**IMAGE STEGANOGRAPHY**

Prepared by:

**Emmanuel Maneswa**

Submitted to the

Graduation Projects Examination Jury

in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

Software Engineering

European University of Lefke

June 2020

Approval of the Software Engineering Department

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assist. Prof. Dr. Ferhun Yorgancıoğlu

Head of Department

This is to certify that we have read this graduation project and that in our opinion it is fully adequate, in cope and quality, as an Undergraduate Project.

Assist. Prof. Dr. Cem B. Kalyoncu

Supervisor

Members of the examining committee

Name Signature

1. Assoc. Prof. Dr. Hüseyin Ademgil …….………………………

2. Assist. Prof. Dr. Cem B. Kalyoncu …….………………………

3. Assist. Prof. Dr. Ferhun Yorgancıoğlu …….………………………

4. Assist. Prof. Dr. Vesile Evrim …….………………………

5. Dr. Ersin Çağlar …….………………………

Date: …….………………………

# Abstract

**IMAGE STEGANOGRAPHY**

by

Emmanuel Maneswa

Software Engineering Department

European University of Lefke

Supervisor: Assist. Prof. Dr. Cem B. Kalyoncu

The project deals with the best approach in image steganography using Least Significant Bit (LSB) that further improves the quality of the existing LSB substitution methods to improve the security strength of the hidden information.

It is a new technique to substitute LSB of BGR true color image. The new security formation hides the secret information within the LSB of the image where the secret key encrypts the hidden information to protect it form unauthorized people. Generally, in LSB techniques hidden information is embedded into a fixed position of LSB of the image. For this purpose, knowing retrieval techniques, anyone can extract the hidden information. In my project, hidden information is embedded into different position of LSB of the image depending on the secret key.

As a result, it is difficult to extract the hidden information knowing the retrieval techniques. The implemented technique results in LSB based image steganography using secret key which gives good security issue than LSB based image steganography techniques.

**Keywords:** Steganography, Cryptography, Data Hiding, LSB, Digital Image, Hash, Security.

# Acknowledgments

I would like to express my gratitude to my project supervisor, Assist. Prof. Dr. Cem B. Kalyoncu, who guided me throughout this project. I would also like to thank my advisor, Assist. Prof. Dr. Ferhun Yorgancıoğlu, for the continuous support of my BSc study and his motivation. I would also like to thank my family and friends who supported me.

# Table of Contents

APPROVAL ii

ABSTRACT iii

ACKNOWLEDMENTS iv

TABLE OF CONTENTS v

LIST OF FIGURES vi

LIST OF TABLES vii

1. INTRODUCTION 1

1.1. DEFINITIONS 1

1.2. GOALS 2

1.3. ETHICS 4

1.4. REQUIRED SOFTWARE 5

2. LITERATURE REVIEW 6

3. BACKGROUND INFORMATION 15

3.1. TITLE OF THE SUBSECTION 19

3.2. TITLE OF THE SUBSECTION 23

4. IMPLEMENTATION DETAILS 24

3.1. TITLE OF THE SUBSECTION 26

3.2. TITLE OF THE SUBSECTION 27

5. CONCLUSION AND FUTURE RECOMMENDATION 29

5.1. BENEFITS 29

5.2. CONCLUSION 32

5.3. FUTURE RECOMMENDATIONS 33

6. REFERENCES 35

APPENDIX A 38

A.1. TITLE OF THE SECTION 38

A.1. TITLE OF THE SECTION 44

APPENDIX B 46

B.1. TITLE OF THE SECTION 49

# List of Figures

Figure 1.1. A Distributed System 8

Figure 1.2. ER Modeling 11

Figure 2.1. xxxx xxxxx 13

Figure 2.2. xxxxxxx 22

Figure 3.1. xxxxx 25

# List of Tables

Table 1.1. Project Goal 1 2

Table 1.2. Project Goal 2 3

Table 1.3. Project Goal 3 3

Table 1.4. Project Goal 4 3

Table 1.5. Project Goal 5 3

Table 1.6. Project Goal 6 3

Table 1.7. Project Goal 7 4

# INTRODUCTION

* 1. Definitions

Usually nowadays if we want to transfer sensitive data, we encrypt the data before transferring it across the internet. Transferring messages like this, still can cause suspicion: there is clearly secret/sensitive data in your encrypted message that you are trying to hide. Attackers know precisely where to look to try to procure the information [1]. But privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to commune secretly and covertly. Steganography is the art of concealing information. In computer science, it refers to concealing data within a file or message. It serves a related motive to cryptography, but rather than encrypting data, steganography simply hides it from the user [2]. The word steganography comes from New Latin steganographia, which merges the Greek words steganos, meaning “concealed or covered”, and -graphia meaning “writing” [3].

