Mixed Stegnography: A New Privacy Protection Software for Hiding Valuable Data from Digital Media

Arasada Praveen Kumar[#1], Challapalli Sai Madhuri [#2], J. Santoshi Kumari[*3]

[#1]B.Tech Student, [#2] B.Tech Student, [*3] Assistant Professor

Department of Computer Science & Engineering,
VITS college of Engineering, Sontyam, Visakhapatnam,
Visakha District , AP, India.

Abstract

We consider stegnography as a new method of providing security for secret/sensible communication. While transferring a file from one point to another through Intranet and Internet, we need more file secure concepts. As we know that ordinary file encryption and decryption concepts, which are readily available in java examples are easily captured by middle way (I.e. During transmission) itself. So we need more security combination for sending the digital form of data. This paper helps to analyze how to send a file from one place to another in a secured manner. Firstly the target file is encrypted using our own algorithm called Bit Shifting and it is embedded into an audio or video or any media file. The resultant file will be protected by a password. This resultant media file is no change in its original format and it can be run in the player, we can't find any encrypted data inside it. This format will be sent through Internet or through any form of wired communication networks. In the destination point it will be retrieved only by our software and giving the relevant password. So it is highly secured.

Keywords

Data Hiding, Information Hiding, Stegnography, Watermarking, Embedding, De-Embedding.

1. Introduction

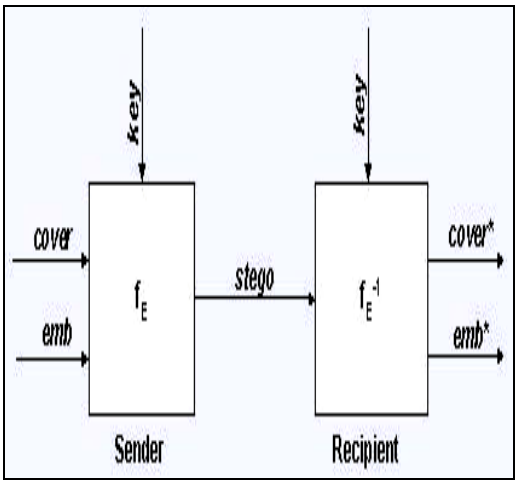
Today's communication of valuable digital data (I.e. Image, Video, and Audio) through public or un-Secured channels have become a most critical problem in the society. This major problem is solved by using the new concept called steganography, which is the art and science of hiding valuable information into Master channels so as to conceal the information and prevent the detection of the hidden message. Steganography is also defined as hiding information within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected [1] by the un-authorized users.

According to greek literature ,steganography is also known as "covered writing method", a branch which deals mainly with only two methods like Embedding and De-Embedding of original valuable content within a Cover file like image, video, or audio. 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 Stegnographic System

We can clearly find the advantages of stegnography mechanism from the below figure .1, which clearly states the explanation of stegnography

method used for embedding an image within an image, the same principle is used for embedding audio and video also within same type of formats or different type of formats like audio in image, image in audio, video in image, image in video, image in image, video in video, audio in audio and so on. So in this paper we clearly explain the advantage of mixed stegnography of how one type of digital media data is embedded with other type of digital data by giving password for the embedded data.



Where $\mathbf{f_E}$ **:** Which clearly denotes Stegnographic Function for embedding.

$\mathbf{f_E^{-1}}$: Which clearly denotes stegnographic function for extracting.

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

Emb: This is the function which indicates message to be hidden.

Key: Parameter of f_E

Stego: This is a function which denotes cover data with hidden data.

In this paper, we are not following the regular Cryptographic encryption and regular cryptographic decryption techniques. We are introducing a new algorithm called 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 double embedding is increase the level of security. Password Protection of this entire works 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.

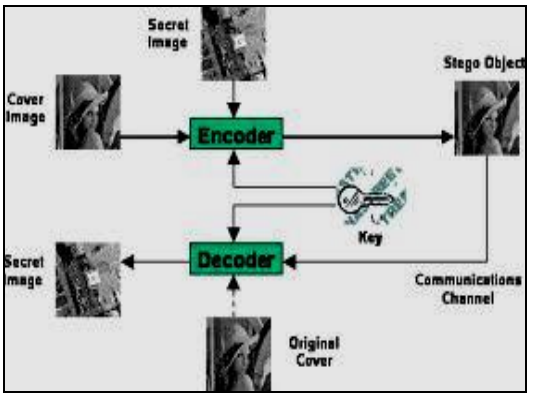


Figure. 1. Block diagram of Stegnography Mechanism

2. Related Work

In this section, we will try to find some of the related data regarding stegnography which was practically used in the real time applications.

