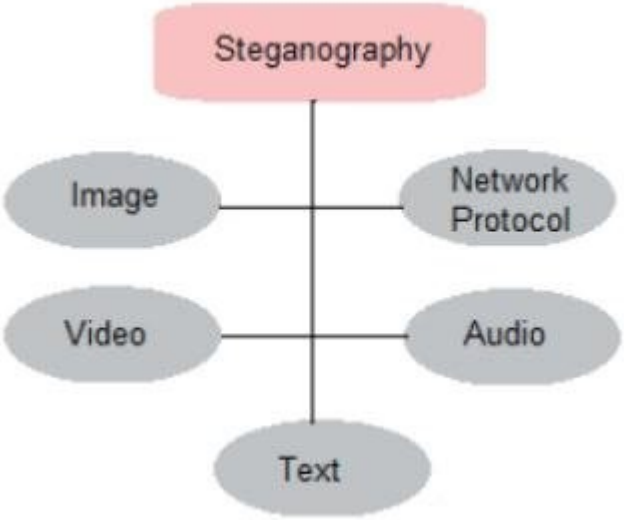
STEGANOGRAPHY

4.1 TYPES OF STEGANOGRAPHY



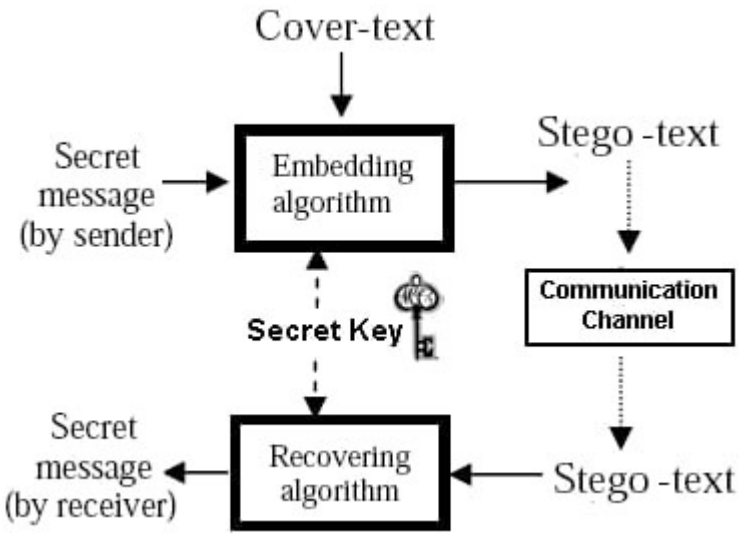
4.1.1 TEXT STEGANOGRAPHY.

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every word of text message. Numbers of methods are available for hiding data in text file. These methods are:

i) Format Based Method

ii) Random and Statistical Method

iii) Linguistics Method



Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (eg., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of node) yet largely indiscernible to the reader. These criteria, reliable decoding and minimum visible change, are somewhat conflicting herein lies the challenge in designing document marking techniques. The three coding techniques that we propose illustrate different approaches rather than form an exhaustive list of documents marking techniques. The techniques can be used either separately or jointly. These are following:

1.Lino-Shift Coding: This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely.

2.Word-Shift Coding: This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely

