Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 10, pp.21169-21172, October, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SECURE TRANSMISSION OF MULTIMEDIA OBJECTS

Santhi Mol, P. and Supriya, L. P.

Computer Science and Engineering, SBCEW, Elavumthitta, India

ARTICLE INFO

Article History:
Received 27th July, 2015
Received in revised form
04th August, 2015
Accepted 25th September, 2015
Published online 20th October, 2015

Key words:
Cryptography, Encryption,
Hash value, Security.

ABSTRACT

Network security measures are needed to protect data or information during the transmission. Security is an important factor in the network transmission. Secure transmission of multimedia object means the secure transmission of text, image, audio and video. Cryptographic techniques provide the security during transmission of multimedia objects. Cryptography means converting data from readable form to unreadable form. Advanced Encryption Standard (AES) algorithm provides greater security for data. Here, AES algorithm with 128 bit key is used for encryption and decryption process. Secure hash value is calculated for ensuring the security. SHA1 algorithm is used for calculating the hash value of the multimedia objects. AES algorithm prevent various types of attacks like message disclosure, replay attack etc.

***Citation*:** Santhi Mol, P. and Supriya, L. P. 2015. "Secure transmission of multimedia objects", *International Journal of Current Research*, 7, (10), 21169-21172.

INTRODUCTION

Security has become a growingly 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 apply and generally require less processing power when compared with asymmetric key algorithms. Here, SHA1 (Secure Hashing Algorithm) is used for finding the hash value. A cryptographic hash function L is an algorithm which maps a message string s of arbitrary length to a string T = L(s) of fixed length n, called hash value. The AES algorithm is a symmetric key algorithm that encrypts and decrypts multimedia objects. The encryption method converts an object from its original form into encrypted form. So disclosure attacks are not possible. The decryption process is to convert the encrypted object back to the original object. AES algorithm contains large number of processing steps. So it will take more time than other symmetric algorithm. But AES algorithm provides high security during the transmission. 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 (AES) used in this proposed system. The section IV explains SHA-1 algorithm. This algorithm is used to calculate the hash value of the multimedia objects. The section V includes the detailed explanation of secure transmission of multimedia objects. Finally the section VI depicts the result analysis. This section contains the screen shots and discussion.

Corresponding author: Santhi Mol, P.,
Computer Science and Engineering, SBCEW, Elavumthitta, India

Proposed system

Secure Transmission of Multimedia Objects mainly consists of the following modules:

- Browse multimedia objects, which sender wants to transmit securely.
- Calculate the hash value of the object using SHA1 algorithm.
- Append the hash value with this original object.
- Then encrypt this appended object using AES algorithm and send to the receiver.
- Receiver receives the encrypted object.
- Then decrypt the object.
- Separate the hash value.
- Receiver calculates the hash value of the received object.
- Compare the hash values and ensure the security.

AES Algorithm

AES (Advanced Encryption Standard) (Kundankumar Rameshwar Saraf *et al.,* 2014 and Sonu Varghese *et al.,* 2014) 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 contains an initial round (0), 9 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.

General Rounds

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

Add Round Key

Calculating 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.

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).

SHA-1 Algorithm

The Secure Hash Algorithm (SHA-1) (Thulasimani Lakshmanan and Madheswaran Muthusamy 2012; Nalini *et al.,* 2013) 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.

Mulimedia Transmission

This proposed system provides secure transmission of multimedia objects that is text, image, audio and video. Here SHA1 algorithm is used for calculating the hash value of the multimedia object. AES algorithm with 128 bit is used for encryption and decryption. Here, various attacks like message disclosure and replay attacks are not possible. AES algorithm contains large processing rounds. It makes the algorithm stronger. The below subsection explains the process of secure transmission of multimedia objects.

Text

First import the text for transmission. This text contains group of letters. First find out the corresponding ASCII values of this letters. Then arrange these values into 8*8 matrixes. This is the input of SHA1 algorithm. Then find out the hash value of this text and append this hash value with the original text and encrypt using AES algorithm. Then send to the receiver. Receiver receives the encrypted message and decrypts it. Then separate the hash value. Again calculate the hash value of the received text. We can compare these two hash values to ensure the transmission is secure. Attacks like message disclosure and replay attacks are not possible in this system, because secure AES algorithm is used for encryption and decryption process.

Image

Browse the image, which sender wants to transmit securely. Using SHA1 algorithm calculate the hash value of the image. Then append this hash value with the original image then encrypt using AES algorithm and send to the receiver. Receiver receives the encrypted image and decrypts it. Then separate the hash value from the image. Again calculate the hash value of the received image. By comparing these two hash values, we can prove the security.

Audio

Here first load an audio in .wav format and play the audio. Take the samples from this audio and arrange these samples in a 64*64 matrixes. This is the input of SHA1 algorithm. After calculating the hash value of the audio, append this with the audio. Then encrypt and send to receiver. Receiver receives the encrypted audio and decrypts it. Then separate the hash value from the audio. Again calculate the hash value of the received audio. By comparing these two hash values, we can prove the security during transmission.

Video

Here load and play the video. Then convert the video into frames. From this frames take one frame and calculate the hash value of this frame using SHA1 algorithm and append this hash value with the frame. Then encrypt the frame and send to the receiver. Receiver receives the encrypted frame and decrypts it. Then separate the hash value. Again calculate the hash value of the received frame. We can compare these two hash values to prove the transmission is secure.

