A Novel Data Embedding Technique for Hiding Text in Video File using Steganography

K.V.Vinodkumar
M.Tech Student,
Department of CSE,
K.S.R.M College of Engineering, Kadapa.
Y.S.R. Dist., A.P. (INDIA)

V. Lokeswara Reddy
Associate Professor,
Department of CSE,
K.S.R.M College of Engineering, Kadapa.
Y.S.R. Dist., A.P. (INDIA)

ABSTRACT

Today's internet applications require data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the solution for this problem is Steganography. That has to do with secure data transmission between a sender and a receiver; implementing Steganography is the best way. Steganography is hiding private or secret data within a carrier in an invisible manner, in such a way that no one, apart from the sender and intend recipient. This paper focus on hiding text in a computer video file and to retrieve the hidden information. Generally Video files are collection of both images and audio. Hiding large amount of data in video is possible compare with others. Video Steganography deals with hiding secret data or information within a video. This can be done by using LSB technique.

Keywords: Steganography, Data hiding, Least Significant Bit Method (LSB), Compression, De-compression, Encryption, Decryption, Embedding, De-embedding.

1. INTRODUCTION

Steganography is the science of writing hidden messages is such a way that no one except sender and intended recipient can realize there is a hidden message. This subject has been brought into the public attention by intelligence agencies and news media. Now a day's agencies are using cryptology as well as Steganography to support or help themselves with their objective apart from state of art, communication technology and media. Imperceptibility means that text should not be perceptible to the human eye which is a fundamental requirement for this subject. Steganography is derived from Greek word steganos,it is also known as covered or secret and graphy which sense writing or drawing. It is referred to stego. This is existed for 1000's of years and used to pass secret info written in wax covered tablets which is scraped off a tablet, in this itself secret text is written covered with wax. Another technique is by shaving the head again tattoo will be revealed even though shaving a messengers head, tattoo a message or image on a bald head and hair grows which is another technique. The invisible ink is used in World War 2 extensively and traditional stego method. But text gets revealed when heated files are not only the carriers but also hide the messages. In computer image files, audio files, video files and text files secret information can be hidden. The image files are JPEG, GIF, BMP, audio files are WAV, MP3, and video files are MPEG, MP4, and AVI. Steganography expert is unable to detect the hidden information from the image provided with good steganographic algorithm and original video of Stego'd video. Secret information hidden in the carrier can be transmitted quickly, secretly, securely with usage of internet. Proposal of multimedia objects in which hidden text is fixed by Steganography mechanisms over the past few years. Which have a highly useful representation which permits an addition of amount of stego data in presence of simple and subtle modifications. By this perceptual content of underlying cover object can be preserved where perfect candidates use as cover messages. An encrypted or unencrypted message can be hidden in a computer video and transmitted over internet. To extract hidden text image file on receipt can be used. . This design incorporates the most powerful LSB algorithm to encode the message into video file. Steganography is not an alternative to cryptography. Steganography is the dark cousin of cryptography. While cryptography provides privacy, Steganography is intended to provide secrecy. In other words, cryptography works to mask the content of a message; Steganography works to mask the very existence of the message.

2. USES OF STEGANOGRAPHY

Steganography can be a solution which makes it possible to send news and information without being censored and without their fear of the messages being intercepted and tracked back to us. It is also possible to simply use Steganography to store information on a location. For example, several information sources like our private banking information and some military secrets can be stored in a cover source. Which can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside? Steganography can also be used to implement watermarking although the concept of watermarking is not necessarily Steganography, there are several steganographic techniques that are being used to store watermarks in data. The mail difference is on intent, while the purpose of Steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this. E-commerce allows for an interesting use of Steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning and images via Steganography allow for a very secure option to open e-commerce transaction verification. Paired with existing communication methods, Steganography be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital Steganography provides vast potential for both types. Businesses may have similar concerns regarding trade secrets or new product information.

3. PROPOSED METHODOLOGY

The existing systems require high-quality user interface, non-provision of choosing the key and more encode-decode time consumption. There are many steganographic algorithms existing. Some of them are excellent in every esteem; unfortunately, most of them require usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems. The proposed application will be written in Java to defeat the drawbacks of existing system, operability over multiple operating systems and even over different hardware platforms would not be a matter. This Proposed stego technique provides easy way of implementing the methods. The thought behind this design is to provide a first-class, well-organized method for hiding the secret message from hackers and sent to the target securely. This system would be mainly related with the algorithm ensuring the secure data transfer between the source and destination. This proposed system is depends on video Steganography for hiding secret message into the video file, retrieving the hidden secret message from the video using Least Significant Bit(LSB) mechanism. By using Data Encryption Standard (DES) algorithm at the sender side the secret text message is encrypted. The key which is used in DES is shared by both sender and receiver. The encrypted message is passed to embedding phase. In embedding phase the encrypted message will embedded into the cover file (video file) resulting in a Stego'd video file. The embedded Stego'd video file contains the encrypted text message which is extracted at the receiver side. At the receiver side Stego'd video file is passed to the de embedding phase. In extraction process encrypted text will be extracted from embedded video file and encrypted text is decrypted using decryption module.

