

IMAGE STEGANOGRAPHY

Project report submitted in partial fulfilment of the requirement for the degree of

Bachelor of Technology
in

Information Technology

By

Arpit Tyagi (161473)

Vikas Singh (161463)

UNDER THE SUPERVISION OF

Monika Bharti Jindal

to



Department of computer science & engineering and Information technology
Jaypee University of information technology Waknaghat, Solan-173234
Himachal Pradesh

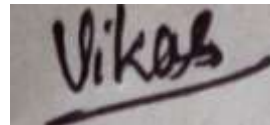
CERTIFICATE

I hereby declare that the work presented here in this report entitled “image steganography” in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Waknaghat are an authentic record of my own work carried out over a period from August 2019 to December 2019 under the supervision of **Monika Bharti Jindal** (Assistant Professor in the department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.



Arpit Tyagi (161473)



Vikas Singh(161463)

This is to certify that the above statement made by the candidate are true to the best of my knowledge.



Monika Bharti Jindal

Assistant Professor

Computer Science & Engineering and Information Technology Dated:December
2nd,2019.

ACKNOWLEDGEMENTS

I would like to thank everyone who had contributed to the successful completion of this project. I would like to express my gratitude to my final year project supervisor, Dr. Monika Bharti Jindal for her invaluable advice, guidance and her enormous patience throughout the development of the research.

In addition, I would also like to express my gratitude to my loving parents and friends who had helped and given me encouragement and support towards the final year project.

ABSTRACT

Steganography is the process of hiding the information that communication is taking place whereas Image based Steganography is the process of hiding the information in the input image. The main motive of this technique is to hide the important information byte by byte in an image pixels. The input image can be of any size but must be greater than the size of a input message. This process is usefull when we to send some important information to somebody without anybody else noticing the secret information. After the transmission the reciever should also use the same technique that was used for encoding to decode the message. This process hides the data in such a manner that there will be no noticeable changes in an image. It basically hides the existence of the data. Each and every byte of data is converted into its binary equivalent and then are processed to get stored in the iamge pixel. The language used for this process is python with some of its in-built libraries. For the image we use PIL(i.e. PYTHON IMAGING LIBRARY). Steganography usually deal with the way of hide the existence of communicated data in such a way that it remains confidential. It maintain secrecy between the two communicating bodies. Secrecy are achieved In the image steganography, by embedded data into the cover images and generating a **stego-images**.

Contents Chapter 1: INTRODUCTION

1.1 What are steganography..... 7

1.2 History..... 8

Chapter 2: LITERATURE REVIEW

2.1 Cryptography basics11

 2.1.1 Cryptography drawbacks 11

2.2 Steganography basics12

2.3 Steganography vs LSB algorithm.....13

Chapter 3: REQUIREMENT ANALYSIS

3.1 Non-functional requirements..... 14

3.2 System requirements15

 3.2.1 Software requirements15

 3.2.2 Hardware requirements15

Chapter 4: IMAGE STEGANOGRAPHY

4.1 Types of steganography.....16

 4.1.1 Text steganography.....16

 4.1.2 Image steganography.....16

 4.1.3 Audio steganography.....17

 4.1.4 Video steganography.....18

4.2 Steganography in image18

Chapter 5: HOW IT WORKS

5.1 Implementation.....20

 5.1.1 Technical details.....20

 5.1.2 The encoding process.....20

5.1.3 Creation of user space.....	20
5.1.4 The decoding process.....	21
Chapter 6: BRIEF ALGORITHM IMPLEMENTATION	
6.1 LSB (Least significant bit)	22
6.1.1 Embedding phase procedure.....	24
6.1.2 Masking and filtering.....	26
Chapter 7: SYSTEM DESIGN	
7.1 Use case diagram.....	27
7.2 Activity diagram.....	29
Advantages and disadvantages	31
Conclusion	32
References	33

Chapter 1 INTRODUCTION

What is Steganography?

The word stegano mean cover and graphical mean write. Thus Stegano and graphy both combine together to make the process in which we hide the important information inside the image using some encoding technique. This process not only hides the data it also hides the communication which means others will not known whether the communication is taking place or not.

Steganography is the secret process of which nobody can known of except the one who is encoding the secret message inside the image(i.e. Sender) and the other for whom the message is being encoded(i.e. reciever). In other words it is also known as the study of unperceivable communication.

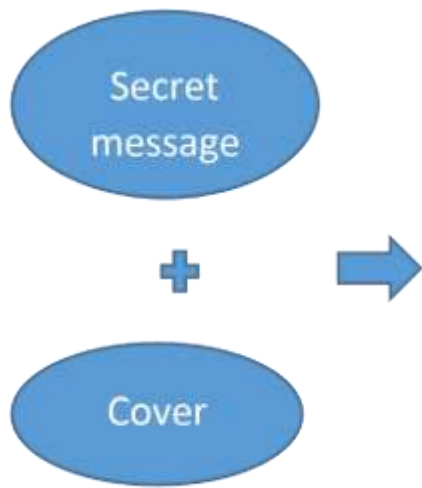
Steganography is the process in which the image is input by the user and after encoding it with the secret data a STEGO-image is generated. Which is slightly change from the original image but the difference in unnoticable.

In the current time, Steganography is used in many places and one of the important example is Army duty stations. This is the place where steganography is the only safe medium to use, because they don't want there secret information to be shared with the ones across the border.

Similar of this process can be seen back in the ancient times where the king use to bald his commander head so that he can write some information on it and hide it with something that doesn't generate any suspects.



Stego
image



Fi

The above pictured diagram can be summed up to image steganography. The secret message is the important information which user wants to hide. Cover is the image which will be used to hide the data. The algorithm used will combine these two and will generate a secret key without which nobody can access the information not even the reciever.

Applications of steganography

1. Confidential communication.
2. Protection of data alteration.
- 3.
4. E-commerce.
5. Media
6. Database system.
7. Digital watermarking.

HISTORY

The first record of steganography technique was recorded in 440BC. Aristagoras was sent by his leader Histiaeus, by shaving the head of his most trusted worker, writing the messages onto his scalp and sending him out after his hair was regrown. He was sent with full guidance of what to do, when he steps out from here.

Steganography principle

Secret message is covered into the cover of the object by a secret hiding algorithm and are sent to a receiver end. Then receiver applies the reverse acting process on the cover image and reveals the secret info.

The secret message is then covered into the cover image using the steganographic algo in a way that do not changes the actual image. The results are now into a new image, the stego-image, which is not different from the original image. From the third party view, but there exist a secret msg. The purpose of using image is of not important, it present only as a carrier for hidden msg. The secret message is embedded into the cover object by steganographic algorithm and are sent to a receiver ends. The receiver then performs the reverse action on the cover image by doing so it can achieve the secret data. The Suitable image, known the cover or carrier, are chosen. The secret message is then embedded inside the cover by using the steganographic algorithm, in a particular way that do not changes the original image info in any human visible way. The results are now in new image, the stegoimage, that are not viewed different from the original info.

