A Survey on Secure Transmission of Multimedia Objects

Santhi Mol P.
M.Tech. Scholar
Dept. of Computer Science & Engg.
Sree Buddha College of Engg for Women.
Pathanamthitta, Kerala, INDIA
santhimol123@gmail.com

Abstract— Secure Transmission of different multimedia objects like image, text, audio, and video are the most demanding aspects in the internet and network application. Recently, network security is the most important issue of the internet. Cryptography is the main category of computer security that changes the information from its normal form into an unreadable form. Encryption techniques are used to securely transmit data in open networks. Steganography is used for hiding the information. This paper provides a comparative study of different methods for end to end secure transmission of multimedia objects.

Keywords- Cryptography, Encryption, Multimedia, Security.

I. INTRODUCTION

Multimedia content is a combination of image, text, audio, and video. Multimedia security deals with the methods of protecting the multimedia objects. Symmetric key algorithms are most acceptable for encrypting this multimedia objects. Here, AES algorithm is used for the encryption and decryption process of multimedia objects. Some existing symmetric key algorithms like DES, triple DES with 3 keys and AES have been implemented in different papers. Out of these algorithms AES algorithm takes minimum time to encrypt and decrypt the multimedia object with various sizes. 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 showed to be a secure and efficient algorithm.

II. SECURE TRANSMISSION METHODS

Euijin Choo et al. [1] proposed a light weight encryption scheme for secure real time multimedia transmission. That is SRMT (Secure Real-time Multimedia Transmission). SRMT is an encryption scheme without loss of security and media QoS. It provides the confidentiality of multimedia data. Here uses one XOR operation and two block transpositions. In order to provide both security and media QoS, here consider three important characteristics. That is processing time, compression rate and security level. The SRMT scheme uses two block 0 transpositions and one XOR operation. Here first transposition is for generating a key frame. Second transposition and XOR operation is main encryption process. SRMT provide faster encryption of MPEG compressed data. Here attack models are classified in to two categories. That is cipher text only attack and chosen plaintext attack.

B.Padmasri et al. [2] proposed Spread Spectrum Image Steganography with Advanced Encryption key implementation (SSISAE). Nowadays the information hiding methods have become an important research area. This paper, explains a framework of effective security for data communication by implementing SSISAE. This system hides and recovers message. The hidden message can be retrieved using appropriate keys without any knowledge of actual image. This paper describes the spread spectrum communication that is the process of spreading the bandwidth of a narrow band signal across a wide band of frequencies. Here AES algorithm is used for encryption and decryption process.

A. Jaishree Singh et al. [3] proposed secure data transmission using encrypted secret message. In this paper the secret message is encrypted before the actual embedding process starts. Here, the hidden message is encrypted using the private key. And also DCT (Discrete Cosine Transform) technique is used for embedding and extraction of files. That is this proposed system encrypts the data with a tiny algorithm and then embed this encrypted data in a cover file. For this DCT algorithm is used. This proposed system provides the security of data. Here the mini algorithm is a Feistel type cipher that uses operations from mixed algebraic groups XOR, ADD and SHIFT. This paper provides two types of security levels, first by encryption and second is embedding or steganography. The below figure depict this proposed system.

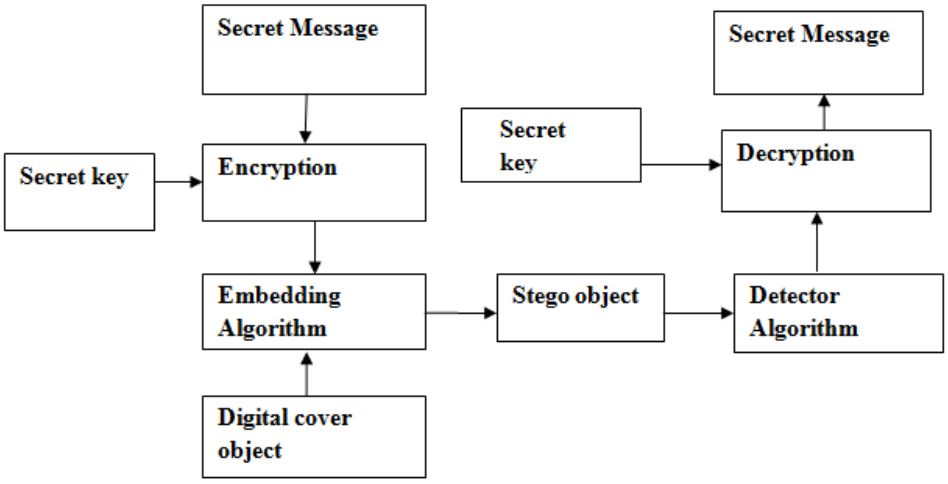

Figure 1. Block diagram of secure data transmission using encrypted messages

Parameshachari B. D. et al. [4] proposed secure transmission of an image using partial encryption algorithm. This paper proposes a novel concept of combined partial image encryption using phase manipulation and sign encryption. The encryption process contains two stages where image to be encrypted are applied to phase manipulation block. In first stage Fourier Transform (FT) is applied to get phase and magnitude of the input image. Phase of the image are crawled to get modified image after applying Inverse Fourier Transform. In second stage the modified image is partially encrypted by using sign encryption. Sign Encryption finally gives resultant partially encrypted image by extracting the sign bits of modified image. Partial encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. This paper presents a novel concept of pixel value manipulation using phase manipulation in frequency domain and sign encryption for partial encryption method.

