A Novel Privacy Preserving Tool for Hiding Sensitive Data in Digital Media Format

Manjeti Prashanthi Rani [#1], V.Lokeshwari Vinya[*2]

Department of Computer Science & Engineering,
Visakha Institute of Engineering & Technology,
57th Division, Narava, Visakhapatnam, AP (INDIA) - 530027.

Abstract

Today's large demand of internet applications requires 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 attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio, video or image files. In Steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists.

Keywords

Data Hiding Method, Information Hiding Process, Steganography, Watermarking, Embedding, De-Embedding.

1. Introduction

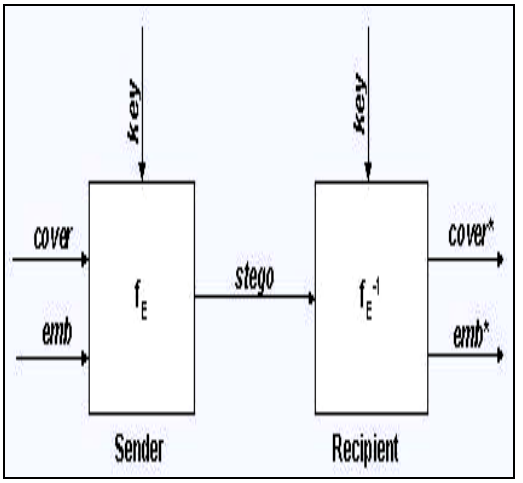
Throughout history Steganography has been used to secretly communicate information between people. In olden days there are some methods to pass information secretly, like

- Invisible ink
- Writing on shaved heads
- Microscopic images

Today's communication of valuable digital data (I.e. Image, Video, and Audio) through public or un-Secured channels have become a most critical problem in the society. This major problem is solved by using the new concept called steganography, which is the art and science of hiding valuable information into Master channels so as to conceal the information and prevent the detection of the hidden message. Steganography is also defined as hiding information [1] within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected by the un-authorized users. This new technique is mainly used by the Indian Government in the Military to establish relationship between more than two military commanders in a much secured manner without releasing or misusing any small part of embedded data **[2], [3], [4], [5], [6].**

1.1 Working Principle of Stegnographic System

We can clearly find the advantages of stegnography mechanism from the working principle diagram from the below figure .1, which clearly states the description about an embedded data either text/audio/video/image inside any digital media like audio/video/image type data, so as the data which is passed through the carrier file cant able to identify or open by any un-authorized users who wish to access the data. So in this paper we clearly explain the advantage of new novel stegnography concept under mixed category of how one type of digital media data is embedded within other type of digital data either of similar type or different type formats by giving password for the embedded data.



Where the function **f_E :** Which clearly denotes Stegnographic Function for embedding.

f_E^{-1}: Which clearly denotes stegnographic function for extracting of hidden data.

Cover File: This is the main source file in which the sensitive data will be hidden.

Emb Function: This is the important function In our process which indicates message to be hidden.

Key Function: Which is a new Parameter of f_E

Stego Function: This is a function which denotes the data that has both cover data with hidden data.

In this current paper, we are not following the primitive Cryptographic encryption and primitive cryptographic decryption techniques. We are introducing a new cryptographic algorithm called as Novel Bit Shift encryption in Random Cycle Order. I.e. totally 4 different types of Bit Shift algorithms are used randomly to encrypt the data like 4-Bit,6-Bit,12 Bit ,16 Bit Shift Encryption Algorithms. This Encryption is embedded into an Audio or Video File. Again it will be embedded into a media data. This new double embedding process increases the level of data security. Also the password protection for the data in this proposed work gives an additional security for this total application, if there was no password facility the user may lost the valuable data in the terms of intruders between data transmission.

