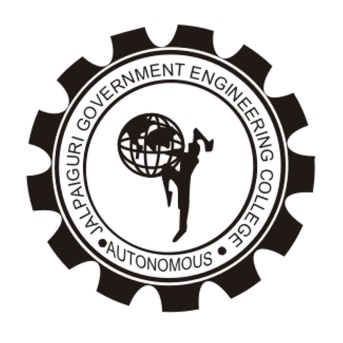
## “DIGITAL IMAGE PROCESSING AND SECURITY”

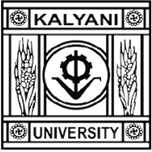
#### (A Report in Partial Fulfillment of Summer Internship Training)



**Submitted By :- INDRANIL BANERJEE**

**Roll No– 15101106026, Registration No- 151010110081 Department of Information Technology**

**Jalpaiguri Government Engineering College (Autonomous)**

****

**Under Supervision Professor**

**Dr. JYOTSNA KUMAR MANDAL**

##### Department of Computer Science & Engineering University of Kalyani

Kalyani, Nadia West Bengal-741235

India

**June’18 -July’18**

**ACKNOWLEDGMENTS**

It gives me immense pleasure to announce the completion of the project on “Digital Image Processing and MOSFET Device Simulation”. A project work is not an obligation done by one person towards a predetermined and very specific goal. Rather, it is the coming together of many elements, some direct and some indirect, towards the planning and implementation of a long-drawn effort.

I am highly indebted to **Dr. JYOTSNA KUMAR MANDAL**, Professor, Department of Computer Science & Engineering, Faculty of Engineering Technology and Management, University of Kalyani, Kalyani, Nadia, West Bengal - 741235, India. I dedicate my summer internship to UNIVERSITY OF KALYANI and the Head of Department of Computer Science & Engineering, University of Kalyani and department’s all teaching & non-teaching staffs, without whose moral help and extensive cooperation we would not be able to complete this project. My sincerest regards goes especially to **Mr. Sujit Das** (PhD Scholar, Department of Computer Science and Engineering, University of Kalyani) and **Mr. Sayantan Biswas** (final year student of M. Tech in Department. of Computer Science & Engineering, University of Kalyani) without whose close guidance I would not be able to complete this project. I am also indebted to Jalpaiguri Government Engineering College for providing me the opportunity to take part in the internship.

Last but not in any way the least, I would like to express my sincere gratitude to my Summer Internship project supervisor **Prof. (Dr.) JYOTSNA KUMAR MANDAL** for his valuable advice, encouragement, whole-hearted cooperation, guidance and unending support right from the stage the project idea was conceived. He was always available with new ideas and suggestions during the difficult phases of the project.

Page 2

Indranil Banerjee

Roll No-15101106026,

Reg No-151010110081

Bachelor of Technology in Information Technology,

Jalpaiguri Government Engineering College

## DECLARATION

I hereby declare that the project work entitled “Digital Image Processing and Security” is an authentic record of my own work carried out at “University Of Kalyani, Kalyani, Nadia” as requirements of four weeks’ summer training for the award of degree of Bachelor of Technology (Information Technology), Jalpaiguri Government Engineering College under the guidance of Prof- Dr. J.K. MANDAL, University of Kalyani, Computer Science and Engineering during the period of 04th June, 2018 to 02nd July, 2018. I further declare that no part of this report is copied from Internet or any other source.

Date: 2nd July 2018 Indranil Banerjee

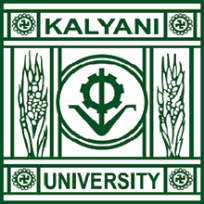
Roll No-15101106026,

Reg No-151010110081

Bachelor of Technology in Information Technology,

Jalpaiguri Government Engineering College

### 

**** University of Kalyani

**Government of West Bengal**

**Kalyani, Nadia**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

Phone: (033) 25809617 (O)

E-mail: [jkm.cse@gmail.com](mailto:jkm.cse@gmail.com)

Website: [www.jkmandal.com](http://www.jkmandal.com/)

**Prof. (Dr.) J. K. Mandal**

Dept. of Comp. Sc. & Egg.

University of Kalyani,

Kalyani, Nadia-741235

West Bengal, India

**CERTIFICATE**

This is to certify Mr. Indranil Banerjee, Roll No. 1510110-6026, and Reg No 151010110081 a student of Bachelor of Technology (Information Technology), Jalpaiguri Government Engineering College, West Bengal has successfully completed four weeks Summer Internship program on “Digital Image Processing and Security” from 04.06.2018 to 02.07.2018. During this internship period he demonstrated excellent analytical skills with a self-motivated attitude to learn the concepts and applications. His performance exceeded expectations and he was able to complete the assignments successfully on time.

I wish him every success in life.

**Internship Guide**

**Prof.-Dr. Jyotsna Kumar Mandal**

**Department of Computer Science & Engineering.**

**University of Kalyani**

### ABSTRACT

##### The ultimate aim in a large number of image processing application is to extract important features from image data, from which a description, interpretation, or understanding of the scene can be provided by the machine. Image processing can be defined as, the processing or altering an existing image in a desired manner. This system allows the user to take hard copy of the image using printer routines and allows the users to store screen image into the disk file using file format. Image processing in its general form pertains to be alteration and analysis of pictorial information. We find instance of image processing occurring all the times in our daily lives. Probably the most powerful image processing system in the human brain together with the eye. This system receives, enhances and stores images at enormous rate of speed.

The objective of image processing is to visually enhance or statistically evaluate some aspect of an image not readily apparent in its original form. The basic principle of image processing operation carried out will assist us in greater perception and vision but does not add any information content. This objective carried out through development and implantation of processing means necessary to operate upon image.

Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. There are many different carriers for steganography. Of which, most popular ones are digital images. Due to recent developments in steganalysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using steganalysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for covert communications between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. The process involves converting a secret image into a text document, then encrypting the generated text into a cipher text using a key (password) based encryption algorithm, and finally embedding the cipher text on to a cover image. This embedding process is carried out using a threshold-based scheme that inserts secret message bits into the cover image only in selected pixels. The security to maintain secrecy of message is achieved by making it infeasible for a third person to detect and retrieve the hidden message.

