Hiding Text in Video by Linked List Method:Dual Steganography

MIEEE **Neha Anjum**[1], **P.Sidharth Kaushik**[2]UG student, **K.Mounika**[3]UG student, **B.Sharon**[4] UG Student,
Sreyas Institute of Engineering and Technology, Hyderabad

[1]nehaaslampasha@gmail.com
[2]sidu1996@gmail.com
[3]mounikareddy.Kankanala@gmail.com
[4]sw33tsonu09@gmail.com

Abstract: **The recent growth in computational power and technology has propelled the need for highly secured data communication. One of the best techniques for secure communication is Steganography-a covert writing. It is an art of hiding the very existence of communicated message itself.The aim is to design a steganography algorithm which not only hide the message behind the image but also provide more security than others .A new steganography technique for embedding both text or image in cover images by using LSB & Link List method is implemented. This steganography technique is completely a time domain (pixel based) and secret messages are embedded directly into 24-bit color image. Two ways are provided for embedding the secret data inside cover image such as sequential encoding and random encoding for both text & image .For the purpose of security, encryption technique is used with a user defined key. RGB image format is used to improve the quality of the stego image. At last that RGB image will saved as BMP image file so that no lossy compression can occur and the original message do not destroy and can be extract as it is. Aspect ratio for both text and image after hiding in cover image maintains exactly same. Performance of proposed steganography technique is evaluated by calculating values of MSE(Mean square error), PSNR(Peak signal to noise ratio), ET(Elapse time). Dual Steganography is the process of using Steganography combined with Cryptography. Steganography is the process of hiding confidential data's in the media files such as audio, images, videos etc. Cryptography is a branch of mathematics concerned with the study of hiding and revealing information and also for proving authorship of messages. In this paper, Dual Steganography concept has been applied to secure the original videos from unauthorized person. The process has been done by embedding the original video inside another video. Both the videos are converted into frames first. Then the individual frames of original video are sampled with the frames of another video. After completing the sampling process, the output frames are combined to get the encrypted video.**

Keywords—**Steganography, PSNR, MSE, ET(Elapse time),Fiestal Network.**

INTRODUCTION

Steganography is the science of invisible communication which hides any private data within

an innocent-looking cover object. The word Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is an information hiding technique developed in recent years. It is a procedure that makes use of human perceptive sense of visual or aural redundancy to digital multimedia, and that embeds the secret information in the public media to transfer digital media carrying confidential information to achieve covert communications. Steganography is different from cryptography. The goal of cryptography is to provide secure communications by transforming the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it cumbersome for a third person to find out the message. Unlike steganography, sending encrypted information may draw attention. Accordingly, cryptography is not the good solution for secure communication but only part of the solution. Both techniques can be used together to better protect information. Basic steganography model is shown below.[1]

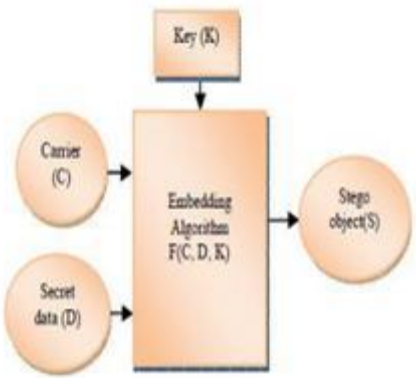

Fig1. Basic Steganography Model.

The basic model consists of Carrier(C), Secret Data(D), Stego Key(K).

- Carrier is the cover object in which the message is embedded.
- Secret data can be any type of confidential data that can be plain text, cipher text or other image.
- Key mainly used to ensure that only recipient having the decoding key will be able to extract the message from a cover-object.
- By using the embedding algorithm, the secret data is embedded into the cover object in a way that does not change the original image in a human perceptible way.

Finally, the stego object which is the output of the process is the cover-object with the secretly embedded data.

