International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Secure Text Transmission using Video Steganography

Sayli Dhulap[1],Tanuja Rao[2], Yuga Vartak [3,] Sushant Patil[4]
[1, 2, 3, 4, 5] *Department of Computer Engineering, St. John College of Engineering and Management, University Of Mumbai*

Abstract*: *Steganography is a method of hiding confidential data and message in various medias like image, audio, video etc. Cryptography techniques are also integrate the process of converting plain text into cipher text and vice-versa. To enhance the security, in this system the standard encryption method known as Advanced Encryption Security (AES), image split and random pixel embedding techniques. The data is encrypted in the system using AES and it is embedded in the least significant bit (LSB) of randomly selected pixels of image. Various sizes of data are stored inside the images and the PSNR (Peak signal-to-noise ratio) is also captured for each of the images tested. Based on the PSNR value of each images, the stego image has a higher PSNR value. Hence this steganography algorithm is very efficient to hide the data inside the video.
Keywords*: *Steganography algorithm, Cryptographic algorithm, secret key, Security, data retrieval.

I. INTRODUCTION

This paper proposes a new algorithm to hide the data inside Video using steganography technique. The word steganography itself originated in Greece and means covered writing. Cryptography combined with image steganography can prove to be the best method to keep our information secured. Video steganography is meant for hiding of information in the form of image. There are many techniques to do the same, including LSB techniques, DCT etc. An algorithm is designed to hide all the data within the image to protect the privacy of the data. This system provides a video platform for user to input video and a text box to insert texts. Once the proposed algorithm is adapted, user can send the stego video to other computer user so that the receiver is able to retrieve and read the data which is hidden in the stego video by using the same proposed system. Steganography is basically application which is developed for hiding the confidential data in a cover file in such a way that no one other than a authorised person knows the presence of such hidden information in cover file. Audio, Video Text or even image can be used as a cover file. Cryptography is basically an art of jumbling the secret information in such a way that nobody can understand it. So it can also be used to counter the above mentioned problems. Though both the techniques are designed for the same purpose i.e. keeping the information secret from unauthorized person, both techniques are different the way they present the secret information to the real world. Cryptography encrypt the secret information in to the jumbled word which is very difficult to decipher. But for the hackers, jumbled word indicates that some kind of secret or confidential information is hidden behind these jumbled word. So they knows that there are some kind of secret information but they are not able to decrypt it. On the other hand in steganography, the secret or confidential information is hidden in a innocent cover file in such a way that nobody can even imagine that such kind of information is hidden inside the cover file which may be any image, audio or video.

The main objective of the system is to provide more security by using AES encryption for data and embedding the encrypted data in randomly selected pixels LSB and then by splitting the image into parts before the data transmission through the public network. The security is achieved by splitting the encrypted data embedded video into parts and transmit the video parts through the network. If any part of the video is received by the intruder and has the key to decrypt it, he only gets a part of the secret data. The intruder gets the whole data only, if he gets the whole splitted video parts and The main objective of the system is to provide more security by using AES encryption for data and embedding the encrypted data in randomly selected pixels LSB and then by splitting the image into parts before the data transmission through the public network. The security is achieved by splitting the encrypted data embedded video into parts and transmit the video parts through the network. If any part of the video is received by the intruder and has the key to decrypt it, he only gets a part of the secret data. The intruder gets the whole data only, if he gets the whole splitted video parts and should arrange the splitted video parts in the correct order, and then only the intruder can achieve the secret data correctly. So data transmitted through the network gets more security by splitting the stego video into fragments while transmitting through the network.

II. LITERATURE SURVEY

A. *Steganography literature survey, classification and comparative study* [1]

The main idea is based on embedding important information in multimedia carrier such as: text, image, audio, and video. The developed methods may be classified as steganography and watermarking. Steganography aims to embed huge amount of secret data in multimedia carrier while watermarking aims to hid small amount of secret data in multimedia carrier. A digital image steganography information hiding techniques is presented. first, a classification of watermarking algorithms based on embedding domain is shown. These domains are spatial domain, transform domain, Spread Spectrum steganography, Model Based steganography. All these algorithms try to satisfy three most important factors of steganographic design i.e. un-detectability, robustness, and capacity

B. Review of an Improved audio Steganography Technique over LSB Through RANDOM Based approach [2]

This paper proposes a method of audio steganographic system that provides a unique platform to hide the secret information in audio file though the information is in text, image or in an audio format. So there is no need to go for different techniques of steganography as per information format. Many steganographic methods follow the LSB insertion technique to hide the secret information. But there are many statistical techniques available to determine if a stego object has been subjected to LSB Embedding. embedding text or image or an audio data in cover audio file using public key encryption algorithm i.e. SHA-1 through random based approach. Emphasis is on comparing proposed scheme with simple LSB based data hiding in audio. The proposed system hides secret information in audio file through random based approach and provides security by using PKE algorithm. This paper focuses on combining the strengths of cryptography and steganography for secured communication.