**ABOUT UNIVERSITY OF KALYANI**

In the early 1950s, the township of Kalyani was developed as the brainchild of Dr. Bidhan Chandra Roy, the then Chief Minister of West Bengal. Kalyani was planned to grow as a satellite town in the long-term perspective plan of the Calcutta Urban Agglomeration. For planned development of the town, the need for emphasizing education and health infrastructure was duly emphasized in the master plan and the University of Kalyani was established in November 1960, as a unitary university with the faculties of Arts, Science, Education, and Agriculture. Since inception, the University marked its progress and attracted students of the region as well as many eminent scholars of the country. However, in its early stage of growth, the University was bifurcated in the year 1975 when its Faculty of Agriculture evolved into a full-fledged agricultural university, named as Bidhan Chandra Krishi Vishwavidyalaya, which was established in the Mohanpur campus. Just after the bifurcation the University of Kalyani was left with 12 teaching departments under the faculties of Arts and Science only. It started reorganizing its activities and by the end of 1970s, the University could introduce four more departments, namely History, Political Science, and Commerce under the Faculty of Arts, which was converted to Faculty of Arts and Commerce, and Bio-chemistry & Bio-physics under the Faculty of Science. Since then, the University has been continuously expanding its area of studies. In the 1980s, the Department of Environmental Science (under Faculty of Science), and the Department of Modern Languages (under Faculty of Arts & Commerce) were started. In the decade of 1990s, three more departments were started, namely, Folklore, Library Information Science (Faculty of Arts & Commerce) and Computer Science (Faculty of Science). Till 1998, the University was a unitary university offering also undergraduate teaching. In 1998 it became an affiliating university with its territorial jurisdiction extended to the districts of Nadia and Murshidabad, and it affiliated 37 colleges, earlier under Calcutta University. Since then the undergraduate teaching programmers at the University were discontinued and were left to its affiliated colleges. In the early part of the first decade of this century, the University introduced 6 new departments, namely, Business Administration, Microbiology, Geography, Molecular Biology & Bio-Technology, Physiology, and Rural Development & Management. It has also introduced the Faculty of Engineering, Technology, and Management, with the departments of Business Administration, Computer Science & Engineering, and Rural Administration & Management. During the last five years, a new Faculty of Music and Fine Arts consisting of the Department of Visual Arts, one new Department in the Faculty of Engineering viz Department of Engineering and Technology Studies, one in the Faculty of Science (Department of Environment and Ecology), and four in the Faculty of Arts and Commerce (Departments of Hindi, Philosophy, Sanskrit, Rural Development Studies) have been established. In addition, research centers such as, Envis, Centre for Bengali Diaspora, Centre for Woman Studies, Rabindra Adhyan Centre, and Centre for Cultural Studies etc. have also been introduced during the last five years. Besides, two of the earlier existing center have been upgraded into two department’s viz. the Department of Adult, Continuing Education and Extension Studies and the Department of Engineering and Technological Studies. Both of these are providing excellent student support in addition to its commendable works. One more faculty, namely Law, is in the process of crystallization

Besides the teaching and research departments, the University has also affiliated several institutes which are providing extension related services through several certificate courses and diplomas.

INDEX

SL. NO.

**TOPIC**

**PAGE NO.**

1. Basics of Image Processing. 8
2. Operation on Images. 11
3. Security. 21
4. Conclusion. 33
5. References. 34
6. Basics of image processing

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Nowadays, image processing is among rapidly growing technologies. It forms core research area within engineering and computer science disciplines too. Image processing basically includes the following three steps:

* + Importing the image via image acquisition tools;
  + Analyzing and manipulating the image;
  + Output in which result can be altered image or report that is based on image analysis.

There are two types of methods used for image processing namely, analogue and digital image processing. Analogue image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. Digital image processing techniques help in manipulation of the digital images by using computers. The three general phases that all types of data have to undergo while using digital technique are pre-processing, enhancement, and display, information extraction.

In this lecture we will talk about a few fundamental deﬁnitions such as image, digital image, and digital image processing. Diﬀerent sources of digital images will be discussed and examples foreach source will be provided. The continuum from image processing to computer vision will be covered in this lecture. Finally, we will talk about image acquisition and diﬀerent types of image sensors.

### Analog image processing

Analog image processing is done on analog signals. It includes processing on two-dimension analog signals. In this type of processing, the images are manipulated by electrical means by varying the electrical signal. The common example include is the television image. Digital image processing has dominated over analog image processing with the passage of time due its wide range of applications.

### Digital image processing

The digital image processing deals with developing a digital system that performs operations on a digital image.

### What is an Image?

An image is nothing more than a two-dimensional signal. It is deﬁned by the mathematical function f (x, y) where x and y are the two co-ordinates horizontally and vertically.



*Figure 1: A PGM Image*

The value of f (x, y) at any point is gives the pixel value at that point of an image.

|  |  |  |
| --- | --- | --- |
| 128 | 30 | 123 |
| 232 | 123 | 321 |
| 123 | 77 | 89 |
| 80 | 255 | 255 |

*Figure 2: Pixel Data of a subsection of an Image*

The above ﬁgure is an example of digital image that you are now viewing on your computer screen. But actually, this image is nothing but a two-dimensional array of numbers ranging between 0 and 255.

Each number represents the value of the function f(x, y) at any point. In this case the value 128,230, 123 each represents an individual pixel value. The dimensions of the picture are actually the dimensions of this two-dimensional array.

### Applications of Digital Image Processing

Some of the major ﬁelds in which digital image processing is widely used are

* + Some Image sharpening and restoration
  + Medical ﬁeld
  + Transmission and encoding
  + Machine/Robot vision
  + Color processing
  + Remote Sensing

### File Handling in Python & Image Processing:

There are four basic operations that can be performed on any ﬁles in Python programming language. They are: -

* + Opening /Creating a ﬁle.

f= open(s,'r')

* + Closing a file.

f.close()

* + Reading a ﬁle.

b=f.read()

* + Writing in a ﬁle.

f.write(“text”)

We are learning ﬁle handling because we have to create a image ﬁle and we have to put all the data into the image ﬁle.

def matrixrep(s):

f = open(s,'r')

b=f.read() lines=b.split("\n")

print(lines[:4])

n=lines[2].split(" ")

row=np.int16(n[0])

col=np.int16(n[1])

a=np.zeros((row,col),dtype=np.int16)

ind=4

for i in range(row):

for j in range(col):

a[i][j]=np.int16(lines[ind])

ind+=1

return a

### Operation on Images

#### Transformation

Transformation is a function. A function that maps one set to another set after performing some operations.

**Image Transformation**

Consider this equation G (x, y) = T{ f(x, y) } .........(1)

In this equation,

F(x,y) = input image on which transformation function has to be applied. G(x,y) = the output image or processed image.

T is the transformation function.

This relation between input image and the processed output image can also be represented as. s = T(r) …………...(2)

where r is actually the pixel value or gray level intensity of f(x,y) at any point. And s is the pixel value or gray level intensity of g(x,y) at any point.

