A
MINI PROJECT REPORT
ON

"DATA SECURITY USING IMAGE STEGANOGRAPHY"

Submitted to the

Dr. Babasaheb Ambedkar Technological University
Lonere, Raigad

in fulfilment of the requirements

for the award of the degree

BACHELORS OF TECHNOLOGY

COMPUTER SCIENCE AND ENGINEERING
2023-2024

BY

Sanket Dubal	**2064191242086**
Tejaskumar Chopade	**2164191242087**
Prianshu Khalde	**2064191242101**
Aditya Chavhan	**2164191242103**

UNDER THE GUIDANCE OF

Prof. Dhammjyoti Dhawase

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

PCET-NMVPM's

NUTAN COLLEGE OF ENGINEERING AND RESEARCH
TALEGAON, PUNE 410507

PCET-NMVPM's

NUTAN COLLEGE OF ENGINEERING & RESEARCH TALEGAON, PUNE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project Report entitled **"DATA SECURITY USING IMAGE STEGAOGRAPHY",** which is being submitted by, **Sanket Dubal, Tejaskumar Chopade, Prianshu Khalde, Aditya Chavhan** as partial fulfillment for the**Degree Bachelor of Technology** (Computer Science and Engineering) of **DBATU, Lonere.**

This is bonafide work carried under my supervision and guidance.

Place: Talegaon Dabhade, Pune

Date: 22/12/2023

Prof. Dhammjyoti Dhawase
Project Guide

Dr. Sanjeevkumar Angadi
Head of Department

Dr. Aparna Pande
Principal

External Examiner [Name & Sign]

SEAL

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible. So, we acknowledge all those whose guidance and encouragement served as a beacon light and crowned our efforts with success.

We have immense pleasure in expressing thanks to the principal ***Dr. Aparna Pande*** for providing all the facilities for the successful completion of the project.

With due respect, we thank our Head of Department ***Dr. Sanjeevkumar Angadi, Computer Science and Engineering***, for his motivating support, keen interest which kept our spirits alive all through.

We would like to express thanks to our guide ***Prof. Dhammjyoti Dhawase,*** Department of ***Computer Science and Engineering*** who has guided us throughout the completion of this project.

Finally, we would like to thank ***all the teaching and non-teaching staff and all our friends*** who have rendered their support in the completion of this report.

Sanket Anandrao Dubal _____

Tejaskumar Jagannath Chopade _____

Prianshu Amar Khalde _____

Aditya Santosh Chavhan _____

ABSTRACT

Image Steganography is the art and science of concealing information within digital images in such a way that it is difficult to detect or decipher without the appropriate knowledge or tools.

Steganography operates on the principle that, in a digital image, there is redundant or unused information that can be utilized to hide additional data. This hidden information can be text, files, or any other form of data, and it is imperceptible to the human eye.

Detection Methods: The continuous advancement of detection techniques poses a challenge to the effectiveness of image steganography. New and sophisticated algorithms can potentially unveil hidden information, compromising the security of the concealed data.

Researchers have introduced more advanced and sophisticated steganographic techniques to improve the security and robustness of hidden information. This includes methods that use machine learning, deep learning, and artificial intelligence to enhance data embedding and extraction processes.

Concealing sensitive information within images provides a covert means of communication. This application is especially relevant in situations where privacy and confidentiality are crucial, such as military communication or confidential corporate messaging.

Embedding invisible watermarks within images for copyright protection and ownership verification. This helps in identifying the source or owner of an image and can be used to deter unauthorized use or distribution.ual distortion have been a focus of research.

Keyword *– Image, Steganography, Data security*

INDEX

Contents	Page No
Acknowledgement	I
Abstract	II
Chapter 1: Introduction	
1.1 Introduction	1
1.2 Necessity	3
1.3 Problem Statement	5
1.4 Objective	6
1.5 **Motivation**	7
Chapter 2 : Literature Survey	8
Chapter 3 : Image Steganography	10
3.1 Detecting Steganography	10
3.2 Characteristics of Steganography	11
3.3 Steganography vs Cryptography	11
3.4 Steganography Design & Analysis	13

Chapter 4 : System Development	14
4.1 Technologies Used	14
4.2 System Overview	15
4.3 Process	17
4.4 Block Diagram	18
4.5 Advantages And Disadvantages	21
4.6 Applications	22
Chapter 5 : Result	23
5.1 Image Steganography	23
Chapter 6: Conclusion and Future scope	24
6.1 Conclusion	24
6.2 Future scope	25
Chapter 7: References	27

LIST OF TABLES

Table No	Name of Table	Page No
2.1	Literature survey table	8

LIST OF FIGURES

Figure No	Name of Figure	Page No
4.1	Steganography Block Diagram	17
4.2	Block Diagram of Steganography	18
4.3	Flow Diagram of Steganography	20
5.1	Interface	23
5.2	Preview Cover image and Stego image	23

1. INTRODUCTION

1.1 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.

Technology has blitz scaled over the past years leading to a wide usage of multimedia for transferring data, especially Internet of Things (IoT). Usually, the transfer happens over insecure network channels. In particular, the internet has gained accelerated popularity for exchanging digital media and individuals, private companies, institutions, governments use these multimedia data transfer methods for exchanging data. Though there are numerous advantages attached with it, one prominent disadvantage is the privacy and security of the data. The availability of numerous

readily available tools capable of exploiting the privacy, data integrity and security of the data being transmitted has made the possibility of malicious threats, eavesdropping and other subversive activities. The prominent solution is data encryption where the data is converted into a cipher text domain using encryption key.

