Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Smart Data Encryption And Transfer : Steganographic tool for hiding data A JAVA based open source application program

K. Jayamalini[1], Shashank Dubey[2], Ashish Singh[3], Geetesh Tiwari[4], Gaurav Singh[5]
[1,2,3,4,5]*Dept. of Computer Engineering, Shree L.R.Tiwari College of Engineering*

Abstract— Steganography [1] is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique [2] is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In the proposed LSB technique the last two bits of each image byte are replaced with the bits of encrypted form of data that has to be hidden in the cover image.

Keywords- Steganography, LSB, Random-key, Image, secret message, stego-key, cover image, Techniques.

I. INTRODUCTION

The word steganography is derived from the Greek words stages meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the [3] art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data.

Watermarking and fingerprinting related to [4] steganography are basically used for intellectual property protection. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups.

II. REVIEW OF LITERATURE

2.1 PRESENT SCENARIO

The majority of [2] today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia _les and also at the network packet level.

Hiding information into a medium requires following elements

1. The cover medium(C) that will hold the secret message.
2. The secret message (M), may be plain text, digital image file or any type of data.
3. The stegonographic techniques
4. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into four types:

2.1.1 Text steganography:

Hiding information in text file is the most common method of steganography. The method was to hide a [3] secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

2.1.2 Image steganography:

Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm Contents 4 using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message.

2.1.3 Audio steganography:

Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for [7] transmitting vital information to intend sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound. This property allows selecting the channel in which to hide information. Existing audio steganography software can embed messages in WAV and MP3 sound _les. The list of methods that are commonly used for audio steganography are listed and discussed below.

- ✓ LSB coding
- ✓ Parity coding
- ✓ Phase coding
- ✓ Spread spectrum
- ✓ Echo hiding

2.1.4 Video steganography:

Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.

2.2 Existing System

2.2.1 QuickStego:

QuickStego is free steganography software available for Windows. It lets you hide your text in pictures and only users of QuickStego can read this hidden text messages. You can add text by typing or load it from TXT file. Supported input image formats are: BMP, JPG, JPEG, and GIF, but it saves [3] the output image in BMP format with hidden text in it. The interface of this software is simple and easy to understand. First of all use "Open Image" button to open image file and then type your secret text in the big text box. You can also load text from TXT file by clicking "Open Text" button and click "Hide Text" and then click "Save Image" button to save the final BMP file. To retrieve the hidden text; just open the BMP file containing hidden text with it.

2.2.2 OpenStego:

OpenStego is just 203 KB in size and is easy to use steganography application. You can attach any type of secret message file to cover files. Supported file types for cover are: BMP, GIF, JPEG, JPG, PNG, and WBMP. You can set the password also. After finishing you can save output stego file in PNG format. Similarly you can use this software to extract secret data from the above

output file by providing correct password. It is a java based, open source steganography software. You can run either BAT file or JAR file from the installed directory.

III. PROPOSED SYSTEM ARCHITECTURE

In smart data encryption and transfer we are replacing the last two bits if image file byte for hiding the secret message. We are also encrypting the data file prior to embedding process and sharing the stego file over LAN. The system will also work on audio and video files.

3.1 User Interface Module (Steganograph):

This module will basically provide the main form for accessing the functionality of the application. Since the application will be implemented in the form of MDI parent child property for user interface, this module will work as a parent form for other child forms.

3.2 Embed Module:

This module will basically provide the functionality of embedding the message and the text or data file in the image, audio, video files. It will also have a sub module named "Encrypt" which will be responsible for encrypting the message and the data file. The embed module will make the use of this encrypt module for encryption purpose. This module will handle the backend task for Embed File form.

3.3 Retrieve Module:

This module will basically provide the functionality of retrieving the message and the text or data file from the image, audio, video files. It will also have a sub module named "Decrypt" which will be responsible for decrypting the message and the data file. The retrieve module will make the use of this decrypt module for decryption purpose. This module will handle the backend task for Retrieve File form.

3.4 Sender Module:

This module will basically provide the functionality of sending the files from one machine to another machine. This module will make use of socket programming for sending the file to other machines. This module will also provide the user interface that is child form (Send File).

3.5 Receiver Module:

This module will basically provide the functionality of receiving the files coming from other machines. This module will also make the use of socket programming for receiving the files from other machines. This module will not have any user interface. It will be functioning in the background.

3.6 Help Module:

This module will be responsible for providing the Help to the application. It will be implemented using JAVA and HTML both. The form for this module will be designed in JAVA, whereas the content for the help will be designed using HTML.