Almost any file type can be used for this process, but the type that is more convenient are those having redundancy very large. The redundant bits of an target is those bit that could be altered without the visible changes. Image and audio files especially comply with this need. Since, images are quite famous cover or carrier target used for steganography. In the range of digital images many other image file format exist, For those different image file format, other steganographic algorithm exist The secret message is embedded into the cover object by steganographic algorithm and are sent to a receiver side. The receiver then performs the reverse action on the stego image and reveals the secret info. The embedding, i.e. steganography algorithms, tries to save the perceptible type of the original images. The Suitable image, known the cover or carrier, are chosen. The secret message is then embedded inside the cover by using the steganographic algorithm, in a particular way that do not changes the original image info in any human perceptible way. The results are new images, the stego-image, that are not viewed different from the original info. From an observer's view, the being of a secret message are (visibly) out of sight. The purpose of using image is of not importance, it serve only and only as a carrier for out of sight message

Basic Steganography Model

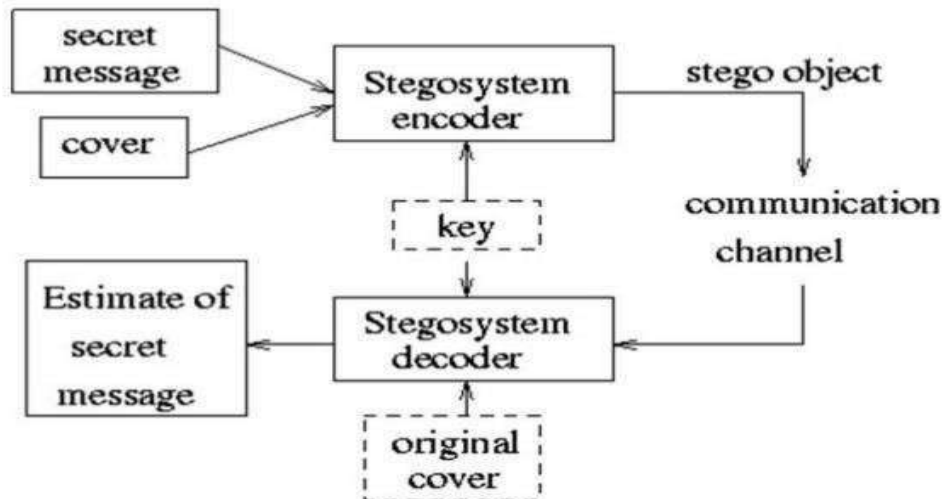


Fig: (ii) steganography model

Summary: The first task is to open the software. In our case this software asks for authentication so every user have to enter there username and passwords for the security purpose. If the id-pass matches.

Four options get available in-front of user as :

1. Input the message.
2. Input the cover-image.
3. Generate a stego-image.
4. Generate a secret key.
5. Send image to the receiver.
6. Abort.
7. Help.

A use case diagram helps the devloper to know how the user will interact with the software. First user enters the secret message that he/she wants to share anonymously. After this he/she inputs the picture and after validiating the image size and data size information gets covered up inside picture and a stego image is generated. At the other end(i.e. receiver's end), receiver gets the stego-image(i.e. generated image) and applies the reverse formula it. After that only the secret content could be achieved.

Chapter 2: LITERATURE REVIEW

Electronic communications are the lifeline of many organisation.

So to keep our lifeline in good hands we need to keep Most of the information communicated on the daily basis private. Information such as financial report and data of an employee need to be transferred in a way that ensure privacy.

2.1 Basics of Cryptography

Cryptography is the process in which user try to communicate secretly in front of the adversaries. In cryptography except encoding and decoding the most important feature is cryptographic hash. In order to encode the secret message by the sender and to decrypt the secret message by the receiver they both should use the same secret key which was generated by the algorithm. This could be done on any messages that user wants to share secretly, such as sending e-mail privately. Hashing in cryptography is a processes of generating a fix length strings from a user entered message.

The three basic type of cryptography most common useds are cryptographic hash function, asymmetric keys system and Symmetric keys ,the strengths of cryptographic system are directly proportional to the length of the key. This clears the fact that the key was picked randomly each and eveyr time the user enetr the secret data. There are many kind of attack that could be used against a cryptographic systems.

Cryptography drawbacks

- A strong encrypt, authentic, and digitally signed information could be difficult to access even for a legitimates user at a crucial time of decisionmaking. The systems or the PC frameworks could be assaulted plus rendered non-utilitarian by an mediator.
- High availabilities, one of the fundamental aspect of information security, could not be ensured through the uses of cryptographic techniques. Different strategies is expected to make preparations for the danger, for eg, forswearing of administration or complete breakdowns of data framework.
- Other than the cryptographic algorithm we need to get the administratice security to guard the system..
- Cryptography is the process which helps us in sending the secret data privately but does not guard us from the bad system vulnerabilities.

Basics of Steganography

Steganography mainly aims to hide secret data into a cover image which was input by the user in such a way that no third party will be able to detect the presence of communication by just viewing the image. This process is way different than watermarking, In this process we convert the every bit of input message into its binary equivalent and then iter through each pixel and change that value according to the corresponding binary value of the message.

Secret message is covered into the cover of the object by a secret hiding algorithm and are sent to a receiver hand. Then receiver apply the reverse acting process on the cover info and reveal the secret info.

The important secret message entered by the user is then covered with the image which is also input by the user and then using the steganographic algorithms in a way that do not change the actual image when viewed by some third party. The results are now into a new image, the stego-image, that are not view different from the original image but carries a very important information. the existence of a secret message is visibly only to the receiver when the secret key is entered correctly. The purpose of using image is of no important, it present only as a carrier for hidden msg, like an envelope. The secret information is embedded into the cover image by steganographic algorithm and then sent to the receiver. The receiver then performs the reverse action on the cover image and reveals the secret message.

Almost any file type could be used for steganography, but the type that is more suitable are those with a large degree of redundancy. Redundancy could be known as the bit of an target that provide correct far greater than important for the object's use and display. The redundant bits of an target is those bit that could be altered without the alteration being known easily. Image and audio files especially comply with this need, while research had also open other file type that could be used for info hiding. There are four main type of file formats that could be used for steganography. Since, images are quite famous cover or carrier target used for steganography. In the range of digital images many other image file format exist, most of them for particular applications. For those different image file format, other steganographic algorithm exist. The secret message is embedded into the cover object by out of sight algorithm and are sent to a receiver side. The receiver then performs the reverse action on the cover info and reveals the secret info. The embedding, i.e. steganography algorithms, tries to save the perceptive type of the original images. The Suitable image, known the cover or carrier, are chosen. The secret message is then embedded inside the cover by using the steganographic algorithm, in a particular way that do not changes the original image info in any human perceptible way. The results are new images, the stego-image, that are not viewed different from the original info. From an observer's view, the being of a secret message are (visibly) out of sight. The purpose of using image is of not importance, it serve only and only as a carrier for out of sight message.