A new research topic, steganography, has gained acceptance in this context to hide the data that is not perceptible to human eyes. Information hiding techniques have been available for a long time but their importance has been increasing recently. The main reason is the increase in the data traffic through the internet and social media networks. Though the objectives of cryptography and steganography are similar, there is a subtle difference. Cryptography makes the data unbreakable and unreadable but the cipher text is visible to human eyes. Steganography, which is used to hide the information in plain sight, allows the use of wide variety of the secret information forms like image, text, audio, video and files. Digital watermarking is another method where confidential information is embedded to claim ownership. Cryptography is the popular method used for information hiding, but, steganography is gaining popularity in recent times. Steganography can be defined as the process of hiding a secret small multimedia data inside another but much larger multimedia data such as image, text, file or video. Image steganography is a technique to hide an image inside another image. In image steganography, the cover image is manipulated in such a way that the hidden data is not visible thus making it not suspicious as in the case of cryptography. Inversely, Steganalysis is used to detect the presence of any secret message covered in the image and to extract the hidden data . Steganalysis helps in classifying if the image is either a stego image or a normal image. Apart from classifying the image, further investigation is carried out to detect the location and the content of the secret image inside the cover image. With the availability of massive amounts of data, deep learning (DL) has become the trend and is extensively used for many applications. Deep learning is a useful tool in various applications like image classification, automatic speech recognition, image recognition, natural language processing, recommendation systems, processing of medical images . Though research on steganography is quite recent, it has benefited from DL methods including convolutional Neural Networks (CNNs) Generative Adversarial Networks (GANs) based methods and their deployment in both steganography and steganalysis. The main goal of this paper is to review the available methodologies, present trends and discuss the challenges that are currently available in the studies. Along with these studies, the datasets that are publicly available and commonly used, the evaluation metrics considered are also discussed. Finally, a comparison on the performance among the methods and a possible discussion identifying the gaps in the present studies, pros and cons of the methods are elaborated.

.

1.2 NECESSITY

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 Through out 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.

Confidentiality: Steganography helps maintain the confidentiality of sensitive information by hiding it within seemingly innocuous data. This can be crucial for protecting classified data, trade secrets, or personal information from unauthorized access.

Covert Communication In certain situations, individuals or organizations may need to communicate covertly without drawing attention to the fact that a secret exchange is taking place. Steganography allows them to embed messages in public communication channels without arousing suspicion.

Security Against Eavesdropping In the digital age, communications are vulnerable to interception. Steganography provides an additional layer of security by making it more difficult for

eavesdroppers to detect and understand the hidden information. This is especially important for military, intelligence, and diplomatic communications.

Digital Watermarking: Steganography is used for embedding digital watermarks within multimedia content such as images and videos. This helps in protecting intellectual property, preventing unauthorized copying, and tracing the origin of content.

Authentication and Tamper Detection: Steganography techniques can be employed to embed information that serves as a form of digital signature or fingerprint within a file. This allows for the verification of the authenticity of the content and detection of any tampering or alterations.

Resistance Against Cryptanalysis: Combining steganography with encryption enhances the overall security of communication. Even if an encrypted message is intercepted, the fact that there is hidden information within the data may make it more challenging for adversaries to break the encryption or understand the true nature of the communication.

Protection of Whistleblowers: Steganography can be used to protect the identity of whistleblowers or individuals sharing sensitive information. By hiding the information in seemingly unrelated data, the risk of detection is reduced.

1.3 Problem Statement

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. In today's digital era, the importance of safeguarding sensitive information has become paramount. As data transmission and storage have increased exponentially, so has the risk of unauthorized access and data breaches. Image steganography, a technique of concealing information within images, has emerged as a potential solution to enhance information security.

1 Detection Vulnerabilities:

- Steganalysis techniques have become more sophisticated, leading to increased detection rates of conventional steganographic methods.
- The need for steganographic algorithms that can resist advanced statistical analysis and machine learning-based detection methods.

2 Capacity and Efficiency:

- Many traditional steganographic methods compromise image quality or have limited payload capacity.
- The development of steganographic algorithms that can embed larger payloads without significantly degrading carrier content.

3 Multi-Media Steganography:

- Extending steganography beyond image files to encompass other multimedia formats, such as audio and video, while maintaining efficiency and security.
- Developing cross-domain steganographic methods for integrated communication across various types of media.

4 Secure Key Management:

- Robust encryption and key management techniques for securing the embedded information within the carrier.
- Addressing vulnerabilities related to key exchange and ensuring the confidentiality of the steganographic keys.

1.4 Objective

The primary objectives of this research include, but are not limited to:

- Develop advanced steganographic algorithms resistant to state-of-the-art steganalysis techniques.
- Enhance the payload capacity of steganographic methods without sacrificing carrier quality.
- Extend steganography to multimedia formats, including audio and video, ensuring seamless integration and security.
- Establish secure key management protocols for steganographic communication.
- Implement dynamic payload adaptation techniques for versatile and efficient steganographic embedding.

1 Expected Outcomes:

The anticipated outcomes of this research include the development of novel steganographic techniques that significantly improve the security and efficiency of information hiding across various digital media. Additionally, the research aims to contribute to the broader field of cybersecurity by addressing vulnerabilities associated with conventional steganographic methods.

2 Significance of the Research:

The successful execution of this research will contribute to advancing the field of steganography, providing enhanced tools for secure communication in an era where the protection of sensitive information is of paramount importance. The outcomes of this research may find applications in fields such as cybersecurity, digital forensics, and secure data transmission.

Security: The hidden information should be resistant to extraction by unauthorized parties. Only those with the appropriate decoding key or method should be able to recover the concealed data.

Undetectability: The alterations made to the carrier image should be subtle enough to avoid detection by statistical analysis or other steganalysis techniques

.

Compatibility: The steganographic method should be compatible with different image formats and types, ensuring versatility in application.

1.5 Motivation

Confidential Communication: Steganography provides a means for confidential communication by hiding information within seemingly innocuous images. This can be essential in situations where privacy and secrecy are paramount, such as in military or intelligence communications.