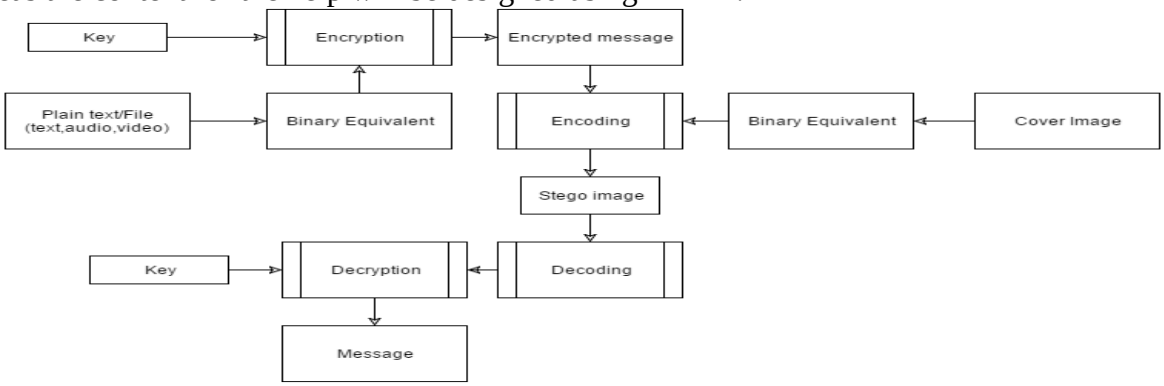

Fig 1: Block diagram of proposed architecture

IV . DEVELOPMENT AND METHODOLOGY

The development and methodology that has been undertaken for the development of smart data encryption and transfer is described below which gives an overview of the basic technology and their usage.

4.1 Selection of Technology:

The system planning also includes the selection of technology for the development of the modules and the application. The technology which will be used in this project is JAVA and HTML. The JAVA technology will be used for providing platform independency to the application and for doing the bit level calculations in the modules. The HTML technology would be used for the development of help modules which will be meant for providing to the application.

The application which we will be developing is a standalone application. This application, apart from providing data security communicates with other machines for file transfer. The machines which will be communicating might not have same platform. So the application needs to be platform independent. For embedding the files and the message the image, audio, video files need to be rendered at bit level. So a very secure technique is required for dealing at bit level.

4.2 System Development Model:

This project deals [1] with the secure transfer of data from one machine to another machine via LAN. The development of such software would really be complex task. It is more of a technical project. Although the requirements and the concepts of the project are clear at the initial stage but would require some advancement at the later stage. This advancement cannot be detected initially. So it would be better to develop those modules that are clear at the current stage. As the development proceeds the further features can be added into the system as per the requirement of the user. The project development also requires the coverage of technical risks.

Since the development of the system can be done and advanced features can be added at the regular interval of time, for this system *Incremental_model* is recommended. In incremental model, iterative development can be done i.e. system can be developed in number of phases. First that module is developed whose requirement is clear. If the user is satisfied [8] with that module then work is done on other iteration. Also incremental model helps us to cover risk for our project.