So far Cryptography is used in many forms but using it with Audio files is another Stronger Techniques. The process of Cryptography happens with Audio File for transferring more secure sensitive data. The Sensitive Data is Encoded with an Video File and Passed over Insecure Channels to other end of Systems. Here we are using .wav file Format for Encryption and Decryption of Message. The given message will be encrypted with a given video file using a secret key. The System will then embed the secret message into the video file. The result will be a new video file, which has the secret message in it. While decrypting the same key should be given for encrypted video file to get the secret message from it.

EXISTING SYSTEM

Video Steganography may be a technique to cover any reasonably files into a carrying video file. The employment of the video primarily based steganography is additional eligible than different transmission files thanks to its size and memory necessities. Videos square measure the set of pictures. Video is associate degree electronic medium for the recording, repetition and broadcasting of moving visual pictures. The average number of still images per unit of time of video is twenty four frames per second. If a person sends

sensitive information over the insecure channels of the system then there may be a chance of hacking it, they can alter the information and sends it over the net. (Example is military persons sending sensitive information over the net.)

PROPOSED SYSTEM

In the proposed system the above problem has been solved by embedding the data into the video file. Before embedding it into the file, encryption operation will be performed by using the encryption key which is provided by the source. Then this video file will be passed over the net, even if hacker hacks it, can be able to see only an video file. At the destination side this data will be encrypted from video file and performs decryption to get original message. The data is embedded inside the video by embedding each byte of information inside the pixel of video frames without affecting the original quality of the video. By using this concept:

- Large amount of data can be stored because of embedding the information inside video. Hence increases the storage capacity.
- More security will be provided to data since the information is encrypted using Feistel network before embedding it inside the video.
- Quality of cover video will not be affected.
- Since Linked List method has been used for embedding information inside video, it will be difficult for the intruders to predict the location of the presence of the information inside each frame. The process is done by, first converting the videos into frames. Then the secrete text should be encrypted using Feistel network and then embedded inside the frames of the cover video to obtain Stego frames. The embedding process is done using

  Linked List Method. In Linked List method, after embedding the byte of information inside one 3*3 pixel, the address of the location of next byte of information should be embedded next to it. The Stego frames are then combined to get the Stego Video.

ARCHITECTURE

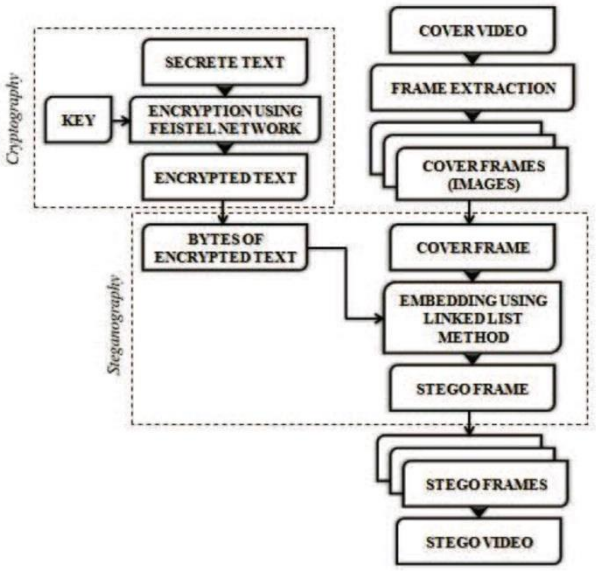

Fig2. Encryption Architecture.

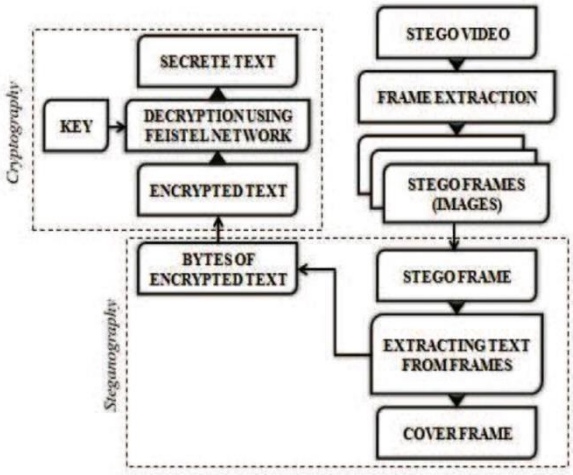

Fig3. Decryption Architecture.