In general, a steganographic system consists of a cover media into which the secret information is embedded. The embedding procedure fabricates a stego medium by replacing the information with data from the information to be hidden. Commonly secret information is embedded into the fixed position of Least Significant Bit (LSB) of a cover image which is the carrier to embed secret information. Since anyone can ensure that particular position of LSB contains secret information, so it is then easier for anyone to extract the secret information using the extraction method. The core purpose of image steganography is to guarantee security of the hidden information [4].

There are several researches available detailing properties of image steganography. Numerous steganographic techniques have been suggested. The most familiar of these is substituting the LSB of the pixels with secret information. A notable LSB established image steganography technique is given in [5] and it suggest an adaptive technique based on inter pixel relationship. The technique tremendously enhances the stego-image quality. Using this method it is feasible to extract the secret information for anyone by using the extraction method [6]. A different LSB established image steganography technique is given in [7] and it suggests three effective steganographic techniques that take advantage of the neighborhood information to approximate the quantity of data to be embedded into the input pixel of the cover image and that embed exactly three bits of secret information in smooth sections and a varying amount of bits are embedded into the edged sections.This technique uses various pixels of the image store too many bits of the secret information but separate pixels stay unchanged. In result, some pixels are manipulated harshly whereas other pixels stay unused. Using this technique it is feasible to extract the hidden information for anyone, since they did not issue any security measures [6].

In order to ensure the security of the secret information, I have tackled it by using creative LSB based image steganography. In this technique I introduced a secret key which guarantee the security of secret information. The embedding of the secret information is determined by the secret key. The secret key determines the suitable location of secret information. It is extremely difficult to extract the secret information without the identical secret key. Here a bit of secret information is put in either LSB of Blue or Green or Red matrix of a particular pixel which is guaranteed by the secret key and the pixel column. I also use the secret key to encrypt the secret information to provide an extra layer of security. So by adding secret key, I increased the security intensity of the secret information in LSB based image steganography.

* 1. Goals

Project Goals (PG)

PG1: Hide secret information inside an image.

PG2: Invisibility.

PG3: Support multiple image formats.

PG4: Extract of all hidden information

PG5: Store more information.

PG6: Secure.

PG7: Support colour images.

*Table 1.1. Project Goal 1*

|  |  |
| --- | --- |
| Goal Identifier | PG1 |
| Project Goal | Hide secret information inside an image. |
| Goal Description | The primary goal of this project is to hide the secret information inside the cover image to produce a stego image containing the secret information. |

*Table 1.2. Project Goal 2*

|  |  |
| --- | --- |
| Goal Identifier | PG2 |
| Project Goal | Invisibility. |
| Goal Description | This goal states that the produced stego-image should be manipulated in away that the human eye will not spot the differences. |

*Table 1.3. Project Goal 3*

|  |  |
| --- | --- |
| Goal Identifier | PG3 |
| Project Goal | Support multiple image formats. |
| Goal Description | This goal states that the system should support cover images of multiple image formats e.g. jpeg, png, tiff, webp, bmp, exr, hdr. |

*Table 1.4. Project Goal 4*

|  |  |
| --- | --- |
| Goal Identifier | PG4 |
| Project Goal | Extract of all hidden information. |
| Goal Description | This goal states that the system should be able to extract the hidden information in its original state, meaning nothing should be missing. |

*Table 1.5. Project Goal 5*

|  |  |
| --- | --- |
| Goal Identifier | PG5 |
| Project Goal | Store more information. |
| Goal Description | This goal states that the system should be able to hide a lot of information. Though this may depend on the size of image selected by the user. The bigger the image the increase in the amount of of information that can be hidden. |

*Table 1.6. Project Goal 6*

|  |  |
| --- | --- |
| Goal Identifier | PG6 |
| Project Goal | Secure. |
| Goal Description | This goal states that the information hidden should be secure, meaning it should be encrypted before being hidden and then should be hidden according to a secret key provided by the user. And that secret key can only be used to know where the hidden information is when extracting it. |

*Table 1.7. Project Goal 7*

|  |  |
| --- | --- |
| Goal Identifier | PG7 |
| Project Goal | Support colour images. |
| Goal Description | This goal states that the system should support colour images, since they have the RGB values for every pixel and it makes the system more secure (PG6) since there are multiple choices to choose from when hiding secret information. |

* 1. Ethics

Association of Computing Machinery (ACM) and the IEEE Computer Society joined forced to create Software Engineering Code of Ethics and Professional Practices and cooperatively approved by the ACM and the IEEE-CS as the principle for practicing and teaching Software Engineering [8].

