**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.

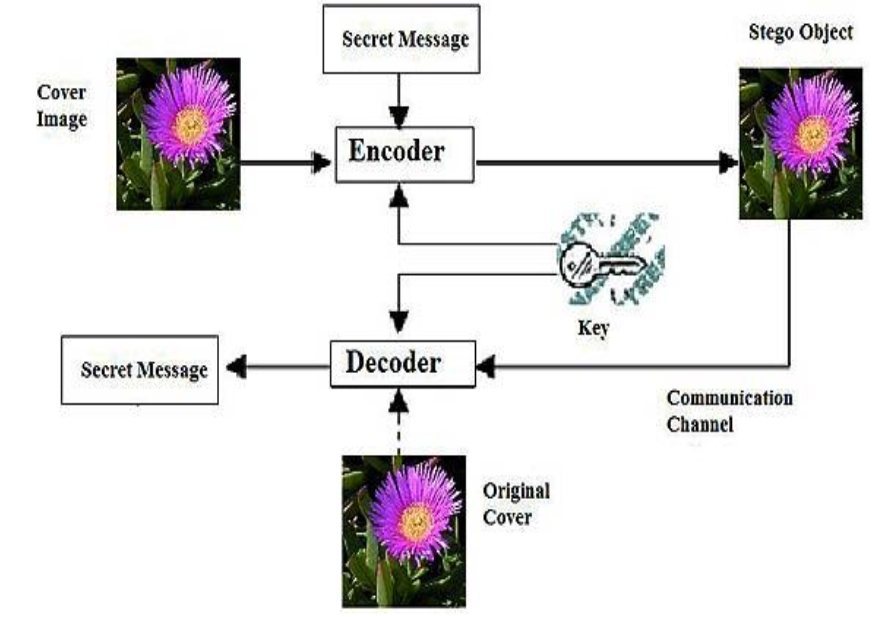
Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized used of the data set back to the user.

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.**

**CHAPTER 2**

**LITERATURE REVIEW**

**“Electronic communication is the lifeblood of many organizations.”**

Much of the information communicated on a daily basis must be kept conﬁdential. Information such as ﬁnancial reports, employee data and medical records needs to be communicated in a way that ensures conﬁdentiality and integrity. This makes good business sense and may even be regulated by legislation like the Health Insurance Portability and Accountability Act (HIPAA). The problem of unsecure communication s compounded by the fact that much of this information is sent over the public Internet and may be processed by third parties, as in e-mail or instant messaging (IM).

**2.1 Cryptography Basics:**

Cryptography can be used to provide message conﬁdentiality and integrity and sender veriﬁcation. The basic functions of cryptography are encryption, decryption and cryptographic hashing. In order to encrypt and decrypt messages, the sender and recipient need to share a secret. Typically this is a key, like a password, that is used by the cryptographic algorithm. The key is used by the sender to encrypt the message (transform it into cipher text) and by the recipient to decrypt the message (reverse the cipher text back to clear text). This process can be done on a ﬁxed message, such as an e-mail, or a communications stream, such as a TCP/IP connection. Cryptographic hashing is the process of generating a ﬁxed-length string from a message of arbitrary length. If the sender provides a cryptographic hash with the message, the recipient can verify its integrity. Modern cryptographic systems are based on complex mathematical relationships and processes. Let’s focus on the common cryptography standards used to secure computer communications and how they are used.

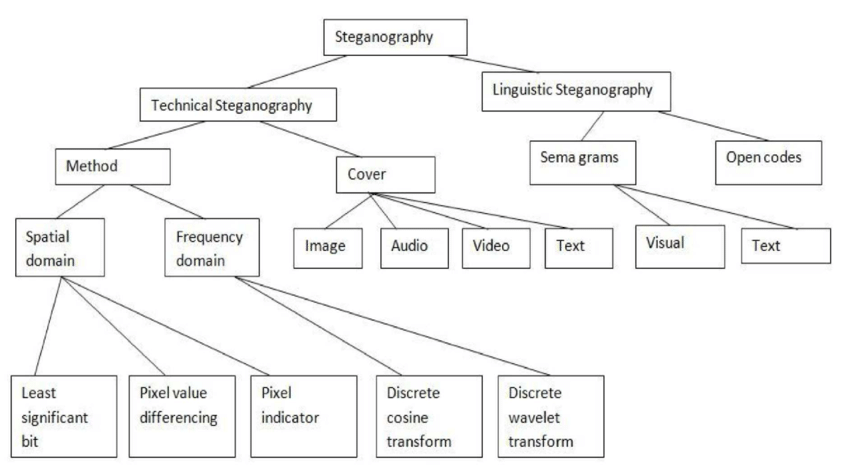
The three basic types of cryptography in common use are symmetric key, asymmetric (public) key systems and cryptographic hash functions. Typically, the strength of a crypto system is directly related to the length of the key. This assumes that there is no inherent weakness in the algorithm and that the keys are chosen in a way that fully utilizes the key space (the number of possible keys).

