A Project Report On

**LSB** **IMAGE** **STEGANOGRAPHY**

A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree.

**Bachelor** **of** **Technology** **In**

**Computer** **Science** **&** **Engineering** **(CYBER** **SECURITY)**

**Submitted by**

**(Student Name)**

1. **NIKHILA**

**T. SAIVASANTH**

**K. GOURAV** **SRIVASTHAV**

**(Roll No)**

**(21H51A6202)**

**(21H51A6235)**

**(20H51A6234)**

Under the esteemed guidance of K.Sharath Kumar

Assistant professor,CSE (Cyber Security)

**Department** **of** **Computer** **Science** **&** **Engineering**

**(CYBER** **SECURITY)**

**CMR** **COLLEGE** **OFENGINEERING** **&** **TECHNOLOGY** KANDLAKOYA,MEDCHALROAD, HYDERABAD – 501401

**(NAACAccredited** **with** **‘A+’Grade** **&** **NBAAccredited)** **(Approved** **by** **AICTE,** **Permanently** **Affiliated** **to** **JNTU** **Hyderabad)**

**KANDLAKOYA,MEDCHAL** **ROAD,** **HYDERABAD-501401** **2021-2025**

**CMR COLLEGE OF ENGINEERING &TECHNOLOGY**

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**(CYBER SECURITY)**



**CERTIFICATE**

This is to certify that the Project report entitled **“Lsb** **Image** **Steganography”** being submitted by **A.Nikhila** **(21H51A6202),** **T.Sai** **Vasanth** **(21H51A6235),** **K.Gourav Srivasthav** **(20H51A6234)** in partial fulfillment for the award of **Bachelor** **of** **Technology** **in** **Computer** **Science** **and** **Engineering** **(Cyber** **Security)** is a record of bonafide work carried out his/her under my guidance and supervision. The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree

**K.Sharath Kumar**

**(AssistantProfessor)**

**(Dept.** **of** **CSE-CyberSecurity)**

**Dr.R.** **VenkateswaraReddy**

**(Assoc.** **Professorand** **HOD)**

**(Dept.** **of** **CSE-Cyber** **Security)**

**ACKNOWLEDGEMENT**

Withgreat pleasure I want to take this opportunity to express my heartfelt gratitude to all the people who helped in making this project work a grand success.

I am grateful to **K.Sharath Kumar,** Assistant Professor, Dept. of Computer Science and Engineering-Cyber Security for his valuable suggestions and guidance during the execution of this project work.

I would like to thank **Dr.** **R.** **Venkateswara** **Reddy**, Head of the Department of Computer Science and Engineering-Cyber Security, for his moral support throughout the period of my study in CMRCET.

I amhighly indebted to **MajorDr.V.A.Narayana**, Principal CMRCET for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching& Non- teaching staffof Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr.** **Ch.** **Gopal** **Reddy**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in completion of this project work

A.Nikhila T.Sai Vasanth

K.Gourav Srivasthav

21H51A6202 21H51A6235 20H51A6234

**DECLARATIONS**

We hereby declare that results embodied in this Report of Project on **“LSB**

**Image** **Steganography”** are from work carried out by using partial fulfillment of the

requirements for the award of B.Tech degree. We have not submitted this report

to any other university/institute for the award of any other degree.

**NAME**

A. Nikhila

1. SaiVasanth
2. Gourav Srivasthav

**ROLL NO** **SIGNATURE**

(21H51A6202)

(21H51A6235)

(20H51A6234)



**ABSTRACT**

This paper, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.

**TABLEOFCONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **CHAPTERS** | | **DESCRIPTION** | **PAGE** **No.** |
| 1 |  | INTRODUCTION | 7 |
|  | 1.1 | OBJECTIVES | 8 |
| 2 |  |  |  |
|  | 2.1 | LITERATURE REVIEW | 9 |
|  | 2.2 | EXISTING SOLUTIONS | 10 |
|  | 2.3 | SYSTEM REQUIREMENTS  SYSTEM REQUIREMENTS | 10 |
| 3 |  | PROPOSEDSOLUTION | 11 |
|  | 3.1 | PROPOSEDSOLUTION | 11 |
|  | 3.2 | LSB METHDOLOGY | 12 |
|  | 3.3 | LSB DECOMPOSION | 13 |
| 4 |  | ARCHTECTURE |  |
|  | 4.1 | BLOCK DIAGRAM | 14 |
| 5 |  | IMPLEMENTATION | 15 |
| 6 |  | RESULT | 18 |
| 7 |  | CONCULUSION AND FUTURE SCOPE |  |
|  | 7.1 | CONCULUSION | 19 |
|  | 7.2 | FUTURESCOPE | 19 |
| 8 |  | REFRENCES | 20 |



**1.** **INTRODUCTION**

Image steganography plays a major role in the data hiding method suitable for various applications like satellite communication, medical field, military and wireless. The use of multimedia digital signal has become very popular in the last decade due to the spread of wireless Internet-based services such as introduction of the fourth-generation mobile communication systems, user can transfer data up to 1 Gbps .Due to the availability of low cost editing tools, digital data can be easily copied, modified and retransmitted in the network by any user. To effectively support the growth of multimedia communications, it is essential to develop tools that protect and authenticate digital information. In this contribution, we present a novel embedding scheme based on the LSB technique. If the value of the pixel of an image is changed by a value of '1' it does not affect the appearance of the image. This idea helps us to for hiding data in an image Applications, etc.

In recent years, communication between two people or between groups of people has become easy due to the enormous growth of internet. So, security and confidentiality of highly sensitive data has become an issue of supreme importance and concern. To protect the information from an unauthorised person data hiding method has been developed. Three methods are interlinked to data hiding are cryptography, watermarking and steganography. The main theme of cryptography is to secure communication by changing the data into a form that an unauthorised person cannot understand. Digital watermarking is the act of embedding a watermark permanently into digital data in which the watermark can be easily detected (or) extracted later in order to ensure the authenticity of the digital data. The digital data may be audio, video, images and text. The embedded watermark is a signature that refers to the ownership of the data for copyright protection

**7**



|  |  |
| --- | --- |
| **1.1** **OBJECTIVE**  The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another”.  1. In a Gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by “3”.This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also.  2.Image can likewise be taken as a medium yet sound steganography is additionally difficult in light of the attributes of human sound-related framework like vast power, dynamic scope of listening to and extensive scope of discernable recurrence.  3.Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.        **8** |  |
|  |  |

**2.1** **LITERATUREREVIEW**

The project focuses on building an image steganography, we have referred few previously published papers and works of the various individual in this field. Our Literature Survey mainly focused onTechniques for detecting forged images.

1.In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), [1] Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional .

2. Presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer.

3. In the year of 2012 Hemalatha, S, Acharya, U.D. and Renuka [6] presented Integer Wavelet Transform (IWT) is used to hide the key thus it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations.

**9**



**2.2** **EXISTING** **SOLUTIONS**

•**Text** **semagrams**: where the information is concealed by using different methods for presenting the data.

• **Visual** **semagrams:** where innocent-looking object hides the message.

• **Jargon** **code:** where the utilization of understood language by agreed parties is used in a different way to common usage.

•**Covered** **null** **cipher:** in which the Payload is concealed into a collection of interlacing instructions agreed upon by the users.

• **Covered** **grille** **cipher:** in which a template is used over a cover object that enables the selection of specific characters which constitute the meant message to be shown while the others are characters that are covered.

