Secure Data Transfer Using Video Steganography

[1]Prof. Dipti Mukadam, [2]Sunita Mahale, [3]Aayushi Dalvi, [4]Prajakta Magar, [5]Swapnil Gawade

[1,2,3,4,5]Mahatma Gandhi Mission's College of Engineering and Technology, Plot No. 1, 2, Sion - Panvel Expressway, Sector 18, Kamothe, Navi Mumbai, Maharashtra, India.

Abstract - Emergence of internet has made it possible to transfer the data from one place to another place rapidly and accurately. This data when goes through the internet may become a victim of the hackers who can steal, modify and misuse the information. Therefore it is necessary to transfer the data with atmost security. The steganography is the art of hiding message inside another medium such as Video, Image, Audio. In this paper, combination of cryptography and steganography is used for data hiding in video clips. This project focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files provides a high level of security. The files composed of insignificant bits or unused areas which can be used for overwriting of other data.

KEYWORDS: Steganography, LSB, Encryption, Decryption, AES.

I. INTRODUCTION

As people become aware of the internet day-by-day, the number of users in the network increases considerably thereby, facing more challenges in terms of data storage and transmission over the internet, for example Information like account number, password etc. Hence, in order to provide a better security mechanism, [7]we propose a data hiding technique called steganography along with the technique of encryption-decryption.

Steganography is the art and science of hiding data into different carrier files such as text, audio, images, video, etc[1]. In cryptography, the secret message that we send may be easily detectable by the attacker. But in steganography, the secret message is not easily detectable. The persons other than the sender and receiver are not able to view the secret message. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact.

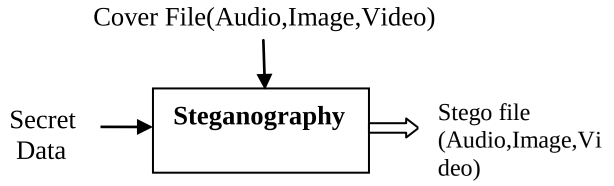

Fig . 1Basic Steganography System

A. Image Steganography

An image can be said an array of numbers which represents light intensities at pixels which results in data.[16] Image is composed of 8 bits per pixel i.e.256colors.Common approach designed for image steganography are LSB(Least Significant Bit) substitution which is the easy and most common approach of hiding data inside images.

B. Audio Steganography

Audio steganography works by slightly changing the binary sequence and concealing with the secret message.[10] Several methods are proposed such as Least Significant Bit(LSB) replacing last digit of carrier file.[12] Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample. Phase coding involves encoding of secret data to phase shifts.

C. Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding.The use of video files as a carrier medium for steganography is more eligible as compared to other techniques.

II. PROPOSED SYSTEM

Research work done in the field of image steganography can be extended to the to the video steganography. One of the most commonly used algorithm of image stegaanography is least undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography. Generally steganography technique is applied where cryptography is ineffective significant bit (LSB) method. Least significant bit based steganography method can also be applied to rext, audio and even for video.[15] steganography technique is generally classified into three main types namely, technique exploiting image format, method embedding in frequency domain and method in spatial domain[2].Stego is a greek word which means hidden. The ancient people used various techniques to send the

DOI : 10.18231/2454-9150.2018.0021

secret messages during the war time. The evaluation of steganography technique is done with three parameters such as capacity, robustness and security[3].The system should be capable of hiding the information into cover media, it should be robust to the changes and it should be secured enough from eavesdroppers or attackers that tends to identify or alter the contents of the secret data[4].

III. Proposed Work

Cryptography is a technique used to encode the data in such a way that even if the encoded data is visible its meaning is unknown to the intruder. A combination of Cryptography and Steganography is the crux of our proposed approach in this paper. Here we make use of the AES algorithm. This algorithm has been chosen after appropriate analysis as it best suits our purpose of implementing security.[3] In this approach the message is subjected to the AES algorithm to generate an encrypted message.

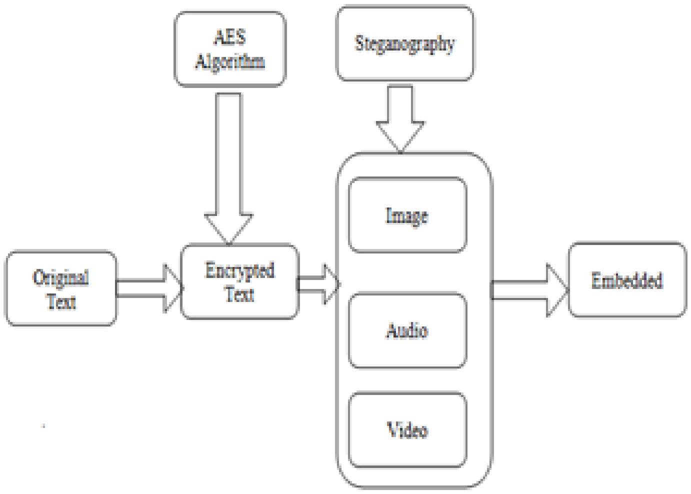

Fig. 2 System Architecture

A. AES Encryption Algorithm

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Tech-nology (NIST) in 2001.It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It supersedes the Data Encryption Standard (DES), which was published in 1977.

The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both en-crypting and decrypting the data.[3] AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Un-like its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 44 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state.