**Fourier Transform of an Image (maps image into spatial frequency domain):**

import cmath

import math

import numpy as np def dft(n,normalize):

matrix = np.zeros((n, n), dtype=np.complex\_)

identity = np.zeros((n, n), dtype=np.complex\_) omega=cmath.exp(-2j\*cmath.pi/n)

factor=1

for a in range(n): value=1

for b in range(n):

matrix[a][b]=value

value=value\*factor if normalize:

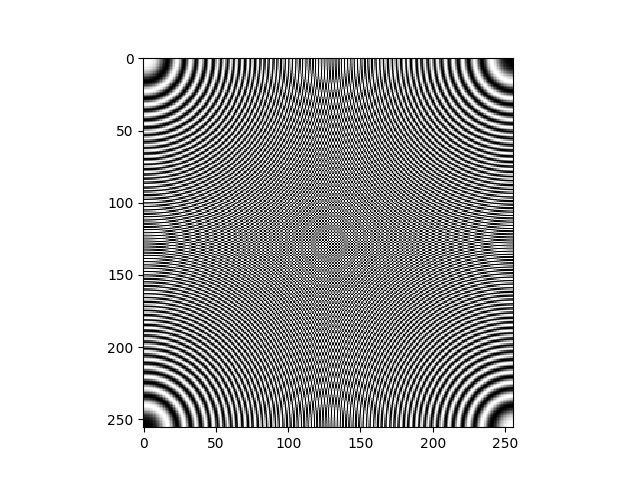
matrix[a][b]=matrix[a][b]/cmath.sqrt(n) factor = factor \* omega

for a in range(n):

for b in range(n): if a is b:

identity[a][a]=1 f\_matrix=np.dot(np.dot(matrix.transpose(),identity),matrix) return f\_matrix

Python program to create Fourier Transformation



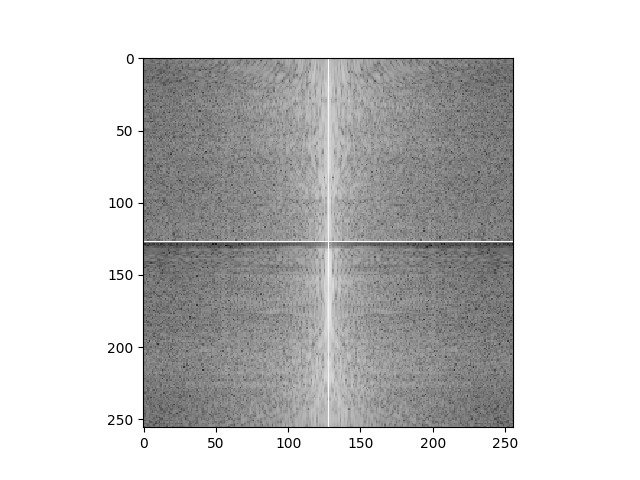


*Figure 3: Original image "tree.pgm" Figure 4: Image "tree.pgm" after Fourier transform*

The image "tree.pgm" is converted to it's Fourier transformation using the above program

We may also use the inbuilt fft() function of numpy package to computes the

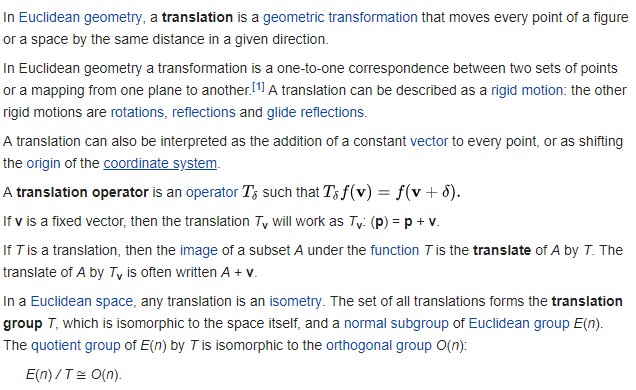
one-dimensional discreteFourier Transform. This function computes the one-dimensional

\*n\*-point discrete Fourier Transform (DFT) with the efficient Fast Fourier Transform (FFT) algorithm [CT].

m=matrixrep("tree.pgm") t=np.fft.fft(m) t=np.fft.fftshift(t) t1=np.log10(abs(t)) plt.figure(1) plt.imshow(t1,cmap="gray") plt.show()

Python program using fft() function *Figure 5: Image "tree.pgm" after transforming using fft() function*

## Translation



def translate (matrix, x,y,crop,top,left): height=np.shape(matrix)[0] if crop else (np.shape(matrix)[0]+y)

width = np.shape(matrix)[1] if crop else (np.shape(matrix)[1] + x) mShift=np.zeros((height,width),dtype=np.complex\_)

if (crop):

if (top and left):

for a in range(y, height): for b in range(x, width):

mShift[a][b] = matrix[a - y][b - x] if (top and not left):

for a in range(y, height):

for b in range(0,width-x): mShift[a][b]=matrix[a][b+x]

if (not top and left):

for a in range(0, height - y): for b in range(x, width):

mShift[a][b] = matrix[a+y][b - x]

if (not top and not left):

for a in range(0, height - y): for b in range(0, width - x):

mShift[a][b] = matrix[a+y][b+x]

else:

if(top and left):

for a in range(y,height): for b in range(x,width):

mShift[a][b]=matrix[a-y][b-x] if( top and not left):

for a in range(y,height): for b in range(0,width-x):

mShift[a][b]=matrix[a-y][b] if (not top and left):

for a in range(0, height-y): for b in range(x, width):

mShift[a][b] = matrix[a][b - x] if (not top and not left):

for a in range(0,height-y): for b in range(0,width-x):

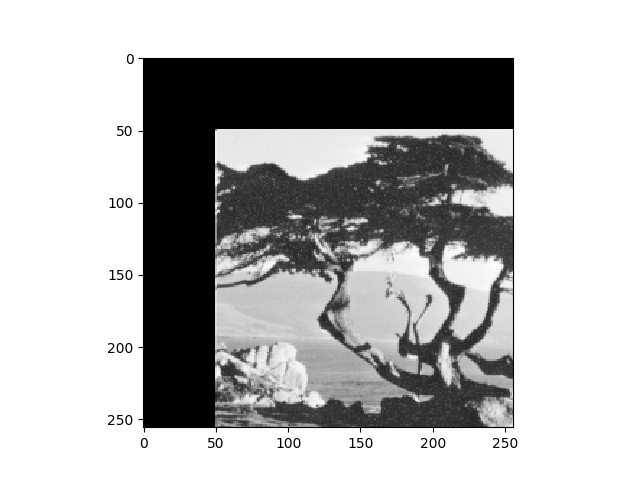
mShift[a][b]=matrix[a][b] return mShift

Python program for translating images from axis

Translation without Cropping

m=matrixrep("tree.pgm") m=translate (m,50,50,Fale,True,True) plt.figure(1) plt.imshow(m.astype(float),cmap=" gray")plt.show()