There are many kinds of attacks that can be used against crypto systems, but these are beyond our scope here. That said, if you use public algorithms with no known vulnerabilities, use reasonable key lengths (most defaults are ﬁne) and choose good keys (which are normally chosen for you), your communications will be very secure. Cryptography Drawbacks Apart from the four fundamental elements of information security, there are other issues that aﬀect the eﬀective use of information:

1. A strongly encrypted, authentic, and digitally signed information can be diﬃcult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
2. High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.
3. Another fundamental need of information security of selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
4. Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be ﬁxed through proper design and setting up of a defensive infrastructure.
5. Cryptography comes at cost. The cost is in terms of time and money 1. Addition of cryptographic techniques in the information processing leads to delay. 2. The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome ﬁnancial budget.
6. The security of cryptographic technique is based on the computational diﬃculty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

**2.2 Basics of Steganography:**

Steganography aims to hiding information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analyzing the information detection. Unlike watermarking, steganography does not intended to prevent the hidden in formation by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remains it undetectable. Steganography is particularly interesting for applications in which the encryption cannot used to protect the communication of conﬁdential information.



**CATEGORIES OF STEGANOGRAPHY**

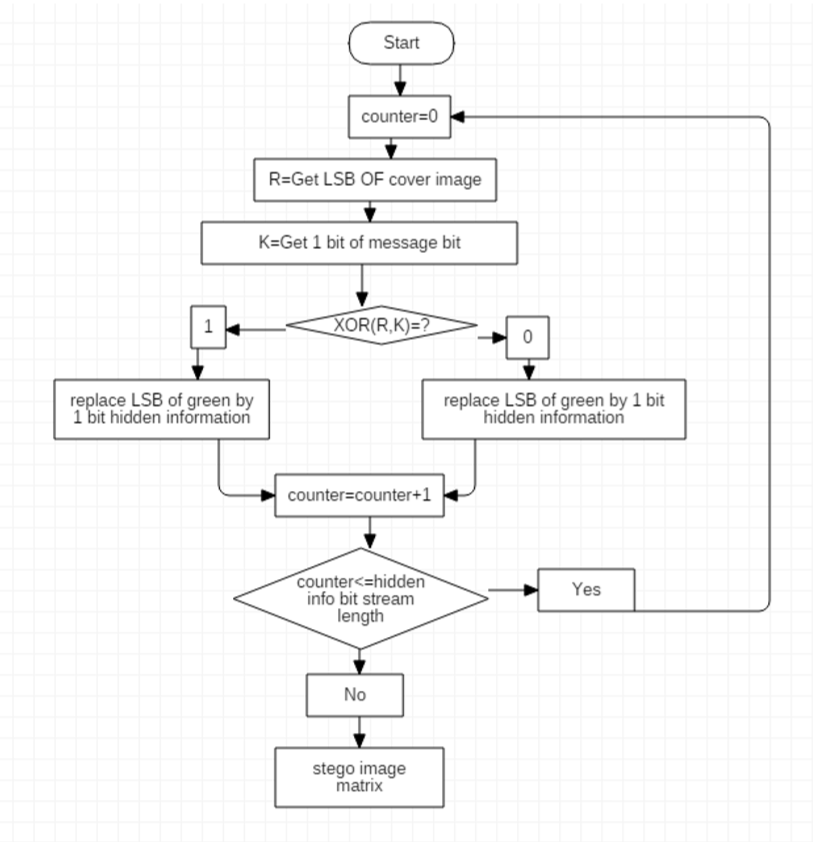
**2.2 Steganography methods used:**

**2.2.1 LSB (Least Significant Bit) technique:**

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by “3”. This helps in storing extra data. The Least Significant Bit (LSB) Steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a PNG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important Steganography techniques in use today.