Nagesh Sharma et al. [5] proposed a novel technique for secure information transmission in videos using salt cryptography. This paper presents a novel technique for transmitting secret information securely from sender to receiver by embedding this information into a video after encryption through salt cryptography. In this encryption method some random data is added to the private keys and passwords. Here define this random data as a salt which is needed to access the encrypted data, along with the password. These passwords alone have no use since they will be able to locate the hidden data only when mixed with proper salt. This salt is handled by a certified third party. Salt is created for different pairs of communicating parties. Here also introduced the concept of Enterprise Dependent Value (EDD), which are the embedding values corresponding to the binary digits and are specific to the communicating enterprises.

A secure audio steganography approach presented in [6] by Mazdak Zamani et al. This paper describes a wide range of steganography techniques. This approach resolves several problems like weakness of substitution technique and the large strength of substitution technique. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using this proposed genetic algorithm, message bits are fixed into multiple, vague and higher LSB layers, resulting in increased robustness.

Three new selective encryption techniques for secure transmission of MPEG-I video bit streams are presented in [7] by Adnan M. Alattar et al. These techniques improve the security level, and provide reasonable processing time. Here, in the first method the encryption is applied to the data associated with every n^{th} I macro block. In the second method, the encryption technique is applied to the headers of the entire predicted macro block as well as to the associated with every n^{th} I macro block. In the third method, encryption is applied to every n^{th} I macro block as well as the header of every nth predicted macro block. Finally with n=2, is found to be the most efficient of the three proposed methods. This method reduces the processing time, and the simulation results show that the encrypted video is fully disguised.

Rucha Bahirat et al. [8] is a survey on different secure data transmission using steganography. The ultimate aim of this steganography is to communicate securely in a completely invisible manner, so that no one can identify the transmission of a hidden data. This paper discusses the concept behind the steganography by describing what is steganography and the terms that are related to steganography. This paper gives the different

steganography methods for image steganography, audio steganography, video steganography, and text steganography that are used to embed the information in digital media. The two most important aspects of this steganography system are the quality of stego object and the capacity of the cover media. This paper found, a better steganography approach to increase the PSNR value and to decrease the MSE. The basic form for steganography is shown in figure below. The basic model of steganography consists of cover object, message, embedding algorithm and Stego key. Nowadays steganographic systems uses multimedia objects like video, image, audio etc. as cover object because people often send out digital pictures over email and other Internet communication.

In text Steganography the secrete message is hidden in the text and we use the different method to hide the message in text by changing the last bit of the message. Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

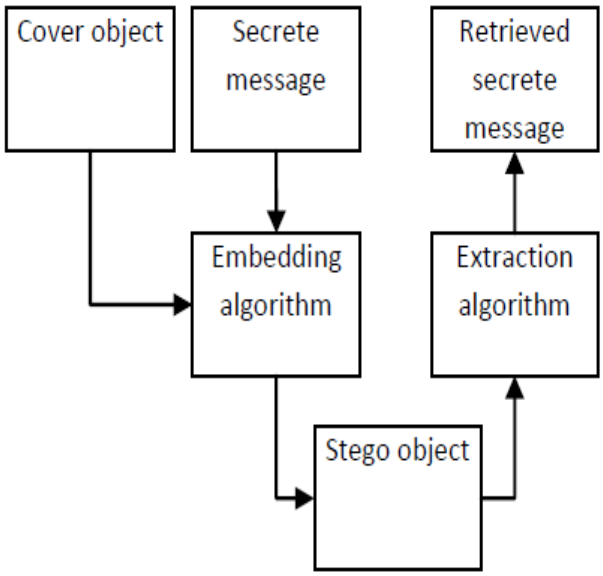

Figure 2. Basic steganography model

In Audio steganography, secret messages are embedding in digital sound. The secret data is embedded by slightly varying the binary sequence of a sound folder. Audio Steganography software can implant messages in WAV, MIDI and even MP3 sound files. Video files are generally a group of images and sounds, so most of the existing techniques on images and audio can be applied to video files too.

III. CONCLUSION

Security is the most challenging aspects of the internet and network application. Several authors proposed different techniques for secure transmission of multimedia elements like text, image, audio, and video. Here a survey is conducted in different methods for secure transmission if multimedia elements. Here explains two important security methods. That is cryptography and steganography. Encryption and Embedding provide higher security. Several encryption and embedding techniques explained here.

REFERENCES

[1] Euijin Choo, Jehyun Lee, Heejo Lee, Giwon Nam, "SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission", Basic Research Program of the Korea Science & Engineering Foundation.

[2] B.Padmasri, M.Amutha surabi, "Spread Spectrum Image Steganography with Advanced Encryption Key Implementation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.

[3] A. Jaishree Singh, Dr. J.S. Sodhi, "Secure Data Transmission using Encrypted Secret Message", International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 522-525.

[4] Parameshachari B D, K M Sunjiv Soyjaudah, Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 63– No.16, February 2013.

[5] Nagesh Sharma, Dr. Rakesh Rathi , Vinesh Jain, Mohd. Waseem Saifi,"A Novel Technique for Secure Information Transmission in Videos Using Salt Cryptography," Information and Knowledge Management ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol.3, No.10, 2013.

[6] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki, "A Secure Audio Steganography Approach," International Islamic University Malaysia.

[7] Adnan M. Alattar, Ghassan I, AI. Regib, "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-streams", IEEE, 1990.

[8] Rucha Bahirat , Amit Kolhe, "Overview of Secure Data Transmission using Steganography", International Journal of Emerging Technology and Advanced Engineering Website, Volume 4, Issue 3, March 2014.