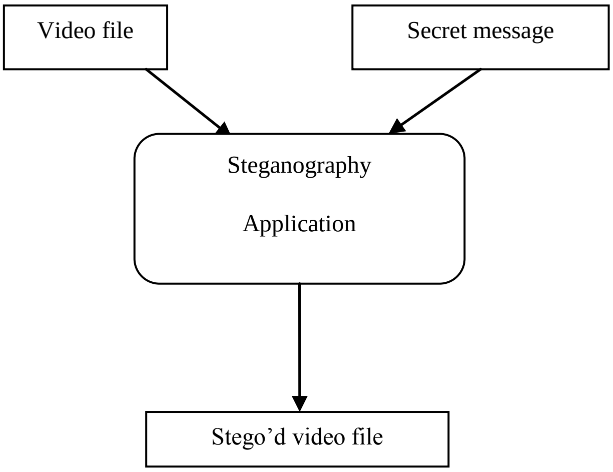

Fig 1: Hiding secret message/Conceal secret message.

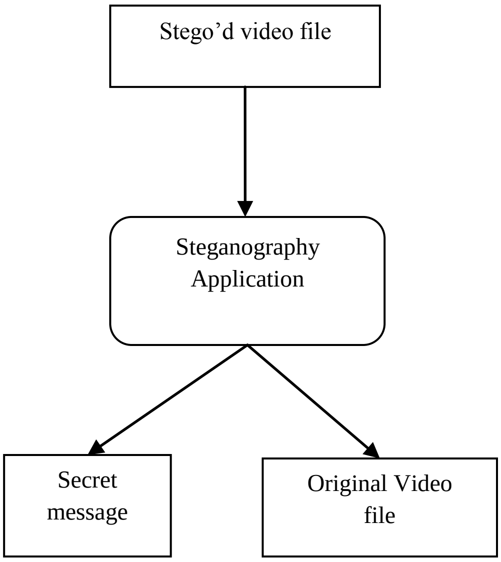

Fig 2: Retrieving original data from Stego'd video file.

3.1. Compression:

Procedure for compressing the secret message

Step1: Read the original file.

Step2: Count the total number of words, alphabets, special characters and digits in the file.
Step3: Find out the repeated words in the file.
Step4: Prepare the words dictionary for the original file context.
Step5: Create compress file, in the compressed file place the words number instead, of actual words.
Step6: Add the dictionary to the compressed file.
Step7: Save the compressed file along With the Dictionary. For compression technique Lempel-Ziv algorithm was used.

Steps for encoding algorithm.

3.1.1. Encoding Algorithm

```
Step1: Initialize dictionary to contain one entry for each byte. Initialize the encoded string with the first byte of the input stream.
Step2: Read the next byte from the input stream.
Step3: If the byte is an EOF go to step 6.
Step4: If concatenating the byte to the encoded string produces a string that is in the dictionary:
    • Concatenate the byte to the encoded string
    • Go to step 2.
Step5: If concatenating the byte to the encoded string produces a string that is not in the dictionary:
    • Add the new sting to the dictionary.
    • Write the code for the encoded string to the output stream.
    • Set the encoded string equal to the new byte.
    • Go to step2.
Step6: Write out code for encoded string and exit.
```

3.1.2. Decoding Algorithm

Step 1: Initialize dictionary to contain one entry for each byte.
Step 2: Read the first code word from the input stream and write out the byte it encodes.
Step3: Read the next code word from the input stream.
Step 4: If the code word is an EOF exit.
Step 5: Write out the string encoded by the code word.
Step 6: Concatenate the first character in the new code word to the string produced by the previous code word and add the resulting string to the dictionary.
Step 7: Go to step 3.

3.2. Least Significant Bit Algorithm

The Least Significant Bit Algorithm is used to encode the secret message into the video file. It performs bit level manipulation to encode the secret message. The following steps are

Step1: Receive the video file in the form of bytes and convert bytes into bit pattern.