4.3 User Interface of Smart Data Encryption And Transfer

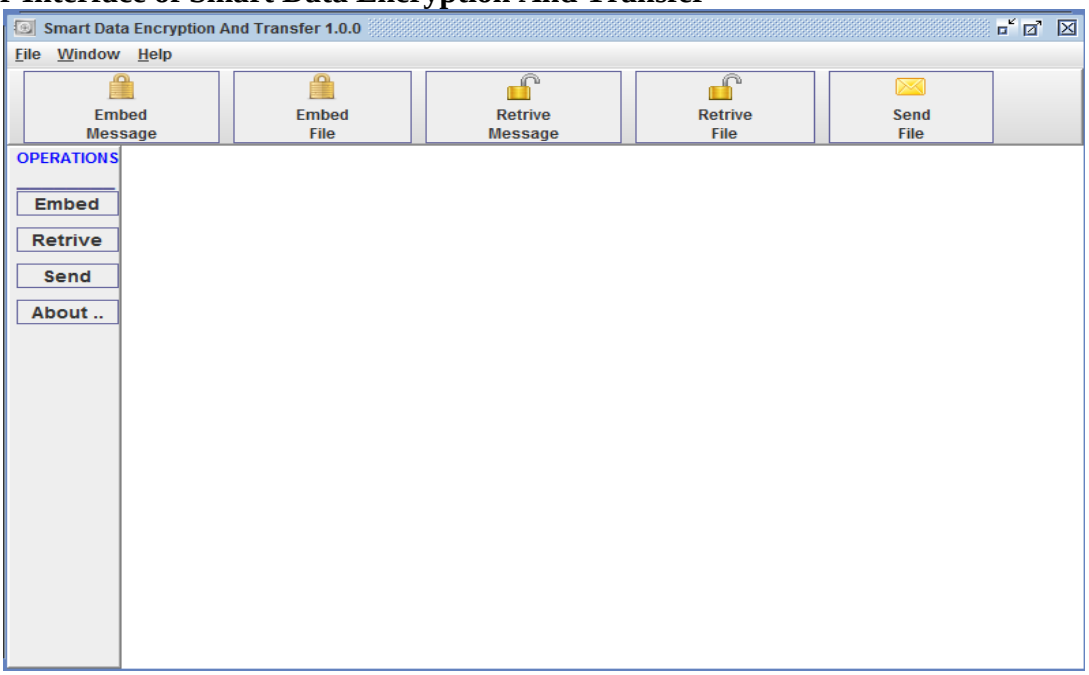

Fig 2: The User Interface

V. RESULTS

The features mentioned in the previous section can be observed in the screenshots taken from a Test run while testing the application and have successfully embedded the text behind the image file and have also encrypted the data before embedding it. We have provided two option in the application either select a text file to hide or type the string to be embedded behind the image file.

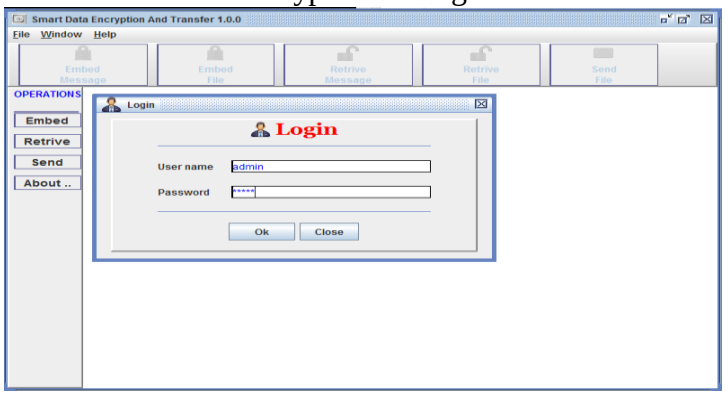

Fig 3: The first UI and the login page

Here is the home page of the application which include option to select a text file or enter the text in the text box. We have provided the check for file size while embedding the data in the image file that's shows the difference between initial image and final image. The content of the file can be seen in the text area provided for displaying the message

The below images depict the successful working of the embedding plain typed text and retrieving of the same.The embed and the retrieve module successfully perform the embedding and the retrieving operations.

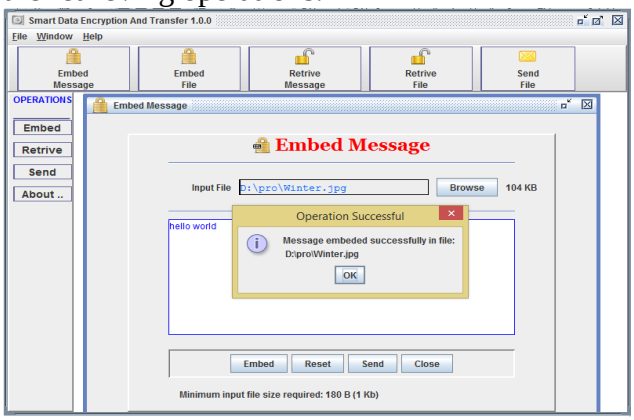

Fig 4: Embed message

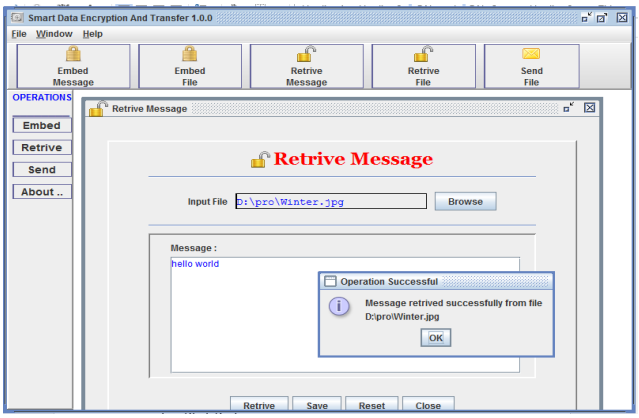

Fig 5: Retrieve message

The below images depict the successful working of the embedding plain typed text and retrieving of the same.The embed and the retrieve module successfully perform the embedding and the retrieving operations.