2.3 STEGANOGRAPHY VS LSB ALGORITHM

Byte of each pixel holds one messages bit. Rest of the bit in the pixel continues as before. Steganography is the secret process of which nobody can know of except the one who is encoding the secret message inside the image(i.e. Sender) and the other for whom the message is being encoded(i.e. reciever). In other words Steganography is also known as the study of unperceivable communication.

The term steganography are gotten from Greek and true implies secure composing. Steganography system consist of three elements: **COVER-IMAGES**, **THE SECRET MESSAGES** and the **STEGA-IMAGE**.

Digital image are described using a 2-D matrices of the colours intestines at each grid points. Typically, grey image use 8-bit.

Chapter 3: REQUIREMENT ANALYSIS

3.1 FUNCTIONALS REQUIREMENTS

The ways in which the system works:

- Login. Login function will help the system in order to check both the receiver and sender authenticity, if the entered detail is correct the system will move to encoding phase otherwise it will exit from the system.
- Secret information: In this process the sender have two options whether it could upload the secret data file or it could write it.
- Cover image : cover image is the image which is chosen for the process, in this the secret message will get hidden.
- Sender: The person who wants to send the secret infromayyion to someone with the help of steganographic system.
- Receiver : Receiver receives the stego image and after system validates the autheticity it opens the option for decrypting the image to get the hidden text inside that stego-image.

3.2 NON-FUNCTIONAL REQUIREMENTS

- **Safety requirements:**

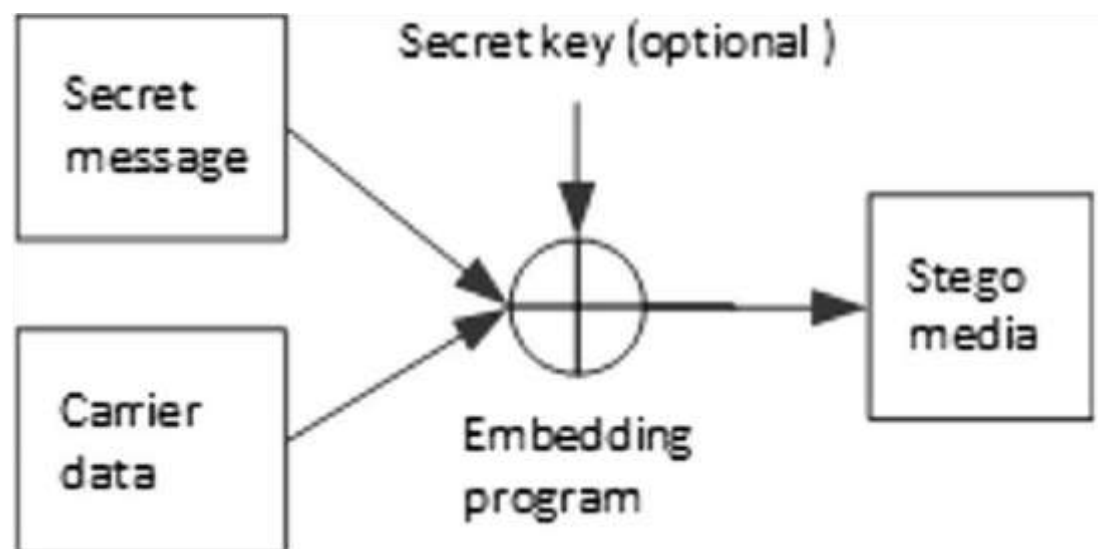
For the safety purpose the sender and receiver should have the same software to encrypt an decrypt the message and the secret key generated by the algorithm should not be shared with other than the receiver.

- **Security requirements:**

As the software hides the secret information so it should not get into wrong hands.

- **Software quality attributes:**

The quality of the software is a very important issue which maintained in such a way that the communication can only be take place with the help of image between sender and receiver.



3.3 SYSTEM REQUIREMENTS 3.3.1 SOFTWARE REQUIREMENTS

- Bootstrap.
- OS: Windows 10.

3.3.2 HARDWARE REQUIREMENTS

- Minimum hardware requirements: Pentium 3166 HZ or Higher 128 mb RAM
- Intell I7 4.80 GHZ 8GB Ram

Chapter 4: IMAGE STEGANOGRAPHY

4.1 Types of steganography

4.1.1 Text steganography

This is a method in which we hide the secret information inside the other text file, the main motive in this process is to share our secret information with the help of another normal message which doesn't get suspicious. .

There are a lot of strategies which is accessible for embedding information in text file. Text steganography could be achieved by changing some text organizing, or by adjusting quality of several component. The goal into develop a coding method that is reliably decode able yet largely different to the reader point of view. The three coding technique that we propose illustrate different approaches rather than form an exhaustive list of documents marketing technique. This technique could be used either separately or joint. These are as follows:

- **Word-move coding:** This is a method in which a changing of record is done by a level plane relating the words area inside the content line to encoded the report perfectly.
- **Line-move coding:** This is a technique in which we change a record by vertically moving the content line areas to encoded the archive extraordinarily.
- **Feature-coding:** This is a method in which we either apply to a format file 'r' or to a bitmaps images of a file.

