# Implementing Desktop-Based Application using Steganography


**By**

**Jaralve, Jean Rose V.**

**Piedad, Shannie Mae A.**

**ATENEO DE DAVAO UNIVERSITY**

**COMPUTER STUDIES CLUSTER**

**DAVAO CITY**

**March, 2015**

# IMPLEMENTING DESKTOP-BASED APPLICATION USING STEGANOGRAPHY

**A Mini-Thesis**

**Presented to the**

**Undergraduate Faculty of the**

**Computer Studies Cluster**

**Ateneo de Davao University**

**In Partial Fulfillment**

**of the Requirements for the Degree**

**Bachelor of Science in Information Technology**

**By**

**Jaralve, Jean Rose V.**

**Piedad, Shannie Mae A.**

**ATENEO DE DAVAO UNIVERSITY**

**COMPUTER STUDIES CLUSTER**

**March, 2015**

Ateneo de Davao University
COMPUTER STUDIES CLUSTER
SCHOOL OF ARTS AND SCIENCES
P.O. Box 8016 Davao City
Philippines

---

Recommendation for Oral Defense

*In partial fulfillment of the requirements for the degree of* **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**, *this UNDERGRADUATE MINI-THESIS entitled*

**IMPLEMENTING DESKTOP-BASED APPLICATION USING STEGANOGRAPHY**

*has been prepared and submitted by* Jean Rose V. Jaralve and Shannie Mae A. Piedad and is recommended for ORAL DEFENSE.

**Jose Mari V. Freires**
*Adviser*

Ateneo de Davao University
COMPUTER STUDIES CLUSTER
SCHOOL OF ARTS AND SCIENCES
P.O. Box 8016 Davao City
Philippines

Recommendation for Acceptance

*The Undergraduate Faculty of the Computer Studies Cluster of the Ateneo de Davao University accepts the Undergraduate Mini-Thesis entitled*

**IMPLEMENTING DESKTOP-BASED APPLICATION USING STEGANOGRAPHY**

*which has been prepared and submitted by Jean Rose V. Jaralve and Shannie Mae A. Piedad in partial fulfillment of the requirements for the degree Bachelor of Science in Information Technology.*

**Mr. Antonio G. Bulao II**
*Panelist*

**Mr. Patrick Angelo P. Paasa**
*Panelist*

**Mr. Jose Mari V. Freires**
*Chair Panelist*

**ACKNOWLEDGMENT**

To our Thesis Two adviser, Mr. Jose Mari V. Freires who helped us throughout the entire semester, thank you for the time, patience, and guidance. Whenever we asked your time for some consultations, you really try to give us some solutions that we may use for the betterment of our project. Even though we are so hopeless about it, you really try to keep in our minds that we have to do it and we can do it.

To our panelist, Mr. Antonio G. Bulao and Mr. Patrick Angelo P. Paasa, thank you for your guidance, patience and for the questions you asked us before, during and after our thesis presentation. Those things had really helped us to push until the very end. Though we show some weaknesses about our skills, you accept it and push us to try again.

To our subject teacher, Ms. Maria Teresa T. Quindoy, who gave us proper encouragement to do the best for our project, thank you for the way of collecting progress reports that had helped us to keep on track and to manage our time for project completion and for proper consultation with our adviser and panels.

To Ms. Michelle P. Banawan, who had become our Thesis One adviser/subject teacher, thank you for your guidance since Thesis One made a big impact in our project. We can't go through all of these without your support.

To our friends and classmates, most especially to Renz Garret L. Platon, Marielle P. Banawan and Arlene Adrianne B. Go, thank you for helping us to test, proofread everything and encourage us in our thesis.

To our families, who gave their moral support and love. Who's with us up to the very end of our defense. Without them we cannot be the person we want to be.

To God, who gave us strength, believe and nothing is impossible. With him you never have to be afraid of everything. Trust and you can do it.