Security and Protection: Transmitting sensitive information in a covert manner helps protect it from unauthorized access. Steganography adds an extra layer of security by concealing the existence of the hidden data, making it less likely to be intercepted or tampered with.

Digital Watermarking: In the context of copyright protection, steganography is employed for embedding digital watermarks in images or media files. Watermarks can be used to identify the creator or owner of the content and deter unauthorized use or distribution.

Authentication and Integrity Checking: Steganography can be used to embed authentication information within digital media. This helps verify the integrity of the content and ensures that it has not been altered or tampered with during transmission.

Covert Communication in Hostile Environments: In scenarios where communication needs to occur in hostile environments or under surveillance, steganography provides a way to discreetly exchange information without attracting attention.

Journalism and Whistleblowing: Journalists and whistleblowers may use steganography to protect their sources and transmit sensitive information without risking exposure. This can be crucial for exposing corruption or human rights violations.

Research and Education: Steganography is also explored in research and educational contexts to understand its principles, develop detection methods (steganalysis), and enhance information security practices.

2. LITERATURE SURVEY

Sr. No	Paper Name	Publishing year	Author	Methodology /Algorithms	Advantage	Disadvantage
1	Steganography: The Essential Guide to work life and learning	2014	Viktor Mayer	But this ideology is fading. In the age of big data, we can crunch an incomprehensible amount of information, providing us with invaluable insights about the what rather than the why.	Easy and efficient And return to normal activities.	System failure
2	Data Smart : Using Data Science to transfprm Information	2013	John Foremen	After reading this book, you too will learn how to use math and basic spreadsheet formulas to improve your business or, at thevery least, how totrick senior executives into hiring you as their data scientist	Efficient OS managem ent	System failure

3	Steganography Science	2006	David Aron	This book provides a comprehensive survey of techniques, technologies and applications of Steganographyand its analysis.	Process and Device Management	Fragmentation and expensive
4	Steganography: Concepts , Data	2016	Doughlas Conas	Executives and managers wholead teams responsible forkeeping or understanding large datasets will also benefit from this book	Memory management	We are aware of the fact that OS is the heart of a computer
5	Hadoop: The Big Data	2015	James Adam	This book is ideal for programmers looking to analyze datasets of anysize, and for administratorswho want to set up and runHadoop clusters	Security and Threat Protection	Microsoft Windows operating systemwith GUI and other in-built features carry a costly price

3.IMAGE STEGANOGRAPHY

Using bitmap pictures for hiding secret information is one of most popular choices for Steganography. Many types of software built for this purpose, some of these software use password protection to encrypting information on picture. To use these software you must have a 'BMP' format of a pictures to use it, but using other type of pictures like "JPEG", "GIF" or any other types is rather or never used, because of algorithm of "BMP" pictures for Steganography is simple. Also we know that in the web most popular of image types are "JPEG" and other types not "BPM", so we should have a solution for this problem. This software provide the solution of this problem, it can accept any type of image to hide information file, but finally it give the only "BMP" image as an output that has hidden file inside it. Bitmap type is the simplest type of picture because that it doesn't have any technology for decreasing file size. Structure of these files is that a bitmap image created from pixels that any pixel created from three colors (red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is MostSignificant-Bit (MSB) and last bit Least- Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside BMP pictures. So if we just use last layer of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have 3*hight*width bits memory to write our information. But before writing our data we must write name of data(file), size of name of data & size of data. We can do this by assigning some first bits of memory.

3.1 Detecting Steganography

The art of detecting Steganography is referred to as Steganalysis. To put is simply Steganalysis involves detecting the use of Steganography inside of a file. Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it. There are many methods that can be used to detect Steganography such as: "Viewing the file and comparing it to another copy of the file found on the Internet (Picture file). There are usually multiple copies of images on the internet, so you may want to look for several of them and try and compare the suspect file to them. For example if you download a JPED and your suspect file is also a JPED and the two files look almost identical apart from the fact that one is larger than the other, it is most probable you suspect file has hidden information inside of it.

3.2. Characteristics of Steganography

Some characteristics of steganography are:

Covert communication: Steganography aims to hide the existence of a secret message, not just its content. It uses a cover-object, such as an image, audio, video, or text, to conceal the message in a way that is imperceptible to human senses or statistical analysis.

Invisibility: A good steganography technique should not alter the cover-object significantly or introduce any noticeable artifacts. The stego-object, which is the cover-object with the embedded message, should look and sound as natural as the original cover-object.

Robustness: A robust steganography technique should be able to resist various attacks that attempt to remove, destroy, or detect the hidden message. Such attacks may include compression, filtering, cropping, noise addition, or steganalysis.

Security: A secure steganography technique should use a secret key or password to ensure that only the intended recipient can extract the hidden message. The key or password should be shared between the sender and the receiver beforehand, and should not be easily guessed or cracked by an adversary.

Capacity: The capacity of a steganography technique refers to the amount of information that can be hidden in a given cover-object. The capacity depends on the size, format, and quality of the cover-object, as well as the embedding algorithm and the level of invisibility and robustness required.

3.3 Steganography vs Cryptography:

Steganography is the technique of concealing a secret message within another message, such as an image, audio, video, or text. The goal of steganography is to hide the existence of the communication, so that no one can detect or intercept it. Steganography is less popular and less secure than cryptography, but it can be used to enhance the security of encrypted data by adding another layer of obscurity. Some examples of steganography are hiding a text message in the pixels of an image, embedding a voice message in a music file, or inserting a secret code in a web page.

Cryptography is the science of encrypting and decrypting data using mathematical algorithms and keys. The goal of cryptography is to make the data unreadable to anyone who does not have correct key to decrypt it. Cryptography is more popular and more secure than steganography, but it also attracts more attention and suspicion from potential attackers. Some examples of cryptography are using a password to protect a file, using a digital signature to verify the identity of a sender, or using a public-key encryption to exchange confidential information over the internet.

