IMAGE STEGNOGRAPHY USING LSB TECHNIQUE

Abstract

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other forms of data. 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 exists a large variety of stenographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project intends to give an overview of image steganography, its uses and techniques. For a more secure approach, the project embeds the message using secret key and then sends it to the receiver. The receiver then decrypts the message to get the original one.

Introduction to the topic

Image steganography in a broad scale

Steganography derives from the Greek word ‘steganos’,meaning covered or secret, and graph (writing or drawing).On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper. Where cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first embedding a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of embed , steganography’s role is gaining prominence. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called ‘Steganalysis’ (Detecting use of Steganography.) Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

Where is the hidden data present?

With graphic images, you can remove redundant bits of color from the image and still produce a picture that looks intact to human eye and is difficult to discern from its original. It is in those bits that the program hides its data. A program uses an algorithm, to embed data in an image file, and a password scheme to allow you to retrieve information.
It is also worth noting that the image noises observed are Gaussian Noises as each pixel is being affected independently in its Least Significant Bit (LSB) to its core binary value.

What is Gaussian Noise?

Gaussian Noise in digital images arise due to acquisition. A typical model of image noise is Gaussian, additive, independent at each pixel, and independent of the signal intensity, caused primarily by Johnson–Nyquist noise (thermal noise), including that which comes from the reset noise of capacitors.

We can observe that at each pixel the value of the RGB is changed in the slightest by changing the LSB making the image that has the embedded image have Gaussian Noise.

Our aim in this project

1. Hiding the text message in an image file
2. The decoding of the message, decryption an source message retrieval are also supported

Objective

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings.

The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application area

This project has following objectives:

- To product security tool based on steganography techniques.
- To explore techniques of hiding data using embed module of this project
- To extract techniques of getting secret data using decryption module.

Steganography sometimes is used when embed is not permitted. Or, more commonly, steganography is used to supplement embed . An embedded file may still hide information using steganography, so even if the embedded file is deciphered, the hidden message is not seen.

Module Description

Home Module

This page will have the home display of the software and it will have the link to other modules also. Once the module is open it can then link to the database and retrieve the settings from the database. This module is also responsible to apply the settings on the other modules. This module will have only database reading capabilities and not writing.

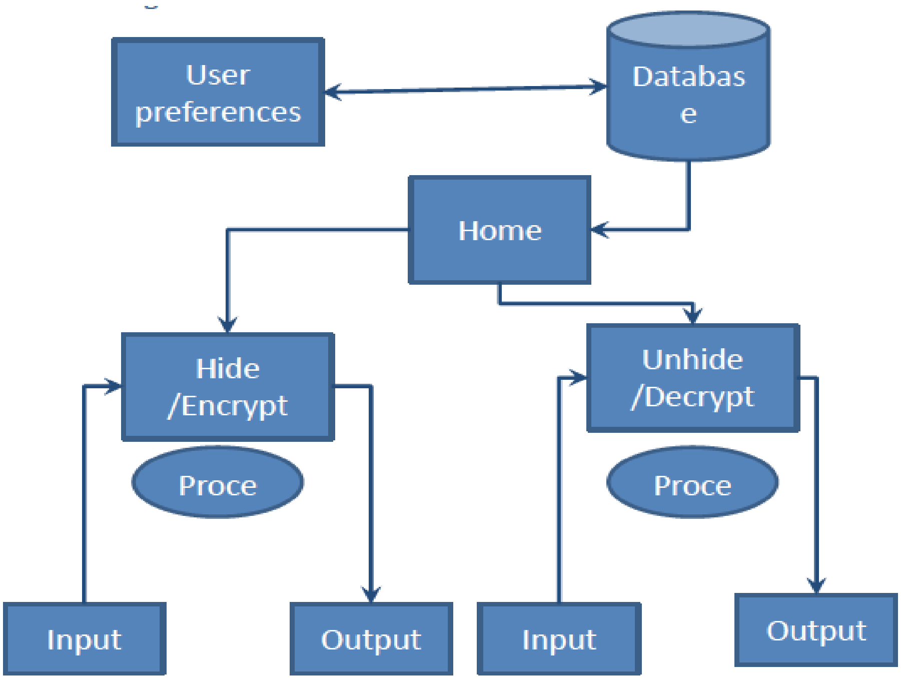
Hide and Embed data

CREATE A FILE USING TEXT EDITOR-: This module will be used to create a file that will contain the Plaint text with no formatting. Also the file created under this module will not be saved in the system and can and will only be saved as an Embedded (Visual embed) or will be concealed under an image file.