According to the ACM code of ethics principle 1.01. [8] and in accordance with the principle I take full responsibility in accepting this project as my own work. According to principle 1.03 [8] and in accordance with the principle I approve the software because I believe that it’s safe, meets specifications, passes proper tests, and does not decrease quality of life, decrease privacy, or harm the environment. In general I believe the software is of public good [8].

According to the ACM code of ethics principle 3.02. [8] and in accordance with the principle I ensured proper and achievable objectives and goals for this project. According to principle 3.10. [8] and in accordance to the principle I ensured adequate testing, debugging, and review of the software. According to principle 3.12. [8] and in accordance with the principle I worked to develop software that respect the privacy of those who will be affected by it. In general I believe I ensured software meets the highest professional standards possible [8].

According to the ACM code of ethics principle 8.01. [8] and in accordance with the principle I shall regularly try to further my knowledge of developments in the specification, analysis, design, development, maintenance, and testing of software and related documents, in conjunction with the management of the development process. According to principle 8.02. I shall regularly try to improve my ability to create reliable, safe, and useful quality software within reasonable time and at reasonable cost. According to principle 8.03. [8] I shall regularly try to improve my capacity to provide accurate, informative, and well-written documentation. In general, as a software engineer I shall take part in lifelong learning concerning the practice of my profession and shall encourage an ethical approach to the practice of the profession [8].

* 1. Required Software

1. [Visual Studio Code](https://code.visualstudio.com)

Visual Studio Code is a lightweight yet powerful free source code editor developed by Microsoft. It runs on desktop and is available for Linux, Windows and macOS. Its features include support for syntax highlighting, debugging, intelligent code completion, embedded Git, code refactoring, and snippets, and has a rich ecosystem of extensions for other features and programming languages [9]. This is the environment I used to write my code because it has a lot of advantages and it’s also a personal preference.

1. [Git](https://git-scm.com)

Git is a free and open source distributed and version control system for tracking changes in source code throughout software development. It is developed for collaborating work between programmers, however it can be used track changes in any type of files [10]. I used it as as the version control system.

1. [Bitbucket](https://bitbucket.org)

Bitbucket is a web based version control repository repository hosting service owned by Atlassian. It is for hosting source code and development projects that use either Git or Mercurial version control systems [11]. I used it as the hosting service for the project.

1. [OpenCV](https://opencv.org)

OpenCV is a library of programming functions mostly focused on real time computer vision. The library is cross platform and free for use under the open source BSD licence [12]. I used it to load, alter, and save images and read image data.

1. [Qt](https://www.qt.io)

Qt is a free and open source widget toolkit for developing Graphical User Interfaces (GUI) together with cross platform platform applications that run on numerous hardware and software platforms for instance Linux, Windows, macOS, Android or embedded systems with little to no change in the primary codebase and at the same time still being a native application with native capabilities and speed [13]. I used on of its modules Qt QML for developing the GUI.

1. [Trello](https://trello.com/)

Trello is a web based Kanban style list making application [14]. I used it to organize and prioritize project tasks in a scrum board style.

# 2. LITERATURE SURVEY

Typically, should cover the following items (at least 3 pages):

A survey and comparative analysis of sufficiently large number of works (publications) in the area of study. This survey should include a brief history of the subject, but main attention should be paid to publications in journals, conference proceeding and published thesis during the last 5 – 7 years. It is desirable to include and comment here an appropriate classification of used methods and approaches in the form of a table or a diagram. The student should avoid referencing Internet (Web) publications in the project, since many of them are not reliable sources of related information.

A detailed description and analysis of two or three published works that are most close to the topic of the project. Clearly specify positive and negative aspects of these works. Use appropriate illustrations and figures here to make your analysis clearer. This part of the project can take two or more sections.

# 3. BACKGROUND INFORMATION

This chapter explains theoretical aspects of the project. It should give, in 3 – 4 sections, a detailed description of what you propose as a new contribution to the area (your method or approach). The chapter can include a general description of the proposed approach, specification of tools (theoretical and experimental) to solve the problem, flowcharts of algorithms, their descriptions, timing diagrams, related mathematical expressions, proposed models and their descriptions, with necessary assumptions under which your method or solution can work.

# 4. IMPLEMEMTATION DETAILS

This chapter also should contain a scheme of the implementation of your method or solution, organization of experiments, based on computation, simulation, and statistical analysis, with appropriate graphs and other illustrations. The obtained results must be discussed and compared with the results given in published works.