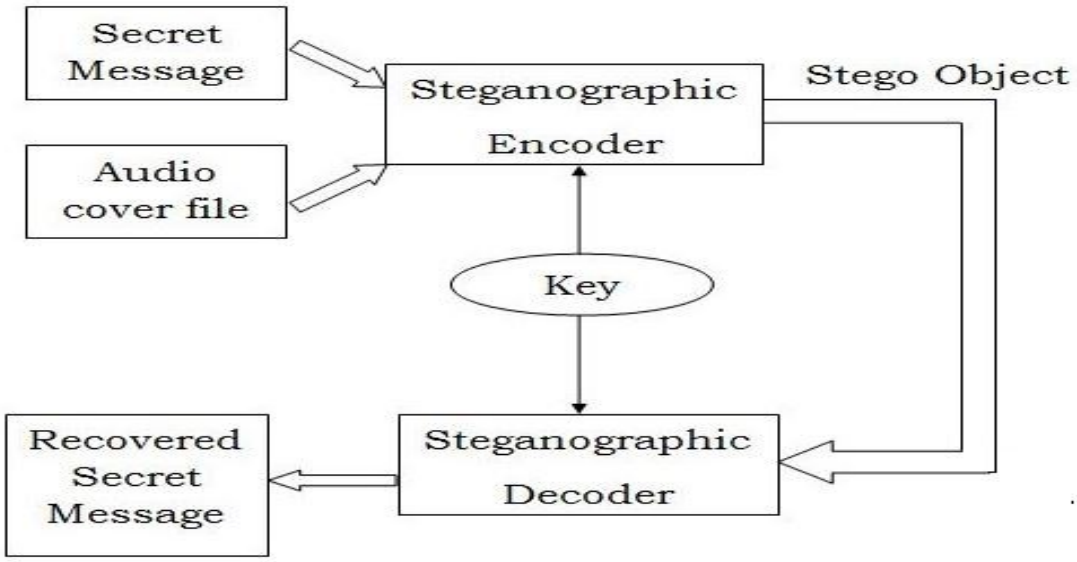
3.Feature Coding: This is a coding method that is applied either to a format file or to a bitmap image of a document

4.1.2 AUDIO STEGANOGRAPHY.

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several

methods are available for audio steganography. We are going to have a brief introduction on some of them. It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. Those methods are

i) Low Bit Encoding
ii) Phase Coding
iii) Spread Spectrum



Audio steganography is an approach of hiding information within an audio signal. As data is embedded in the signal, it gets changed. This modification should be created indistinguishable to the human ear. Image can also be taken as a medium but audio steganography is more impressive because of the features of Human Auditory System (HAS) like large power, powerful range of hearing and high range of audible frequency.

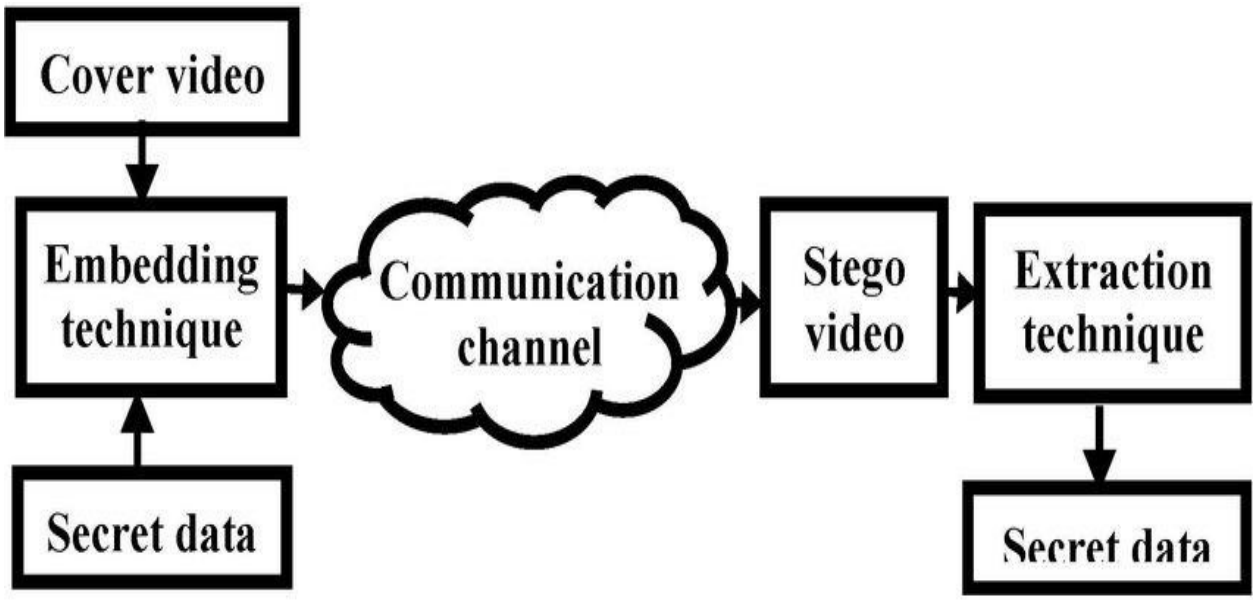
Cryptography includes the encryption of message. It creates no attempt to conceal the encrypted message. In steganography, the original message is not changed but the very continuation is secret from the intruder by embedding the message in the selected medium.