* + - 1. **LSB (Least Significant Bit) Encoding Algorithm:**

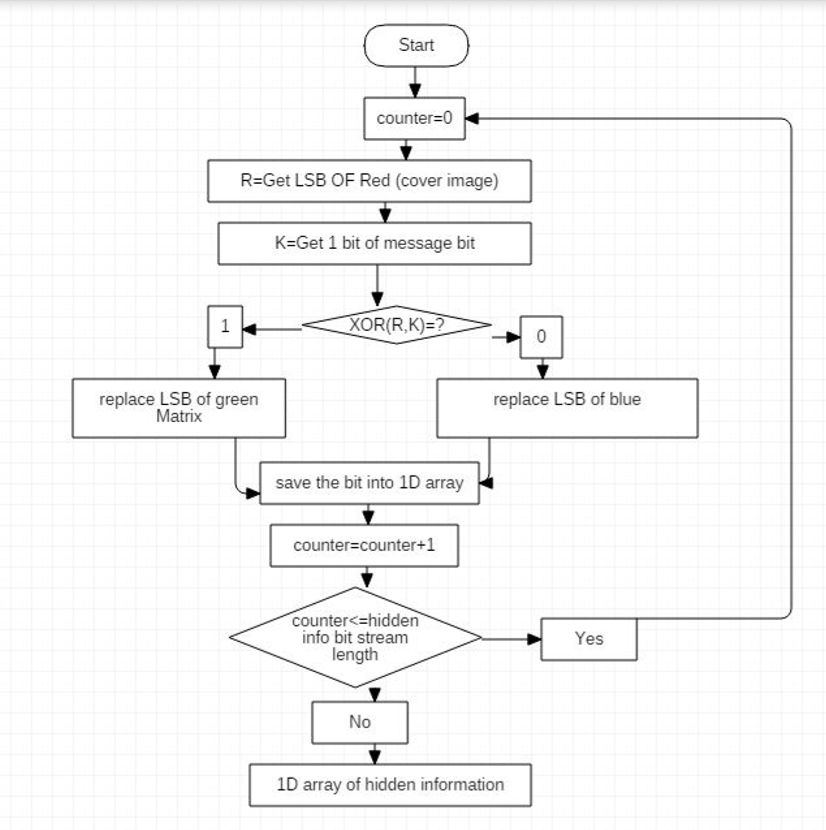
1. Choose an Image which is a RAW format image and can be used as a Cover Image or Vessel Image.
2. Take the secret text message and convert each character to ASCII code and the convert each digit into 8-bit binary code.
3. Take the 4-digit key provided by user or use 0000 as a default key and take a sum of digits and then covert whole digit of sum into 8-bit binary code.
4. Use binary coded key to perform the XOR operation with binary secret text message.
5. Access Image in a 2-D Matrix format and extract RED, GREEN and BLUE values from each pixel one by one. In case of gray scale image only gray value is present instead of RED, GREEN and BLUE.
6. In each Pixel, convert the values of RED, GREEN and BLUE in binary format.
7. In each color binary value right most bit is known as least significant bit; know extract single bit of binary text message and LSB bit from RED color binary value. If they both are equal then do nothing but when they are different replace LSB bit from RED color binary value with extracted single bit of binary text message.
8. Do the 7th step for GREEN and BLUE pixels values.
9. Convert RED, GREEN and BLUE binary values to decimal values and replace it with the original pixel.
10. Repeat the 6th, 7th, 8th, 9th steps until all the pixels values are not explored.

****

**LSB ENCODER FLOW CHART DIAGRAM**

* + - 1. **LSB (Least Significant Bit) Decoding Algorithm:**

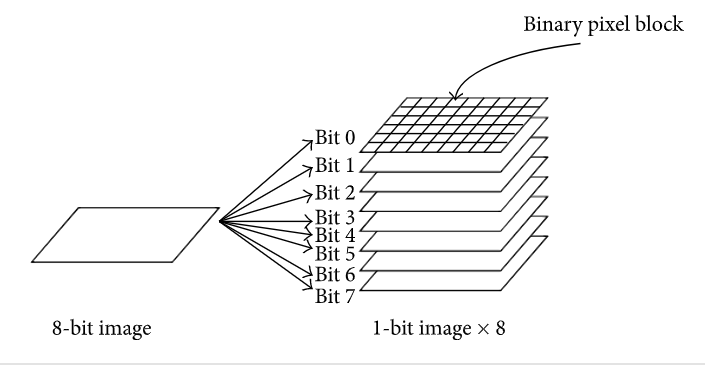
1. Choose an Image which is Steganographed by the sender and contains secret message.
2. Access Image in a 2-D Matrix format and extract RED, GREEN and BLUE values from each pixel one by one. In case of gray scale image only gray value is present instead of RED, GREEN and BLUE.
3. In each Pixel, convert the values of RED, GREEN and BLUE in binary format.
4. Know extract LSB bit from RED color binary value and store in a string variable.
5. Do the 4th step for GREEN and BLUE pixels values.
6. Repeat the 4th and 5th steps until all the pixels values are not explored.
7. Take the 4-digit key provided by user or use 0000 as a default key and take a sum of digits and then covert whole digit of sum into 8-bit binary code.
8. Use binary coded key to perform the XOR operation with each 8-bits of string variable and update the string variable.
9. Take the string variable and convert each 8-bits to a digit and covert that to characters as per ASCII code notations.
10. Now we have the secret text message in the string variable.