C. Secure Transmission of data By Splitting Image [3]

Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. This paper aims to provide an efficient and a secure method for video Steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are located. Hence, during the extraction process, instead of analyzing the entire video, the frames containing the secret data are analyzed with the help of index at the receiving end When steganography by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner. It also reduces the computational time taken for the extraction process.

III. PROPOSED SYSTEM

Our proposed algorithm is using two layers of security to maintain the privacy, confidentiality and accuracy of the data. Fig. 1 shows the architecture for the overall process of the system. The inside the video. Without the secret key, the data cannot be retrieved from system is able to hide the data inside the video as well as to retrieve the data from the video. For hiding the data, a username and password are required. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen video. Using a steganography algorithm, these data will be embedded and hided inside the video. For retrieving the data, a secret key is required to retrieving back the data that have been embedded the image. This is to ensure the integrity and confidentiality of the data.

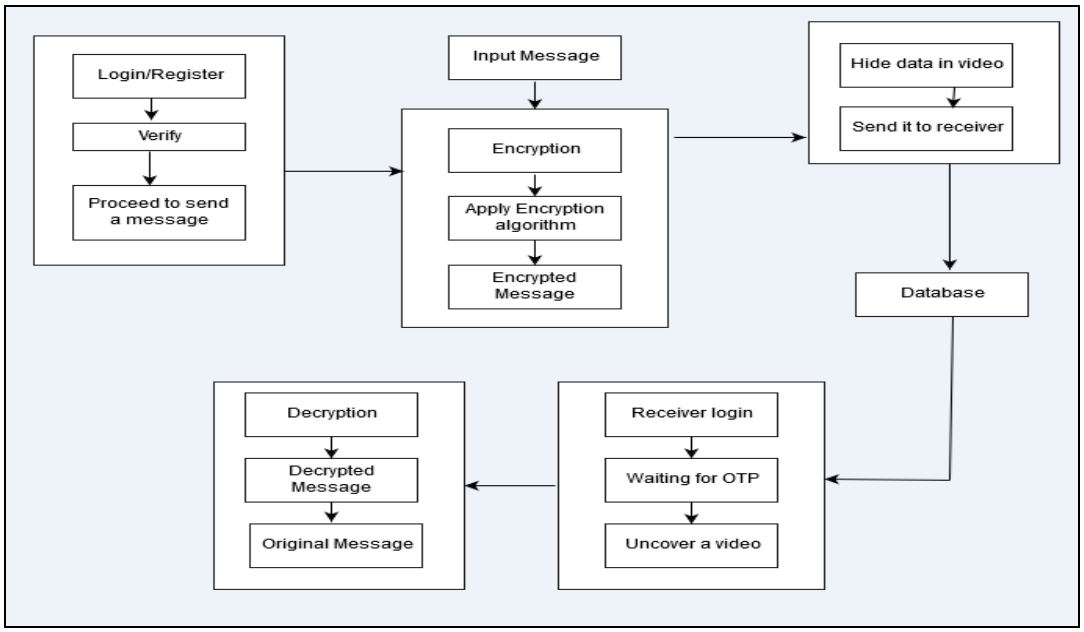

fig.1 Architecture of System

IV. METHODOLOGY

Process in the video sequence eg. Making video stego while the overall process divided into two parts. First part deal with the message embedding the second part deal with the extraction of message from the stego video.

A. LSB Technique

The most popular method for steganography is the Least Significant Bit (LSB) encoding. Using any digital image, LSB replaces the least significant bits of each byte by the hidden message bits. Depending on the image format the resulting changes made by the least-significant bits are visually detectable or not. For example, the GIF format is susceptible to visual attacks while JPEG being in the frequency domain is less prone to such attacks.

B. AES Algorithm

According to the modified AES algorithm, four types of transformations are used likes AES; substitution (SubBytes), permutation (ShiftRows), MixColumns, and key adding, to provide security. Because of the AES is based on the Rijndael cipher, it performs four types of transformation based on the operations in finite field .Several operations are defined at byte level, and used with bytes representing as elements in the finite field .Then, it represents the input and the output in form of hexadecimal digits .Therefore, AES algorithm is modified to make the input and the output in the form of MPK digits because the PVD_MPK and MSLDIP-MPK methods use the MPK digits for hiding the data. This modified AES algorithm called AES_MPK algorithm.