An audio environment is decided by two considerations such as first, its digital description and second, its transmission media. The transmission channel of an audio signal defines the environments the signal can go through, on its method from encoder to decoder. This can be digital

end-end, analogue transmission, and increasing-decreasing resampling or “over-the-air” environments.

4.1.3 VIDEO STEGANOGRPHY.

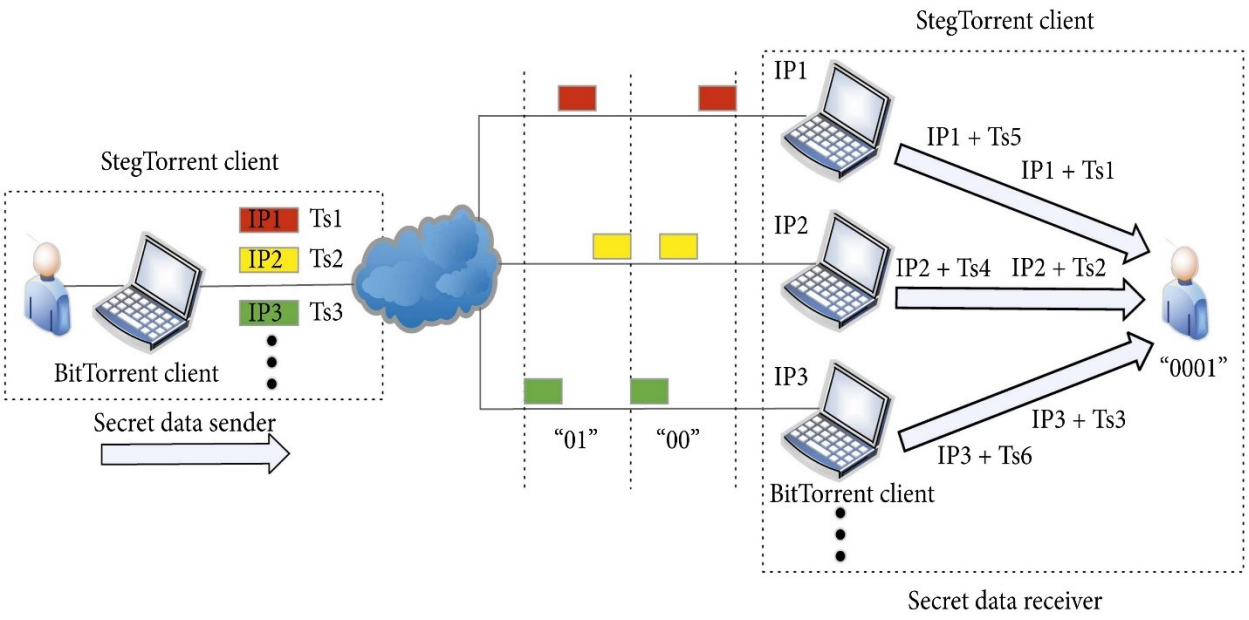
Video steganography is becoming an important research area in various data hiding technologies, which has become a promising tool because not only the security requirement of secret message transmission is becoming stricter but also video is more favored. In this paper, according to the embedded position of secret message, video steganography is divided into three categories: intra-embedding, pre-embedding and post-embedding. Intra-embedding methods are categorized according to the video compression stages such as intra-prediction, motion vectors, pixels interpolation, transform coefficients. Pre-embedding methods are manipulated on the raw video, which can be classified into spatial and transform domains. Post-embedding methods are mainly focused on the bitstreams, which means the procedure of embedding and extraction of video steganography are all manipulated on the compressed bit stream. Then we introduce the performance assessment for video steganography and the future popular video steganography including H.265 video steganography, robust video steganography and reversible video steganography. And challenges are finally discussed in this paper.