2.1 Graphical Version of the Stegnographic System

The graphical version of the stegnography system is clearly represented in figure 2, where the stegnographic messages must be first encrypted and then it is hidden inside a master file, which results

in forming the stegno text. Only those who know the exact technique which was used by the sender can recover the message and, if required, decrypt it.

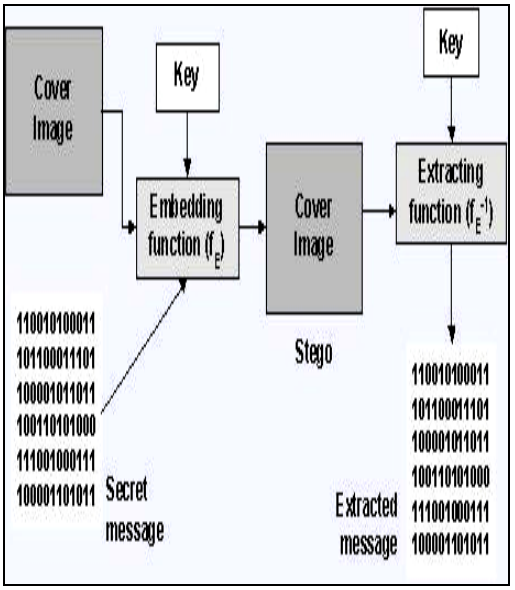


Figure. 2. Represents Graphical Version of the Stegnographic System

Digital images are commonly stored in either 24-bit or 8-bit files. For Example if an 8-bit image is viewed as a grid (I.e. Grid is nothing but representing of data in rows and columns as a tabular matrix), these cells are called as pixels. Each pixel consists of an 8-bit binary number (or a single byte), and each 8-bit binary number refers to the color palette (a set of colors defined within the image). All color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by 1 byte (= 8 bits).

2.2 Stegnography Techniques

Now a day's the data hiding techniques are receiving more and more attention. The main motivation 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
B. Masking And Filtering
C. Algorithms and Transformations

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

For Example

The below represented figure is a Embedded Image where we embedded show how the image is taken into matrix form with all Zero's and One's.

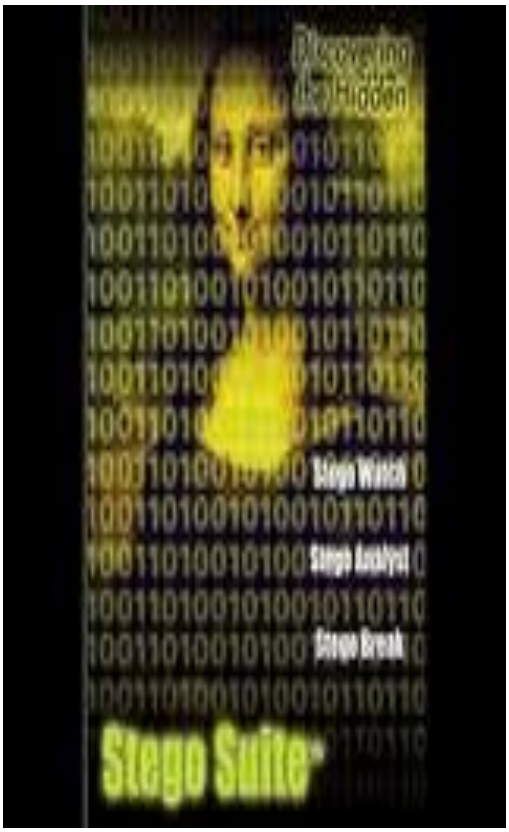
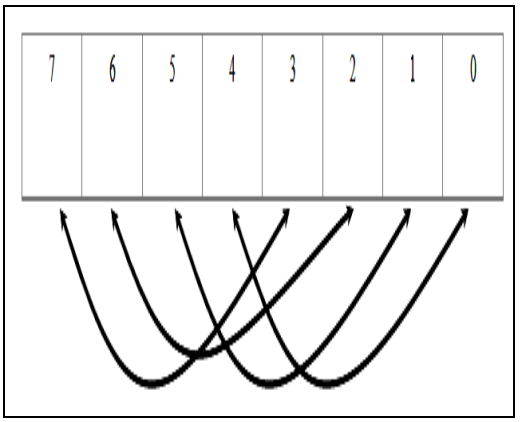