## Table of Contents


| | |
|---|---|
| Background | 1-2 |
| Technology Application Context | 2 |
| Technology Background | 2 |
| Objectives | 2-3 |
| Significance of the Study | 3 |
| Scope and Limitations of the Study | 3 |
| Review of the Related Literature | 3-7 |
| Project Methodology | |
| a. Conceptual Framework | 7 |
| b. Methodology | 8 |
| c. Data Gathering | 8 |
| Results and Discussion | 9 |
| a. Tests and results for maximal length | 10-12 |
| b. Questionnaire | 12-13 |
| c. Code snippet | 13-19 |
| Conclusion | 20 |
| Recommendation and Future Work | 20 |
| Definition of Terms | 20-21 |
| References | 21-22 |


## Tables and Figures


| | |
|---|---|
| Table 1 - Review of Related Literature Summary Table | 6-7 |
| Table 2 - LSB and F5 Comparisson | 9 |
| Table 3 - Maximal character testing for solid colored image | 10 |
| Table 4 - Maximal character testing for mixed colored image | 11 |
| Table 5 – Questionnaire | 12 |
| Figure 1 - Conceptual Framework | 7 |
| Figure 2 – Menu | 13 |
| Figure 3 - Encoding and Encryption | 13 |
| Figure 4 - Decoding and Decryption | 14 |
| Figure 5 - Sending Mail via Gmail | 14 |
| Figure 6 - Received email from the application | 15 |
| Figure 7 - Opened email with the password and message | 15 |

Figure 8 - Embedding Process Code (C#) 15
Figure 9 - Embedding Process Code (C#) continuation 16
Figure 10 - Decoding Process Code (C#) 17
Figure 11 - Encrypting Process Code (C#) 18
Figure 12 - Decrypting Process Code (C# 18
Figure 13 - Sending Mail Process Code (C#) 19
Figure 14 -Conversion Image File Format Process Code(C#) 19

# IMPLEMENTING DESKTOP-BASED APPLICATION USING STEGANOGRAPHY

Jean Rose V. Jaralve
Ateneo de Davao University
jrvjaralve@addu.edu.ph

Shannie Mae A. Piedad
Ateneo de Davao University
smapiedad@addu.edu.ph

In this paper, the proponents proposed a desktop-based application for enhancing security service using the technology of steganography. The application has the features of embedding the message into the image, encrypt the message for additional security and send the stego image via Gmail. It can also decrypt and extract the message that was sent via Gmail.

General Terms: Steganography, Crytography, AES Algorithm, F5 Algorithm, LSB Algorithm
Additional Key Words: stego image, embed, extract, encrypt, decrypt

## INTRODUCTION

Manipulation, stealing or illegal copying and destroying of data or information on the internet are one of the internet crimes present nowadays. It has been around the world and is a threat to business sectors, experts and other people who are using the internet. Some of them are having files and are vulnerable because of the low security especially on the Internet which can be hacked. There are hackers who are illegally manipulating the files for their own reasons or purposes. This situation can't be avoided because of the vulnerability and disadvantages of some things. There are added securities in things such as having a password to unlock a certain thing. It adds security to files because of the password but it is not enough to protect the files. Having the key to unlock a folder containing the "confidential" files is still vulnerable. It can still be hacked and the manipulator can steal or change the files on that folder. There's this technology which can help or add security to files called steganography. By using steganography, you can hide your file by not being visible to the possible manipulators. Steganography is the art and science of hiding information. The concept of steganography is to hide the whole file into another file. The concept is the same with cryptography but in cryptography it only hides the content of the file or the message/text. Steganography can be done in many ways like hiding an audio file containing a conversation into an image to protect the audio file. This study focuses on hiding messages on an image. Steganography protects the information from unwanted invasion of privacy. But there are some parties who can still manipulate and extract the information hidden in the carrier that's why the proponents added the password feature in embedding and extracting the message in the stego image and encrypting the message.

## BACKGROUND OF THE STUDY

Most of us have some text files or messages which we don't want others to see, read or have it except for the person we intended to see or read it. The proponents came up with the idea of hiding the messages to keep it away from an unwanted party. As the proponents were finding the right technology in protecting or hiding the text file, they first found out cryptography. Cryptography hides the message of a file by encrypting it or changing the original letters, numbers or special characters into random uppercase or lowercase letters, numbers and mostly special characters or simply by scrambling the message. But as the proponents were researching about cryptography, they found out that the level of suspicion is much higher than steganography. This is the time steganography entered the scene and they learned that there are many ways to hide the text files in steganography. Text files are not the only file which can be hidden but also audio, image and other files. To also add more security to the message and the file, the proponents will use cryptography in encrypt the message.