Video Steganography is to hide the existence of the message from unauthorized party using Video as cover file and hiding data in video. Steganography means covered writing it includes process of concealing information within other file and also conceals the fact that a secret message is being sent. In this paper a technique proposed is Hash based least significant bit technique for video steganography. Least Significant Bit insertion method embed data in the lower bits of RGB pixel of video and these changes will be minimal. Data hiding is the process of embedding information in a video without changing its perceptual quality and also keep away from knowledge of existence of massage.

4.1.4 NETWORK STEGANOGRAPHY.

Network steganography is a hidden communication technique, which utilizes the legitimate traffic as the vehicle to transfer the secret information covertly over the untrusted network. BitTorrent (BT) is one of the most prevalent P2P services for transmitting video files over wireless networks. An enormous amount of video data is transmitted over BitTorrent traffic continuously, to make it potentially available for confidential information transfer. Hence, in this paper, the Bit torrent file-sharing service of P2P is chosen as the host for information hiding, and a multimode steganographic method based on Bitfield message is proposed. Taking advantage of BitTorrent cooperative transmission and the non-content-authentication mechanism of Bitfield message, the secret information is delivered during the exchange process of Bitmap Info between two peers. The steganographic mode is dynamically selected in view of the secret size, achieving adaptive bandwidth. The experimental results show that our scheme can resist statistical-based detection effectively and outperform the existing method by obtaining a lower degree of detection rate under machine learning-based steganalysis.



Network steganography exploits the normal traffic as the carrier to transmit information stealthily via untrusted networks. Compared with the static multimedia steganography, such as image steganography, it is difficult for the monitor to locate and extract the covert data in tremendous network flow. Hence, network steganography is an effective means of transporting confidential information in networks. In recent years, it has become a hot research topic in the field of information security due to the fine properties of network traffic. There are two broad types of network covert channels: covert storage channel and covert timing one. Covert storage channel embeds the secret information into the redundancies of network protocols Although it is simple and easy to implement, it can be easily detected by the existing methods.

4.1.5 IMAGE STEGANOGRAPHY.

Hiding the data by taking the Image as cover object is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

Image Steganography, as the name implies, is the process of concealing data within an image file. The image chosen for this purpose is referred to as the cover image, and the image obtained after steganography is referred to as the stego image.