Figure 3. Stegno Image for Data Hiding

2.3 Shift Transformations

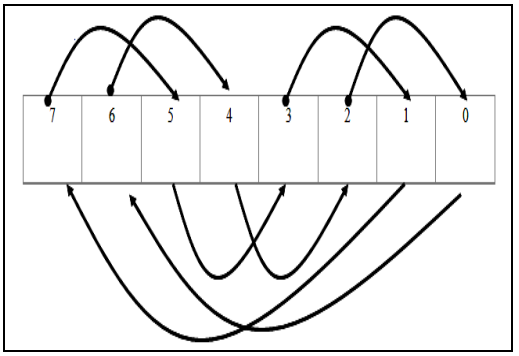
The following are the bit shift operations that are used in our present paper. They are as follows

Bit Position



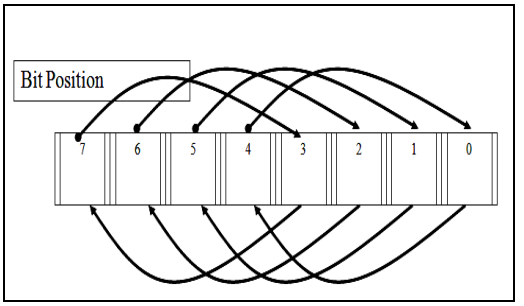
Shift Algorithm – 4 Shift

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

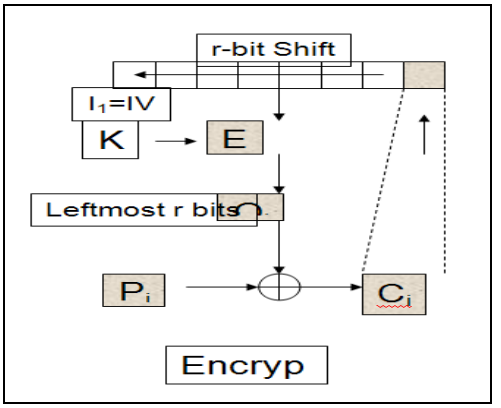


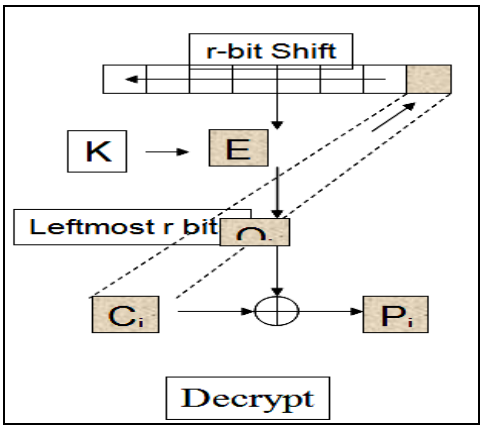
Shift Algorithm – 6 Shift

The above Bit Position clearly indicates it is a 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

As our application is implemented in Java as the chosen technology with Java Swings as front end user interfaces. In this application we are not using any data base as back end for storing the output file or any form of hidden data. The following paper is divided into following four modules. With the help of these four modules we are able to provide security for the hidden data over transmission channel. They are as follows:

1. **Embedding a Message in any Form of Digital Data:**

Here in this module, we will embed a plain text message inside a .wmv format video file or any form of digital data file in order to hide valuable message like audio/image/video. We also give security for that hidden master file containing message with a password by encrypting the message with a key.

2. **Embedding a data file within any form of digital data:**

Here in this module, we will embed a data file containing valuable data inside a .wmv format video file or any form of digital data file in order to hide that sensible data like image/audio/video .We also give security for that hidden master file containing sensible with a password by encrypting that data file with a key.

3. **Retrieving Message from hidden Master File:**

Here in this module, retrieving message from a Master file: 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. If the message is encrypted and decrypted by the same password only.