RESULTS

The Screen shots of the secure transmission of multimedia objects are represented below. Fig. 1 is the home page of this work. We can select any multimedia object from that window. Fig. 2 depicts the secure transmission of images. Nowadays, security is an important factor of internet and network application. Likewise, secure transmission of images is the most challenging aspects. This work 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. That is first load the image, then find the hash value of that image using SHA-1 algorithm. Then append this value with the image. Then encrypt this appended image using AES algorithm and send to receiver.

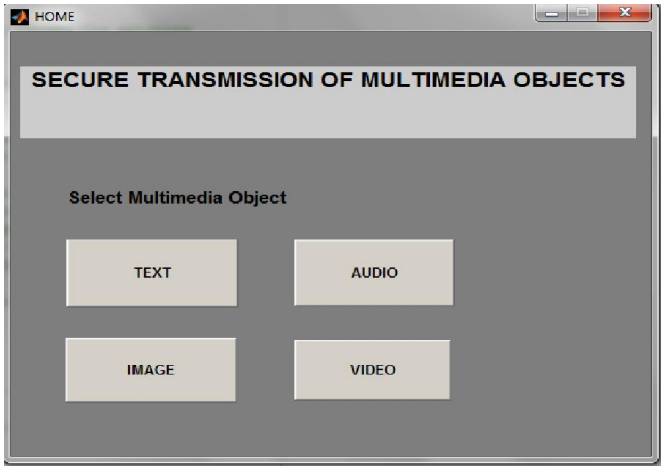

Fig. 1. Main page

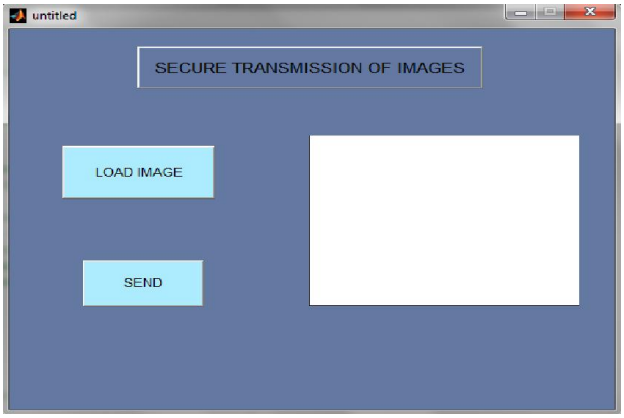

Fig. 2. Transmission of Images

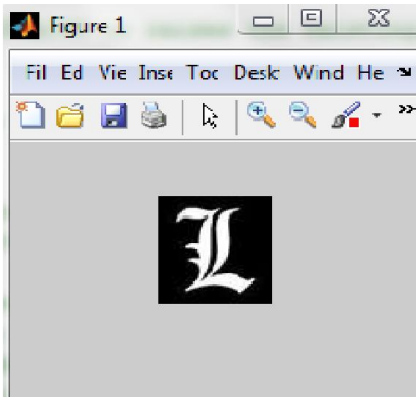

Fig. 3. Original Image

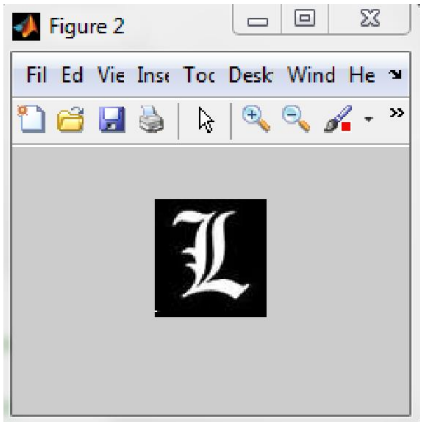

Fig. 4. Appended Image

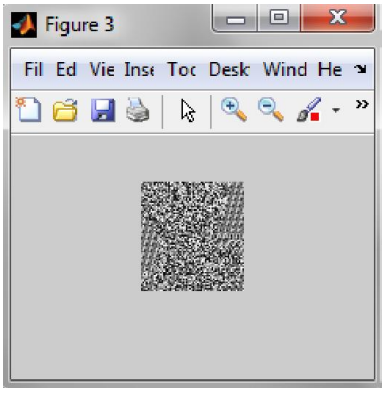

Fig. 5. Encrypted Image

Some existing symmetric key algorithms like DES, Triple-DES with 2-keys, Triple-DES with 3-keys, and AES have been implemented in (Neetesh Saxena, 2014). The standard key size used in DES, Triple DES with 2-keys, Triple-DES with 3-keys and AES are 64 (out of which 56 bits are used), 112, 168, and 128 bits respectively. DES and Triple-DES algorithms are not considered as very secure algorithms, since previously some attacks have been found on both algorithms. Thus, AES is the best option for this purpose which is considered one of the best secure algorithms. AES with 128-bit key has proved to be an efficient algorithm to encrypt and decrypt the objects.

Conclusion

The secure transmission of multimedia objects used in different areas. The main issue of the multimedia transmission is its security. Here calculate the hash value of the object and append this value with the original multimedia object. Then encrypt the object 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 (Jawahar Thakur *et al*., 2011) 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

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.

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.

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.

Neetesh Saxena, "EasySMS:A Protocol for end to end SecureTransmission of SMS", IEEE Transactions On Information Forensics and Security, Vol. 9, No. 7, July 2014 1157.

Sonu Varghese K, Faisal K K, Vinayachandran K K, "Image Security Using F5 and AES Algorithm", Proceedings of IRF *International Conference*, 13th April-2014.

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.

****