## TECHNOLOGY APPLICATION CONTEXT

The application is a desktop-based application where the user can type-in the message directly and hide it in the user's chosen cover image in an image with a security password. The user can simply retrieve or extract the file by entering the password.

The proposed steganography desktop-based security tool will have the following features:

(1) User-friendly environment
(2) Password protection in embedding and extraction process
(3) Ability to send stego image to another user through e-mail
(4) Invisibility of the stego image

## TECHNOLOGY BACKGROUND

Steganography has been around since the ancient Greece. It is derived from the Greek word “steganos” meaning “cover” or “hidden”. It is used to hide the pass codes or the messages on the scalp of the slaves in the ancient times. But now in the modern times, the message is hidden in a text file, image file, and audio file and or in a video file. Back then and now, steganography has the same purpose, to hide data in a looking cover and send it to the proper recipient who is aware of the sent message.

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable. (http://www.webopedia.com/TERM/C/cryptography.html)

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code. (http://en.wikipedia.org/wiki/Microsoft_Visual_Studio)

F5 is enhanced version of F4 algorithm with respect to 2 main features stated below which help in preventing statistical attacks and improving embedding efficiency: PERMUTATIVE STRADDLING and MATRIX ENCODING. (Rhagavendra, K)

LSB Algorithm is a common, simple approach to embedding information in a cover file. Unfortunately, it is vulnerable to even a slight image manipulation. To hide an image in the LSBs of each byte of a 24-bit image, you can store 3 bits in each pixel. A 1,024 ´ 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information. (Johnson N, Jajodia S)

## OBJECTIVES OF THE STUDY

- To develop a desktop-based steganography service by securing the capability of hiding messages.

Specific Objectives

- To compare LSB Steganography Algorithm and F5 Algorithm for embedding data into the image and use the better result for the embedding process,
- To determine the most appropriate image file format to use between other image file format for the cover image and the quality of the computer image,

- To find out the maximal length of characters for the message content of the text file to maintain the undetectability of the stego image, and;
- To add public key feature in retrieving or extracting the message in the stego image

**SIGNIFICANCE OF THE STUDY**

People nowadays have personal messages or information that they want the right recipient to receive which must not be seen or read by unwanted parties. By the use of steganography, users can use this technology to hide their messages or information from unwanted parties and from what has been discussed in the intro part of this paper, this project is not only for users but also for the society to help and to prevent the spreading of scandalous or private conversations or messages. There are a lot of issues regarding the security of the messages in stego image that the proponents of this project want to improve. This could also be an alternative in hiding messages with the improve security of the image. In terms of applications available online or in desktop-based, there's no application which can directly send the image to the recipient which can be more convenient to the user so the proponents made this project to enhance the steganography applications.

**SCOPE AND LIMITATIONS OF THE STUDY**

The study will focus on developing a desktop-based application that will embed messages to the cover image and can be sent via Gmail. Image-to-image, video-to-image, or etc. are out of this study.

**REVIEW OF RELATED LITERATURE**

2.1 Exploring Steganography: Seeing the Unseen

The article talks about what is steganography, steganography's history, different steganography approach and the tools used in using steganography. According to the authors, steganography is an art of hiding data or information in ways that prevents the detection of hidden messages. Its goals are to explain the history, methods, and different algorithms of steganography. It also explains the different techniques of steganography and different steganography tools.

The techniques discussed in this article are LSB insertion and masking and filtering. In LSB insertion, it is the common embedding process and the quick and easy way to hide information but unfortunately it is prone to suspicion because of the visible changes in the stego image. The other technique is masking and filtering where it is similar to watermarking.

The article provided information in steganography for the proponents especially in the LSB insertion. This article gave the proponents the idea that LSB is the easiest way of embedding but because of the visible marks or changes in the stego image, it is not recommended to use this technique.

