GENERATION OF REFLECTION SUMMARY FOR TEXT USING STEGANOGRPHY

[1]Akash Kamble [2]Anurag Mulay [3]Prathamesh Kalambate [4]Swapnil Joijode

[1]BE Student [2]BE Student[3]BE Student[4]BE Student

Department of Electronics and Telecommunication

Shivajirao S. Jondhale College of Engineering

Dombivli(East), Thane, Maharashtra 421204, India

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. This project intends to give an overview of image steganography, its uses and techniques. It also supports steganography in image files. For a more secure approach, the project watermarked image as carrier the secret message text file is embedded inside on it and then sends it to the receiver. The receiver then decrypts the message to get the original one and store the same message in a text file.*

Keywords – discrete cosinetransform, discrete wavelettransform, least significant bit, stenography, watermarking

1. Introduction

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [2]. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [2]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [3].Data hiding and data embedding can be classified as methods between steganography and watermarking. Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties.

2. Literature Survey

The basic idea behind the steganography is to hide the secrete data into the carrier file and send it to the other party over the network. The carrier files may be text, image, audio or video. The paper [4] explains that, Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us. It is also possible to simply use steganography to store information on a location. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data.

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

1. **Text steganography:-** Hiding information in text is the most common method of steganography. The method was to hide a secret message into a text message. It hides the text behind some other text file.
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.

3. **Audio steganography: -** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. The different methods that are commonly used for audio steganography are LSB coding, Parity coding, Phase coding, Spread spectrum, Echo hiding.

4. **Video steganography:** -Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.

5. **Protocol steganography:-**The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

The research paper [5] gives an overview of image steganography, its uses and techniques.Practically in most of the cases images are taken as the carrier file. Because the digital images are very useful and secure carrier for hiding the secret massage. Image is a collection of colour pixels. In standard, 24 bit bitmap we have three colour components per pixel: Red, Green and Blue. Each component is 8 bit and has 256 values. In 3 megapixel image we can hide 9 megabits of information using this technique, which is equivalent of 256 pages of book. If we only change the lowest bits of each pixel, then the numeric values can only change by a small percentage. We can only alter the original pixel colour value by ±7. Such a minute alterations in the pixel value does not make any difference in the visibility of the image. The original image and embed image both looks similar to the human eye.

3. Software Support

Operating system: -Windows 8.1

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 in the form of a binary product aimed at Java

Developers on Solaris, Linux, Mac OS X or Windows. Java is fast, secure, and reliable. I am using Java because of some of the most desirable features of Java. Some of those are list below-

3.1. Security
3.2. Portability
3.3. Java Architecture
3.4. Object-Oriented Robust
3.5. JDBC (Java Database Connectivity)

Swing:

Swing, which is an extension library to the AWT, includes new& improved components that enhance the look and functionality of GUIs. Swing can be used to build Standalone swing GUI Applications as well as Servlets and Applets. 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. The architecture of Swing components makes it easy to customize both their appearance and behaviour.

4. Methodology

The figure below shows the basic idea of hiding a secret data into a watermarked JPEG image.

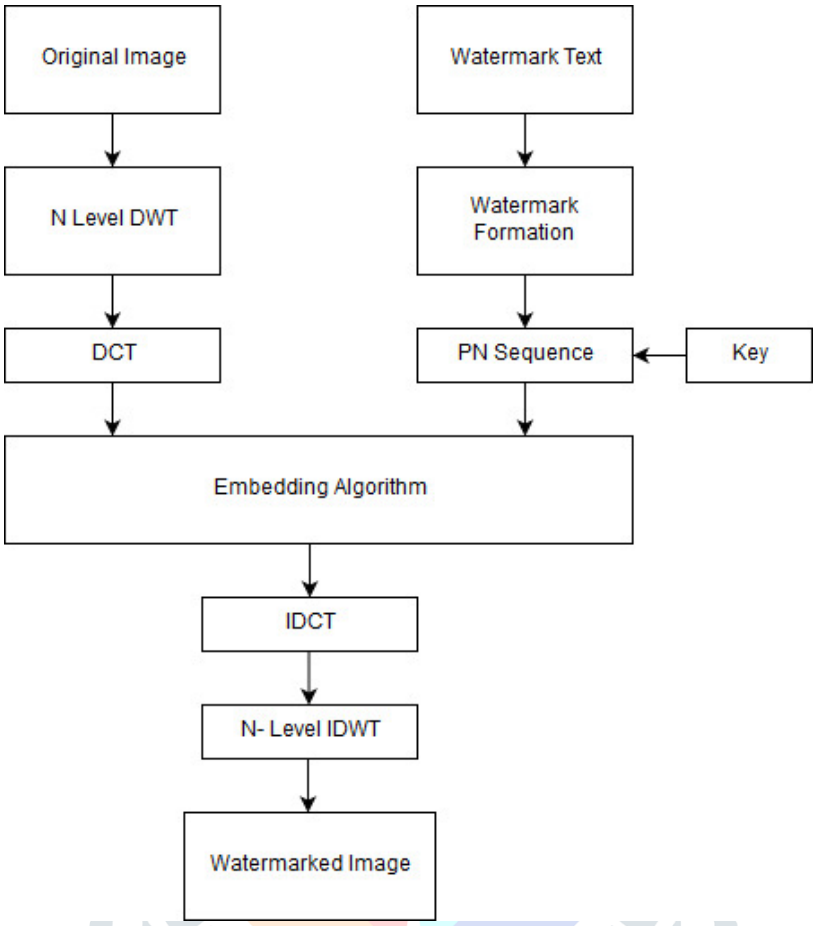

fig 4.1. Watermark embedding flow

4.1. LSB implementation

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).