Comparison between steganography and cryptography:

- Steganography hides the presence of information, while cryptography hides the meaning of information.
- Steganography does not usually alter the structure of data, while cryptography changes the data into a different form.
- Steganography provides confidentiality only, while cryptography provides confidentiality, integrity, authentication, and non-repudiation.
- Steganography does not have specific algorithms, while cryptography has various recognized and approved algorithms.
- Steganography is vulnerable to steganalysis, while cryptography is vulnerable to cryptanalysis.

Therefore, a system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image. Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level. Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

3.4 Steganography Design & Analysis

Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively. It is a non-questionable fact that delectability of a vessel with an introduced data (steganographic message or a watermark) is a function of the changeability function of the algorithm over the vessel. That is the way the algorithm changes the vessel and the severity of such an operation determines with no doubt the delectability of the message, since delectability is a function of file characteristics deviation from the norm, embedding operation attitude and change severity of such change decides vessel file delectability. A typical triangle of conflict is message Invisibility, Robustness, and Security. Invisibility is a measure of the in notability of the contents of the message within the vessel. Security is sinominous to the cryptographic idea to message security, meaning inability of reconstruction of the message without the proper secret key material shared. Robustness refers to the endurance capability of the message to survive distortion or removal attacks intact. It is often used in the watermarking field since watermarking seeks the persistence of the watermark over attacks, steganographic messages on the other hand tend to be of high sensitivity to such attacks. The more invisible the message is the less secure it is (cryptography needs space) and the less robust it is (no error checking/recovery introduced).The more robust the message is embedded the more size it requires and the more visible it is. Invisibility Robustness Security Steganography Techniques: Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Commonly approaches are include LSB, Masking and filtering and Transform techniques. Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel.

4.SYSTEM DEVELOPMENT

4.1 Technologies we used

Python :

Python is a high-level, general-purpose programming language known for its readability, simplicity, and versatility. It was created by Guido van Rossum and first released in 1991.

- Readability: Python emphasizes code readability and clarity, making it easier for developers to write and maintain code. It uses a clean and straightforward syntax, relying on indentation to define code blocks.
- Versatility: Python supports multiple programming paradigms, including procedural, object-oriented, and functional programming. This versatility makes it suitable for a wide range of applications.
- Extensive Libraries and Frameworks: Python has a rich ecosystem of libraries and frameworks that simplify common tasks. Popular libraries include NumPy for numerical computing, Pandas for data manipulation, TensorFlow and PyTorch for machine learning, Django for web development, and Flask for building web applications.
- Community Support: Python has a large and active community of developers. This community contributes to the language's growth, development of libraries, and provides support through forums, online communities, and resources.
- Platform Independence: Python is platform-independent, meaning that code written in Python can run on different operating systems without modification. This enhances its portability and makes it easy to deploy applications on various platforms.
- Interpreted Language: Python is an interpreted language, which means that it does not require compilation before execution. This allows for rapid development and testing.
- Open Source: Python is open-source, and its source code is freely available. This fosters collaboration and allows developers to modify and contribute to the language's development.
- Dynamic Typing: Python is dynamically typed, meaning that variable types are determined at runtime. This provides flexibility but requires careful consideration to avoid runtime errors.
- Large Standard Library: Python comes with a comprehensive standard library that provides modules and packages for various functionalities, such as file I/O, networking, regular expressions, and more.

4.2 System Overview

The word steganography comes from the Greek “Seganos”, which mean covered or secret and – “graphy” mean writing or drawing. Therefore, steganography mean, literally, covered writing. It is the art and science of hiding information such its presence cannot be detected and a communication is happening. A secrete information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The main goal of this projects it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. There has been a rapid growth of interest in steganography for two reasons: The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. The basic model of steganography consists of Carrier, Message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. Basically, the model for steganography is shown on following figure: Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a coverobject. The cover-object with the secretly embedded message is then called the Stego-object. Recovering message from a stego-object requires the cover-object itselt and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. There are several suitable carriers below to be the cover-object:

- Network protocols such as TCP, IP and UDP Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc
- File and Disk that can hides and append files by using the slack space
- Text such as null characters.

1 Cover Medium:

- Digital Images: The most common cover medium for steganography is digital images. Pixels in an image can be manipulated to hide information without noticeably altering the visual appearance.
- Audio Files: Steganography can also be applied to audio files, where imperceptible changes are made to the audio signal to embed hidden data.

- Video Files: Videos provide a larger canvas for hiding data, and steganography can be applied to individual frames or frames within a video stream.

2 Steganographic Techniques:

- LSB Substitution (Least Significant Bit): This technique involves replacing the least significant bits of the cover medium with the hidden data. The human eye is less sensitive to changes in the least significant bits, making this a common method for hiding information in images.
- Frequency Domain Techniques: Transformations like Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) can be applied to hide information in the frequency domain. This is often used in audio and image steganography.
- Spread Spectrum Techniques: Similar to the concept in telecommunications, spread spectrum steganography spreads the hidden information across the entire cover medium, making it harder to detect.

3 Embedding and Extraction Process:

- Embedding: The process of hiding information within the cover medium. This involves applying steganographic algorithms to embed the secret data while maintaining the cover medium's overall integrity.
- Extraction: The process of retrieving the hidden information from the steganographic container. Knowledge of the steganographic algorithm and key is required for successful extraction.

4 Security and Detection:

- Security Measures: The security of a steganographic system relies on the strength of the algorithm used and the key management. The more robust the algorithm, the harder it is to detect or extract hidden information without the correct key.
- Detection Techniques: Steganalysis is the process of detecting the presence of hidden information. Various statistical and mathematical analyses can be applied to identify anomalies in the cover medium that may indicate the presence of hidden data.