IMPORT FILE-: In this module we will be able to import a file from the computer and that will be concealed under an image file.

Unhide and Decrypt data

IMPORT FILE-: This module will have the ability to import file(s). It will be able to decrypt, Unhide the file from the image file and it will also be able to retrieve the message from the image files generated by the embed module using the Visual Cryptography.



Method of Data flow

Software Support and Applications Required

Operating System Required-:

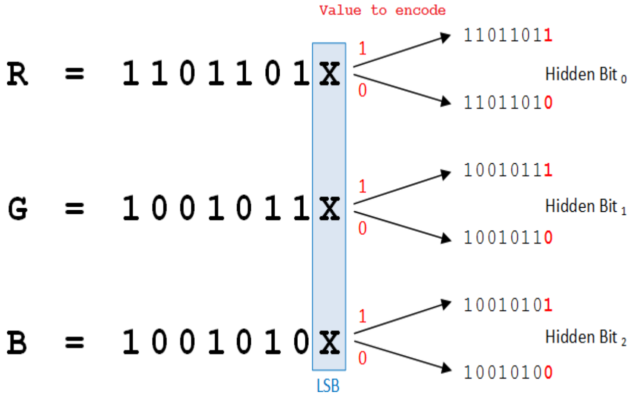
Windows or any Linux platform

JDK(1.7)-:The Java Development Kit (JDK) is an implementation of either one of the Java SE, Java EE or Java ME platforms released by Oracle Corporation

Swing-: Swing, which is an extension library to the AWT, includes new & improved components that enhance the look and functionality of GUIs. It employs model/view design architecture. Swing is more portable and more flexible than AWT. Swing is built on top of AWT and is entirely written in Java, using AWT's lightweight component support.

LSB algorithm used in the implementation of IS

Structure of image files is that an image is created from pixels that any pixel created from three colors (Red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is Most-Significant-Bit (MSB) and last bit Least-Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside pictures. So if we just use last layer (8st layer) of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have 3*height*width bits memory to write our information. But before writing our data we must write name of data(file), size of name of data & size of data. We can do this by assigning some first bits of memory (8st layer).



Implementation Of Image Steganography

1. **Technical details of Implementation**

   o Using java.awt.Image , ImageIO o The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

2. **Basic Encoding Algorithm**

   The steganography technique used is LSB coding.

   The offset of the image is retrieved from its header.

   That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process.

   For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.

   Creation of User Space:
   a. User Space is created for preserving the original file, so that all the modifications are done in the user space.
   b. In the object of Buffered Image, using ImageIO.readmethod we take the original image.
   c. Using createGraphics and drawRenderedImage method of Graphics class, we create our user space in BufferedImage object.

   The text file is taken as input and separated in stream of bytes.

   Now, each bit of these bytes is encoded in the LSB of each next pixel.

   And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using ImageIO.write method.

3. **Basic Decoding algorithm**

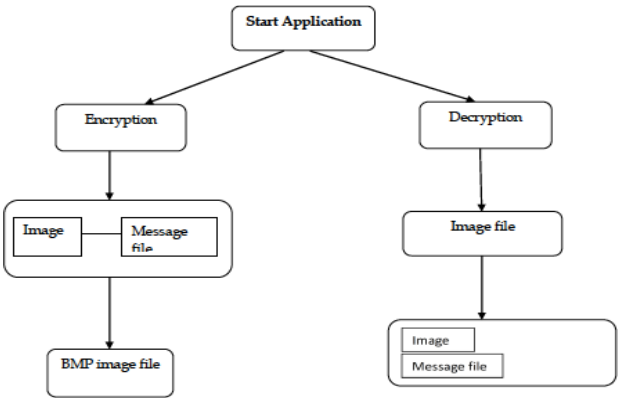
   The offset of the image is retrieved from its header.

   Create the user space using the same process as in the Encoding.

   Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes. The data of image is taken into byte array.

   Using above byte array, the bit stream of original text file, is retrieved into the another byte array.

   And above byte array is written into the decoded text file, which leads to the original message.



Diagramatic Representation of the process