Project Report

STEGANOGRAPHY

COMPUTER NETWORK

in the supervision of teaching assistant

Shoeb Chikte

Group - 4

Kushal Jangid
Dilip Puri
Raghuvar Prajapati

April 20, 2015

Contents

Introduction 1
Steganography vs Cryptography 1
Types of Steganography 1
Text Steganography 1
Image Steganography 2
Spatial domain Techniques 2
Transform Domain Techniques 6
Audio Steganography 6
Challenges in Steganography 6
Conclusion 7

The Art of Hiding :

Stegano -graphy

(An Overview)

Abstract

Steganography is the art of hiding. In this art we hide some information in some other information. The fact that communication is taking place. 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 steganographic 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 report intended to give an overview of Steganography, its use sand techniques.

Introduction

Steganography is the are or practice of concealing a file, message, image, audio, or video withi another file message, image, audio or video.
The word **Steganography** combines the ancient GREEK words **STEGANOS** meaning *"covered, concealed, or protected"* and **GRAPHEIN** meaning *"writing"*.

The information to be hidden is embedded into the cover object which can be a text matter, some image, or some audio or video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resulted object exactly same as the original. The main goal of steganography is to hide the fact that the message is present in the transmission medium.

Steganography vs Cryptography

Cryptography is the science of encrypting data in such a way that one cannot understand the encrypted message, whereas in Steganography the mere existence of data is concealed, such that even its presence cannot be noticed. Using Cryptography might raise some suspicion whereas in Steganography the existence of secret message is invisible and thus not known. We can think of Steganography as an extension of Cryptography, and it is commonly used under the circumstances where encryption is not allowed.

Types of Steganography

On the basis of cover object steganography may be of many types like Audio Steganography, Video Steganography, image Steganography etc. Image Steganography is very popular because of popularity of digital image transmission over the internet.

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography

Text Steganography

Text Steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts. **Text steganography is believed to be the trickiest due to deficiency of redundant information which is present in image, audio or a video file.** The structure of text documents is identical with what we observe, while in other types of documents such as in picture, the structure of document

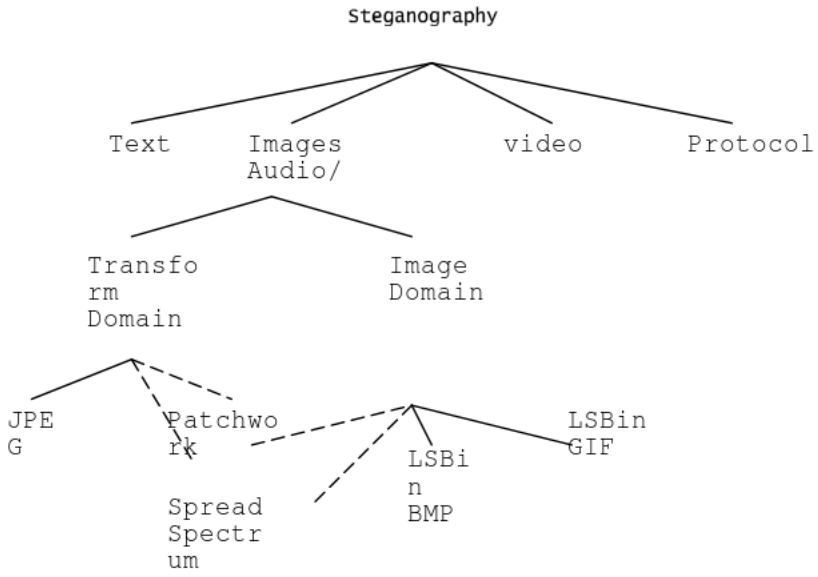


Figure 1: categories of image stegonography

Figure 1: Steganography

is different from what we observe. Therefore, in such documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output. Unperceivable changes can be made to an image or an audio file, but, in text files, even an additional letter or punctuation can be marked by a casual reader. Storing text file require less memory and its faster as well as easier communication makes it preferable to other types of steganographic methods.