Step2: Each character in the secret message is converted into bit pattern.

Step3: Replace the LSB bit of video file with the secret message bit.

Step4: Repeat step3 until the completion of secret message bits.

3.3. Data Encryption Standard (DES)

DES is a symmetric block cipher, operating on blocks of 64 bits of data and a key of 64 bits. Deciphering is done with the same key but in reverse order. Only 56 bits of the key are used actually in the process. The remaining 8 bits are used for parity check, therefore can be discarded.

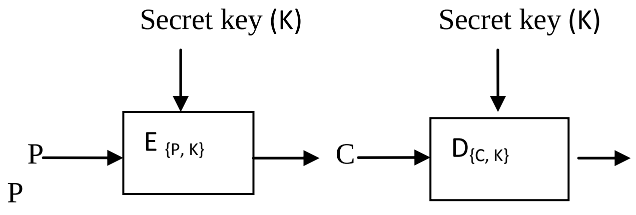

Fig 3: Encryption and decryption with DES

In the above diagram the terms

P=Plain text

C= Cipher text

K= Secret key

3.3.1 Encryption algorithm

The overall structure of encryption steps are as follows:

Step1: A block of 64 bits is permuted by an initial permutation called IP.

Step2: Resulting 64 bits are divided in two halves of 32 bits, left and right.

Step3: Right half goes through a function F(Feistel function).

Step4: Left half is XOR with output from F function above.

Step5: Left and right are swapped (except last round).

Step6: If last round, apply an inverse permutation IP-1 on both halves and that's the output else, go to step 3.

Steps 3 to 5 constitute a round. DES has 16 identical rounds. The two halves are processed alternately. This structure represents a Feistel network.

Feistel function F is represented by the following operations:

a. Key mixing – round key combined with 48 bits from previous step by XOR operation.
b. Expansion – 32 bits to 48 bits based on an expansion table.
c. Permutation based on a fixed permutation table.
d. Substitution – previous result divided into 8x6bits blocks before processed by s-boxes (substitution boxes).

3.3.2 Decryption Algorithm

The decryption process with DES is essentially the same as the encryption process and is as follows:

Step1: Use the cipher text as the input to the DES algorithm.

Step2: Use the keys Ki in reverse order. That is, use K16 on the first iteration, K15 on the second until K1 which is used on the 16th and last iteration.

3.4. Embedding data

In this the actual process of Steganography can be performing. The carrier file (video file) is converted into binary. The result is overwritten to the data part of the video file and as well as written into the newly created text file. For this system secret message, video file are inputs Stego'd video file is an output [1], the key file is shared by a secure channel.