4. **Retrieving Data File from Hidden Master File.**

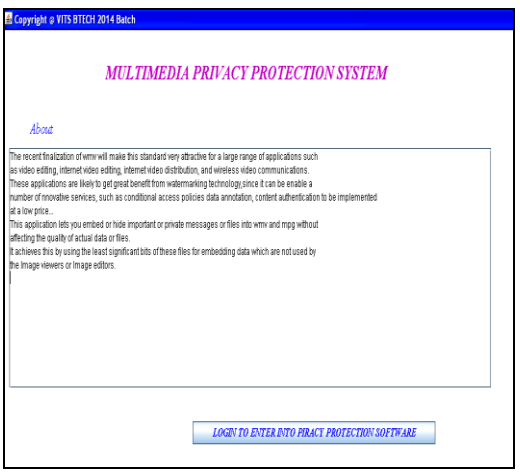
Retrieving file from a Master file: check whether compression and encryption have been used and the compression ratio if compression has been used. It also shows you the request you have made. If the message is encrypted and decrypted by the same password only

4. Experimental Results

In this paper, we have mainly sender who want to embed the valuable hidden data onto a cover page and wants to transmit over communication channel, for this the window we created in java looks like below

The below window is the starting window or home window for our proposed project. In this window we will tell the project abstract in detail in the text area that is present in that main window. If the user who wishes to participate in stegnography process, he should click on submit button so that he can be enter into the home page, if not he will not be directed to stegnography page.

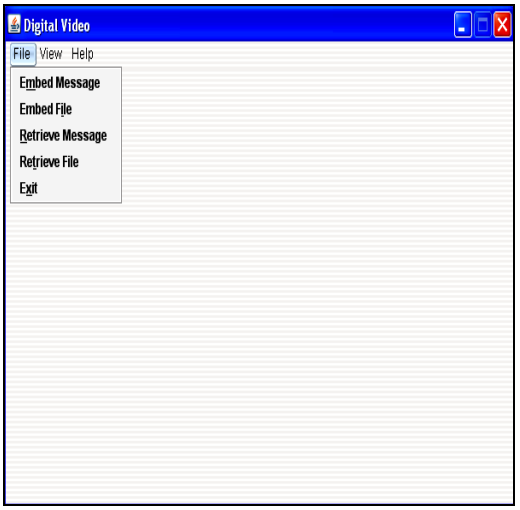
Main Frame



Once after we click on login button the following Stegnography window will displays in which we have facility of embedding message, embedding a file.

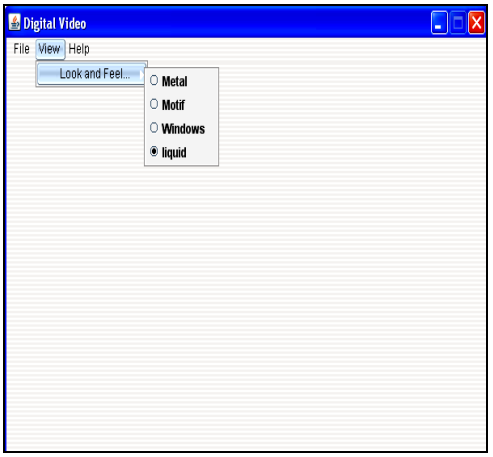
Stegnography Main Window

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.



Look and Feel Design Window

In this application we have Look and Feel options for changing the default window appearance as the user wish .This is available in the view menu with various look and Feel options.



Exit Window

This window is mainly designed in order to ask confirmation whenever any user who wish to close the current process. If the user clicks on yes option then window gets closed otherwise it will be in same stegnography window.

5. Conclusion

In this paper, we mainly targeted on the problem of hiding sensitive valuable information into any digital form of data 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. Now that this ancient art and science has been applied to modern communications systems, it has become a very effective form of sending imperceptible messages.

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

Arasada Praveen Kumar is currently pursuing his B.Tech in Dept of Computer Science & Engineering, VITS College of engineering, Visakha District. His area of interests includes Networks and Research of Interests (R&D).

Challapalli Sai Madhuri is currently pursuing her B.Tech in Dept of Computer Science & Engineering, VITS College of Engineering, Visakha District .Her area of interests includes Networks and Research of Interests (R&D).

J. Santoshi Kumari received her M.Tech degree in Computer Science & Engineering from St.Theresa College of Engineering, A.P, India. Currently she is working as an Assistant Professor in Computer Science & Engineering, VITS College of Engineering, Visakha District. Her research interests include Networks, Mobile Computing and Wireless Networks.