EUROPEAN UNIVERSITY OF LEFKE

FACULTY OF ENGINEERING

Graduation Project I

Image/Picture Steganography

Emmanuel Maneswa

154409

Abstract: Steganography is the study of invisible communication, that works in ways of hiding the existence of the transferred message. If successfully accomplished message does not attract attention from third parties. Main goals are robustness, undetectability and capacity of the hidden data. Since this can be done in different ways, this paper is based on Image Steganography.

Supervisor

Asst. Prof. Dr. Cem Kalyoncu

May 2019

1. Introduction

1.1. Problem definition

In the current era, the internet provides good convenience in transmitting large amounts of data from anywhere in the world. But, security and safety of the communications are still an issue. In order to solve this problem steganography schemes has been developed[1]. Steganography is the practice of concealing messages or information within other non-secret text or data. Unlike encryption, where it's obvious that information is being hidden, steganography hides information in plain sight, inside a file such as an image, which makes it difficult for observer to figure out where exactly the data is.

1.2. Literature survey

The word steganography is derived from Greek words which mean "covered message". For thousands of years it has been used in various forms. five hundred years ago, the Italian mathematician Jerome Cardan reinvented the Chinese ancient method of secret writing which works as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text[1]. Nazis also invented several steganographic methods during World War 2 such as microdots and have reused invisible ink and null ciphers. With advances in computing power, with the development of Digital Signal Processing and the internet, information theory and coding theory, steganography has now gone "digital". In the realm of digital steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing is guaranteed. Kurak and McHugh were credited to one of the earliest methods of digital steganography, they proposed a method which resembles embedding into the 4 Least Significant Bits(LSBs). They examined image downgrading and contamination which is known as image-based steganography. Provos and Honeyman, at the University of Michigan took three million images from popular websites looking for any trace of steganography. They have not found a single hidden message. Despite the fact that they attributed several reasons to this failure it should be noted that steganography does not exist merely in still images. Embedding hidden information in video and audio files is also possible. In 2008 a reversible data hiding method was proposed called Haar Discrete Wavelet Transformation(HDWT). In this technique a spatial domain image is transformed into a HDWT-based frequency domain image and then the high frequency coefficients are used to

embed the the secret data. This technique provides a good stego-image quality and a high hiding capacity[1]. In recent years couple of of techniques have been created. People have been working on better methods to even reduce the noise levels of a stego-image by using techniques like the Discrete Cosine Transform Coefficient[2]. This method works by converting an image into series of cosine waves and we have coefficients telling us how much of each of those waves we have. By changing those coefficients instead of changing the raw pixel values, we have a much less predictable effect on the image. So we're not going to be able to see the clear sort of steganographic noise that we see if use a technique like the LSBs.

1.3. Goals

The main aims of this project is to encapsulate an image into another image and enclose text into an image and then reveal the hidden image or text. By this I'm aiming to accomplish this without having to reduce the quality of the original cover image to a recognizable level. From the project I'm planning to learn how digital images are processed how to manipulate images and store a secret text or image into them and then reveal them. I also plan to learn the different techniques used in image steganography and the differences between the techniques.

2. Resources

2.1. Required software

i. **Visual Studio Code [2]**: It is free. It provides support for most of the the languages available. It also have an option for extension to add features that I may want to use. It provides easy code editing.

ii. **BitBucket [3]**: For secure workflow, knowing that the project is secure online. For version control. Provides unlimited free private repositories.

iii. **TortoiseHg [4]**: It is free. For Repository synchronization. Support for serving a repository hosted on bitbucket

2.2. Others

i. **Computer**: To be used for creating the application and testing the software.

ii. **Human**: To interact with the application as users. To develop the application as developer and tester.

3. Modules

3.1. Encryption Module

The module is in charge of encrypting both secret data and secret key[8]. The output of this module is the secret data bits in encrypted form. The secret data bits are the ones that are then sent to the second module the steganographic encoding module. The development of this mode may take 10 days.

3.2. Steganographic Encoding Module

This module is in charge of taking the produced encrypted secret data bits and the cover image and the secret stego-key. The output of module operation is the stego-image. The stego-image will be the image containing the secret data. The development of this module may take 16 days.

3.3. Steganographic Decoding Module

This module is in charge of taking the stego-image and the stego-key. The output of this module will be the encrypted secret data bits that will be now ready for decryption. The stego-key will be used to reveal the hidden secret data. The development of this module may take 16 days

3.4. Decryption Module

This module is in charge of decrypting the revealed encrypted secret data. This module will take the secret key needed for decryption and the encrypted secret data . The Output of this module will be the secret data original form. The development of this module may take 10 days.

4. Risk analysis

i. **Sudden Growth in Requirements**: As I progress with the issue that I don't recognize earlier can create a last-minute problem. The probability of this happening is low. The effect of this risk is serious.

ii. **Productivity Issues**: I may tend to take easy things to begin with. As a result, I might loose important time to complete the project. The probability of this happening is high. The effect of this risk is serious.

iii. **Estimation and Scheduling**: The software project may create problems in development time. The probability of this happening is very low. The effect of this risk is tolerable.

iv. **PC Issues**: My PC may crash or die while doing the project. I might even lose all the files about the project form my PC. The probability of this happening is moderate. The effect of this risk is catastrophic.

5. Conclusion

5.1. Benefits

Steganography is useful for securely storing sensitive data, this data might be passwords or keys within other files[6]. Information security means protecting your information from unauthorized access, modification, disruption, use, recording and destruction. Steganography is associated to cryptography and is just about as old. Ancient Greeks used it to hide information about troop movements by tattooing it on someone's head and then allowing them to grow grow their hair. The idea of cryptography you keep a message a secret by encoding it in such a way that no one can read it. Nevertheless, sometimes communicating in secret can trip alarms and make others suspicious. Therein lies cryptography, it may be unbreakable but encrypted information is easy to tag. When a third party finds that you are communicating in secret, they may urge you or the other person to tell them what you are hiding. This is where steganography comes in. Unalike cryptography the motive is to hide the message[7]. This way the third party cannot notice the difference between normal message and a steganographic message. Basically I would be comfortable communicating to someone about anything without the the fear that someone may know that we are talking. When Storing sensitive information, it is better to hide it in plain site, such that no one will notice than having to let people know where you are hiding it.

5.2. Future works

There is a high chance of expanding this project. It will not only be offering image steganography but it will add video and audio steganography. Video steganography is when the hidden information is now being hidden within video files. Audio steganography is when the hidden information is now being hidden within audio files. Yes I will continue this project after graduation.

References

[1] : Image Steganography, Shikha sharda, 2013, https://pdfs.semanticscholar.org/a966/6879d98f9b2d8d0680703b7391aea5e93681.pdf

[2] : Image Steganography, Savitha Bhallamudi, 2015, https://www.researchgate.net/publication/314116270_Image_Steganography

[3] : Visual Studio Code, Microsoft, 2019, https://code.visualstudio.com

[4] : Bitbucket, Atlassian, 2019, https://bitbucket.org/product/

[5] : TortoiseHg, Yoki Kodama, 2019, https://tortoisehg.bitbucket.io

[6] : Using Steganography for securing data not concealing it, Micheal Cobb, 2006, https://searchsecurity.techtarget.com/tip/Using-steganography-for-securing-data-not-concealing-it

[7] : An Introduction to Steganography and its uses, Adam Billman, 2014, https://null-byte.wonderhowto.com/how-to/introduction-steganography-its-uses-0155310/

[8] : Secure Image Steganography, Jamil Ahmad, Muhammad Sajjad, 2015, https://arxiv.org/pdf/1510.04413.pdf