5 Applications:

- Digital Watermarking: A form of steganography used to embed information (often copyright or ownership details) in multimedia content to prove authenticity.
- Covert Communication: Steganography can be used for covert communication in sensitive or secure environments where traditional encryption methods might raise suspicion.

4.3 Process

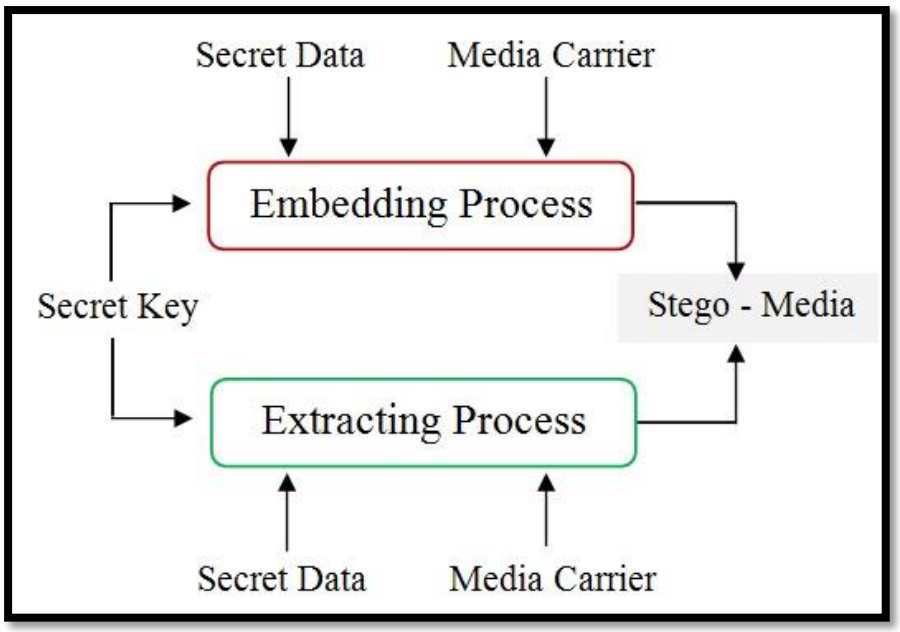

Figure 4.1 : Steganography Block Diagram

Selection of Carrier Medium: Choose an appropriate carrier medium for hiding the secret information. This could be an image file (most common), an audio file, a video file, or even text.

Preprocessing: Before embedding the secret information, preprocessing of the carrier medium might be done. This could involve compressing the file, converting it to a specific format, or applying other transformations to prepare it for steganographic embedding.

Encryption: Encrypt the secret information to add an extra layer of security. This step ensures that even if the steganographic content is discovered, the information remains secure without the decryption key.

Embedding: The secret information is embedded into the carrier medium. In the case of image steganography, this typically involves modifying the pixel values of the image to represent the hidden data. The alterations should be subtle enough to avoid noticeable changes in the carrier.

Key Generation: If encryption is used, a key may be generated to facilitate the extraction of the hidden information. Without the key, it should be extremely difficult for anyone to retrieve the concealed data.

Steganalysis Resistance: To enhance the robustness of the steganographic method, techniques may be employed to resist steganalysis, which is the process of detecting the presence of hidden information. This might involve adding noise or employing other countermeasures to make detection more challenging.

Transmission or Storage: The steganographically altered carrier medium is transmitted or stored as needed, appearing as a regular file to anyone who is not aware of the hidden information.

Extraction: When the recipient receives the steganographic content, they use a specific extraction process to retrieve the hidden information. This process often involves knowledge of the steganographic algorithm, a key for decryption, and any other relevant parameters.

4.4 Block Diagrams

Creating a block diagram for steganography involves illustrating the key components and processes involved in hiding information within another medium. Steganography is the practice of concealing information within other data to avoid detection. Here's a simple block diagram outlining the major steps in a typical steganographic process:

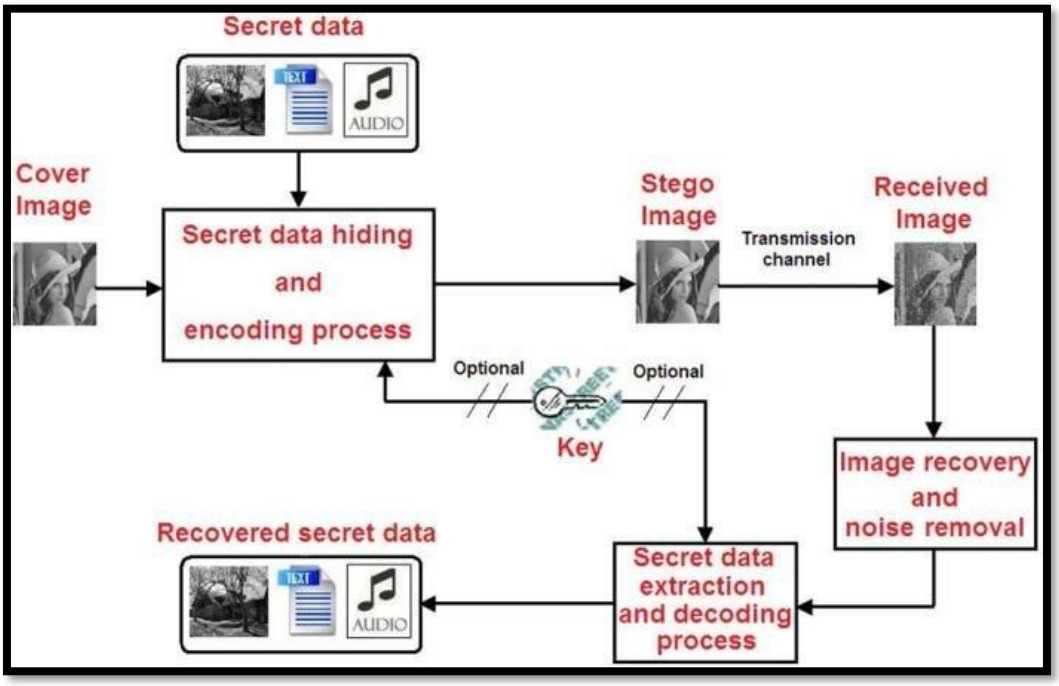

Figure 4.2 : Block diagram of Steganography

1 Input Data (Cover Media):

- Original data that will be used as the carrier for the hidden information.
- This could be an image, audio file, video, or any other form of digital media.