Chapter 3 and this chapter together represent the most important parts of your new contribution to the area of study. If necessary, the material of this chapter can be divided into two chapters.

# 5. CONCLUSION AND FUTURE RECOMMENDATION

This Chapter can conclude the project. It should summarize the results of study, emphasize their positive and negative aspects and suggest directions of a further study of the topic to improve the proposed scheme, method or approach.

# 6. REFERENCES

1. Zdziarski, Z. (2018, Oct 5). Image Steganography - An Introduction, Zbigatron. Viewed May 27, 2020, from <[https://zbigatron.com/image-steganography-an-introduction](https://zbigatron.com/image-steganography-an-introduction/)>
2. Christensson, P. (2020, Feb 24). Steganography Definition. Viewed May 27, 2020, from <<https://techterms.com/definition/steganography>>
3. Merriam-Webster. (n.d.). Steganography. Merriam-Webster.com dictionary. Viewed May 27, 2020, from <<https://www.merriam-webster.com/dictionary/steganography>>
4. Gangwar, A & Shrivastava, V. (2013). Improved RGB-LSB Steganography Using Secret Key. International Journal of Computer Trends and Technology. [Online]. 41(2). pp. 85-89. Viewed May 28, 2020, from

<[https://pdfs..semanticscholar.org/7a7b/54d6557fd5f2945f8720d098fbf77d165457.pdf](https://pdfs.semanticscholar.org/7a7b/54d6557fd5f2945f8720d098fbf77d165457.pdf)>

1. Long, Min & Li, Fenfang. (2018, July). A Formula Adaptive Pixel Pair Matching Steganography Algorithm. Advances in Multimedia. 2018. 1-8. 1155/2018/7682098. Viewed May 28, 2020, from

<<https://www.researchgate.net/publication/326229819_A_Formula_Adaptive_Pixel_Pair_Matching_Steganography_Algorithm>>

1. Karim, S. M. Masud & Rahman, Md & Hossain, MD. (2011, Dec). A new approach based image steganography using secret key. 286-291. 10. 1109/ICCITechn. 2011.6164800. Viewed May 28, 2020, from

<<https://www.researchgate.net/publication/261421805_A_new_approach_for_LSB_based_image_steganography_using_secret_key>>

1. Haque, Sadia & Sharmin, Farhana. (2010, June). Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information. Int. Arab J. Inf. Technol.. 7. 34-38. 10. 1109/ICCIT. 2009. 5407128. Viewed May 28, 2020, from

<<https://www.researchgate.net/publication/220413577_Variable_Rate_Steganography_in_Gray_Scale_Digital_Images_Using_Neighborhood_Pixel_Information>>

1. Gotterbarn, Donald & Miller, Keith & Rogerson, Simon & Barber, Steven & Barnes, P & Burnstein, I & Davis, Michael & El-Kadi, Amr & Fairweather, NB & Fulghum, M & Jayaram, N & Jewett, T & Kanko, M & Kallman, E & Langford, D & Little, Joyce & Mechler, E & Norman, MJ & Phillips, D & Werth, LH. (2001). Software Engineering Code of Ethics and Professional Practice. Science and Engineering Ethics. 7. 231-238. 10.1007/s11948-001-0044-4. Viewed June 2, 2020, from

<<https://www.researchgate.net/publication/278417404_Software_Engineering_Code_of_Ethics_and_Professional_Practice>>

1. Getting Started. Microsoft. (n.d.). Viewed June 3, 2020, from

<<https://code.visualstudio.com/docs>>

1. Git --distributed-is-the-new-centralized. (n.d.). Git. Viewed June 3, 2020, from

<[https://git-scm.com](https://git-scm.com/)>

1. Bitbucket. (2020, May 22). Wikipedia. Viewed June 3, 2020, from

<<https://en.wikipedia.org/wiki/Bitbucket>>

1. OpenCV. (2020, May 22). Wikipedia. Viewed June 3, 2020, from

<<https://en.wikipedia.org/wiki/OpenCV>>

1. Qt (software). (2020, May 27). Wikipedia. Viewed June 3, 2020, from

<<https://en.wikipedia.org/wiki/Qt_(software)>>

1. Trello. (2020, April 20). Wikipedia. Viewed June 3, 2020, from

<<https://en.wikipedia.org/wiki/Trello>>

# APPENDIX

(if any) can contain additional material, such as source texts of programs, large tables of obtained results, descriptions of used protocols, utility programs, etc. Each Appendix must have its title on a separate page.