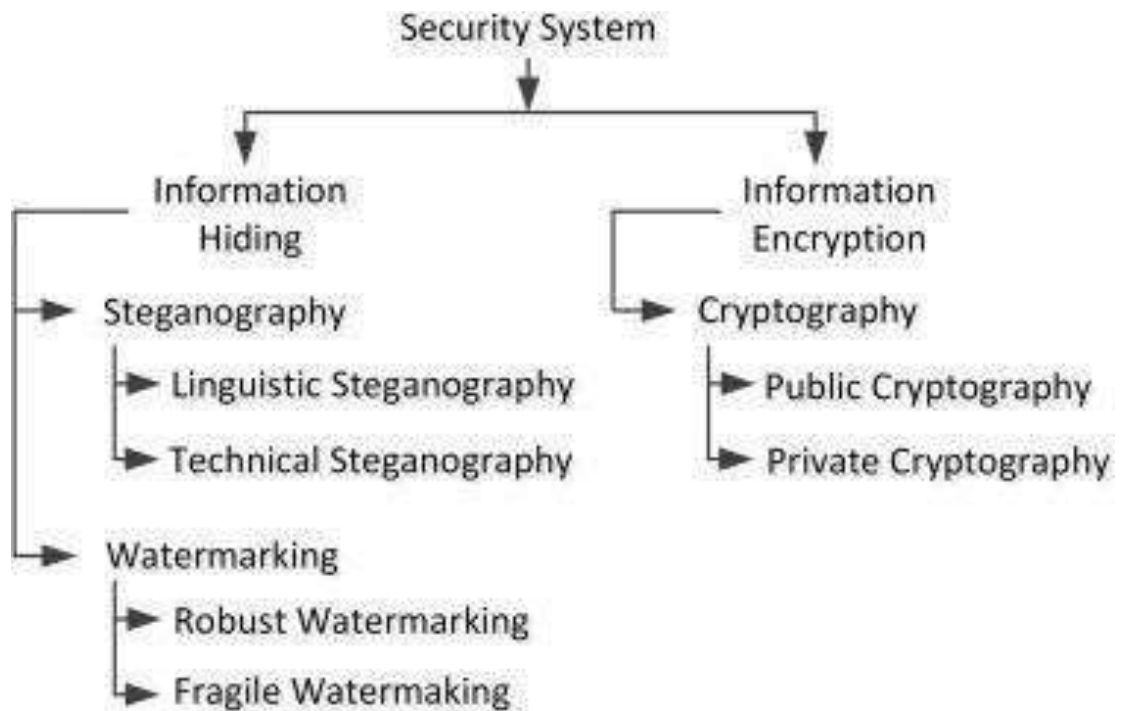


Fig – (iv) security system

4.1.3 Audio steganography

In sound steganography, we insert mystery message into digitized sound sign which output slight modifying of double grouping of the relating sound document. There are a few strategies are accessible for sound steganography. We will have a short report presentation on some of sound. It includes concealing knowledge in sound documents. This techniques shrouds the information in WAV, AU and MP3 sound records. There are many type of strategies for sound steganography. These techniques are:

1. Lower bit encoding.
2. Phase en-coding.
3. Spread spectrums.

4.1.4 Video steganography

It is a method of steganography in which we hide the secret information inside the video file. In this discrete cosine transform is used to alter the digit which are used to hide the info in each of the image in the videos, which can only be detected by some software but is unnoticeable by the human eye.

Configurations utilized by video steganography are Mp4, MPEG, AVI.

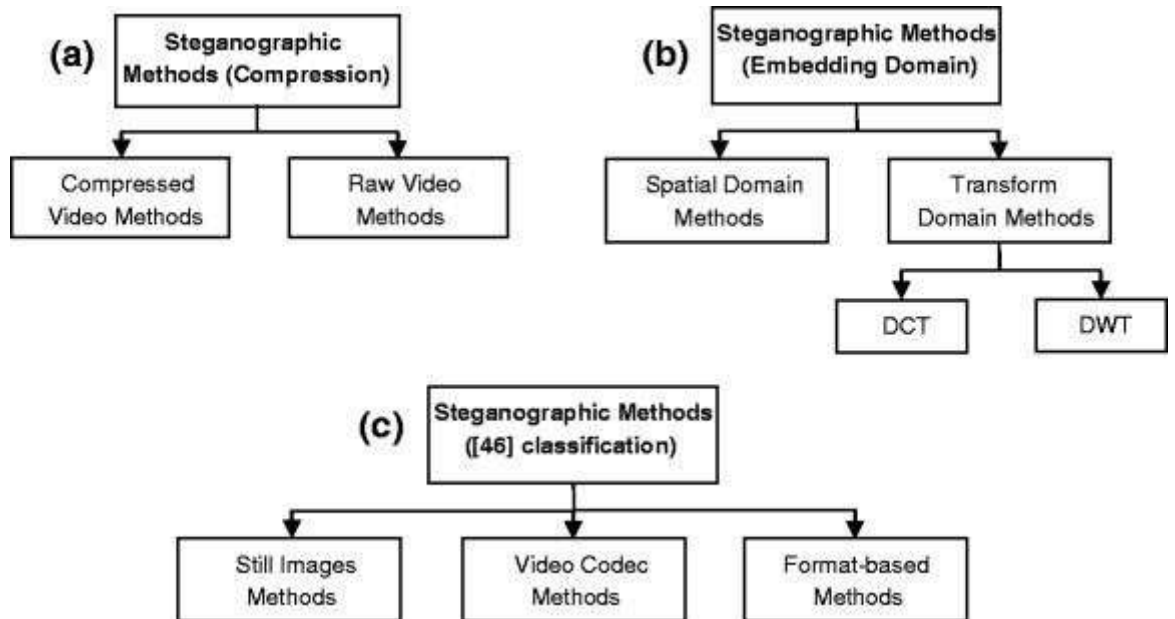


Fig – (v) compression and embedding domain

4.2 STEGANOGRAPHY IN IMAGES

Storing data inside picture is a famous procedure these days. An image with a mystery message inside is spreading over the WWW very fast. The utilization of steganography in source group had been inquired about by German Stenographic master Niels provos, he made a calculating bunch which recognize the nearness of shroud message inside picture that was posted on the net. In any case, subsequent to check one million pictures for info, no one concealed message was found, so the very down utilization of steganography still are by all accounts constrained. Image steganography is the procedure for storing the data inside the picture so that it doesn't get showed up to unintended client from the recognition of the shrouded messages or information. To hide a message inside a picture without changing its properties in such a manner that it can't get noticed, the source should be maintained in loud areas with many varieties, so that less consideration will get attracted to the alteration. The most widely recognized techniques is LSB to change on the spread picture. These systems could be utilized with fluctuating degrees of accomplishment on various types of image record. Image steganography is performed on images and the concerning

secret data which is likewise unscrambled to recover the message picture. Since this should be possible in a few different ways, picture steganography are contemplated and one of the strategies are utilized to show it. Picture steganography alludes to concealing data. The present undertaking means to utilize steganography for a picture with

another picture utilizing spatial space strategy. This shrouded data could be recovered uniquely through legitimate translating procedure.

Chapter-5 : HOW IT WORKS

5.1 Technical details are as follows:

Using python imaging library (PIL) for importing the image inside the compiler.

- 1) from **PIL** import **IMAGE**.
- 2) **img=image.open(path)**.
- Interfaces is build into the packages contain all the required classes and method which is necessary for any changes made in the image.

5.1.2 The encoding phase

The steganography's method performed in LSB coding. The offset of the cover-image which has to perform is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next bytes, the encoding process gets started to hide the secret information. For this process, the first task will be to get the input carrier files which have to perform for the process.