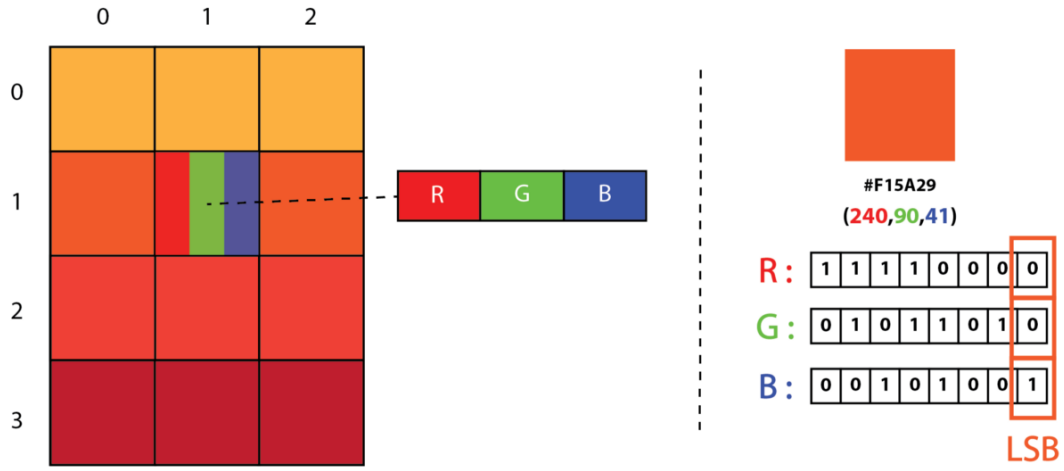


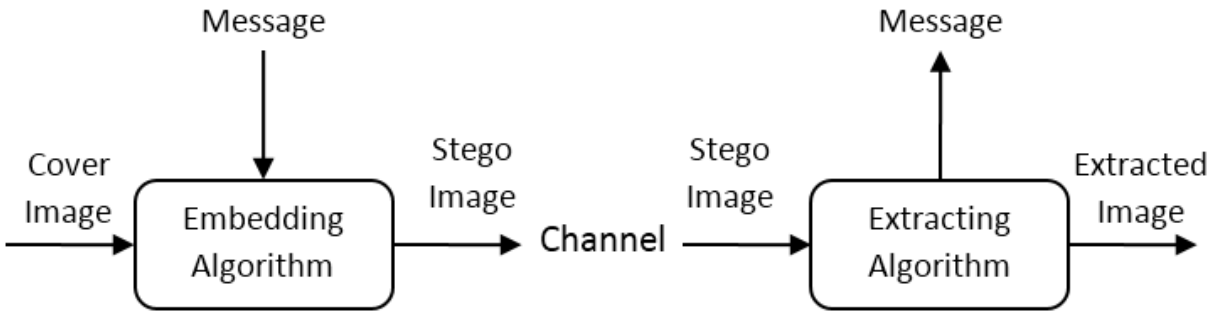
Image steganography is performed for images and the concerning data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it. Image steganography refers to hiding information i.e., text, images or audio files in another image or video files. The current project aims to use steganography for a text with image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique. Images are an excellent medium for concealing information because they provide a high degree of redundancy – which means that there are lots of bits that are there to provide accuracy far greater than necessary for the object's use (or display).

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert NielsProvos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were