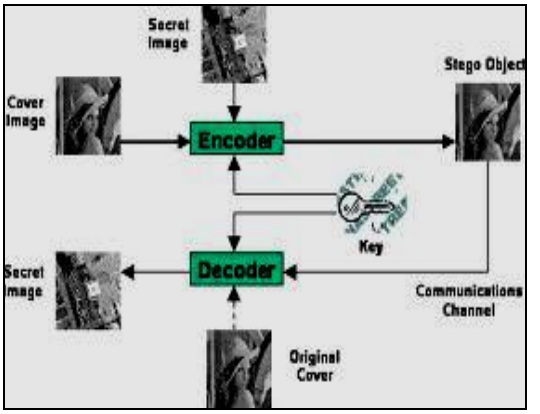


Figure. 1. Working Nature of Stegnography Mechanism

2. Background Theory

In this section, we will try to find some of the background work that was carried out in order to

prove the stegnography concept in detail by taking real time environment into consideration.

2.1 Applying Stegnography on text type of data

The development of the current Steganography is based on cryptographic features to the TEXT file data. Steganography is a Component suite that can be used as a component in any application to provide the security to the text file. Steganography provides several functions.

It will take the TEXT file and password as input and gives the Encrypted and embedded audio/video/image file as output.

It will take the password and embedded audio/video/image file as input and will give decrypted and original TEXT file.

Functional requirements for the promised text based security system are as follows:

Expected Inputs:

File details: Audio/Video/Image file

Text details: Input Text file or Text message

Here in the above file details we have mentioned the input file type as audio/video/image file where the input data can be of any type and the text details indicates the type of data that is used for hiding.as per the current survey we will take any type of text documents or .java files for hiding inside the file type.

Expected Outputs:

Audio/video/image details: Embedded audio/video/image

Text details: Original Text file or Text message

Storage Details:

Cipher text generated from plain text

Cipher text extracted from Audio/Video/Image file.

Generating cipher text: Using the DES algorithm the cipher text is generated.

Hiding the cipher text in audio/video/image: Using low bit encoding method the cipher text is kept hidden in the audio/video/image file.

2.2 Different Stegnography Techniques

In the recent days, the data hiding techniques are receiving more and more attention in its usage. The main motivation of several users attention for this new technique is largely due to fear of encryption services getting outlawed. There are several ways to hide information in digital images. We look at the following 3 important approaches:

A. Least Significant Bit Insertion(LSBI) Approach
B. Masking And Filtering Approach
C. Algorithms and Transformations Approach

Each of these Techniques has Varying Degrees of Success in comparison.

For Example

The Following example in figure 3 clearly represents the stegnography of image which hides the valuable sensitive information internally with representing in the form of a matrix. As the stegno image is converted in the form of matrix, this was represented with two notation like zero's and’one’s.Where zero’s represent there was no matching found on the image and one’s represent there was a matching internally.

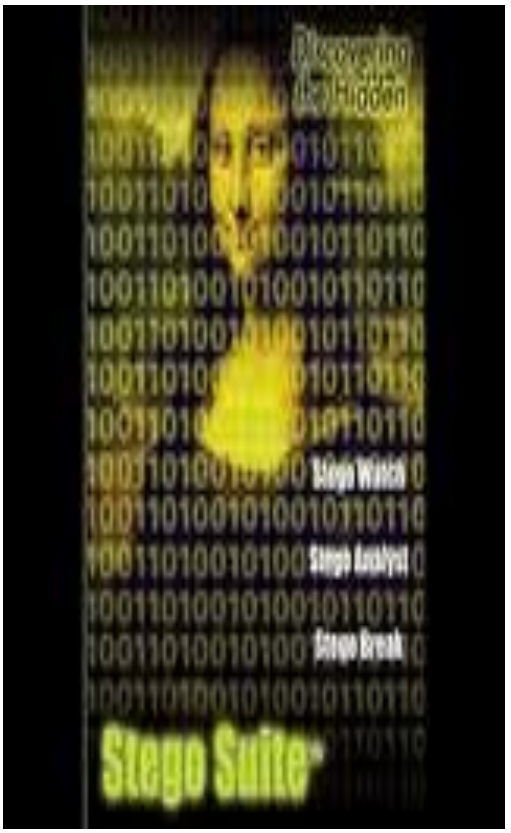
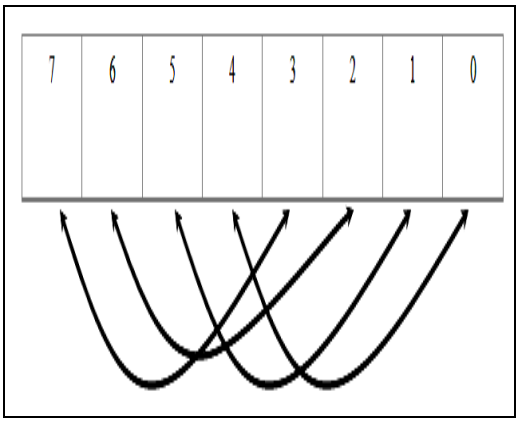