*Figure 6: Translating image 50 pixels from top and left axes without cropping*



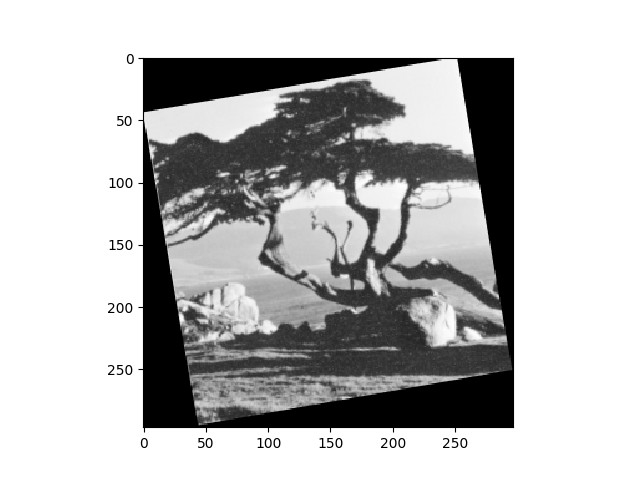
Translation with Cropping

m=matrixrep("tree.pgm") m=translate (m,50,50,True,True,True) plt.figure(1) plt.imshow(m.astype(float),cmap=" gray")

plt.show()

*Figure 7: Translating image 50 pixels from top and left axes with cropping*

1. **Rotation**

Image rotation is performed by computing the inverse transformation for every destination pixel. Output pixels are computed using bilinear interpolation. RGB images are computed by evaluating one color plane at a time.

.

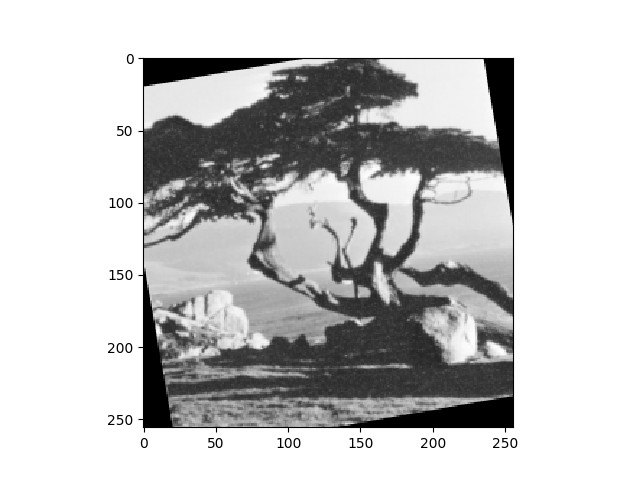
Rotation without clipping

from skimage.transform import rotate

m=matrixrep("tree.pgm") m=rotate(m,10,True) plt.figure(1)

plt.imshow(m.astype(float),cmap=" gray")plt.show()

*Figure 8: Rotating image 10 degrees without cropping*

Rotation with clipping

from skimage.transform import rotate

m=matrixrep("tree.pgm") m=rotate(m,10,False) plt.figure(1) plt.imshow(m.astype(float),cmap=" gray")plt.show()

*Figure 9: Rotating image 10 degrees with cropping*

1. **Histogram Analysis**

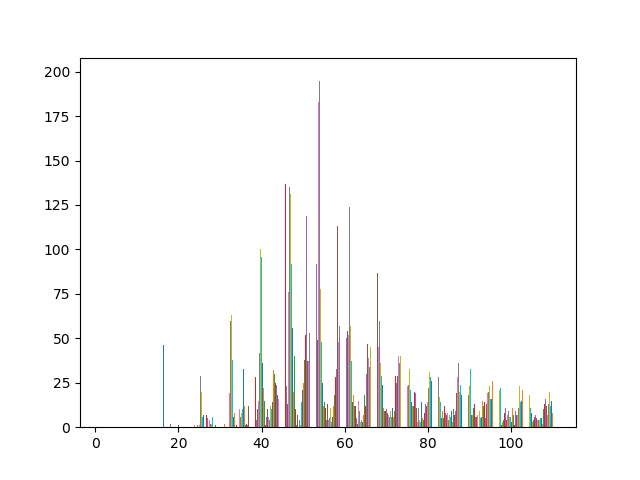
The histogram plots the number of pixels in the image (vertical axis) with a particular brightness value (horizontal axis) because the information contained in the graph is a representation of pixel distribution as a function of tonal variation, image histograms can be analyzed for peaks and/or valleys.

m=matrixrep("tree.pgm") plt.figure(1)

plt.hist(matrix, bins="auto")

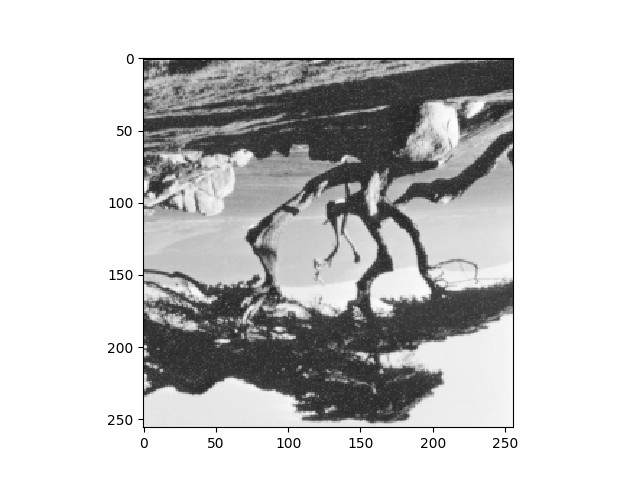
plt.show()

Python program to perform histogram analysis

*Figure 10: Histogram Analysis output of above program*

### Reflection

A standard morphological operation is the reﬂection of all of the points in a set about the origin ofthe set. The origin of a set is not necessarily the origin of the base.