Image Steganography

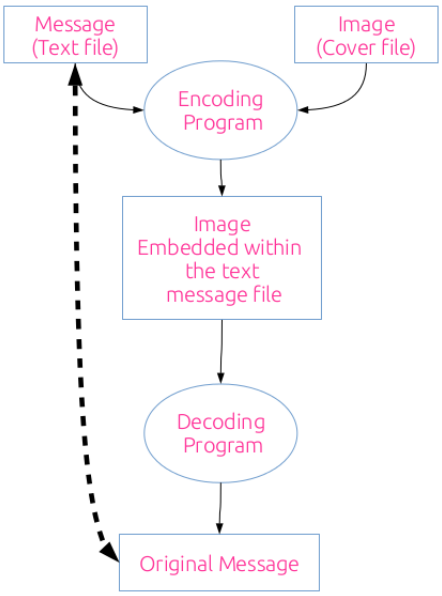
Image Steganography use redundancy of digital image to hide the secret data. It may be divided into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain, the secret messages are embedded in the image pixels directly. In the frequency-domain, however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed.

- Spatial domain Techniques
- Transform domain techniques

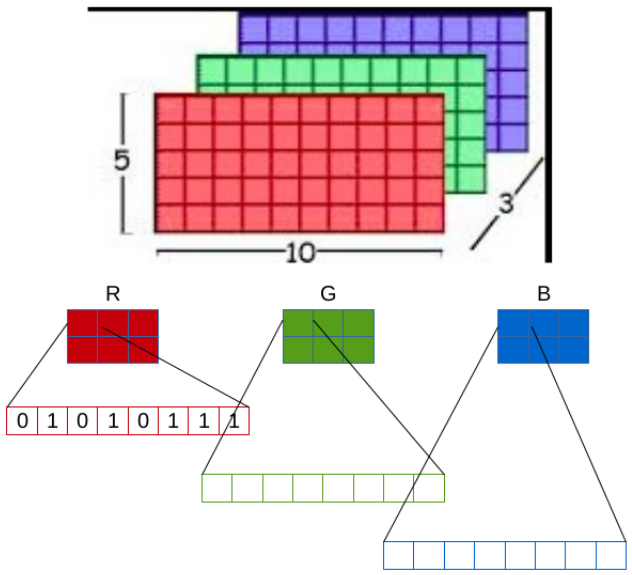
Spatial domain Techniques

- Least Significant Bits(LSB) substitution
- Distortion technique

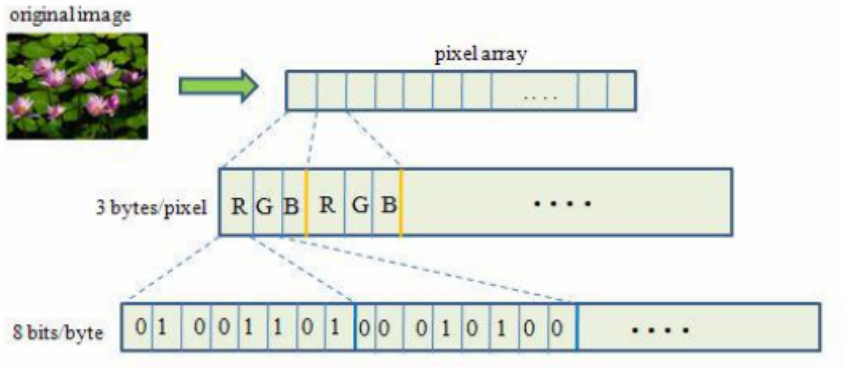
Least Significant Bit (LSB) substitution:- LSB is the most popular techniques of steganography. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy".
A simple approach for embedding information in cover image is using Least Significant Bits. The message directly embed into lsb plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitute of the change is small.
An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector.
The numeric represantation form a grid and the individual points are refered to as pixel.



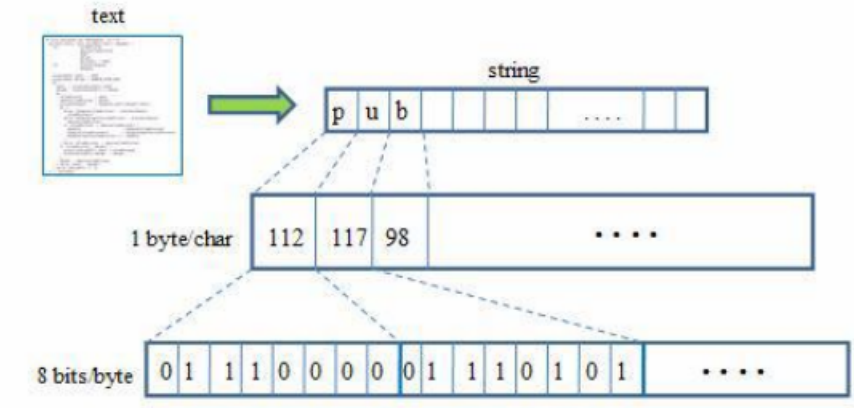
RGB representation of a pixel of an image- In digital image(raster form) 2-dimensional rectangular array of static data elements called pixels. In a pixel the three 8-bits parts red-R, blue-B,and green-G constitute 24-bits.