Figure 3. Representing Image Stegnography for Hiding Sensitive Information

2.3 Bit Shift Transformations Approach

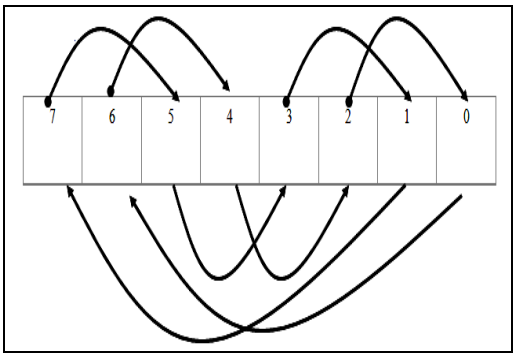
This was the second steganographic technique which was used in order to give more security for the data by applying bit shift operation. There are several types of Bit Shift Operations like 2-Shift, 4-Shift, and 6-Shift and so on. We apply four Bit-Shift operations in the current application in order to give more security by applying these transformation techniques.

Bit Position



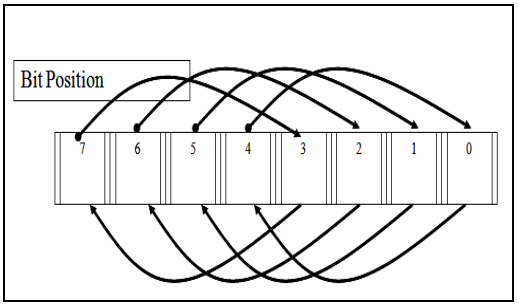
Shift Algorithm – 4 Shift

The above is the 4 Bit transformation approach which is used for shifting 4 bit positions from left to right, starts from the middle bit position.

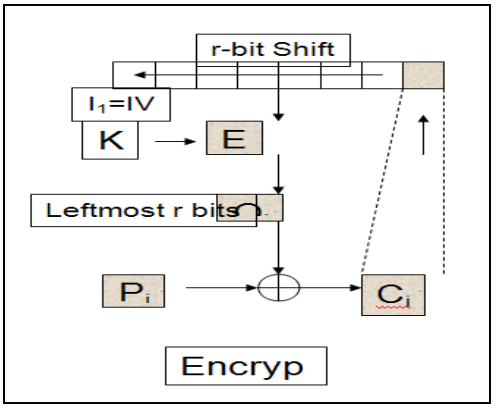


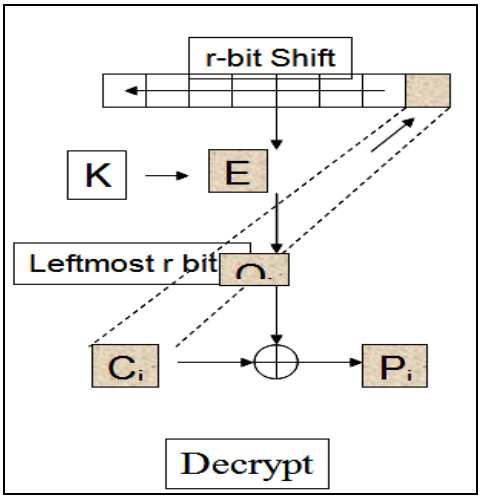
Shift Algorithm – 6 Shifts

The above Bit Position clearly indicates it is an 8 bit string with change of 6 bit positions from left to right side. In the same way we can do continue with remaining other bit positions like 12 and 16 bit positions.



