**TITLE: INFORMATION HIDING USING IMAGE BASED STEGANOGRAPHY**

Faith Chelangat

Com/b/01-00083/2018

BCS 226 COMPUTER SCIENCE PROJECT 1

**SUPERVISOR: Dr Charles**

A Project Proposal Submitted in Partial Fulfillment of the Requirements for the Degree of Computer Science of the University of Science and technology Masinde Muliro University of Science and Technology”.

**March 2021**.

**Declaration**

“This proposal is my original work prepared with no other than the indicated

Sources and support and has not been presented elsewhere for a degree or any

other award.”

Student Name: FAITH CHELANGAT Registration No: COM/B/01-00083/2018

Signature: --------~~fccyy~~-------------------------- Date: -----------------------------------------------

The undersigned certifies that he has read and hereby recommend for

Acceptance of Computer Science Department in Masinde Muliro University of

Science and Technology a project proposal entitled Hiding Secret Messages Using Image Based Steganography.

**DR CHARLES**

**Signature: ------------------------------------------- Date: -----------------------------**

**Chapter 1: Introduction**

Steganography is the art of hiding secret messages in apparently an image or objects. It is the art of hiding information in a cover medium in such a way that the existence of any communication itself is undetectable. The cover medium might be an image, audio, video or text. In my project I will use the image as a cover medium. This helps people to make sure that only those who know about the presence of the message can obtain it. Images are composed of digital data which describes what is inside the picture which is usually the colors of all pixels.

The more information that is placed in the public’s reach on the internet, the more owners of such information need to protect themselves from theft and false representation. The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption.

However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a “steganography” technique to hide data in a cover media so that other cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness.

In this document, I propose a new system for hiding data stands on many methods and algorithms for image hiding where I store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage

1.1 **Background information**

Steganography can be traced back to the ancient Greece, where they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers’ hair to see the secret message”, (Babu et al., 2008). “Another method was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax. The recipient of the message would simply remove the wax from the tablet to view the message”, Babu et al. (2008). “During World War II invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye”, Babu et al. (2008).

“The modern formulation of steganography comes from the prisoner’s problem proposed by, where two prisoners named Alice and Bob wish to communicate in secret to hatch an escape plan. All of their communications pass through a warden named Eve who will throw them in solitary confinement if she suspects any type of secret communication. So they must find out some way of hiding their secret message which gave the birth of steganography. The warden is free to examine all communication exchanged between Alice and Bob which can either be active or passive. An active warden will try to alter the communication with the suspected hidden information deliberately in order to remove the information whereas a passive warden takes the note of covered communication, informs the others and allows the message to pass through. The assumption that can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as the secret key steganography, otherwise, it is public key steganography”, (Simmons, 1984).

**1.2 Statement of the problem**

The study of image steganography was mainly supported by the fact that modern day social media technologies are driven by images. Example Facebook, twitter, Instagram, WhatsApp, Messenger, Telegram etc. Also most of the technological systems nowadays rely mainly on images that is Geographical Information Systems, Medical Imaging, CCTV Surveillance etc. All these proves that technology relies mainly on images and hence is an area which should not be ignored

This project addresses the security problem of transmitting the data over internet network, the main idea coming when we start asking that how can we send a message secretly to the destination?

In this document, I propose some methods and algorithms of an image steganography system to hide a digital text of a secret message using least significant bit steganography and at the back-end to have a software for hiding data based on hiding algorithms.

A possible threat to image steganography, specifically for use with secure communication, is that a firewall attached to an e-mail server could remove images from an e-mail thereby removing the secret communication. However, none of the image steganography systems proposed in this dissertation rely exclusively on e-mail as communication channel and alternative channels, for example websites, can be used to distribute stego images.

* 1. **Objectives**

1. To analyze the developed tool and algorithm used experimentally to find out if this   
   proposed method works properly and is considered to give almost the optimum solution.
2. To design the best platform for communicating secret information
3. To implement and develop a prototype that will represent the use of genetic algorithm in text steganography

1.4 **problem justification**

“There is some evidence to support the need to provide quality ICT security solutions in organizations. A recent study of technical operations in organizations concurs with this observation, concluding that: "In every organization, computer users are affected in one way or another by the current ICT security breaches and threats” (Adams and Sasse, 1999).

