LSB Image steganography

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

Abstract

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. 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 steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

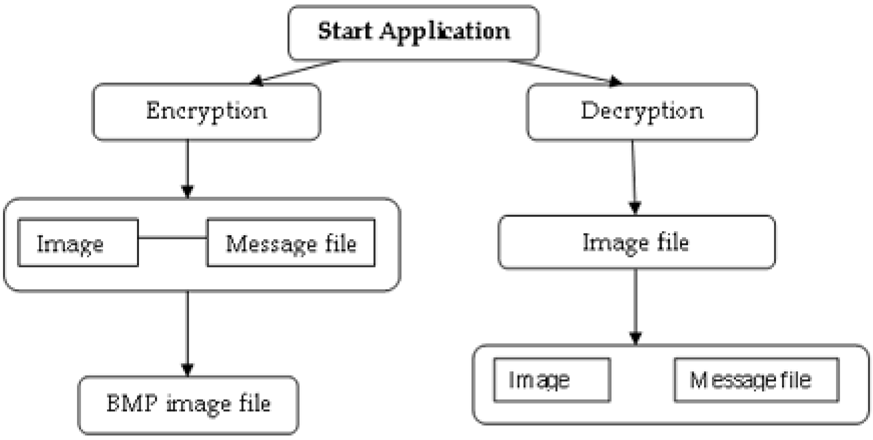
Project Scope

This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

Methodology

User needs to run the application. The user has two options – encrypt and decrypt.
If user select encrypt, application give the option to select image file, information file and option to save the image file.
If user select decrypt, application gives the option to select only stego image file and ask path where user want to save the secrete file.
This project has two methods – Encrypt and Decrypt.
In encryption the secret information is hidden in the bmp image file.
Decryption is getting the secret information from image file.

Graphical Representation
The graphical representation of Steganography system is as follows:



System Analysis & Design

Steganography system requires a BMP image file and the information or message that is to be hidden. It has two modules encrypt and decrypt. Project is implemented using C on linux platform (but it is platform independent).

The **encrypt module** is used to hide information into the image; no one can see that information or file. This module requires an BMP image and message and gives the only one image file in destination.

The **decrypt module** is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

Steganography in image

Think of all those pixels in an image and each pixel has three color numbers , there are zillions of numbers in an image. If you were to change a few of these color numbers the resulting picture would probably look a lot like the original image; in fact, most people probably couldn't tell that you had changed the image at all.
Steganography works by changing a few pixel color values; we will use selected pixel values to represent characters instead of a color value. Ofcourse, the resulting image will still look mostly like the original except that a few tiny ”blips” might seem a little out of place if you look very closely. We can then send the image to a buddy and they can extract the message if they know which pixels to decode.
Most famous algorithm is using changing LSB :

Note : pixel consist of 24 bit (3 bytes) the first byte for blue , second for green and the third for red

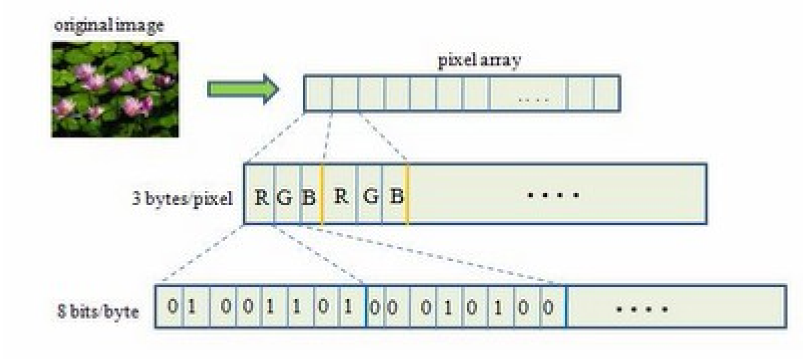
.

.