Bit Shifting – Encrypt & Decrypt





3. Project Implementation Modules

We have implemented our application in Java technology with Java Swings as front end user interfaces. We used no back end data base for this application because there was no data storage or data retrieval needed for this application as it can able to select or browse data from anywhere of entire desktop. The application is divided into following four modules. With the help of these four modules we are able to provide highest security for the hidden data over transmission channel. They are as follows:

1. Embedding a Text Message inside a Digital Data:

In this module, the sender can hide a plain text message inside a **.wmv** video format file or other form of digital data file like video/audio/images in order to hide valuable message. The file which is hidden with secret message is called as a carrier file which will be transferred to the receiver through any form of media. We also give security for that hidden carrier file containing message with a password by encrypting the message with a key that was generated by using DES algorithm with 64-Bit Key Encryption and Decryption.

2. Embedding a data file(I.e Audio/Video/Image) inside a Digital Data (I.e. Audio/Video/Image) :

In this module, the sender can hide a data file like video/audio/images inside a any form of digital data file like video/audio/images in order to hide valuable data file. The file which is hidden with secret data is called as a carrier file which will be transferred to the receiver through any form of media. We also give security for that hidden carrier file containing message with a password by encrypting the message with a key that was generated by using DES algorithm with 64-Bit Key Encryption and Decryption.

3. Retrieving Message from Carrier File:

Here in this module, retrieving message from a carrier file is done by the receiver. The Receiver after receiving the carrier file into his system, he will use the same tool for retrieving the hidden message from the carrier file. Initially when he uploads the carrier file in the stegnography tool, he will be check whether compression and encryption have been used and the compression ratio if compression has been used. It also shows you the request you have made. So after all these, the receiver should substitute the valid password what that is used by the sender in order for retrieving that hidden data file.

4. Retrieving Data File from Carrier File.

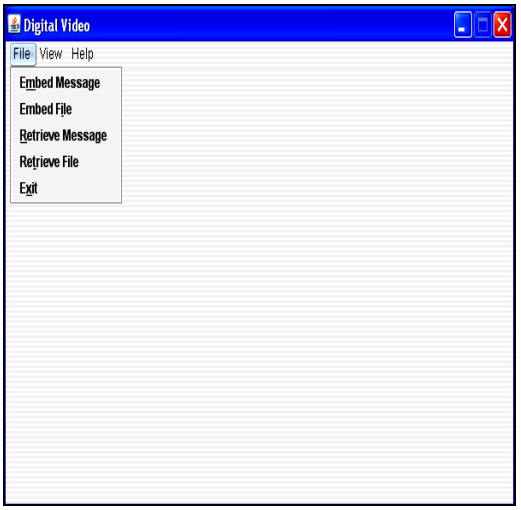
Retrieving file from a Carrier file is done by the receiver. The Receiver after receiving the carrier file into his system, he will use the same tool for retrieving the hidden data file from the carrier file. Initially when he uploads the carrier file in the stegnography tool, he will be check whether compression and encryption have been used and the compression ratio if compression has been used. It also shows you the request you have made. So after all these, the receiver should substitute the valid password what that is used by the sender in order for retrieving that hidden data file.

4. Experimental Results

The below window is the starting window or home window for our proposed project.

Stegnography Main Window

In this window we have a facility of embedding a message as well as embedding a data file for giving security as well as retrieving a Message/data file for getting the hidden data. This was the main interface that was designed by suing java Swings Technology as front end User Interface.



5. Conclusion

In this paper, we mainly concentrated on the transmission of sensitive valuable information to different location user with the help of stegnography mechanism like hiding valuable data of any type into any type format like audio, video, image. If one were able to hide the message in the video file in such a way, that there would be no perceivable changes in the audio file after the message insertion. At the same time, if the message that is to be hidden were encrypted, the level of security would be raised to quite a satisfactory level.

6. References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[2] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F.

Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[3] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[4] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[5] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.

[6] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[7] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.

7. About the Authors

Manjeti Prashanthi Rani is currently pursuing her 2 Years M.Tech (CSE) in Computer Science and Engineering at Visakha Institute of Engineering & Technology, Narava, Visakhapatnam. Her area of interests includes Information Security. Her mail id is prashanthi.manjeti@gmail.com

V.Lokeshwari Vinya is currently working as Assistant Professor, in Computer Science and Engineering at Visakha Institute of Engineering & Technology, Narava, Visakhapatnam. Her research interests include Networks, Information Security. Her mail id is vinya593@gmail.com