2.2 Steganography in digital images: Common approaches and tools

The article talks about the different approaches, types, techniques and the history of steganography. According to the article, steganography is the art and science of using digital images for secret communication and only the intended recipient can extract the information of the stego image. Its goals are to explain the history of steganography and its use to today's modern world. It also discussed the common threat to stego images, the steganalysis.

Steganography has a variety of useful applications like in bank transactions and file authentication. Image Steganography is the most common among all the categories of steganography. One of the embedding processes discussed is the Frequency Domain Steganography. DCT is the most widely used lossy digital compression system. The F5 algorithm is a method in embedding information which is the improved F4 algorithm.

The article provided information in the different techniques, categories and tools in steganography. The proponents found many good methods or techniques to use in their project.

2.3 JPEG Compression Steganography & Cryptography using Image- Adaptation Technique

The article explains the definition on steganography, comparison between steganography and cryptography, types of compression and the comparison of the different image steganography algorithm. They also provided their main ingredients on embedding methodology.

The DCT or the Discrete Cosine Transform is discussed in the article which it transforms a signal from an image representation into a frequency representation, by grouping the pixels into a frequency representation. There are two types of compression: lossy and lossless. The comparing of the different steganography algorithms such as LSB and JPEG Compression is designed in a table that shows the highest to lowest in different categories such as invisibility and payload capacity.

The article provided information on the many steganography algorithms and the types of compression but it is much easier to understand the comparison of the different image steganography algorithm because of the table. It showed which is high, medium and low in different categories.

2.4 Image Steganography

The article shows how Steganography behaves in a modern context while searching or finding the real meaning of using it and how does it work. They will focus on the use of Steganography within digital images such as BMP and PNG.

The proponent of the said article has identified three effective methods in applying image steganography: LSB Substitution, Blocking and Palette Modification. Among the three methods, the proponent had decided to implement only one method which is the LSB Substitution because it can easily convert Image Steganography to Audio Steganography, larger scope when it comes to carrier formats and only have few limitations. It was also said there that by LSB Substitution, it works by going through the pixel of an image and extracting RGB values and then it separates the color channels and it will get the least significant bit. There it goes through the characters of the message setting the bit to the corresponding binary value.

The article was helpful because the proponent was able to implement it and provided some codes on how it was implemented. Also, the proponents of this

article were able to provide ways on how to detect or to verify Steganographed images which is very useful for evaluation.

2.5 Design of a Data Hiding Application using Steganography (April 2007)

The purpose of this project was to make or create a user friendly steganography application that will lessen the vulnerabilities to steganalysis than the existing steganography and to prevent or to block attackers from breaking or damaging user vulnerabilities or private files. It was also discussed in the article that there were a lot of steganography tools that was really capable in hiding data in an image and the following were divided into five categories: spatial domain based tools, transform domain based tool, document based tools, file structure based tools and other categories such as video compress encoding and spread spectrum technique based tools.

The article shows the implementation of LSB Algorithm because among all the techniques that was discussed, LSB Algorithm has a simpler method for embedding sequentially. It was also discussed in the article that there were a lot of Steganography Tools such as S-Tools, Hide and Seek, Hide4PGP and Secure Engine Professional. Those tools support BMP, GIF, PNG images and WAV audio files as the carriers. According to proponents of this article, each of those tools has unique features but it did solve the problem because those applications did not analyze the image file after it has embedded with data to see or to base how vulnerable it is to steganalysis.

This article was different among the other articles who had already implemented LSB Algorithm because according to the proponents, “the application ranks images based on their suitability as cover images for some data.” It allows a user to choose an image suited for hiding particular data that will reduce the threat of steganalysis attacks. For Data Hiding Algorithm, it will specify the data that the user wants to hide, which can be in any format then it will encrypt that data using the recipient's RSA public key. By the time that the encrypted data is obtained, each bit of the encrypted data is compared to the least significant bit of the pixel bytes in an image. Comparisons will start from the first byte until the last byte that will permit all the data to be hidden in the image user has chosen.

