.**

I. INTRODUCTION

Security has become an increasingly important feature with the growth of electronic communication. Cryptography is the main category of computer security. It hides the information from its readable form into an unreadable form. In this system Secure AES algorithm is used for encryption and decryption process. A large number of rounds make the algorithm slower, but it provides greater security. Several attacks like message disclosure, replay attacks are not possible in this system. Symmetric key algorithms are much faster and easier to implement and generally requires less processing power when compared with asymmetric key algorithms. Here, SHA1 algorithm is used for finding the hash value. SHA1 stands for Secure Hashing Algorithm. A cryptographic hash function h is an algorithm which maps a message string s of arbitrary length to a string x = h(s) of fixed length n, called hash value.

The National Institute of Standards and Technology (NIST) declared Rijndael algorithm as the Advanced Encryption Standard (AES) in October 2000 [2]. The Advanced Encryption Standard specifies a Federal Information Processing Standard (FIPS) that has approved cryptographic algorithm which is used to protect sensitive information. The AES algorithm is a symmetric key algorithm that encrypts and decrypts information. The encryption method converts an original image into encrypted image. The decryption process is to convert the encrypted image back to the original image.

The rest of the paper is arranged as follows. In the next section we discuss the proposed system. The section III explains the encryption technique used in this proposed system. The section IV explains SHA-1 algorithm. This algorithm is used to calculate the hash value of the image. Finally the section V contains the screen shots.

II. PROPOSED SYSTEM

Secure Transmission of Images mainly consists of the following modules:

- Browse any standard grayscale or colored image which sender wants to transmit securely.
- Calculate the hash value of the original image.
- Append the hash value with this original image.
- Then encrypt this appended image and send to the receiver.
- Receiver receives the encrypted image.
- Then decrypt the image.
- Separate the hash value.
- Compare the hash values and ensure the security.

III. AES ALGORITHM

In cryptography AES (Advanced Encryption Standard) [1] [2] is a symmetric key encryption standard adopted by U.S government. AES is a block cipher with a block length of 128 bits. This means that the number of bytes that it encrypts is fixed. AES can currently encrypt in blocks of 16 bytes at a time; no other block sizes are presently a part of the AES standard. 128 bit data block of the input is divided into 16 bytes and then arranged into 4 * 4 matrixes. This matrix is called state matrix.

AES encryption includes an initial round (0), nine general rounds (1 to 9) and a final round (10). In round Zero the two matrices are simply XORed under Add Round Key transformation. The output of Round 0 is given as the input to the Round 1. Any general round is composed of four distinct uniform and invertible transformations: Sub Bytes, Shift Rows, Mix Column and Add Round Key. The final round is same as general round except that Mix Column is omitted. Each of the cipher operations is byte-oriented The sub keys needed for all the rounds from Round1 to Round 10 are derived from the original 128-bit key provided. After finishing all the ten rounds the output is 128 bits, which is the encrypted output.

A. General Rounds

- Add Round Key
- Sub Bytes
- Shift Rows
- Mix Column

Add Round Key: Computing the round key for each round. Each of the 16 bytes of the state is XORed against each of the 16 bytes of a portion of the expanded key for the current round. The Expanded Key bytes are never reused.

Sub Bytes: is a non-linear byte substitution operation. That is, substituting by bytes from S Box. Sub Bytes mean byte-by-byte substitution during the forward process. The matching substitution step used during decryption is called Inv Sub Bytes.

Shift Rows: Shifting rows. That is, it operates individually on each of the last three rows of State matrix shifting cyclically a certain number of bytes. The first row is left unchanged. The second row is left rotated by one byte, third row by two bytes and fourth row by three bytes. The matching transformation during decryption is called Inv-Shift-Rows for Inverse Shift Row Transformation.

Mix Column: XOR operation on columns. Mix Columns for mixing up of the bytes in each column separately during the forward process. The matching transformation during decryption is called Inv-Mix-Columns and stands for inverse mix column transformation.