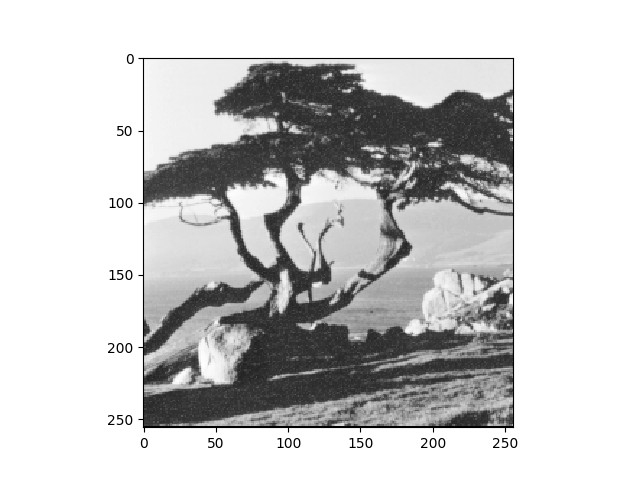
*Figure 11: Image after vertical reflection*

def reflect\_vertical(matrix): midline=int(np.shape(matrix)[0]/2) for a in range(1,midline):

for b in range(0,len(matrix)): temp=matrix[midline+a][b] matrix[midline+a][b]=matrix[midline-a][b] matrix[midline-a][b]=temp

return matrix

Python program to perform vertical reflection



def reflect\_lateral(matrix): midline=int(np.shape(matrix)[1]/2) for b in range(1,midline):

for a in range(0,len(matrix)): temp=matrix[a][midline+b] matrix[a][midline+b]=matrix[a][midline-b] matrix[a][midline-b]=temp

return matrix

*Figure 12: Image after lateral reflection*

Python program to perform lateral reflection

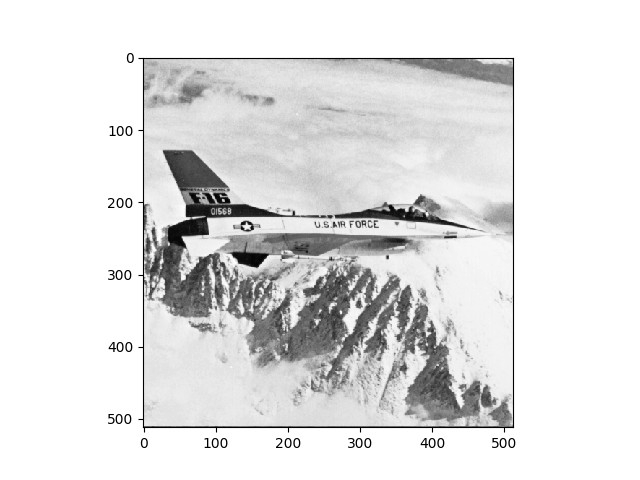
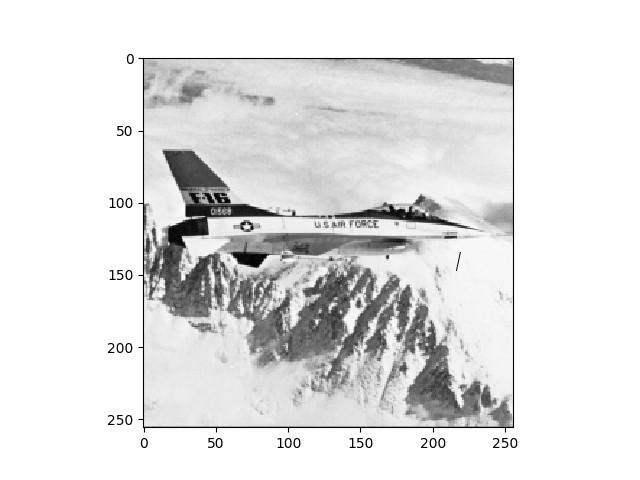
### Image Resizing

Image interpolation occurs when you resize or distort your image from one pixel grid to another.Image resizing is necessary when you need to increase or decrease the total number of pixels, whereas remapping can occur when you are correcting for lens distortion or rotating an image.

m=matrixrep("tree.pgm") m=resize(m,(256,256)) plt.figure(1)

plt.imshow(m.astype(float),cmap="gray") plt.show()

Python program to resize image



*Figure 13: Resized Image*

*Figure 14:*

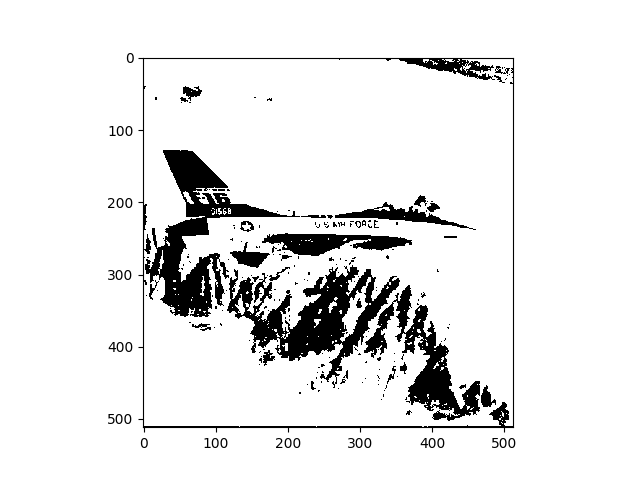
*Original Image*

*( 256 X 256 ) ( 512 X 512 )*

### Manipulating Pixels

The individual pixels of the image may be stored in a matrix. A function may be applied to each individual pixel and the resultant image is displayed. These functions may be

* ceiling function
* floor function
* round function
* a function that converts image to binary form depending on a threshold value





Python program to convert image to binary form *Figure 15: Image after binary conversion*

### Security

###### Fundamentals of Security

In today’s world of growing technology security is of utmost concern. With the increase in cybercrime, providing only network security is not suﬀicient. Security provided to images like blueprint of company projects, secret images of concern to the army or of company’s interest, using image steganography and stitching is beneﬁcial. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is diﬀicult to ﬁnd. More over since the secret image is broken down into parts and then sent to the receiver. This makes it diﬀicult for the trespassers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly diﬀicult for the intruder to detect the and decode the document. There is no limitation on the image format that can be used right from bmp to a giﬀ image can be used. It can be grey scale or colored images. The size of the message needs to be of only 140 characters

###### Cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Earlier cryptography was eﬀectively synonymous with encryption but nowadays cryptography is mainly

based on mathematical theory and computer science practice. Modern cryptography concerns with:

* Conﬁdentiality - Information cannot be understood by anyone
* Integrity - Information cannot be altered.
* Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage
* Authentication - Sender and receiver can conﬁrm each

Cryptography is used in many applications like banking transactions cards, computer passwords, and e-commerce transactions.