According to the article, the proponents of this article added another one algorithm for public key or password for encryption called Encryption Algorithm. It was mentioned that the application will use RSA Algorithm for two reasons. First, by using a public key algorithm the need for a private shared key between the sender and recipient of the data is eliminated. Shared keys are impractical that is why the proponents require a secure way of distributing or giving the key to the other user who the user wants to send the files with. Second, the RSA algorithm is a widely known and secure for large enough prime numbers that are used to generate the keys. RSA Algorithm has a principle of open design of secure software system and is with the knowledge of the public. This RSA Algorithm will be a big help for the project because it will lessen the vulnerabilities of the user. There are three policies for computer security:

confidentiality, integrity, and availability and it is a good basis for evaluation.

| Related Literature | Research Problem | Method | Findings | Limitations |
|---|---|---|---|---|
| Exploring Steganography: Exploring the Unseen<br><br>(Johnson N, Jajodia S. Exploring Steganography: Seeing the Unseen) | To determine the limitations and flexibility of available software. | The authors evaluated several stega packages: StegoDos, White Noise Storm and S-Tools. | StegoDos uses LSB, less successful. White Noise Storm is effective for DOS, detects no degradation, problems with noise interfering, uses encryption to randomize bits within an image S-Tools hides information in the "unused" areas on floppy disks, uses LSB insertion, the most impressive results | The authors stated that Steganography itself does not ensure secrecy and they stuggested that Steganography + Cryptography = strong. |

| | | | | |
|---|---|---|---|---|
| Steganography in digital images: Common approaches and tools<br>(Atawneh S, Almomani A, Sumari P. Steganography in digital images: Common approaches and tools. IETE Tech Rev 2013;30:344-58 webopedia.com/TERM/L/lossy_compression.html ) | To research available steganography and encryption algorithms to pick the one the offer the best combination of strong encryption, usability and performance. | The authors Proposed a framework for hiding large volumes of data in images embedding methodology: transform domain, encoder employs local criteria to select which subset ofcoefficients it will actually embed data in. | All steganographic algorithms have to comply with a few basic requirements: Invisibility. Payload capacity, Robustness against statistical attacks, Robustness against image manipulation. Independent of file format and unsuspicious files. | A tool named JPEG-JSteg has no secret or private key for the stego image thus it is proned to attacks. |
| JPEG Compression Steganography & Cryptography using Image- Adaptation Technique<br>(Kumari M. et.al. 2010. JPEG Compression Steganography & Cryptography Using Image-Adaptation Technique) | Comparisons between different image steganography algorithms Benefits and drawbacks of steganography domains are highlighted Defeating Steganography | Defeating steganalysis: an combination of defeating methods, utilizing lossy compression, | "Steganographers are advised to create their cover images and avoid using familiar carriers. Some scholars recommend that once the cover image has been used, it should be destroyed and not to be used again." | A application described in the article allows other users to hide private information. Other user might manipulate and extract a picture the original user has. This might leak the private message of the original user of the application. |
| Image Steganography<br>(Nabavian N. 2007. CPSC 350 Data Structures: Image Steganography) | How to discover if an image has stega applied | LSB substitution, Blocking, Palette Modification: 1) encrypting message 2) create header 3) enhanced LSB attack | "With LSB substitution it is quite easy to tell if an image has been Steganographed with an Enhances LSB attack" Chi-square analysis can detect much more than enhanced LSB attack | Hiding text isn't just enough because if the third party discovers the image and extract the message, the message will be seen. |
| Design of a Data Hiding | Design a data hiding | Data Hiding | Images are identical | RSA has no |

| | | | | |
|---|---|---|---|---|
| Application using Steganography<br><br>(Bahramshahry A. et.al. 2007. Design of a Data Hiding Application Using Steganography April 2007) | application using steganography and make stega app less vulnerable to attacks | Algo, RSA public key, Encryption algorithm Used StegaAlyzerSS to analyze LSB of the images | and an image should be chosen as a cover based on its suitability to hide particular data | infrastructure in place for ensuring integrity of an individual's public key BMP and annot hide large data |