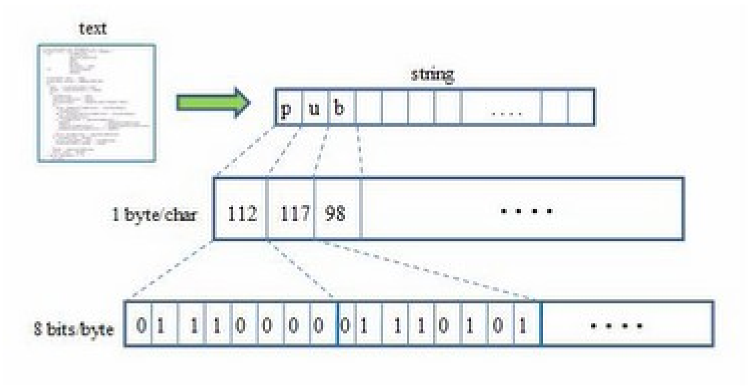
.

The original image

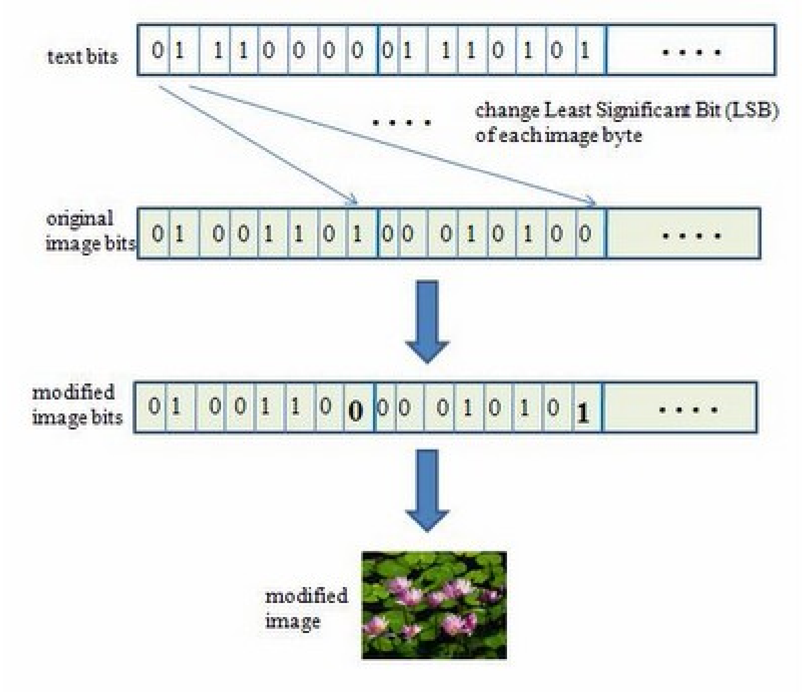
notice the LSB of each byte of image stream bytes.



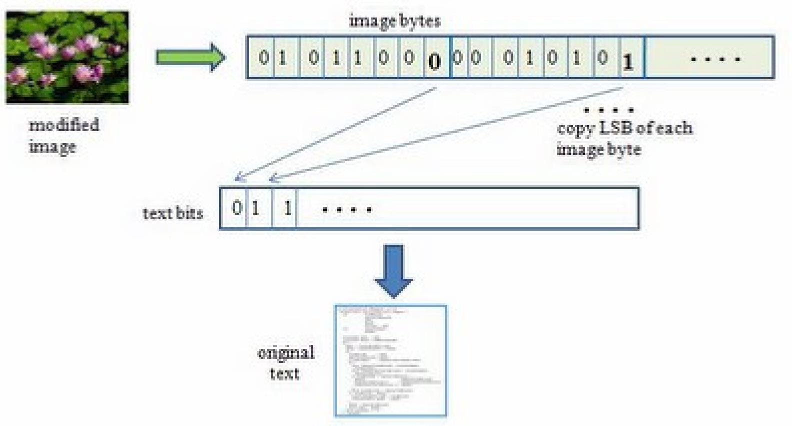
The text which will be hide in the image



Hiding text into image



To extract text from image



humans eyes may not notice the difference between two images