2 Secret Data (Payload):

- Information that needs to be concealed within the cover media.
- This can be a message, file, or any data that the user wants to hide.

3 Embedding Algorithm:

- An algorithm responsible for embedding the secret data into the cover media.
- This process alters the cover media in a way that is imperceptible to the human senses.

4 Stego Media (Output):

- The result of embedding the secret data into the cover media.
- The stego media appears unchanged to the human eye or ear but contains hidden information.

5 Steganography Key (Optional):

- A key or password used to enhance the security of the steganographic process.
- Optional but can be used to encrypt or decrypt the hidden information.

6 Transmission/Storage:

- The stego media can be transmitted over a network or stored without arousing suspicion.
- The goal is for the hidden information to go unnoticed during transmission or storage.

7 Reception/Retrieval:

- The recipient retrieves the stego media and uses a decoding algorithm to extract the hidden information.
- This process should ideally be reversible and not cause any noticeable degradation in the cover media.

8 Decoding Algorithm:

- An algorithm designed to extract the hidden information from the stego media.
- It must be compatible with the embedding algorithm used during the encoding phase.

9 Output Data (Recovered Secret Data):

- The information that was hidden within the stego media.
- It should be identical to the original secret data that was embedded in the cover media.

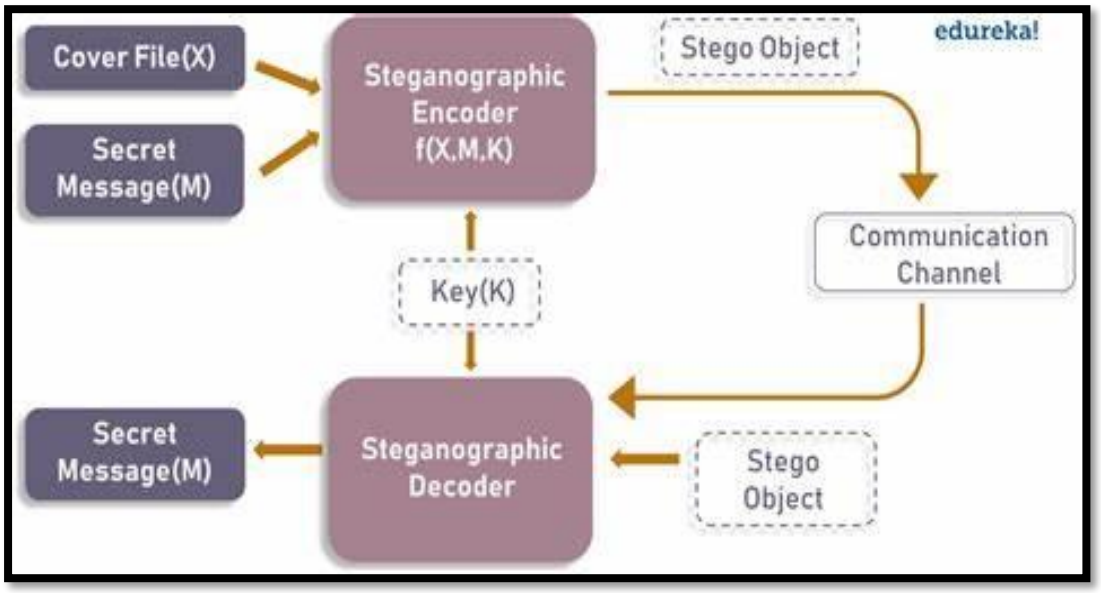

Fig 4.3 : Flow Diagram of Steganography

1 Start:

- Begin the steganography process.

2 Select Carrier File:

- Choose the file (e.g., image, audio) that will be the carrier for the hidden information.

3 Select Message:

- Decide on the information or message that needs to be concealed within the carrier.

4 Encode Message:

- Use a steganographic algorithm to encode the message into the carrier file without causing noticeable changes.

5 Generate Stego File:

- Combine the carrier file with the encoded message to create the stego file.

6 Review Stego File:

- Examine the stego file to ensure that it appears normal and does not raise suspicion.

7 Transmit or Store:

- Share or store the stego file as needed, such as sending it over a network or saving it to a storage device.

8 Receiver Side:

a. Receive Stego File:

- Acquire the stego file on the receiving end.

b. Detect Steganography:

- Use steganalysis techniques to check if the file contains hidden information.

c. Decode Message:

- If steganography is detected, use the appropriate algorithm to decode and extract the hidden message.

d. Reveal Message:

- Retrieve the concealed information from the carrier file.

9 End:

- Conclude the steganography process.

4.5 Advantages And Disadvantages

Steganography is the art and science of hiding information within other information. It can be used for various purposes, such as protecting sensitive data, communicating secretly, avoiding censorship, and more. Some of the advantages of steganography are:

- It can conceal the existence of the hidden information, making it less likely to be detected or intercepted by unauthorized parties.
- It can provide an additional layer of security, by combining it with encryption or other techniques.
- It can embed digital signatures or watermarks into a file, making it possible to verify its authenticity or ownership.
- It can preserve the integrity of the original file, by not altering its appearance or functionality.