Three types of cryptographic techniques used in general.

* 1. Symmetric-key cryptography
  2. Hash functions.
  3. Public-key cryptography

###### Symmetric-key Cryptography

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

###### Public-Key Cryptography

This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

###### Hash Functions

No key is used in this algorithm. A ﬁxed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

### Steganography

**Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the Greek words *steganos* (meaning "covered, concealed, or protected", and *graphein* meaning "writing").

The first recorded use of the term was in 1499 by Johannes Trithemius in his [*Steganographia*](https://en.wikipedia.org/wiki/Steganographia), a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in [invisible ink](https://en.wikipedia.org/wiki/Invisible_ink) between the visible lines of a private letter. Some implementations of steganography that lack a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) are forms of [security through obscurity](https://en.wikipedia.org/wiki/Security_through_obscurity), and key-dependent steganographic schemes adhere to Kerckhoffs's principle.

The advantage of steganography over [cryptography](https://en.wikipedia.org/wiki/Cryptography) alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which [encryption](https://en.wikipedia.org/wiki/Encryption) is illegal.

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

### Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every hundredth [pixel](https://en.wikipedia.org/wiki/Pixel) to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

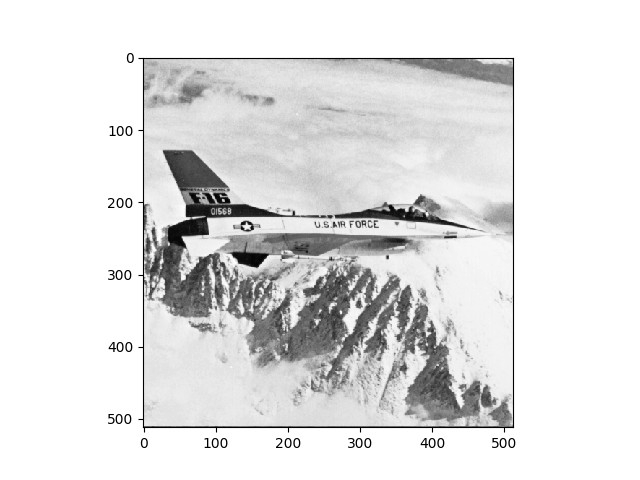
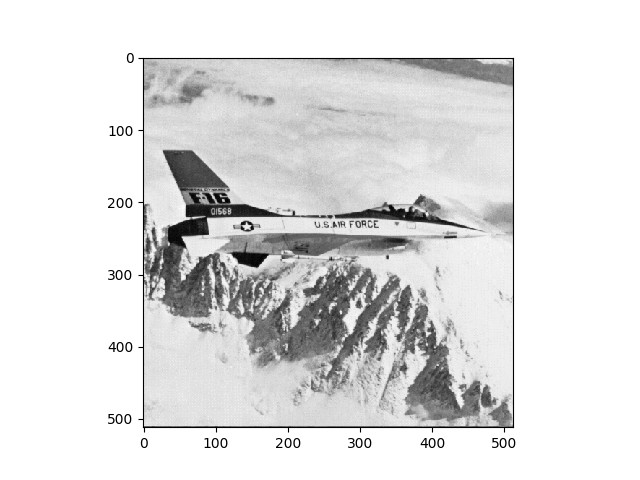
#### Embedding:

Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially.

The medium in which the message is embedded is referred as cover image and the resulting image and the message combined is referred as stego–image. Pixels of cover images will be modified after data embedding and also distortion occurs. The notion of distortion caused by data embedding is called the embedding distortion. In LSB embedding, the pixels with even values will be increased by one or more even it kept unmodified. The pixels with odd values will be decreased by one or more even it kept unmodiﬁed. LSB replacement is a well – known steganographic technique. In this embedded scheme, only LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms.



Python program to embed secret image in cover image



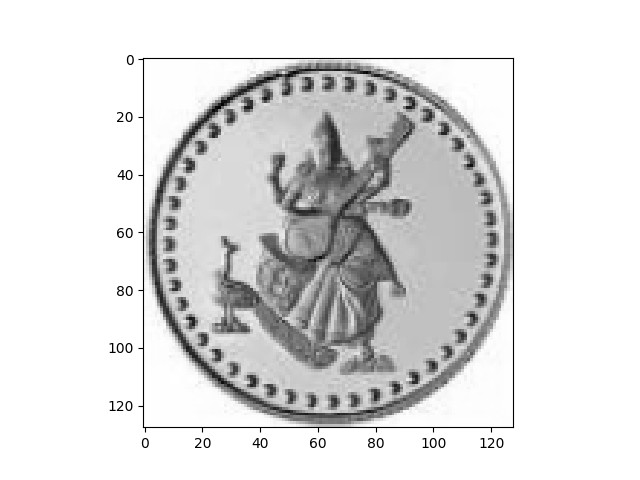
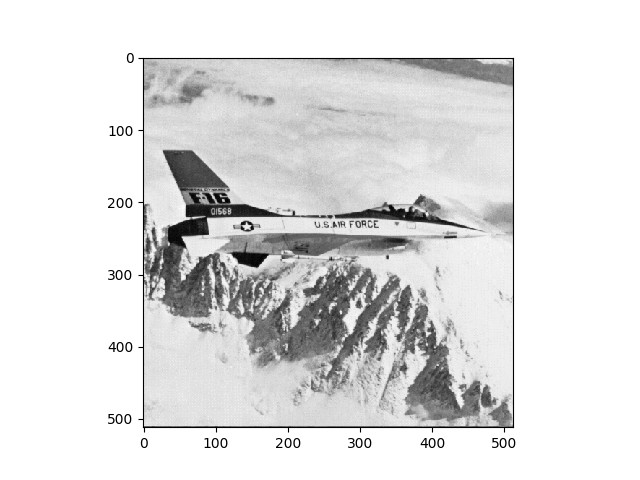
*Figure 16: Cover Image Figure 17: Cover Image steganographed with secret . image*

###### Extraction:

The eventual goal of steganalytic forensic is to extract the hidden messages embedded in steganographic images. A promising technique that addresses this problem partially is steganographic payload location, an approach to reveal the message bits, but not their logical order. It works by ﬁnding modiﬁed pixels, or residuals, as an artifact of the embedding process. This technique is successful against simple least-signiﬁcant bit steganography and group-parity steganography. The actual messages, however, remain hidden as no logical order can be inferred from the located payload. This paper establishes an important result addressing this shortcoming: we show that the expected mean residuals contain enough information to logically order the located payload provided that the size of the payload in each stego image is not ﬁxed. The located payload can be ordered as prescribed by the mean residuals to obtain the hidden messages without knowledge of the embedding key, exposing an inherent vulnerability in these embedding algorithms. Experimental results are provided to support our analysis