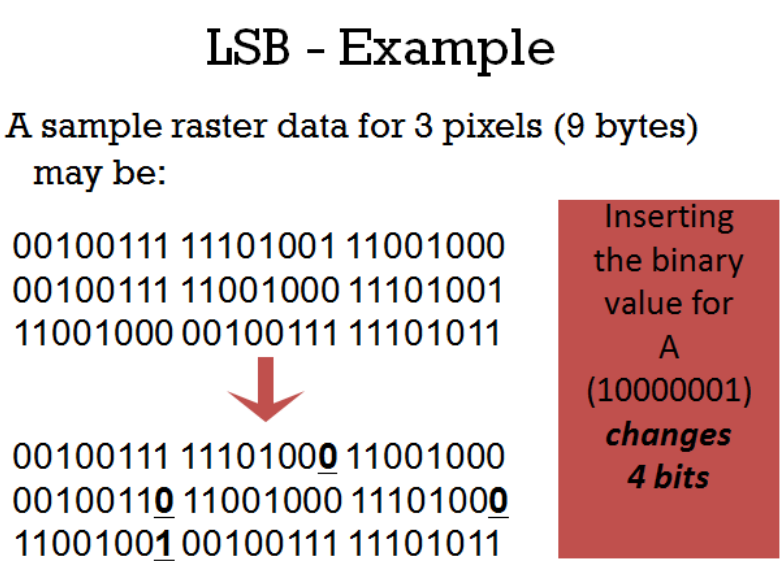

fig 4.2. LSB example

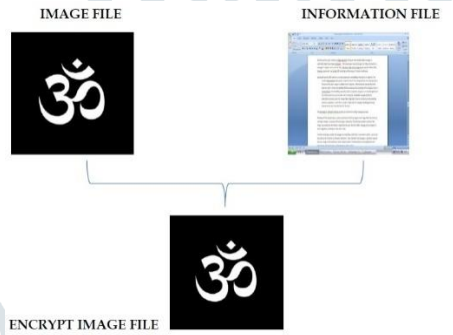

fig 4.3. Encryption process

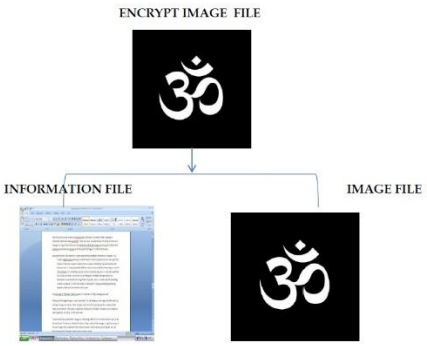

fig 4.4: Decryption process

5. Result

5.1. The images shown below are the screenshot images of the software.

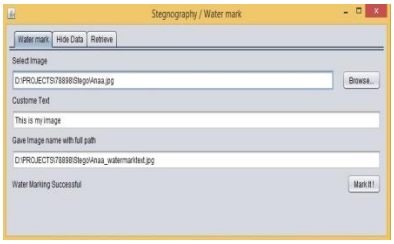

fig 6.1.1. Embedding Watermark Image

fig 6.1.2. Hiding Text File In Watermarked Image

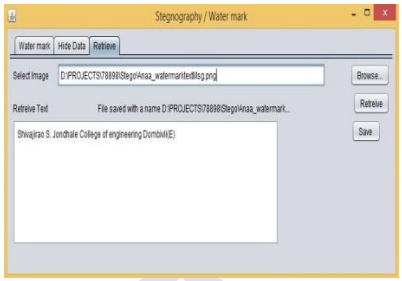

fig 6.1.3. Data Extraction

5.2. The images shown below are the sample image fed to the software, the text that is to be hidden in the watermarked image of the sample image and the resulting compressed image obtained from the software.

fig 6.2.1. Original Image

fig 6.2.2. Watermarked Image

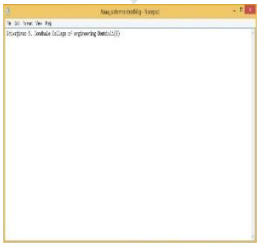

fig 6.2.3. Secret Message in Notepad

fig 6.2.4. Compressed Image

6. Conclusion and Future Scope

As steganography becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data.
For a system to be considered robust it should have the following properties:

•The quality of the media should not noticeably degrade upon addition of a mark.
• Marks should be undetectable without secret knowledge, typically the key.
• If multiple marks are present they should not interfere with each other.

In our project we have combined digital water marking and steganography. In future same project can be implemented using audio file as a carrier

References

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf
[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004
[3] Anderson, R.J. &Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998
[4] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 'AN OVERVIEW OF IMAGE STEGANOGRAPHY',Information and Computer Security Architecture (ICSA) Research Group. Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.
[5] Arvind Kumar Km. ' Steganography- the data hiding technique', International Journal of Computer Applications (0975 – 8887) Volume 9 - No.7, November 2010.