1.5 **Scope of the project**

My project scope is developed for hiding information in any image file to ensure the safety of exchange the data between different parties and provide better security during message transmission. 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. I will use LSB technique; the proposed approach is to use the suitable algorithm for embedding the data in an image files.

**Chapter 2: Literature review**

**Introduction**

With the widespread use of Internet and wireless networks, and the blooming growth in consumer electronic devices and advances in multimedia compression techniques, multimedia streams are easily acquired nowadays. In an attempt to ensure protection of the a-fore-mentioned multimedia contents and effective hiding of additional data into such digital content, several techniques emerged. Nevertheless, none of the existing schemes can fully shield against all detection attacks. Texts with hidden data are expected to have higher entropy than those without.

Throughout history, a multitude of methods and variations have been used to hide information. Accounts throughout history have been recorded with tales of cryptography and steganography during times of war and peace (44-60). One of the first documents describing steganography is from the histories’ of Herodotus. In ancient Greece text was written on wax –covered tablets.

There are basically three types of protocols used in Steganography [Katzenbeisser11 Fabien and Petitcolas 2000]; Pure Steganography; Secret Key Steganography; and Public Key Steganography.

**Chapter 3: Project Methodology**

**3.1 Introduction**

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

My project will have two methods that is Encrypt and Decrypt.

In encryption the secret information is hiding in with any type of image file.

Decryption is getting the secret information from image file.

**3.2 Development paradigm**

The waterfall model is more suitable when the requirements are well known, product definition is stable, technology is understood, there are no ambiguous requirements, adequate resources with required expertise are available freely and the project is short. This, therefore, prompted its selection and use

**3.3 Hardware requirements price**

* Laptop (owned) – battery 3500
* phone owned
* Bundles 2GB 1000
* Flash disk 1500
* Hard drive 8gb

**3.4 Software requirements**

* Operating system
* Technology – Thonny7 IDE

**3.5 Functional requirements**

1) The system should be able to capture .txt files that is the Secret file

2) The system should be able to encrypt or decrypt files

3) Convert the secret file contents from characters to ASCII

4) System should be able to embed the secret message into the cover image

5) The stego image should be able to be reverted back to its original secret message

**3.6 Non-functional requirements**

* User interfaces will have a standard look and being user friendly at the same time to make sure that users' attention will not be distracted and interface to provide more flexibility and scalability.
* The program must be able to hide the image within the image and then extract image from the image properly.
* The program must be fast in processing
* All functions must work well for the system to be of a higher quality

**3.7 Conceptual framework**

Stego image

Cover image

 

Embedding function

10000111 10110110 01101101 10100101 01001010 10110110

Extracting function

10000111 10110110 01101101 10100101 01001010 10110110

Secret message

**3.8 Schedule**

|  |  |
| --- | --- |
| **ACTIVITIES** | **NUMBER OF WEEKS FROM THE MONTH OF MARCH** |
| **Supervisor meeting** |  |
| **Submission** of proposal |  |
|  |  |
|  |  |

**References**

**1. Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Message inside an Image http://www.iaeng.org/publication/WCECS2010/WCECS2010\_pp144-148.pdf**

**2. Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography** [**http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf**](http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf)

**3. Bere Sachin Sukhadeo, User Aware Image Tag Refinement** [**http://www.ijcsmr.org/eetecme2013/paper19.pdf**](http://www.ijcsmr.org/eetecme2013/paper19.pdf)

**4. Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011** [**http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf**](http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf)

**5. ANALYSIS MODEL WATERFALL MODEL** [**http://www.scribd.com/doc/87322736/Analysis-Model-Waterfall-Model**](http://www.scribd.com/doc/87322736/Analysis-Model-Waterfall-Model)

**6. Dalkey, N. and Helmer, O., 1963. An experimental application of the Delphi method to the use of experts. Management science, 9(3), pp.458-467.**

**7. Deepa, S. and Umarani, R., 2013. A Study on Digital Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 3(1), pp.54-57.**

**8. Dempsey, J. and Rowe, J.K., 2004. Why poststructuralism is a live wire for the Left. Radical theory/critical praxis: making a difference beyond the academy, pp.32-51.**

**9. Doerr, G. and Dugelay, J.L., 2003. A guide tour of video watermarking. Signal processing: Image communication, 18(4), pp.263-282.**

Secret message