Python program to extract secret image from Steganographed image



*Figure 18: Steganographed Image Figure 19: Secret Image after extraction*

The secret image extracted from the steganographed image is checked against the original secret image which was embedded and was found to have a PSNR of infinity decibels and a IF ratio of 1.0

###### Quality Parameters

Image quality (often Image Quality Assessment, IQA) is a characteristic of an image that measures the perceived image degradation (typically, compared to an ideal or perfect image). Imaging systems may introduce some amounts of distortion or artifacts in the signal – for example by transcoding –, which affects the subjectively experienced quality and Quality of Experience for end users

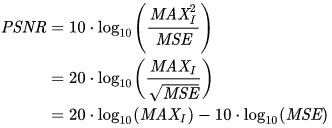
###### PSNR

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that aﬀects the ﬁdelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as:



................(3)

...............(4)

..............(5)

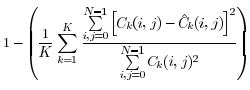


Python program to calculate PSNR value

###### IF

Image fidelity is a measure of the accuracy of the steganographed image. It is obtained by the following formula and as can be observed has no units.

### Image fidelity is also the measure of the accuracy of the reconstructed sky brightness distribution. A related metric, dynamic range, is a measure of the degree to which imaging artifacts around strong sources are suppressed, which in turn implies a higher fidelity of the on-source reconstruction. With conventional external calibration methods, even under the best observing conditions, the achieved dynamic range will rarely exceed a few hundred.



................(6)

Image Fidelity Ratio=

The original image will have a IF ratio of 1 which represents the ideal case. In practice this high a value is not obtainable. Thus we may conclude that IF ratio lies in the range [ 0, 1 ).



Python program to calculate IF ratio

###### Steganography on 10 images

Using a selection of 10 images from the miscellaneous image database from the *Signal and Image Processing Institute* of the *University of Southern California* the accuracy of the steganography process implemented isevaluated using the PSNR and IF quality parameters. The results thus obtained are tabulated below

Tabulated results of Steganography

**Image**

**Image Description**

**Size(in Kilobytes )**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 228.7 | 2 | 131072 | 34.7374618591506 | 0.998985709880603 |
| 228.7 | 1 | 65536 | 37.9121817344151 | 0.999511696083797 |
| 228.7 | 0.5 | 32768 | 40.8874922970601 | 0.999753873060701 |

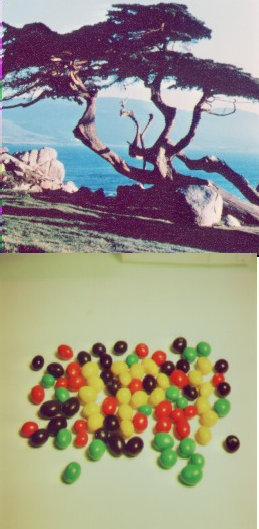
**Payload (in bpB)**

**Bit Capacity**

**PSNR**

**( in decibels ) IF**

tree



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 250.5 | 2 | 131072 | 34.5499405377818 | 0.999267084170642 |
| 250.5 | 1 | 65536 | 37.9336914342847 | 0.999663737055214 |
| 250.5 | 0.5 | 32768 | 40.8783630683984 | 0.999829308518224 |

candy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 242.5 | 2 | 131072 | 34.76805484058 | 0.998991407725784 |
| 242.5 | 1 | 65536 | 37.8317616427052 | 0.999501867409029 |
| 242.5 | 0.5 | 32768 | 40.8395385009569 | 0.999750788963705 |

house

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 953.8 | 2 | 524288 | 34.7706578263199 | 0.998903792918743 |
| 953.8 | 1 | 262144 | 37.8936649974265 | 0.999465937743878 |
| 953.8 | 0.5 | 131072 | 40.890815927238 | 0.999732159163235 |

peppers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 998.8 | 2 | 524288 | 34.7161849968069 | 0.999360878267818 |
| 998.8 | 1 | 262144 | 37.8720118642004 | 0.999690969817433 |
| 998.8 | 0.5 | 131072 | 40.8980817366449 | 0.999846044959887 |

f16

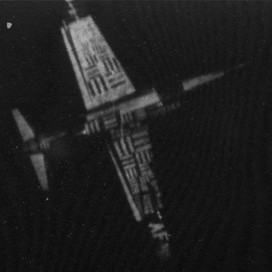
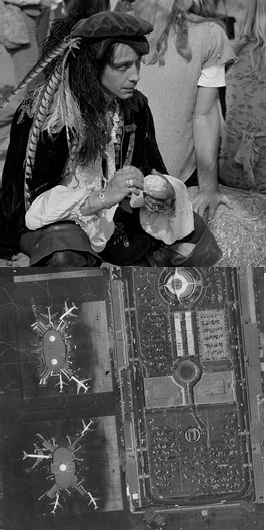
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 906.3 | 2 | 524288 | 34.7145294694091 | 0.998622930905314 |
| 906.3 | 1 | 262144 | 37.8297826180381 | 0.999327905383436 |
| 906.3 | 0.5 | 131072 | 40.8192863156695 | 0.999662339665021 |

bridge

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 969.7 | 2 | 524288 | 34.7977073360538 | 0.998866322740403 |
| 969.7 | 1 | 262144 | 37.9216300382577 | 0.999447799030238 |
| 969.7 | 0.5 | 131072 | 40.9581491673562 | 0.999725561364039 |

boat

bomber



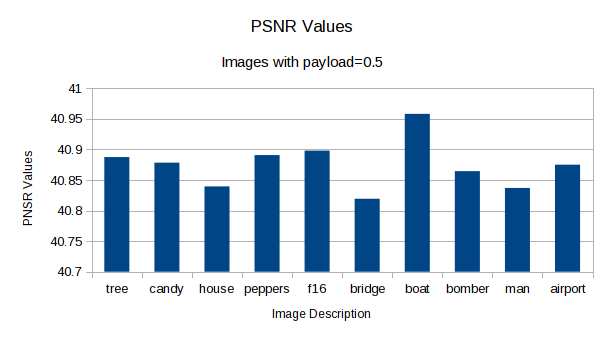
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3072 | 2 | 2097152 | 34.8184359210479 | 0.987487494424918 |
| 3072 | 1 | 1048576 | 37.9688870849062 | 0.993942419871568 |
| 3072 | 0.5 | 524288 | 40.8644354008967 | 0.996890114954186 |