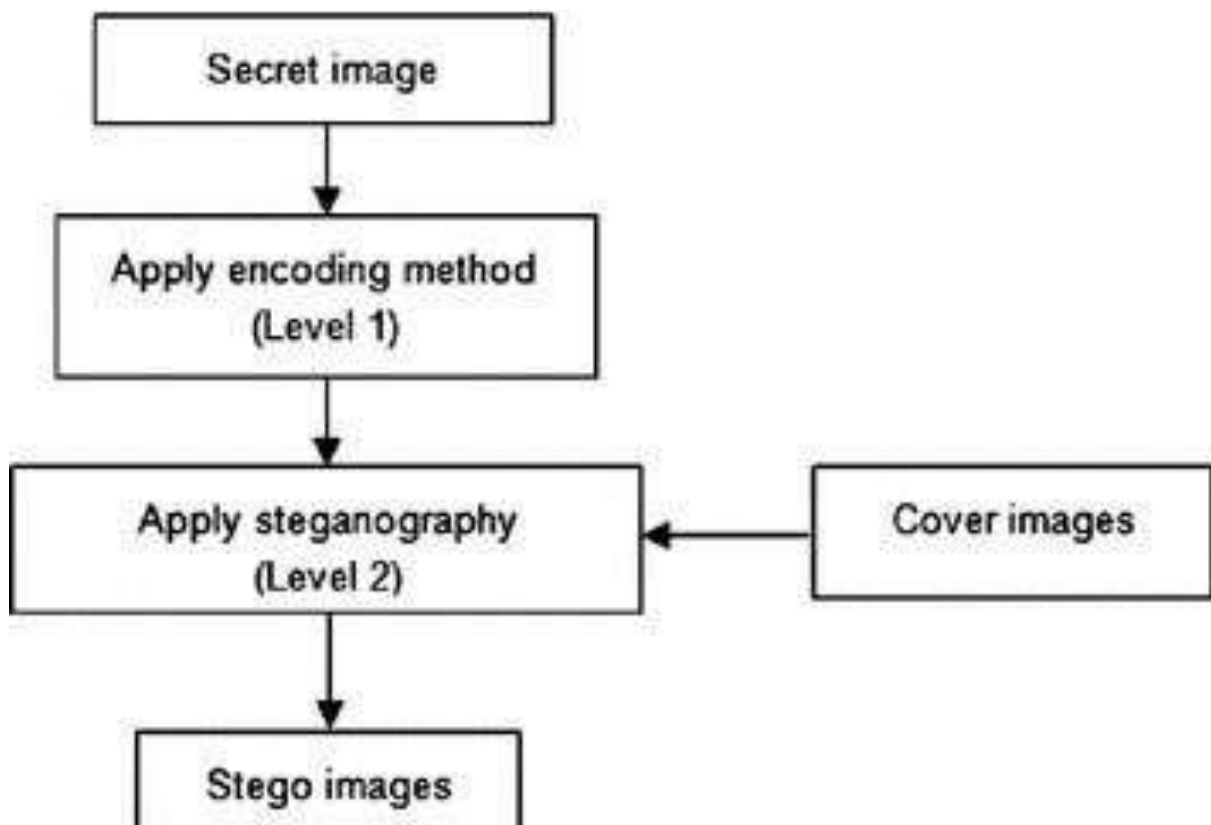


Fig: (vi) encoding process

5.1.3 User spaces

- User spaces are created in order to save the original files, So that all the changes which are necessary is done in this.
- In the object of I/p Image, using `img=image.open(path)` methods we took the original image.

5.1.4 The decoding process

The offset of the image are retrieved from its header. Create the user space using the same process as in the encoding. The data of image are taken into byte array. And above byte array are written into the decoded text file, which leads to the original mess

age.

Chapter 6: BRIEF ALGORITHM IMPLEMENTATION

6.1 LSB (Least significant bit)

There are two kinds of method for the process of image steganography:

- Transform method
- Spatial method

The method we used is Spatial method

In this process, the one of most commonly used method are LSB substitution methods. LSB methods are a very easy way in order to put data in a cover image for the process. In steganography, LSB substitute form are mostly used. Since every images has three component (RED, GREEN, BLUE). This pixel info is then saved in original format in one bytes each. The 1st bit store secret info for each and every pixel could be changed to store the hidden info.

The secret information has to be the same size as of the image or it can be smaller also. The (LSB) based method is a spatial methods But when we talk about noise deduction technique this method is vulnerable. The (most significant bit) of the data images is to be stored in the LSB of the images(i.e. cover images.) It are true that the pixel in an image is store in the form of bit.

The change could not be detect by human visuals system (HVS) w.r.t intensity and color of a pixels. When we change the LSB bits. Algorithms of LSB methods of

steganography, embedding phases and extracting phases these are two phase of LSB method. Algorithms are given below for both of the phases:

ENCODING PHASE:

Step 1: Array name (image_array) store all the pixel from the i/p image and extract **Step2:**

Array called (message_array) save text files of all extract message.

Step3: Character retrieved from the stego-keys is to be saved in an array called key_array. A stego- key or secret key is the pair of alphabets or numbers which is used to prove the authenticity of the user. This key is generally with sender and receiver only.

Step4: From keys-array the first pixel and character is used and gets placed in the first component of the image pixels. If there is some left characters in keys-array, then it also gets placed into the LSB of upcoming pixel.

Step5: The end of the key is filled with with some digit that is either even or odd depending upon the value.

Step 6: place each word of the message array in each components of upcoming pixel by replacing it.

Step 7: Repeat step six until all the words gets placed.

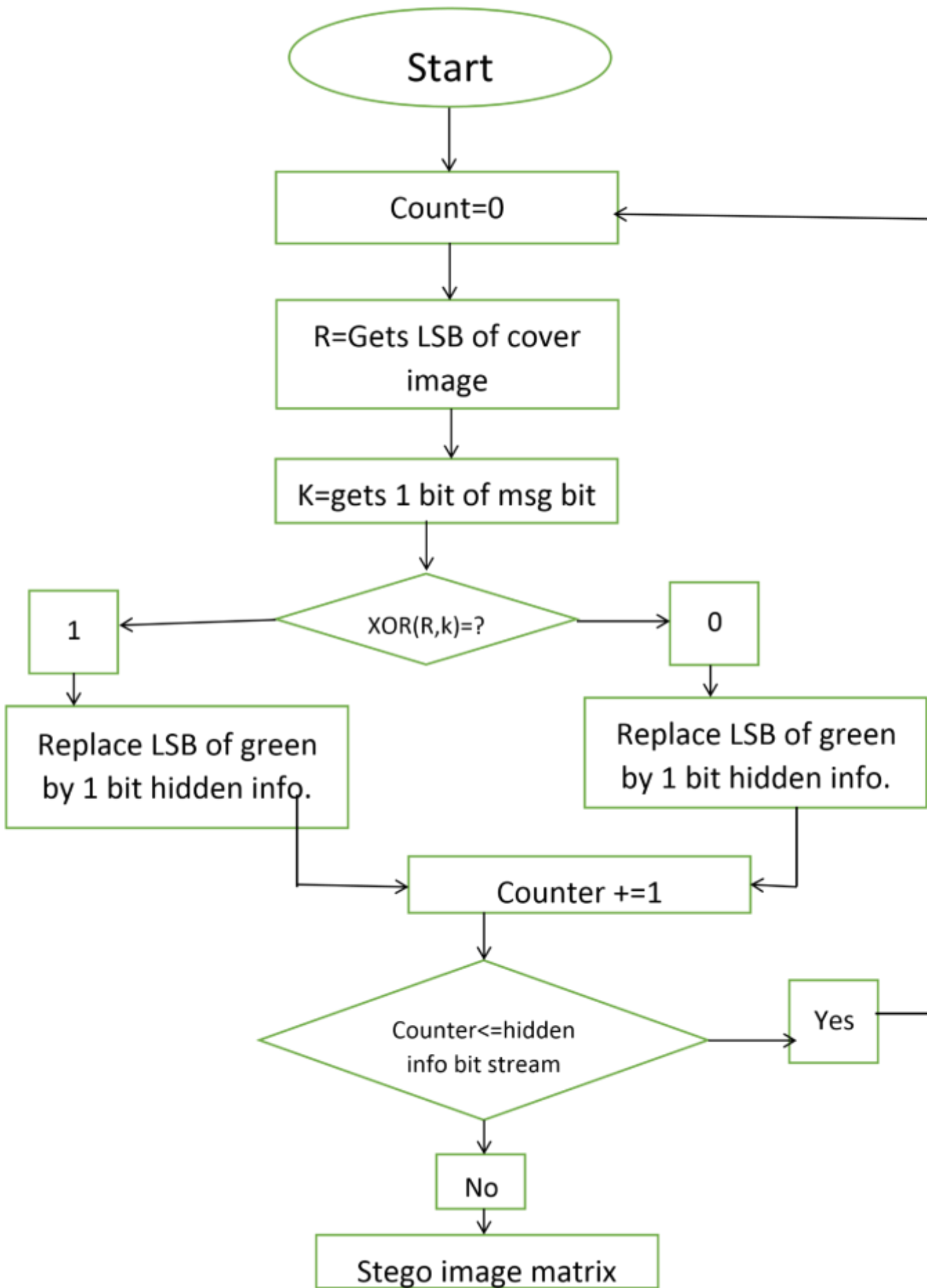
Step 8: Again if it ends the place some encoding symbol to indicate end of the character.