**Table 1. Review of Related Literature Summary Table**

**CONCEPTUAL FRAMEWORK**

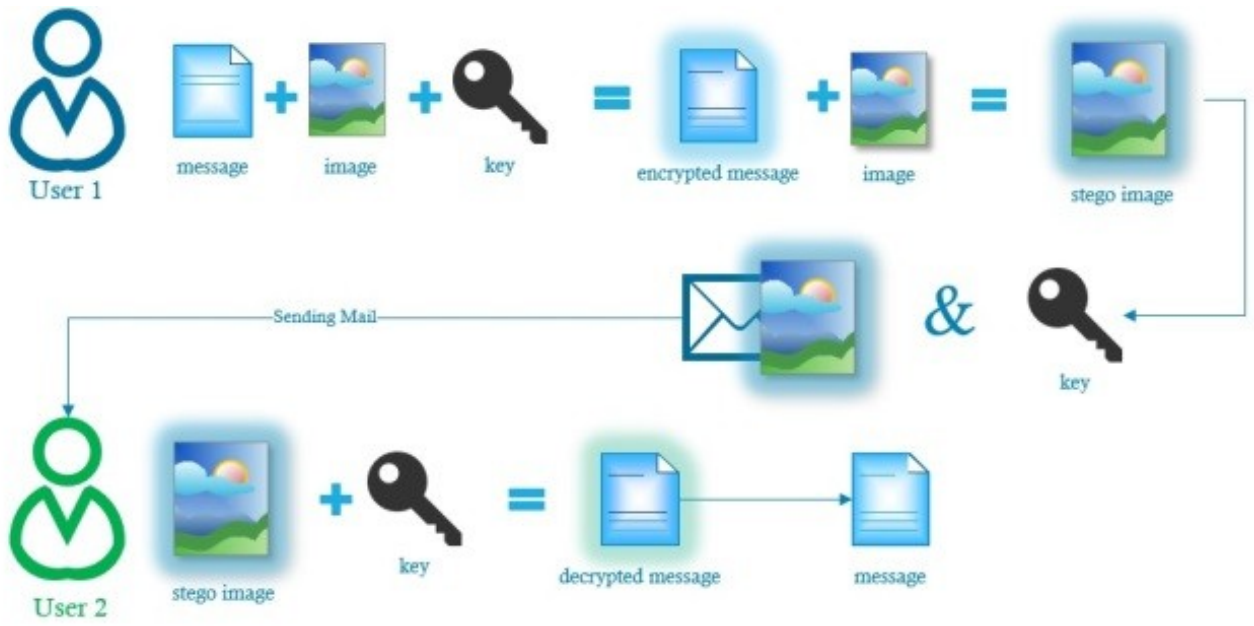


**Figure 1. Conceptual Framewor**

**METHODOLOGY**

In making this research project, the proponents used different measures in securing the invisibility of the stego image as part of the design of the steganography system and for the completion of the application such as:

- Invisibility – ability to be unnoticed by the human eyes

- Security – both the message and the image. For the message, it will be encrypted to increase its security or privacy when extracted and to secure the communication. While for the image, the closer the cover image to the stego image, the more assured it is that there are no visible changes or visible distortion that can suspect other party
- Capacity – the amount of information or characters that can be hidden relative to the size of the cover image.

Binarization is used for the converting of 0's and 1's. All information on the computer is stored in a binary format as either 1's or 0's. (Clark J.) Histogram analysis is used in visualizing the changes made to the cover image due to embedding. The histogram of the cover image or the original image and the histogram of the stego image will be used as a basis to compare any changes made between the two images during the embedding process. PSNR or Peak Signal-to-Noise Ratio measures the quality variation between the cover and the stego images. If it is more than 40 dB, the invisibility of the image is maintained. LSB Algorithm to embed secret data in least significant bits of pixels in a cover image. AES algorithm (128 bits) was also used for the public-key encryption so that it will prevent attackers from accessing user private files.

**DATA GATHERING AND FEATURE SELECTION**

The proponents have decided to implement the project by accepting text and the text can be of any size but it will depend because as what the proponents have found on their research, the more number of characters you put in a low quality image, the more visible the changes or distortion in the image will be. Text or messages and images will be used as the data in the research. The text will be in an ordinary text and not in a cipher text and any unique characters. The source would be the user uploading the text file and the JPEG image. The user can use any image and it is recommended to be in high quality so that the user can input many number of characters. The user must be specific in saving files to avoid confusion and to secure the messages in the stego image.