B. Key Expansion

Prior to encryption or decryption the key must be expanded. Assuming a 128-bit key, the key is also arranged in the form of a matrix of 4 × 4 bytes. As with the input block, the first word from the key fills the first column of the matrix, and so on. The expanded key is used in the Add Round Key function. Each time the Add Round Key function is called a dissimilar part of the expanded key is

XORed against the state. The key expansion routine executes a maximum of 4 successive functions. These functions are:

- Rot Word
- Sub Word
- Rcon
- Ek(Offset)

IV. SHA-1 ALGORITHM

In cryptography, the Secure Hash Algorithm (SHA-1) [3] [4] originally developed by the National Security Agency (NSA) as SHA-0 and later handed over to the National Institute of Standards and Technology (NIST).That is SHA-1 is a hashing algorithm designed by the United States National Security Agency and published by NIST. Currently SHA-1 is the most widely used SHA hash function in cryptography. In construction SHA-1 is similar to the previous MD4 and MD5 hash functions, in fact distributing some of the initial hash values. It operates a 512 bit block size and has a maximum message size of 2 ^ 64 – 1 bits. The SHA-1 algorithm belongs to a set of cryptographic hash functions similar to the MD family of hash functions. But the main difference between the SHA-1 and the MD family is the more frequent use of input bits during the course of the hash function in the SHA-1 algorithm than in MD4 or MD5. SHA-1 provides greater resistance to attacks. Here, the image its hash code are appended together. Then encrypt that image and send to the receiver. The receiver decrypts the encrypted image and separates out its hash value, which is then compared with the hash code calculated from the received image. The hash code provides authentication and the encryption provides confidentiality.

The Screen shots of the secure transmission of images are represented below. First sender loads the image. Then find the hash value of that image using SHA-1 algorithms and append this hash value with the original image. Then encrypt this appended image using AES algorithm. Then send this encrypted image to the receiver. The receiver receives the encrypted image and decrypt using AES algorithm. After that receiver separate the appended hash value.

V. SCREENSHOTS

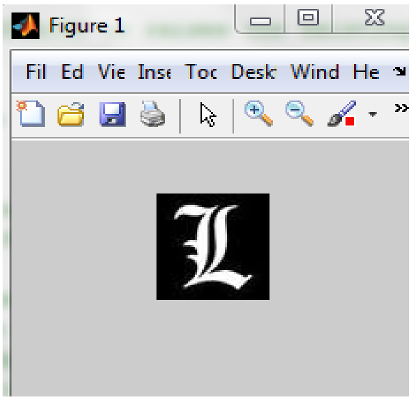

Fig. 1: Original Image

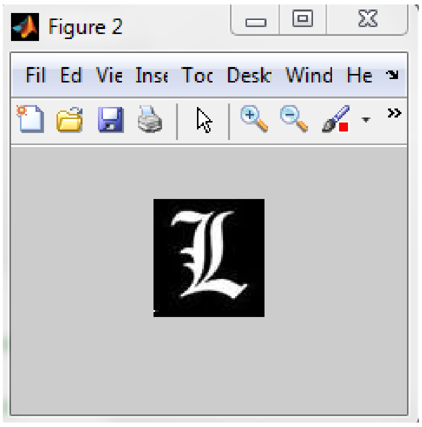

Fig. 2: Image with Hash value

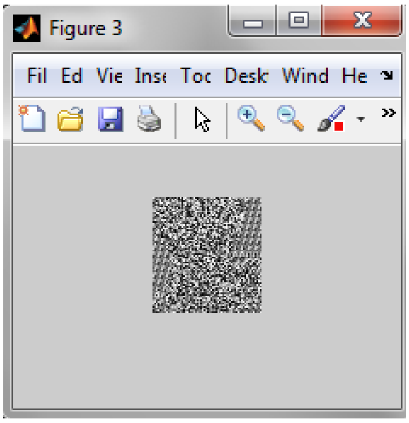

Fig. 3: Encrypted Image

VI. CONCLUSION

The secure transmission of images used in different areas. The main issue of the image transmission is its security. Here calculate the hash value of the image and append this value with the original image. Then encrypt the image and send to the receiver. AES algorithm is used for encryption and decryption process. Some existing symmetric key algorithms like DES, triple DES with 3 keys and AES have been implemented by different authors. Out of these algorithms AES takes minimum time to encrypt and decrypt the image with various sizes where one message size is 160 characters. DES and Triple DES [5] are not considered as secure algorithms, since some attacks have been found on both algorithms. AES with 128 bit key has proved to be a secure and efficient algorithm. SHA1 is used for calculating the hash value.

REFERENCES

[1]. Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, “Text and Image Encryption Decryption Using Advanced Encryption Standard”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 3, May – June 2014.

[2]. Sonu Varghese K, Faisal K K, Vinayachandran K K, “Image Security Using F5 and AES Algorithm”, Proceedings of IRF International Conference, 13th April-2014.

[3]. Thulasimani Lakshmanan and Madheswaran Muthusamy, ”A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes”, The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[4]. Nalini C. Iyer and Sagarika Mandal, ” Implementation of Secure Hash Algorithm-1 using FPGA”, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 8 (2013), pp. 757-764.

[5]. Jawahar Thakur, Nagesh Kumar,”DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011.