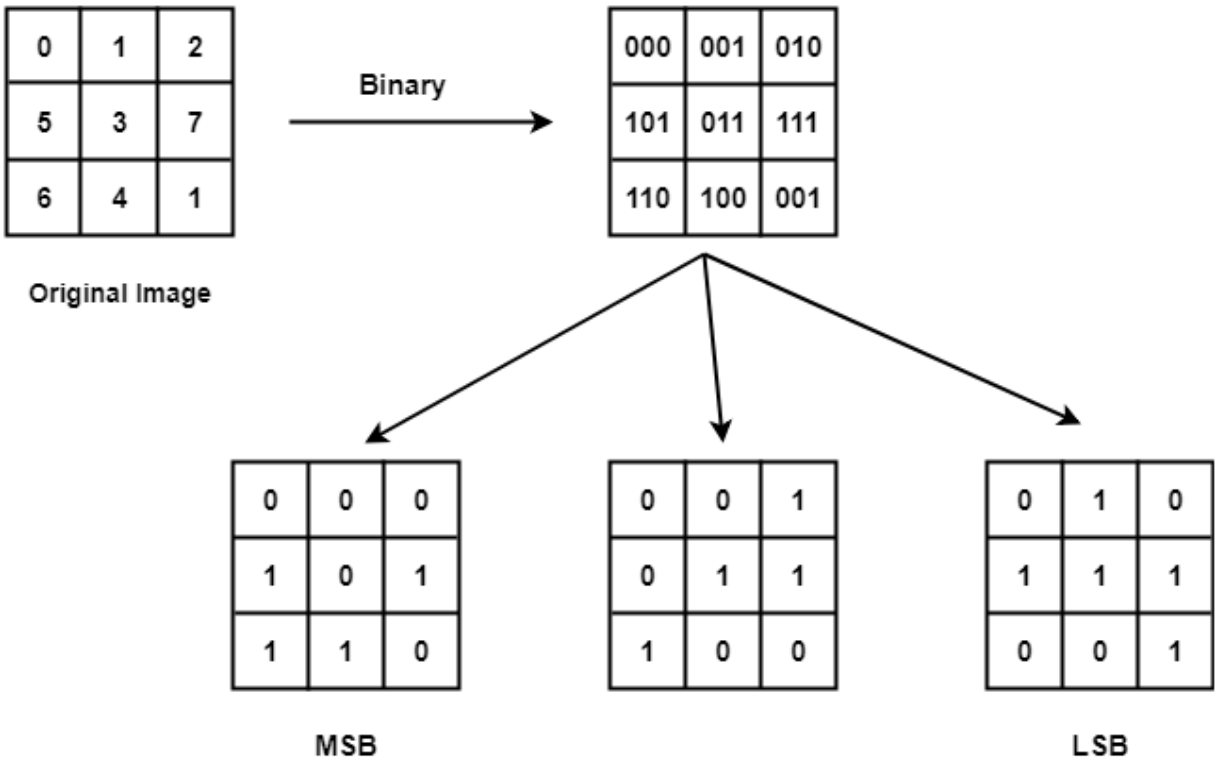
found, so the practical use of steganography still seems to be limited. Image Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden messages or data.

To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files The project deals with learning about the various types of steganography available. Image steganography is performed for images and the concerning data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it.

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color. These pixels are displayed horizontally row by row.



The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits. Thus, in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours. Not surprisingly the larger amount of colours that can be displayed, the larger the file size.



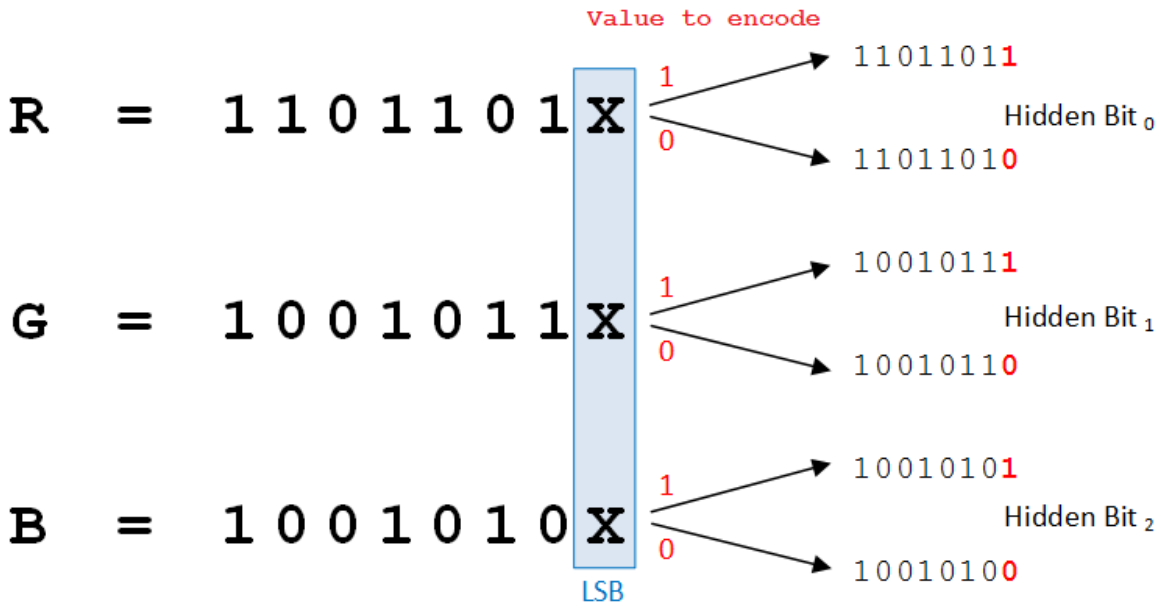
When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. This process is called compression.