Some of the disadvantages of steganography are:

- It has a limited capacity for hiding information, meaning that only small amounts of data can be embedded within a file.
- It can increase the size of the file, making it more noticeable or suspicious.
- It can be complex and require specialized software and skills to perform or analyze.
- Large overhead: Steganography requires a lot of extra space to hide a small amount of information. For example, hiding a short message in a large text file is limited by the size of the text file. Text files are not big enough to hide more complex data like images or audio files.
- Detection: Steganography can be hard to detect, but with the advancement of technology and techniques, it becomes easier to uncover the hidden information. For example, steganalysis is the artof detecting steganography by analyzing the statistical properties of the carrier file
- File size increase: The process of hiding information within a file can cause the file size to increase, making it more obvious and easier to detect. For example, hiding a message in an image file can make the image file larger than the original one

4.6 Applications

- Confidential communication and secret data storing: Steganography can be used to send or store sensitive information in a way that is difficult to detect or decrypt. For example, one can embed a secret message in an image or a sound file and send it to another person who knows how to extract it using a key or a program. This can be useful for avoiding censorship, espionage, or surveillance.
- Protection of data alteration: Steganography can also be used to verify the integrity or authenticity of data by embedding a digital watermark or a signature in the data. For example, one can embed a watermark in a document or an image that identifies the owner or the source of the data. If the data is modified or copied without permission, the watermark can be used to detect or trace the alteration.
- Access control system for digital content distribution: Steganography can also be used to implement a system that allows or restricts access to digital content based on some criteria. For example, one can embed a code or a password in a video or a song that enables or disables some features or functions of the content. This can be useful for protecting the intellectual property rights or the privacy of the content creators or users.
- Media database systems: Steganography can also be used to enhance the functionality or the performance of media database systems by embedding some metadata or information in the media files. For example, one can embed some keywords or tags in an image or a video that can be used for indexing, searching, or retrieving the media files.

5.RESULT

5.1 Image Steganography

- Interface

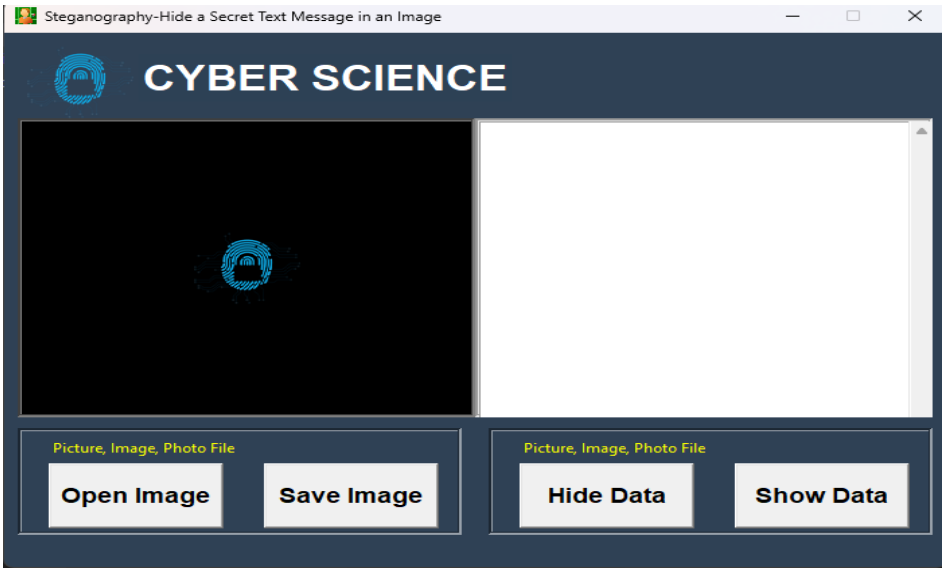

Figure 5.1 : Interface

- Preview of Cover image and Stego image:

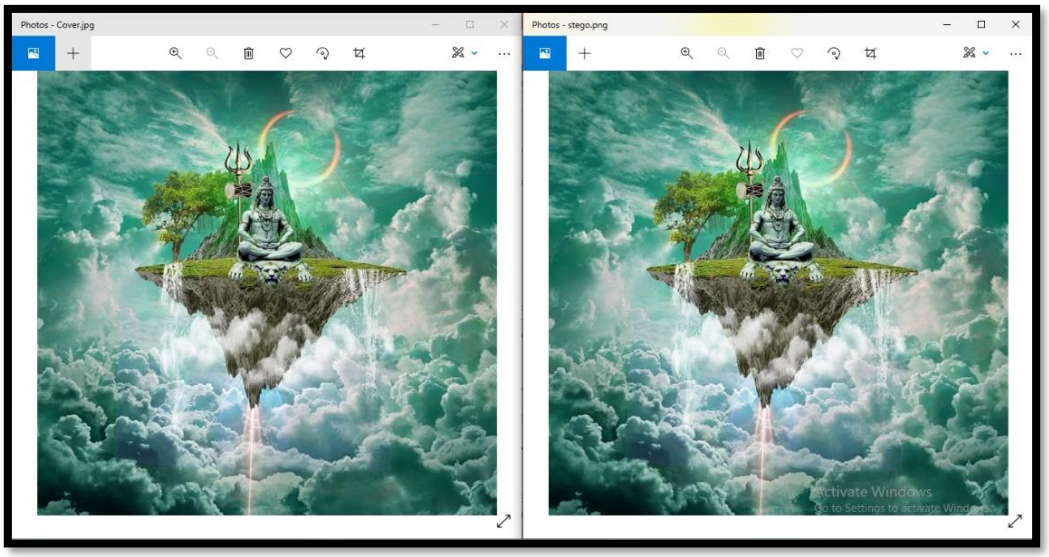

Figure 5.2 : Preview of Cover image and Stego image

6. CONCLUSION & FUTURE SCOPE

6.1 Conclusion

Steganography plays a vital role in securing sensitive information and ensuring covert communication across various domains. As a technique for hiding data within seemingly innocuous carrier media, such as images or audio files, steganography provides a layer of confidentiality crucial in fields like military communication, intelligence, and privacy-sensitive applications. Its versatility extends to digital watermarking, copyright protection, and safeguarding the identity of whistleblowers and journalists.