****

**LSB DECODER FLOW CHART DIAGRAM**

* + 1. **BPCS (Bit-Plane Complexity Segmentation) technique:**

BPCS Steganography was first put forward by Kawaguchi and Eason. The basic principle is that firstly cover image is divided into “informative region” and “noise-like region.” Then the secret information is hidden in noise-like blocks of cover image. In LSB technique, data is hidden in the lowest bit-plane. But in BPCS technique, data is hidden in pixel blocks of all the planes, from the highest plane (most significant bit, MSB plane) to the lowest plane (LSB plane), which have noisy patterns. In BPCS, a gray image consisting of bit pixels can be decomposed intobinary planes. For example,

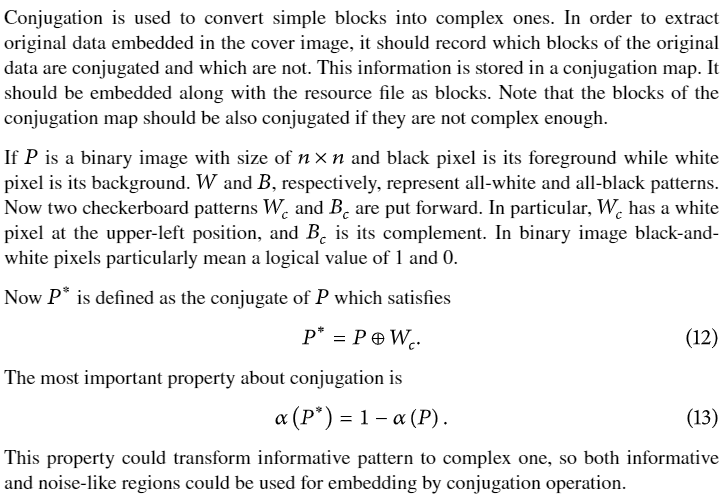


For example,  is a gray image; here. Therefore, where  is the MSB bit-plane and  is the LSB bit-plane. Each bit-plane can be segmented into “informative” region and “noise-like” region. It is simple in informative region and cannot be used for hiding information. However, it is complex in noise-like region and each noise-like region could be replaced with another noise-like pattern in BPCS. As a result, it will not change the overall quality of image after embedding. The most important step in BPCS is how to locate noisy regions in a cover image correctly. The regular method is to divide each bit-plane of the cover image into small square binary pixel blocks. The blocks are considered as noisy regions; those have complex black-and-white patterns. Often  is defined as a criterion to judge whether the block is complex or not:

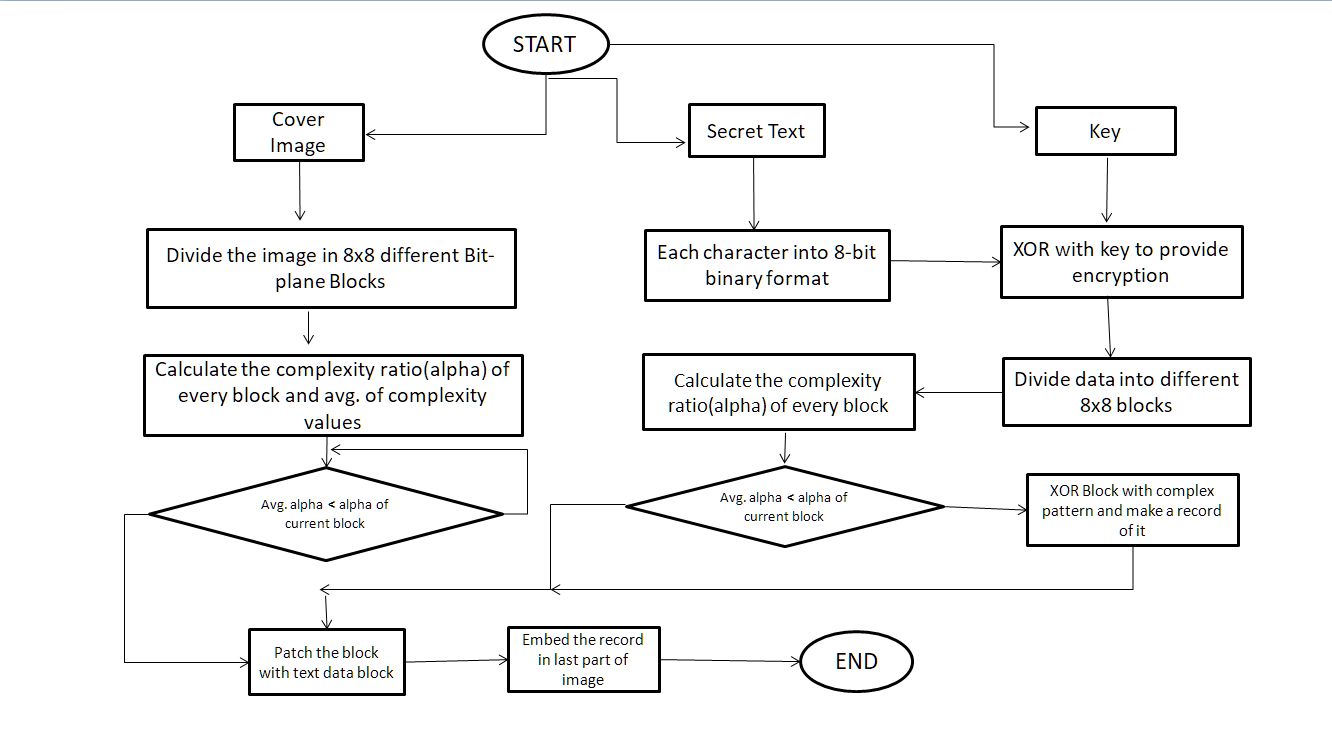
, (1)

Where the total length of border in a block is,  is the row or column of the block, and  is between 0 and 1. If  is higher than the given threshold value, then the block is regarded as complex.

**#Conjugation Operation**

****

**2.2.2.1 BPCS (Bit-Plane Complexity Segmentation) encoding algorithm**

1. Choose an Image which is a RAW format image and can be used as a Cover Image or Vessel Image.
2. Take the secret text message and convert each character to ASCII code and the convert each digit into 8-bit binary code.
3. Take the 4-digit key provided by user or use 0000 as a default key and take a sum of digits and then covert whole digit of sum into 8-bit binary code.
4. Use binary coded key to perform the XOR operation with binary secret text message.
5. If image is RGB then split the image in three channels RED, GREEN and BLUE.
6. Take a RED channel image and covert each pixel to binary format where each pixels value is represented by 8-bit of binary code.
7. Split the binary coded image to 8-bit binary planes where the most significant bit is and is the least significant bit.
8. Taking into consideration take plane and extract blocks. Then check value of If yes then jump to 9th step else extract a new block and re-check value of.
9. Now, also extract binary secret text message in blocks and check value of. If yes then replace the block of bit-plane image with the block of binary secret text message. Otherwise, conjugate the block of binary secret text and then replace it.
10. Make sure conjugation is noted.
11. Repeat 8th and 9th step for P1, P2 and P3.
12. Repeat 6th to 11th step for GREEN and BLUE pixels.
13.  Pack the channels into one image and secret message is coded to image.

**BPCS ENCODER FLOW CHART DIAGRAM**

**2.2.2.2 BPCS (Bit-Plane Complexity Segmentation) decoding algorithm**

1. Choose an Image which is Steganographed by the sender and contains secret message.
2. If image is RGB then split the image in three channels RED, GREEN and BLUE.
3. Take a RED channel image and covert each pixel to binary format where each pixels value is represented by 8-bit of binary code.
4. Split the binary coded image to 8-bit binary planes where the most significant bit is and is the least significant bit.
5. Taking into consideration take plane and extract blocks. Then check value of If yes then jump to 6th step else extract a new block and re-check value of.
6. Now, check if block is conjugated then re-conjugate that block and extract each bit sequentially in a string variable.
7. Repeat 5th and 6th step for P1, P2 and P3.
8. Repeat 3rd to 7th step for GREEN and BLUE pixels.
9. Take the 4-digit key provided by user or use 0000 as a default key and take a sum of digits and then covert whole digit of sum into 8-bit binary code.
10. Use binary coded key to perform the XOR operation with each 8-bits of string variable and update the string variable.
11. Take the string variable and convert each 8-bits to a digit and covert that to characters as per ASCII code notations.
12. Now we have the secret text message in the string variable.

**BPCS DECODER FLOW CHART DIAGRAM** 