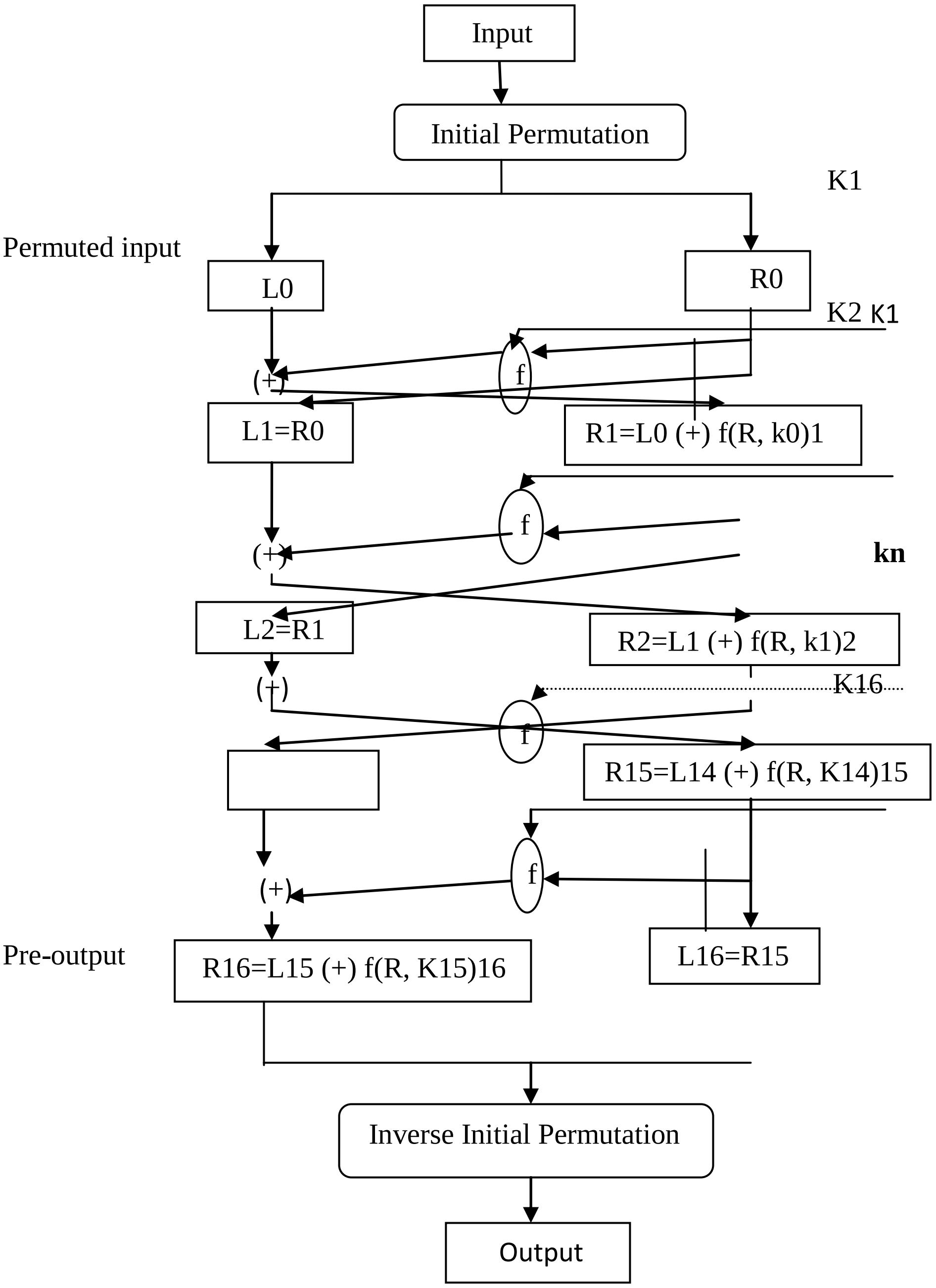

Fig 4: A Diagram of the Enciphering Computation

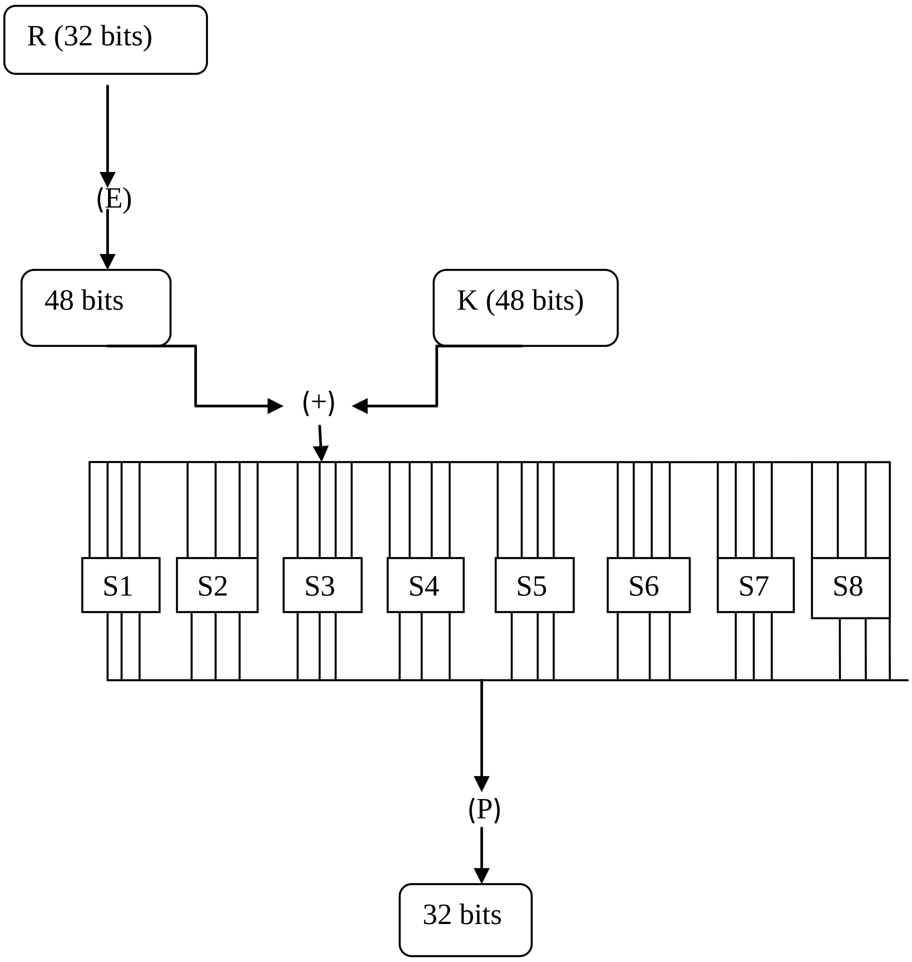

Fig 5: The DES algorithm of the complex F function.