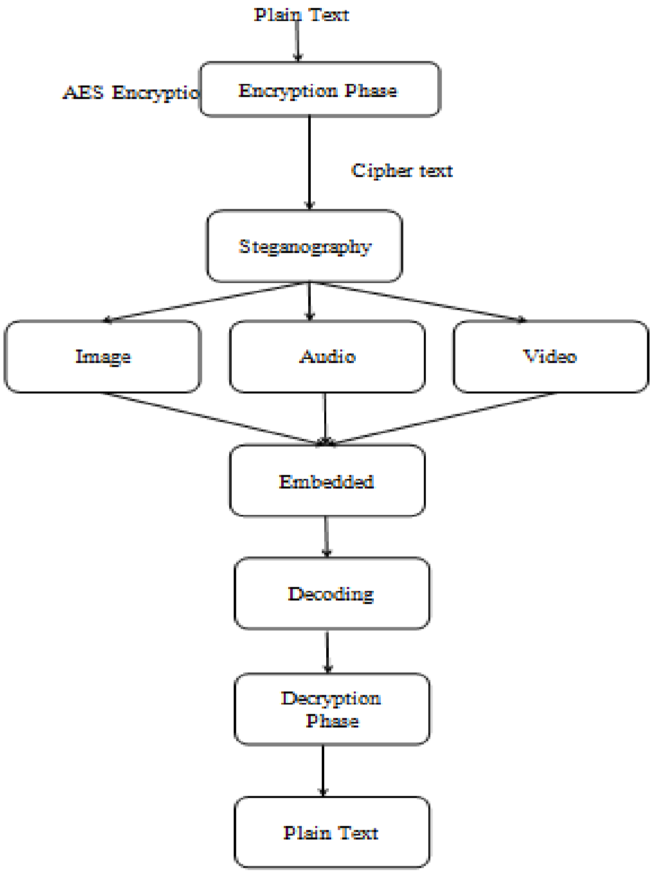

Fig. 3 Flow Diagram

B. Steganography over Cryptography

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in countries where encryption is illegal [1]Steganography's goal is to keep the presence of a message secret, or hide the fact that communication is taking place.[2]Cryptography's goal is to Obscure a message or communication so presence of a message secret, or hide the fact that communication is taking place.[2]Cryptography's goal is to obscure a message or communication so that it cannot be understood.

C. Encoding Secret Messages in Audio, video and image

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secrete message in audio without being detected.

D. Embedding

Embedding the hidden data into the cover message and sending it, you can gain a sense of security by the fact that no one knows you have sent more than a harmless message other than the intended recipients.

IV. Conclusion

Today one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. By taking this problem into consideration ,we have designed a System "Data security using video steganography" which prevents the user from any kind of hacking data.[1] The Steganography is hidden communication to protect confidential information.

In this paper we presented several ways of hiding the secret data inside the cover medium such as image, audio, video. The proposed system for data hiding uses AES for encryption which results in more secure technique for data hiding .We can conclude that the proposed system is more effective for secret communication over the network channel.

References

[1] A. Swathi, Dr. S. S.K Jilani, "*Video Steganography by LSB Substition Using Different Polynomial Equations*," International Journal Of Computational Engineering Research,vol.2 ,Issue.5, sept.2012.

[2] Vipula Madhukar Wajgade , Dr. Suresh Kumar , International Journal of Emerging Technology and Advanced Engineering Website:www.ijetae.com ,ISSN 2250-2459, ISO 9001:2008 Certified Journal,vol.3, issue.4,

April 2013.

[3] Hamdy M. Kelash , Osama F. Abdel Wahab ,Osama A. Elshakankiry ,Hala S. El-sayed (2013) "*Hiding Data in Video Sequences Using Steganography algorithms*" IEEE.

[4] H. Yuh-Ming and J. Pei-Wun , *"Two improved data hiding schemes,"* in Image and Signal Processing (CISP), 2011 4th International Congress on,2011,pp.1784-1787.

[5] L. Reyzen and S. Russell, "*More efficient provably secure Steganography* " 2007.

[6] Sunil. K. Moon , Rajeshree. D. Raut (2013) *"Analysis of Secured Video Steganography Using computer forensics Technique For Enhance Data Security* " IEEE.

[7].Jamil ,T., "*Steganography :The art of Hiding Information is Plain Sight*",IEEE potentials ,18:09,1999.

[8]RigDas, Themrichon Tuithung"*A Novel Steganography Method for International Journal of Advance Research, IJOAR .org ISSN 2320-9194 30 IJOAR© 2013 http://www.ijoar.org Image Based on Huffman encoding*" IEEE, 2012.

[9].B. Pfitzmann *,"Information Hiding Terminology* ,"proc. First Int'l Workshop Information Hiding, Lecturer Notes in Computer Science No. 1,174 Spring- Verlag ,Berlin, 1996,pp. 347-356.

[10] Masoud Nosrati Ronak Karimi Mehdi Hariri (2012) *"Audio Steganography: A Survey on Recent Approaches"* World Applied Programming, Vol (2), no(3).

[11] Blossom Kau r, Amandeep Kaur2, Jasdeep Singh (2011) *"steganographic approach for hiding image in dct domain "IJAET,vol.1,issue.3.*

[12] S. M. Masud Karim, Md. Saifur Rahman "*A New Approach for LSBBased Image Steganography using Secret Key*" International Conference on Computer and Information Technology (ICCIT 2011)22-24 December, 2011 , IEEE.

[13] N. Provos and P. Honeyman, *"Hide and Seek: An introduction toSteganography*," IEEE Security &Privacy Journal 2003.

[14]Steven W. Smith, the Scientist and Engineer's Guide to Digital Signal Processing.

[15] V. Lokeswara Reddy, Implementation of LSB Steganography and its Evaluation for Various File Format.

[16] Al-Qersh *"Image Steganography Techniques: An Overview"* International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3):2012.

DOI : 10.18231/2454-9150.2018.0021