Step 9: All the i/p character will be hide after the process done. The most straightforward steganography procedures insert the bit of the message legitimately into least huge piece planes of the spread pic in a deterministic succession. Balancing the least noteworthy piece do not bring about human-recognizable distinction on the grounds that the sufficiency of the changes are little. To shroud a mystery message inside a pic, a legitimate spread picture are required. Since this strategy utilizes bits of every pixel in the picture, it is important to utilize a lossy pressure position, generally the shrouded data will become mixed up in the change of a loosy pressure calculation. When using a 24 piece shading pic, a touch of every single one of the red, green and blue shading part can be utilized, so an aggregate of 3 bit can be put away in every pixels. For instances, the accompanying matrices can be consider as 3 pixel of a 24 piece shading pic, utilizing 9 byte of main memory.

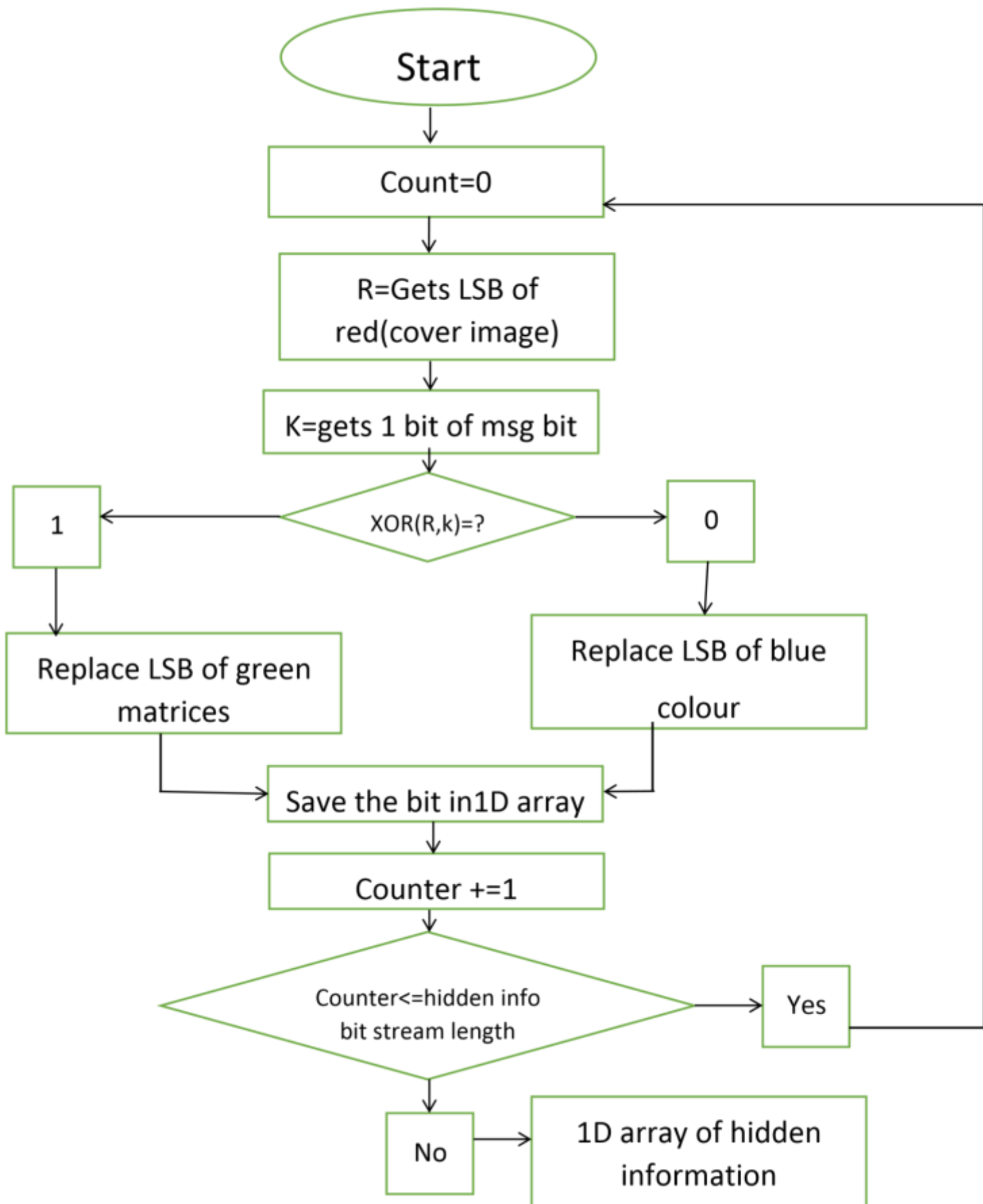
```
(00100111 11101001 11001000)    (00100111  
11001000 11101001)  
                (11001000 00100111 11101001)
```

When the character H, which binary value equals 01101000, are inserted, the following

```
(00100111 11101000 11001000)  
(00100110 11001000 11101000)  
(11001000 00100111 11101001)
```



Fig(vii)activity diagram(i)

