**A**

**Project Report**

**On**

**IMAGE STEGANOGRAPHY USING PYTHON**

Submitted in partial fulfillment of the

Requirements for the award of the degree

Of

**BACHELOR OF COMPUTER APPLICATION**

**Session: 2017-20**

Submitted by

**HIMESH MAURYA 201710101130001**

**TARUN VERMA 201710101130003**

Under the guidance of

**Mr. Kshitiz Srivastava**

**DEPARTMENT OF COMPUTER APPLICATION**

**SHRI RAMSWAROOP MEMORIAL UNIVERSITY,**

**LUCKNOW- DEWA ROAD, BARABANKI, U.P,**

**MAY- 2020**

**DECLARATION**

I hereby declare that the work which is being presented in the project entitled “**Image Steganography Using Python**” in partial fulfilment of the requirements for the awardof **Bachelor of** **Computer Application** from **Shri Ramswaroop Memorial University, Uttar Pradesh** is an authentic record of my own work carried out during the period From February, 2020 to May, 2020 under the supervision and guidance of **Mr.** **Kshitiz Srivastava.**

**Student signature:-**

**HIMESH MAURYA TARUN VERMA**

**Place:**

**Date:**

**CERTIFICATE**

This is to certify that the synopsis entitled **Image Steganography Using Python** being submitted by **Mr. Himesh Maurya** and **Mr. Tarun Verma** in partial fulfilment for the award of the **Degree of Bachelor of Computer Application** to **Shri Ramswaroop Memorial University** is a record of bona fide work carried out by them under my guidance and supervision.

The results embodied in this project synopsis have not been submitted to any other University or Institute for the award of any Degree or Diploma.

**Dr. Bineet Kumar Gupta Mr. Kshitiz Srivastava Dr. Promila Bahadur**

**(Head of the Department) (Supervisor) (Project Coordinator)**

**ACKNOWLEDGEMENT**

**IMAGE STEGANOGRAPHY USING PYTHON** is the final year project for the department of Computer Application **SHRI RAMSWAROOP MEMORIAL UNIVERSITY**, 2020 batch this report is prepared by **Mr. Himesh Maurya** and **Mr. Tarun Verma** under the guidance of **Mr. Kshitiz Srivastava**, **SRMU**. So first and for most we would like to express our gratitude to our **HOD Dr. Bineet Kumar Gupta** Sir and other faculty member for giving us wonderful opportunity to work on the project. We are also thankful to all our teachers of **SHRI RAMSWAROOP MEMORIAL UNIVERSITY** who were simply full ideas and whenever there was any need they shared those great ideas and concept with us. And in the end, we would like to thank all those who helped us during the testing phase of the project.

**Student signature:-**

**Himesh Maurya Tarun Verma**

**ABSTRACT**

The aim of this Project is to develop software which can be used to hide secret data to an **Image**. The software is mainly used when a user wants to send secret information but does not wants any other person to see that data. This type technique is mainly used by **secret organisations** to send secret information through **dark web**. **Organisations** can also use this to store and secret **Chemical Formula** or **Future Plans for the organisation.** Using **VISUAL STUDIO CODE, PYTHON, SQLITE** the system is designed. This software takes the a **cover image** and a **secret text message** as input and gives a **steganographed image** based on the algorithm applied and also we can extract **secret text message** from the **steganographed image.**

**CHAPTER 1**

**INTRODUCTION**

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

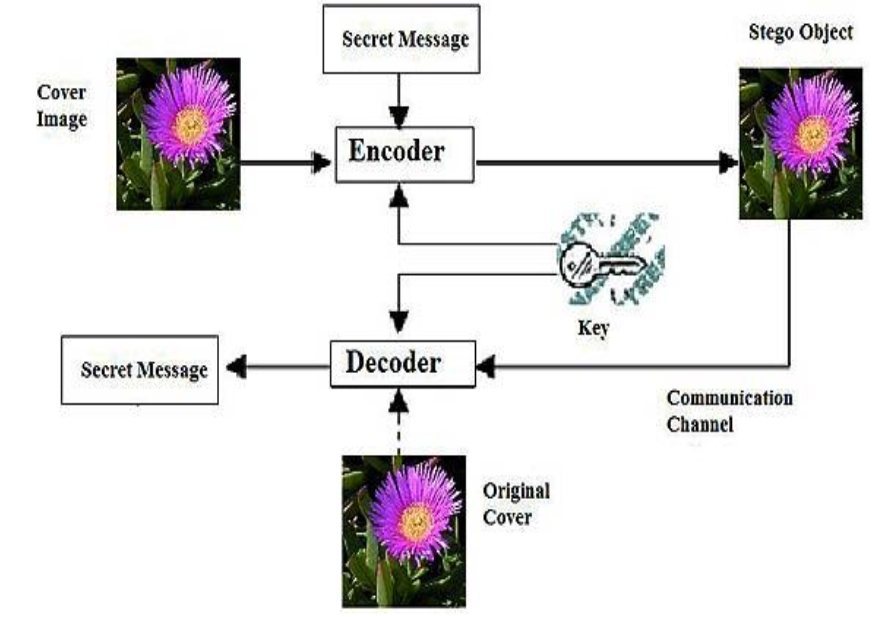
Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized used of the data set back to the user.

Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

**1.1 What is Steganography?**

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.



**BASIC IMAGE STEGNOGRAPHY MODAL**

**1.2 History of Steganography**

Throughout history Steganography has been used to secretly communicate information between people.

Some examples of use of Steganography is past times are:

**1.** During World War 2 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 are heated they darken and become visible to the human eye.

**2.** In Ancient Greece 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 secrete message.

**3.** During World War II, Velvalee Dickinson, a spy for Japan in New York City, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, and the concealed ”plaintext” was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman. During World War II, photosensitive glass was declared secret, and used for transmitting information to Allied armies.

4. Jeremiah Denton repeatedly blinked his eyes in Morse code during the 1966 televised press conference that he was forced into as an American prisoner-of-war by his North Vietnamese captors, spelling out ”T-O-R-T-U-R-E”. That conﬁrmed for the ﬁrst time to the US Naval Intelligence and other Americans that the North Vietnamese were torturing American prisoners-of-war. In 1968, crew members of the USS Pueblo intelligence ship, held as prisoners by North Korea, communicated in sign language during staged photo opportunities, to inform the United States that they were not defectors but captives of the North Koreans. In other photos presented to the US, crew members gave “the ﬁnger” to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

**1.3 Project Scope:**

This project is developed for hiding information in any image file. 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.

**1.3.1 Methodology:**

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.

This project has two methods – **Encoder** and **Decoder**

* In **Encoder** the secret information is hiding in with any type of image file.
* In **Decoder** is getting the secret information from image file.

**1.3.2 Limitations of the Software:**

This project has an assumption that is both the sender and receiver must have shared some secret information before imprisonment. Pure steganography means that there is none prior information shared by two communication parties.

**1.4 Project Requirement:**

**1.4.1 Software Requirements:**

* .**Visual Code Studio**
* **Anaconda 3**
* **Python 3.6.9 or Greater**

**1.4.2 Python Libraries Requirement:**

* **Numpy**
* **Pandas**
* **Opencv**
* **Pillow**
* **Tkinter**
* **SQLite**

**1.4.3 Hardware Requirements:**

* **Processor : Preferably 4.0 GHz or Greater.**
* **RAM : 4 GB or Greater.**