In images there are two types of compression: lossy and lossless. Both methods save storage space, but the procedures that they implement differ. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).

Lossless compression, on the other hand, never removes any information from the original image, but instead Represents data in mathematical formulas. The original image's integrity is maintained and the Decompressed image output is bit-by-bit identical to the original image input. The most popular image Formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file).

Compression plays a very important role in choosing which steganographic algorithm to use. Lossy Compression techniques result in smaller image file sizes, but it increases the possibility that the embedded Message may be partly lost due to the fact that excess image data will be removed. Lossless compression Though, keeps the original digital image intact without the chance of lost, although it does not compress the Image to such a small file size. Different steganographic algorithms have been developed for both of these Compression types and will be explained in the following sections.

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image domain also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform domain also known as frequency – domain, images are first transformed and then the message is embedded in the image. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are Sometimes characterized as "simple systems". The image formats that are most suitable for image domain Steganography are lossless and the techniques are typically dependent on the image format.



Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. Many Transform domain methods are independent of the image format and the embedded message may survive Conversion between lossy and lossless compression.

Image steganography is a GUI-based project in which we are hiding a secret message within the image using encoding and decoding functions. We are creating a window in which there are two buttons: encoding and decoding.

For encoding, select any image, this image will be converted into bmp format. Type message in the message box then it will convert into base64, merge this encoded string into image and the user can save the image where he/she wants.

For decoding, select the image which is encoded, the base64 string will get separated by decoding, and by Tkinter module hidden text is shown in the textbox.

Fig: Encoding Image

Fig: Encoded Image

Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover image and the image obtained after steganography is called the stego image.

This steganography approach entails concealing a huge amount of data (picture) within a colour bitmap (bmp) image. The image will be filtered and segmented in his study, with bits replacement applied to the appropriate pixels. These pixels are chosen at in order.

Detection of the message within the cover image is done by the process of steganalysis. This can be done through comparison with the cover image. While efforts are being invested in developing new algorithms with a greater degree of immunity against such attacks, efforts are also being devoted towards improving existing algorithms for steganalysis, to detect the exchange of secret information between terrorists or criminal elements.

Pictures are utilized as the famous cover objects for steganography. A message is installed in an advanced picture through an inserting calculation. The subsequent stego picture is send to the beneficiary. On the opposite side, it is prepared by the extraction calculation. Amid the transmission of steno picture unauthenticated people can just notice the transmission of a picture yet can't figure the presence of the concealed messages.

The secret information is hidden in a way that it not visible to the human eyes. Deep learning technology, which has emerged as a powerful tool in various applications including image steganography, has received increased attention recently. The main goal of this project is to explore and discuss various deep learning methods available in image steganography field. Deep learning

techniques used for image steganography can be broadly divided into three categories – traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods. Along with the methodology, an elaborate summary on the datasets used, experimental set-ups considered and the evaluation metrics commonly used are described in this project. This project aims to help the fellow researchers by compiling the current trends, challenges and some future direction in this field.

So, let's understand why we use only LSB for storing data instead of MSB. Okay for example lets take the 8-bit value 255. In that the left side first value is most important as we can see in the image if we change the value of MSB to zero then the value will be reduced to 127. On the other side we can see if we change the LSB value to zero then the 8-bit value will be 254. From the above image we can observe that if we change the MSB then color will be changed mostly the human eye can be identified, if we change the LSB the color will be slightly changing so a human eye can be identified. So, we use LSB method in all mediums for storing data.