RELATED WORK

The general architecture consists of two phases:
1. Hiding data in Video (Encryption)
2. Retrieval of original information (Decryption)

A. Overall Design For Encryption

In Encryption architecture, first the cover video is converted into a sequence of frames by extracting them. Each extracted frame represents an image. Then the secrete information which has to be embedded inside the video file is first encrypted using Feistel network with different keys (K0, K1, K2 ... Kn). The encrypted information is then separated into bytes of data. Then, each byte of data is embedded into each video frame in a sequence using Linked List Structure Message Embedding Technique. After embedding the information into frames, a sequence of Stego Frames will be obtained. The embedded frames are called as Stego Frame. Later the Stego Frames are combined to get the Stego Video containing the hidden message inside.

B. Overall Design For Decryption

In Decryption Architecture Fig2, first the Stego Video containing hidden message is converted into a sequence of Stego frames by extracting them. Each extracted frame represents a Stego image. Then the secrete information is extracted from Stego frames using Linked List Structure technique. The extracted text will be in the form of encrypted message. The message is then decrypted using Feistel Network with various keys (K0, K1, K2 ... Kn) and the original message is obtained.

C. Module Description

The modules are:

- Encryption process
- Decryption process

Module 1: Encryption Process

The steps involved in encryption process are:

1. Extracting frames from video
2. Encrypting data using Feistel network algorithm
3. Embedding text inside image frames
4. Obtaining Stego video

Extracting frames from video: The orig inal video (cover video) is converted into a sequence of frames. Each frame represents an image.

Encrypting data using Feistel network algorithm: The secret information is encrypted using Feistel network algorithm. In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German IBM cryptographer Horst Feistel; it is also commonly known as a Feistel network. A large set of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel construction is iterative in nature which makes implementing the cryptosystem in hardware easier.

CONCLUSION

The Linked List method and Feistel Network has been introduced for hiding Information inside Video. The two main algorithms used for data encryption and data embedding are Feistel Network and Linked List method respectively. The work begins with extracting frames from cover video. Then the encryption of data takes place using Feistel Network. After encryption of data, the encrypted data is embedded inside each video frames using Linked List method and Stego frames are produced. Later, the Stego Frames are combined to get a Stego Video. This technique provides a high level security to the information and the quality of stego video will be equal to the cover video. Since Feistel Network is used for encrypting data, it will be difficult for the intruders to decrypt the information.

REFERANCES

[1] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, “Hash Based Least Significant Bit Technique for Video Steganography (HLSB”), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1,No2, April 2012.

[2] A. Swathi and Dr. S.A.K. Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September 2012.

[3]Ronak Doshi, Pratik Jain and Lalit Gupta, "Steganography and Its Applications in Security",International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 6, November-December 2012.

[4] Rohit G Bal and Dr. P. Ezhilarasu, "An Efficient Safe and Secured Video Steganography using Shadow Derivation", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[5] Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. El-sayed, "Utilization of SteganographicTechniques inVideo Sequences", International Journal of Computing and Network Technology, Sys. 2, No. 1 Pg. 17-24, January 2014.

[6]Hemant Gupta and Setu Chaturvedi, "Video Steganography through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol. 14, No. 3, March 2014.

[7] Anwar H. Ibrahim and Waleed M. Ibrahim, "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time",International Journal of Information Technology & Computer Science (IJITCS), Vol. 7, No. 3, February 2013.

[8] Krati vyas and B. L. Pal, "A Proposed Method in Image Steganography to improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 1, January 2014.

[9] Deepak Kumar Sharma and Astha Gautam, "An Approach to hide Data in Video using Steganography",International Journal of Research in Engineering and Technology (IJRET), Vol. 3, Issue 4, April 2014.

[10] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Enhancing Data Security using Video Steganography", International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.

[11] Ms. Fameela. K. A, Mrs. Najiya. A and Mrs. Reshma. V. K, "Survey on Reversible Data Hiding in EncryptedImages".