Python, due to its simplicity and extensive libraries, has become a popular choice for implementing steganographic methods. The language's robust community support and open-source nature contribute to the development of innovative steganography techniques and tools.

However, the ethical and legal implications of steganography should not be overlooked. While it offers legitimate applications, the potential for misuse necessitates responsible usage to ensure compliance with laws and ethical standards. Striking a balance between security, imperceptibility, and ethical considerations is paramount in harnessing the full potential of steganography for safeguarding.

6.2 Future Scope

1. Hybrid Solutions: The future of steganography could see the development of hybrid solutions that combine the best of cryptography with the best of steganography. These new techniques could provide a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered.

2. Network Steganography: With the promotion of packet-switched networks like the internet, there opens more doors towards moving to another level of steganography where instead of using traditional digital data as a cover file, some network protocol or some other services play the role of the cover channel.

3. NFT Techniques: As the art world continues to evolve, NFT techniques change with it. Designing NFTs with private metadata is something we can expect to see more of in the future, and applied in different ways – such as gaming, paywalls, event ticketing and so on.

4. Steganography Tools: A systematic study of the steganography tools developed in the last three decades has been done. The comparative analysis of these tools based on specified parameters represents their strengths, limitations, applicability, and scope for future work.

5. Enhanced Security Measures: As cyber threats evolve, steganography is likely to play a more significant role in enhancing security measures. Advanced steganographic techniques, possibly incorporating artificial intelligence and machine learning, may emerge to create robust and resilient methods for secure communication.

6. Integration with Emerging Technologies: Steganography is expected to integrate with emerging technologies such as blockchain and quantum computing. Blockchain can be utilized for secure and tamper-evident storage of steganographic keys, while quantum-resistant algorithms may be explored to withstand potential threats from quantum computers.

7. IoT Security: With the proliferation of the Internet of Things (IoT), steganography could find applications in securing communication between IoT devices. Hiding authentication information or sensitive data within IoT transmissions can be crucial for preventing unauthorized access and maintaining privacy.

8. Deep Learning and Steganalysis: The ongoing cat-and-mouse game between steganography and steganalysis is likely to intensify. Steganographic methods may leverage deep learning techniques to create more sophisticated and resilient hiding mechanisms, while steganalysis tools will also evolve to detect these advanced methods.

7. REFERENCES

Following research papers are referring to create this project reports:

- Niels Provos, and Peter Honeyman. "Hide and Seek: An Introduction to Steganography." IEEE Security & Privacy Magazine, May-June 2013. Web.

- Nick Nabavian "Image and video steganography & cryptography" Nov. 28, 2007. http://www1.chapman.edu/~nabav100/ImgStegano/download/ImageSteganography.pdf

- Dr Ekta Walia, Payal Jain and Navdeep. "An analysis of LSB & DCT based Steganography." Global Journal of Computer Science and Technology, April2010. https://globaljournals.org/GJCST_Volume10/gjcst_vol10_issue_1_paper8.pdf

- D'Incau, Paolo. "LSB watermarking using MATLAB | Paolo D'Incau's Blog." Paolo D'Incau's Blog | Introduction to erlang and other useful stuff. 22 Mar 2010. Web. 5 Dec 2015. pdincau.wordpress.com/2010/03/22/lsb-watermarking-using-matlab/

- Hardik Patel, and Preeti Dave. "International Journal of Advanced Research in Computer Science and Software Engineering." Http://www.ijarcsse.com/. N.p., Jan-Feb. 2012. Web.

- Deepak Singla, and Rupali Syal. "International Journal of Computational Engineering Research." Citeseerx.ist.psu.edu. N.p., Mar-Apr. 2012. Web.

- Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Information Hiding-A Survey, IEEE, special issue on protection of multimedia content, Jul 1999, 1062-1078

- Analyst, Image. "Re: How to Change least Significant Binary Bits of Each Bit of Cover Image by Other Four Binary Bits??" Blog comment. MATLAB Central. N.p., 29 Jan. 2013. Web. 5 Dec. 2015. www.mathworks.com/matlabcentral/answers/60261-how-to-change-least-significant-4-binary-bits-of-each-bit-of-cover-image-by-other-four-binary-bits#answer_72801

- Balajee, J. "MATLAB CODING's – PART II." researchviews.blogspot.com. N.p., 21 Nov. 2012. Web. 12 Dec. 2015. http://researchviews.blogspot.com/2012/11/matlab-codings-part-ii.html

- G.A. Papakostas, D.E. Koulouriotis and E.G. Karakasis (2009). Efficient 2-D DCT Computation from an Image Representation Point of View, Image Processing, Yung-Sheng Chen (Ed.), ISBN: 978-953-307-026-1, InTech, http://www.intechopen.com/books/image-processing/efficient-2-d-dct-computation-from-animage-representation-point-of-view

- Andrew B. Watson. "Image Compression Using the Discrete Cosine Transform." Mathematical & Cryptography & Steganography Journals by Andrew Watson , 4(1), 1994, p. 81-88 www.vision.arc.nasa.gov/publications/mathjournal94.pdf

Websites

- **http://www.google.com**
- **http://www.microsoft.com**
- **http://www.programmer2programmer.net**
- **http://www.codeproject.com**
- **http://www.asp.net**
- **http://www.asp123.com**
- **http://www.wikipedia.org**