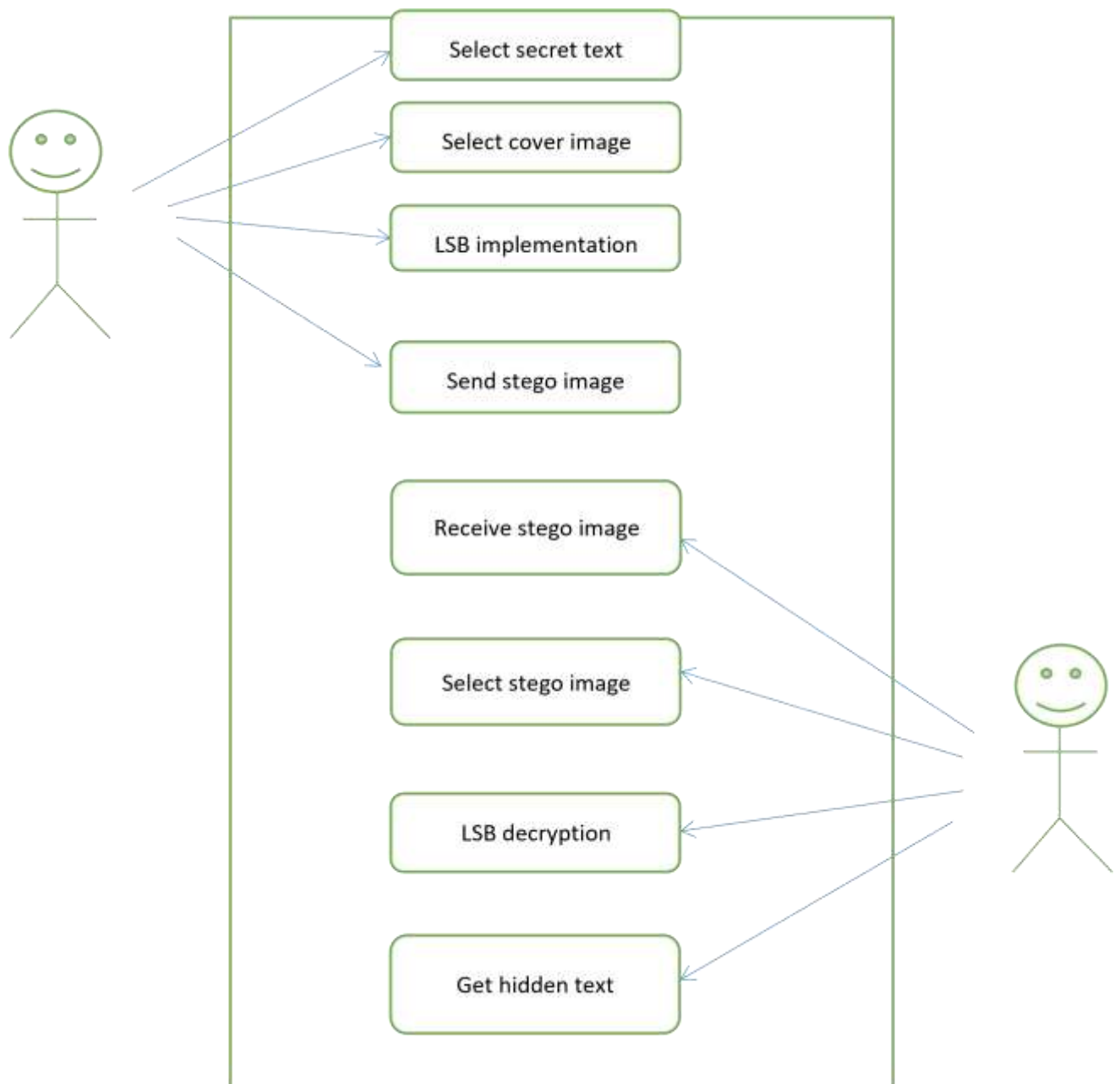


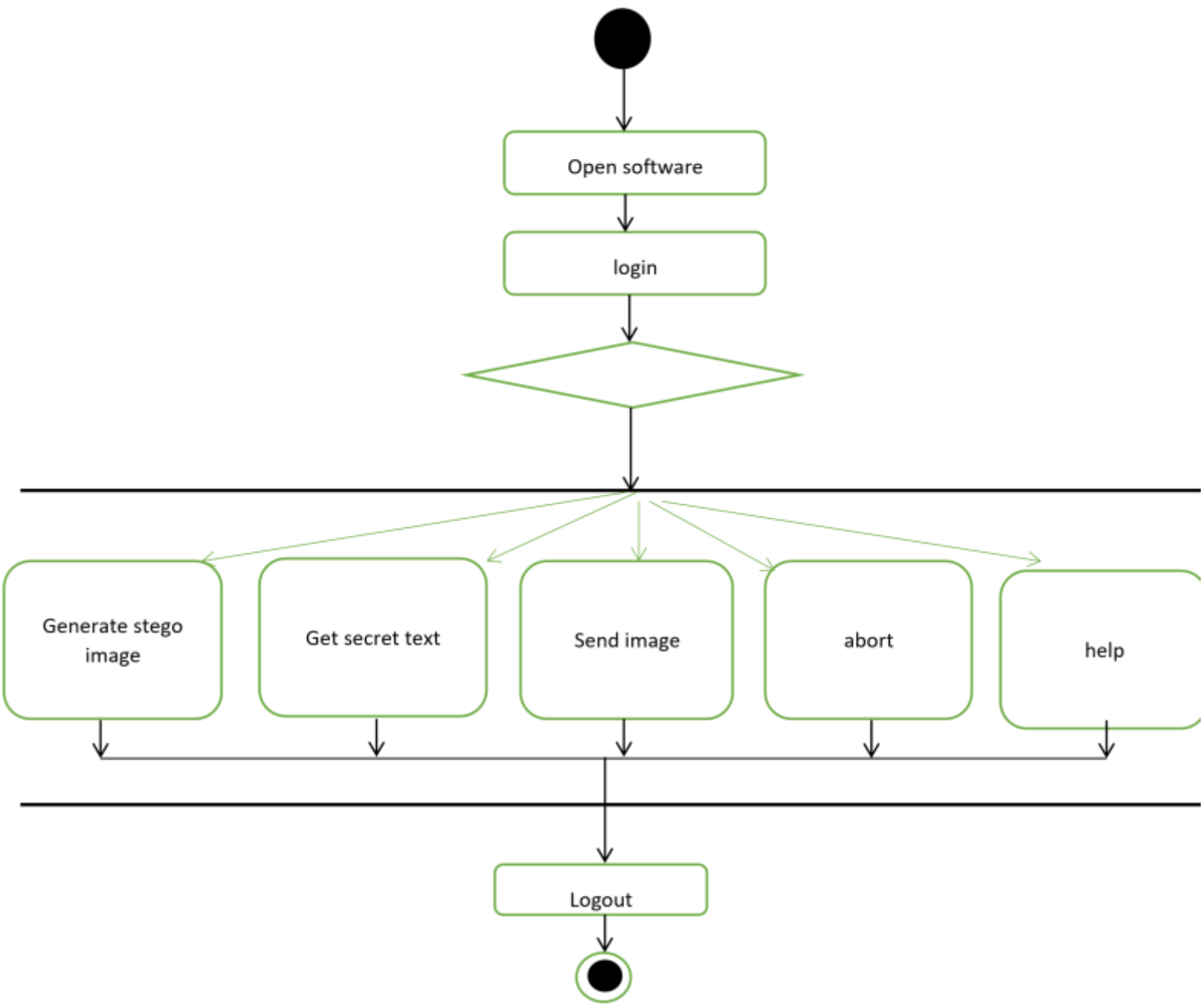
6.1.2 Filtering and masking method

In this method we normally iter through each pixel and change it according to the corresponding message bit such that the cover image doesn't change in a noticeable manner, the last pixel of each word is made odd and even respectively in order to know the ending of each and every word in an image. In this method the main motive is to hide the data in such a manner that the tiny change in the color of the image is not visible by the third party. In other words the image should look like the old image itself.

Chapter 7: SYSTEM DESIGN

7.1 Use case diagram





Advantages of steganography

- Difficult to detect by someone who doesn't know about this communication, whether the transaction is taking place or not.
- In order to view the hidden message user should have to enter the secret key which was generated using the steganographic algorithm.
- Easy to implement with the help of LSB algorithm.
- Can be used in arm forces and intelligence agencies.

Disadvantages of steganography

- Sender and receiver should have the same software to encrypt or decrypt message.
- If encryption key is lost, then important information will be lost too.
- The cover image used should have size greater than the message bytes.
- Hidden information can be viewed by attackers if proper encryption algorithm used.

- Encryption may effect luminance of the cover image.

Conclusion

- Steganography is still in its nascent age.
- The importance of steganography has not been noticed yet, where it is preferred over all its close rival for “Encryption”.

It is analysed that time is not far away when the importance of steganography would be realized by organizations and the arm forces in particular. Until then New technique are being discovered and implemented.

-

References

1. Fridrich, Jessica; M. Goljan; D. Soukal (2004). "[Searching for the Stego Key](#)" (PDF). Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. Security, Steganography, and Watermarking of Multimedia Contents VI. **5306**: 70– 82. [Bibcode:2004SPIE.5306...70F](#). Retrieved 23 January 2014.
2. Pahati, OJ (2001-11-29). "[Confounding Carnivore: How to Protect Your Online Privacy](#)". *AlterNet*. Archived from the original on 2007-07-16. Retrieved 2008-09-02.
3. [^] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "[Information Hiding: A survey](#)" (PDF). *Proceedings of the IEEE*. **87** (7): 1062–78. [CiteSeerX 10.1.1.333.9397](#). doi:10.1109/5.771065. Retrieved 2008-09-02.
4. [^] "[Polygraphiae \(cf. p. 71f\)](#)" (in German). *Digitale Sammlungen*. Retrieved 2015-05-27.
5. [^] [The origin of Modern Steganography](#)
6. [^] Cheddad, Abbas; Condell, Joan; Curran, Kevin; Mc Kevitt, Paul (2010). "Digital image steganography: Survey and analysis of current methods". *Signal Processing*. **90** (3): 727– 752. doi:10.1016/j.sigpro.2009.08.010.
7. [^] [ww31.slidefinder.nethttp://ww31.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218](#). Retrieved 2019-09-17.
8. [^] [Secure Steganography for Audio Signals](#)
9. [^] Cheddad, Abbas; Condell, Joan; Curran, Kevin; Mc Kevitt, Paul (2009). "A skin tone detection algorithm for an adaptive approach to steganography". *Signal Processing*. **89** (12): 2465– 2478. doi:10.1016/j.sigpro.2009.04.022.