C. AES Algorithm

1) Input: Secret Message (SM), Cipher Key K.
2) Output: Cipher Message CM.
3) *Steps:*
a) Make key expansion of K that produces two lists of all sub keys.
b) Partition SM to blocks (B1, B2, B3 …. Bn) each block consists of 16 byte.
c) for each Bi block do
d) Convert each byte to MPK digits (two digits for each byte).
e) Divide Bi to two state arrays (4*4)
f) Filter two states.Make pre round AddRoundKey which is a simple bitwise XOR of the current two states with two sub keysrepeat
g) . Apply the four transformations (SubBytes, ShiftRows, MixColumns, and AddRoundKey) in two states.

D. Flow of system

1) Step 1: Input the message and video.
2) Step 2: Extract audio.
3) Step 3: Convert the video in to a frames and store all the frames in to a folder.
4) Step 4: Select any one frame for storing message .
5) Step 5: Apply AES algorithm for encryption, assign a key.
6) Step 6: Download the encrypted file.
7) Step 7: Receiver downloaded the encrypted file and wait for the OTP.

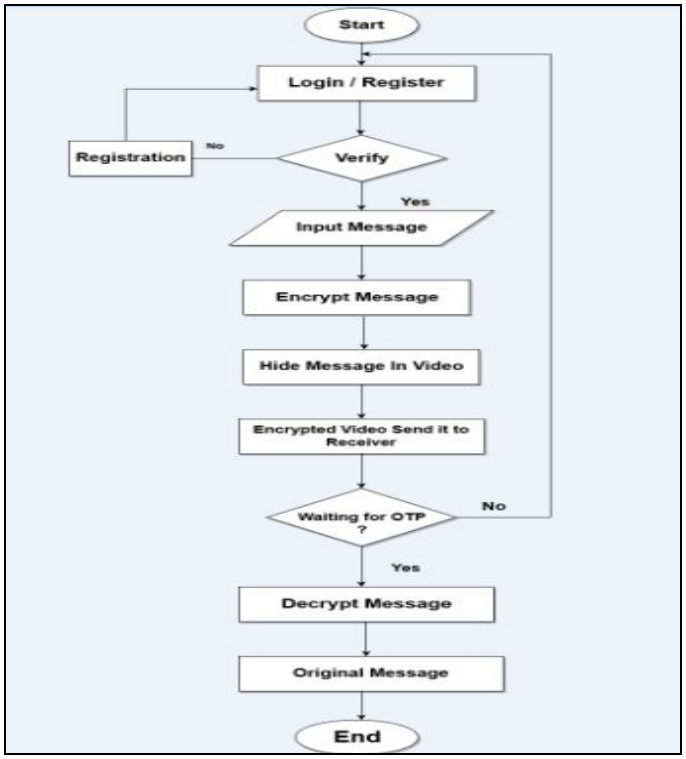

Fig 2:Flowchart of System

V. CONCLUSION AND FUTURE WORK

In this paper, a new secure communication model has been presented that combines cryptography and steganography techniques to provide two layer of security, so the steganalyst can't reach to plaintext without knowing the secret key to decrypt the ciphertext. Experimental results showed that our proposed model can be used to hide much more information than that other existed methods and the visual quality of the stego image is also improved, in addition to it is effective for secret data communication. In the future work, we are looking forward to try applying the proposed method on audio and video. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher.

REFERNCES

[1] Alaa Fkirin, Gamal Attiya" Steganography Literature Survey, Classification and Comparative Study"Communications on Applied Electronics (CAE) – ISSN : 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 5 – No.10, September 2016
[2] [2] Bhagyashri A. Patil1, Vrishali A. Chakkarwar "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013).
[3] "Secure Transmission of Data by Splitting Image "2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India
[4] R. Balaji ,G. Naveen. "Secure Data Transmission Using Video Steganography "
[5] dnan M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. On Image Processing,vol. 13, no.8, Aug, 2004

[6] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani,Dual layer data hiding using cryptography and steganography in IJSET volume 1,issue 4,ISSN : 2277-1581
[7] F. A. P. Petitcolas et al, “Information Hiding-A Survey,” Proceedings of the IEEE, special issue on protection of multimedia content, Vol. 87,Issue. 7PP. 1062-1078, July 1999.
[8] A. J. Altaay et al, “An Introduction to Image Steganography Techniques,” International Conference on Advanced Computer Science Applications and Technologies, PP. 122126, 2012
[9] S. Murphy, “The Advanced Encryption Standard (AES),” information Security Technical Report, Vol. 4, No. 4, PP.12-17, 1999.
[10] S. Sharda and S. Budhiraja, “Image Steganography: A Review,” International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.4, Issue 1, PP. 707–710, January 2013.
[11] Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I., "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on , vol., no., pp.286,291, 22-24 Dec. 2011.