3.5. De-embedding data

To retrieve the hidden message from Stego'd video file, decoding is done on the video file. Here the Stego'd video file is given as input [2]. In the video file to find the starting point of the data, the video and key files are opened in a Random Access Mode. The output for this is original video file and the secret message [2], which is hidden inside the video file.

4. Disadvantages of Existing System

- Existing model provides only embedding of text into audio.
- They do not provide user keys and have less security.
- Multi file embedding is not possible.
- No compression facility.

4.1 Advantages of Proposed System

The advantages of the proposed system are

- A very usable and good looking wizard based GUI (Graphical User Interface) for the system.
- Ability to operate the system with no prior training and consultation of any help files.
- Ability to conceal and reveal the exact hidden data from video file without disturbing the running application or new application.
- The LSB provides high security with user keys.
- It allows multi file embedding.
- Compression facility is provided.

5. EXPERIMENTAL RESULTS

When the system is executed (Graphical User Interface) is displayed. First select the secret message (Here secret message is a text message) then encrypt it with a secret key; this key can be created by the sender. Select the encrypted message and cover file (video file) to embed the encrypted message into video file. In the de-embed process select the embedded video file, click on de-embed button then the de-embed process completed. Select the de-embedded file decrypt it with the same key which was used in the encryption. Finally the original secret message can be displayed without any changes.

6. CONCLUSION

The proposed system developed an application which would be able to hide data into a video file that provides a robust and secure way of data transmission. This Stego system implements Steganography in video and reveals process without restarting the application or starting a different application. Also this system is a Platform-independent application with high portability and high Consistency. In the future secret message can be hiding inside the mobile images.

7. REFERENCES

[1] Melih Pazarci, Vadi Dipcin, Data Embedding in Scrambled Digital Video, in Proceedings of the 8th IEEE International Symposium on Computers and Communication, pp. 498-503, 2003.

[2] B. Chen and G.W. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding,” IEEE Trans. Information Theory,” vol. 47, no. 4, 2001, pp.1423–1443.

[3] Niles Proves and Peter Honey man, “Hide and Seek: An Introduction to Steganography”, University of Michigan, IEEE 2003.

[4] J. Fridrich and M. Goljan, “Practical Steganalysis—State of the Art,” Proc. SPIE Photonics Imaging 2002, Security and Watermarking of Multimedia Contents, vol. 4675, SPIE Press, 2002, pp.1–13.

[5] Aravind Kumar, Km. Pooja, “International Journal of Computer Applications”, Vol.9, No.7, November 2010, pp.19-23.

[6] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.

[7] Mobasseri, B. Direct sequence watermarking of digital video using mframes, Proc. International Conference on Image Processing, Chicago, IL, pp. 399- 403, 1988.

[8] J. J. Chae, B. S. Manjunath, “Data Hiding in Video”, *Proceedings of the 6th IEEE International Conference on Image Processing,*1999, pp.311-315.

[9] Katzenbeisser, S., &Petitcolas, F. A. 2000. Information hiding techniques for steganography and digital watermarking. pp. 43-78.

[10] Mamta Juneja, Provender S. Sandhu, and Ekta Walia,”Application of LSB Based Steganographic Technique for 8-bit Color Images”, WASET 2009.

[11] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn, “Information Hiding-A Survey”, *Proceeding of the IEEE,* vol. 87, no. 7, June 1999, pp.1062-1078.

8. AUTHORS BIOGRAPHY

K.V.Vinokumar did his B.Tech (INFORMATION TECHNOLOGY) from JNTUA , Andrapradesh in the year 2010. He is pursuing his M.Tech (CSE) in K.S.R.M College of Engineering, Kadapa from JNTUA Andrapradesh.

V. Lokeswara Reddy did his M.Tech (CSE) from SRM University, Chennai in the year 2005. He did his M.C.A from S.V. University, Tirupati in the year 2000. He is pursuing his Ph.D from JNTUA, Anantapur. He has a total of 11 years of experience in teaching. Currently he is working as Associate Professor at K.S.R.M College of Engineering, Kadapa. He has presented 5 papers in International, National Conferences and published 3 papers in International journals.