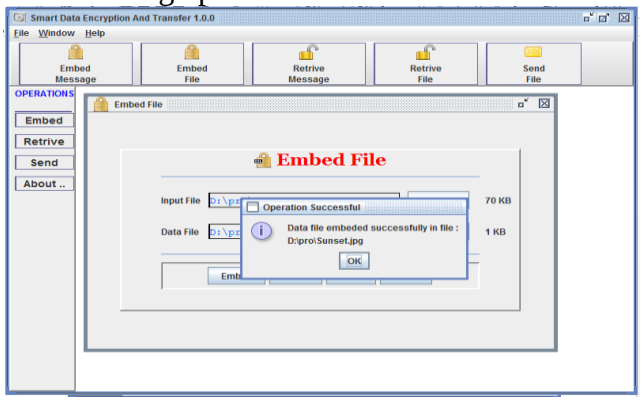

Fig 6: Embed file

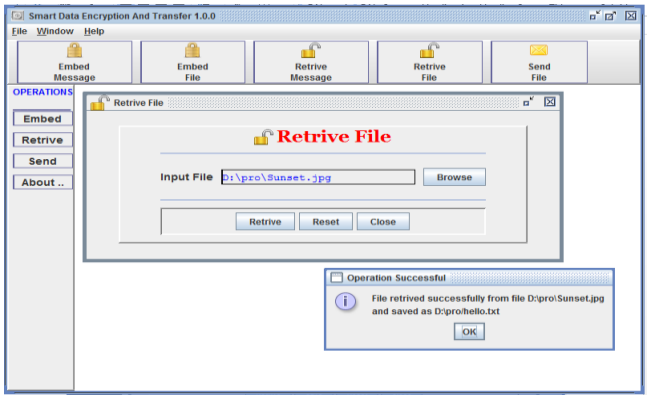

Fig 7: Retrieve file

We have also successfully transferred data from one pc to another using the IP address of the client pc. .

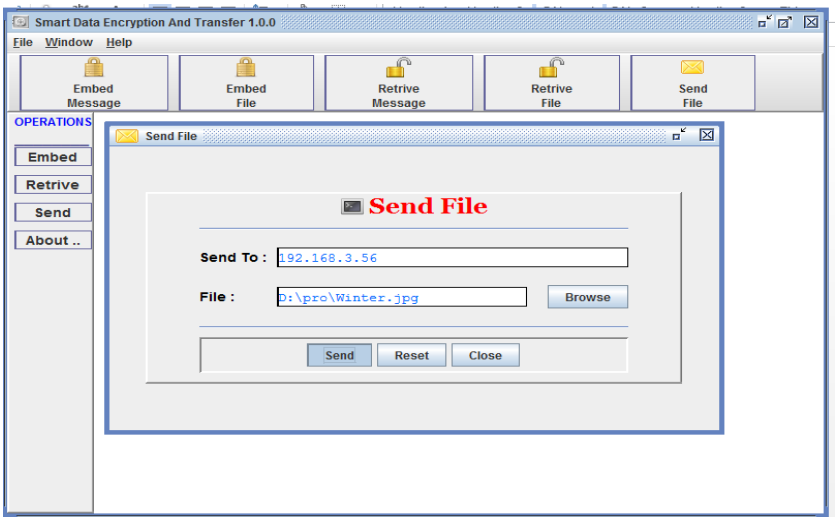

Fig 8: Sharing of stego-image

VI. CONCLUSION

Smart Data Encryption and Transfer is successfully able to fulfill the task of hiding piece of information behind a cover image. The data to be hidden is encrypted successfully using a random key. Smart data encryption and transfer easily embeds and retrieves data from a file or plain text. The stego image can be sent to another PC by entering the IP address of that PC. Smart data encryption and transfer is also able to work on the audio and video files in the same manner as it works on image files and is operational, satisfying the sole purpose of data hiding.

VII. FUTURE WORK

1. The application can have multiple login id and password.
2. Security will not lose by any mean.
3. The application can embed message in text file.
4. Not only text file but also any other file can be embedded in image, audio and video file.
5. The message can be transferred in intranet and in Internet environment.
6. The message can be transferred to any other device such as mobile.

REFERENCES

[1] https://en.wikipedia.org/wiki/Steganography (Accessed on Aug 2015)
[2] Krativyas , B.L.Pal “A Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique” IJARCCE Vol. 3, Issue 1, January 2014
[3] ParmarAjit Kumar Maganbhai , Prof. Krishna Chouhan “A Study and literature Review on Image Steganography” (IJCSIT) Vol. 6 (1) , 2015, 685-688
[4] T. Morkel,J.H.P. Eloff ,M.S. Olivier “An overview of image steganography” ICSA Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa
[5] http://www.programmer2programmer.net/live_projects/project_7/steganography.aspx(Accessed on Aug 2015)
[6] http://www.sans.org/reading-room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment-677 (Accessed on Aug 2015)
[7] Bankar Priyanka R, Katariya Rushabh R, Patil Komal, Shashikant Pingle, Sanghvi Mahesh “Audio Steganography Using LSB” 1st International Conference on Recent Trends in Engineering & Technology, Mar-2012.
[8] Kshetrimayum Jenita Devi “A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique” Department of Computer Science and Engineering National Institute of Technology Rourkela Rourkela-769 008, India. www.nitrkl.ac.in May 2013