man

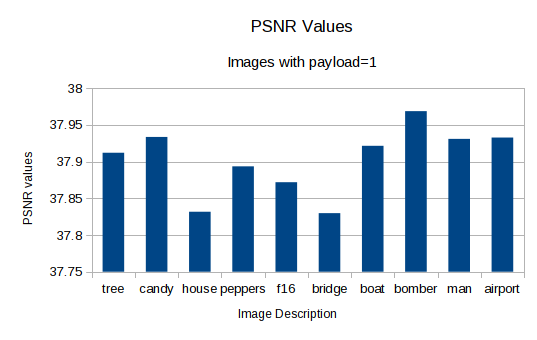
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3379.2 | 2 | 2097152 | 34.808101851223 | 0.998094384514455 |
| 3379.2 | 1 | 1048576 | 37.9310380261728 | 0.999071586053264 |
| 3379.2 | 0.5 | 524288 | 40.837036948306 | 0.999524509588456 |

airport

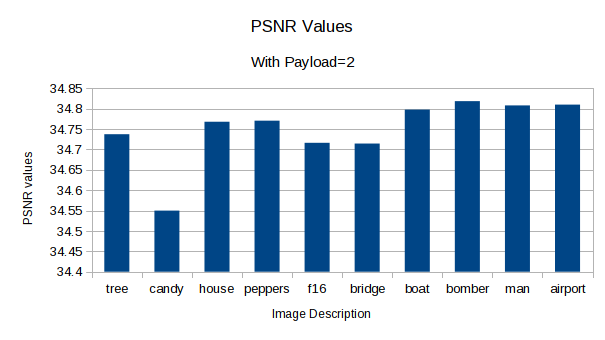
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3379.2 | 2 | 2097152 | 34.8099939481196 | 0.997362836341408 |
| 3379.2 | 1 | 1048576 | 37.9329038684313 | 0.998715168752354 |
| 3379.2 | 0.5 | 524288 | 40.8750855702205 | 0.999347428774448 |



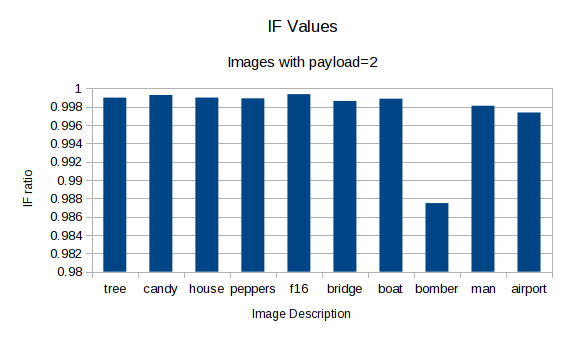
*Figure 20: Bar plot of PSNR values of selected images when steganographed with payload 0.5 X-axis : Image names Y-axis: PSNR Values in decibels*



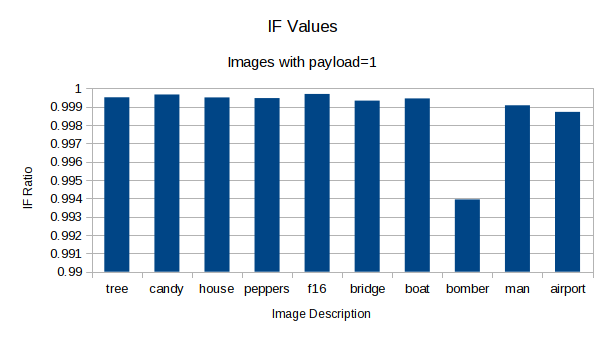
*Figure 21: Bar plot of PSNR values of selected images when steganographed with payload 1 X-axis : Image names Y-axis: PSNR Values in decibels*



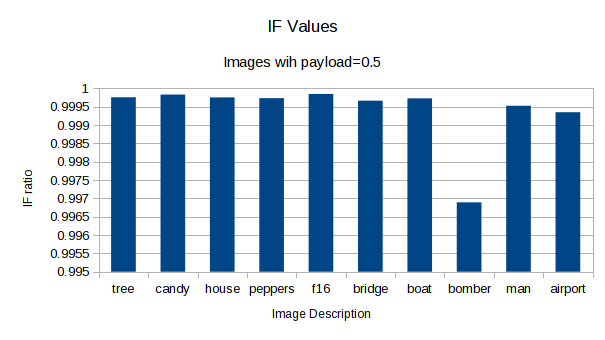
*Figure 22: Bar plot of PSNR values of selected images when steganographed with payload 2 X-axis : Image names Y-axis: PSNR Values in decibels*



*Figure 23: Bar plot of IF ratios of selected images when . steganographed with payload 2 X-axis : Image names Y-axis: IF Ratios*



*Figure 24: Bar plot of IF ratios of selected images when steganographed with payload 1 X-axis : Image names Y-axis: IF Ratios*



*Figure 25: Bar plot of IF ratios of selected images when steganographed with payload 0.5 X-axis : Image names Y-axis: IF Ratios*

## CONCLUSION

We have developed a few good introductory image processing programs. There are many more complex modifications that may be made to the images. For example, we may apply a variety of filters to the image. The filters use mathematical algorithms to modify the image. Some filters are easy to use, while others require a great deal of technical knowledge.

Various techniques have been developed in Image Processing during the last four to five decades. Most of the techniques are developed for enhancing images obtained from unmanned spacecrafts, space probes and military reconnaissance flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices, graphics software etc.

Recent works have been going on in the field of security, and hopefully it will improve the future scope of image processing.

## REFERENCES

1. R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography,” J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.
2. F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding—A Survey,” Proc. IEEE, vol. 87, no. 7, 1999, pp. 1062–1078.
3. J. Fridrich and M. Goljan, “Practical Steganalysis—State of the Art,” Proc. SPIE Photonics Imaging 2002, Security and Watermarking of Multimedia Contents, vol. 4675, SPIE Press, 2002, pp. 1–13.
4. Digital Image Processing, 4th Ed. by Rafael C. Gonzalez and Richard E. Woods © 2018 ISBN: 9780133356724
5. University of Southern California Viterbi School of Engineering Signal and Image Processing Institute miscellaneous image database was used throughout this project. The Miscellaneous volume consist of 44 images, 16 color and 28 monochromes. The sizes are 14 256x256, 26 512x512, and 4 1024x1024.

[http://sipi.usc.edu/database/database.php?volume=misc&image=6#top](http://sipi.usc.edu/database/database.php?volume=misc&amp;image=6&amp;top)

1. A set of secret images where obtained from Google Image Search