10. [^] Akbas E. Ali (2010). "[A New Text Steganography Method By Using Non-Printing Unicode Characters](#)" (PDF). *Eng. & Tech. Journal*. **28** (1).
11. [^] Aysan, Zach (December 30, 2017). "[Zero-Width Characters](#)". Retrieved January 2, 2018. *In early 2016 I realized that it was possible to use zero-width characters, like zero-width non-joiner or other zero-width characters like the zero-width space to fingerprint text. Even with just a single type of zero-width character the presence or non-presence of the non-visible character is enough bits to fingerprint even the shortest text.*
12. [^] Aysan, Zach (January 1, 2018). "[Text Fingerprinting Update](#)". Retrieved January 2, 2018.
13. [^] T. Y. Liu and W. H. Tsai, "A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique," in *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 24-30, March 2007. doi: 10.1109/TIFS.2006.890310 [1]
14. [^] Dachis, Adam. "[How to Hide Secret Messages and Codes in Audio Files](#)". *Lifehacker*. Retrieved 2019-09-17.

for_plagiarism_2.docx

ORIGINALITY REPORT

11%

SIMILARITY INDEX

8%

INTERNET SOURCES

1%

PUBLICATIONS

8%

STUDENT PAPERS

PRIMARY SOURCES



www.slideshare.net

Internet Source

6%



eprints.uthm.edu.my

Internet Source

1%

[Submitted to Oxford & Cherwell Valley College](#)

Student Paper

1%



[Submitted to Christ University](#)

Student Paper

1%

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date:15/07/2020.....

Type of Document (Tick): PhD Thesis M.Tech Dissertation/ Report B.Tech Project Report Paper

Name: ARPIT TYAGI Department: CSE & I.T Enrolment No 161473

Contact No. 8076380541 E-mail. tyagiarpit383@gmail.com

Name of the Supervisor: MS. MONIKA BHARTI

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): _____
IMAGE STEGANOGRAPHY

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

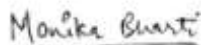
- Total No. of Pages = 30
- Total No. of Preliminary pages = 6
- Total No. of pages accommodate bibliography/references = 1



(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at¹¹ (%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none">• All Preliminary Pages• Bibliography/Images/Quotes• 14 Words String		Word Counts	
Report Generated on		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature

Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck,juit@gmail.com

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: 15/07/2020

Type of Document (Tick): PhD Thesis M.Tech Dissertation/ Report B.Tech Project Report Paper

Name: VIKAS SINGH Department: CSE & I.T Enrolment No 161463

Contact No. 9805088744 E-mail. vikas2071997@gmail.com

Name of the Supervisor: MS. MONIKA BHARTI

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): IMAGE STEGANOGRAPHY

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

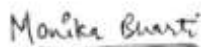
Complete Thesis/Report Pages Detail:

- Total No. of Pages = 30
- Total No. of Preliminary pages = 6
- Total No. of pages accommodate bibliography/references = 1


(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at1.1——(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none"> • All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String 		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature

Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck,juit@gmail.com