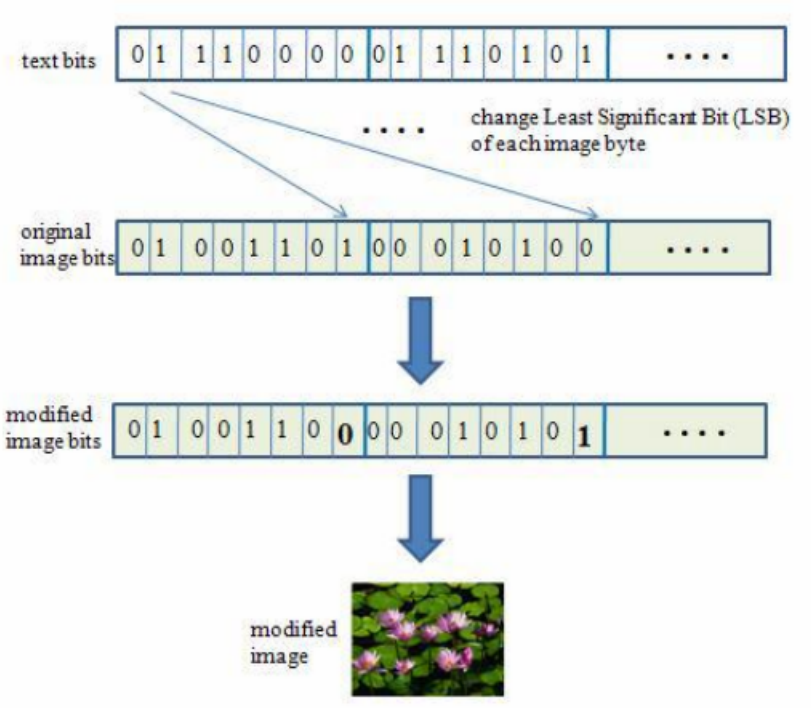
Step I^{st} Accessing the bits of an image file



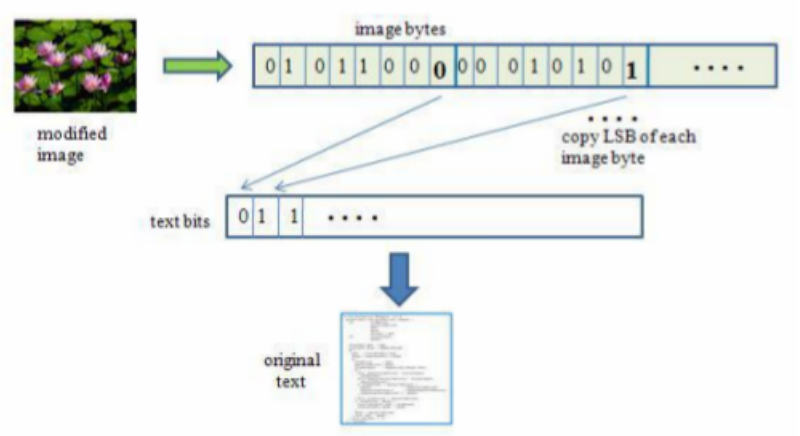
Step II^{nd} Accessing the bits of a text file



Step III^{rd} Embedding text with image



Step IV^{th} Extracting text from received image



Distortion Technique: In distortion technique some pixel property of cover image is changed according to secret message and then deflection of distorted from original image contains secret information.

Transform Domain Techniques

If we embed information in spatial domain, it may be subjected to the losses if the image undergoes any image processing technique like compression, cropping etc. To overcome this problem we embed the information in frequency domain such that the secret information is embedded on the significant frequency values while higher frequency part is omitted. We first apply transformations to the image then data is to be hidden by changing the values of the transformation coefficients accordingly.

Audio Steganography

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.
Basically, Message is the data that the sender wishes to remain it confidential.Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

Challenges in Steganography

The major challenges of effective steganography are:-

Security of Hidden Communication: In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically. Steganography techniques should produce high imperceptible Stego-image.

Size of Payload: Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a tradeoff has to be sought.

Robustness: Stego-image should provide robustness to image processing techniques like compression, cropping, resizing etc. i.e. when any of these techniques are performed on stego-image, secret information should not be destroyed completely.

There is no technique of steganography which provide all the three properties at high level. There is a trade-off between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level. It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time.

Conclusion

Thank You

Have Fun !