**2.3** **SYSTEM** **REQUIREMENTS**

**1.** **HARDWARE** **REQUIREMENTS**

System 32 bit with 4 GB RAM

**2.** **SOFTWARE** **REQUIREMENTS**

Operating System : Coding Language : Tools :

Windows Python

Visual Studio Code

**10**



**3.PROPOSED** **SYSTEM**

**3.1** **PROPOSED** **SOLUTION**

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

**FUTURE** **SCOPE:**

•Understanding the working of code is not complicated in case of both the users and the admin. Easy to operate. In the near future, the most important use of steganographic techniques will probably be lying in the field of least significant bit.

•Ability to read and process a large amount of data

•Scalable

**11**



|  |
| --- |
|  |
| **3.2** **LSB** **Methdology**  In LSB steganography, the least significant bits of the cover media’s digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography changes the last bit of each of the pixel values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale color value. Suppose the first eight pixels of the original image have the following gray color values:  01010010 01001010 10010111 11001100 11010101 01010111 00100110 01000011  To hide the letter Z whose binary value of ASCII code is 10110101, we would replace the LSBs of these pixels to have the following new values:  01010011 01001010 10010111 11001101 11010100 01010111 00100110 01000011  Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats for the color image are difficult to detect contrary to 8 bit form.    **12** |
|  |

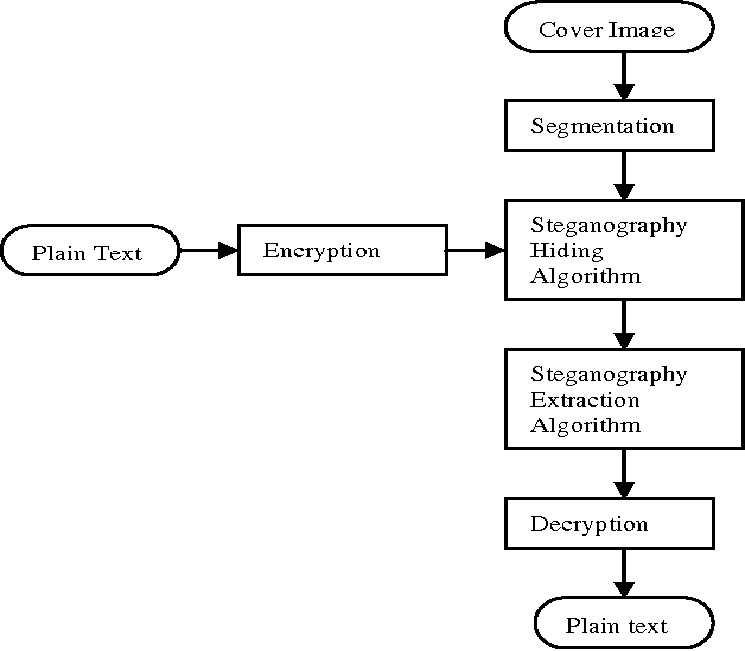


**3.3** **LSB** **DECOMPOSITION**

There are two important components, cover image and hiding data, in data hiding technique. The cover image I is an 8-bit gray scale image. The size of cover image is m×n. The hiding data H embedded in I is g-bits bit stream. We use the equation below to express image C, data D and each pixel separately.

One of the simplest systems for embedding digital data into a digital cover is the Least Significant Bit method .Consider an N×M image in which each pixel value is represented by a decimal number in the range determined by the number of bits used. In a gray-scale image, with 8 bit precision per pixel, each pixel assumes a value between [0, 255] and each positive number P can be represented by: This property allows the decomposition of an image into a collection of binary images by separating the into n bit planes. In the classical LSB embedding methods, the secret message is inserted into the least significant bit plane of the cover image either by directly replacing those bits. The amount of data to be embedded may also be fixed or variable in size depending on the number of pixels selected. The main advantage of such a technique is that the modification of the LSB plane does not affect the human perception of the overall image quality as the amplitude variation of the pixel values is bounded by ±1. The masking properties of the Human Visual System allow significant amounts of embedded information to be unnoticed by imperceptible by the average observer under normal viewing conditions. “Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal. A detailed review of these techniques is given in. Other advantages of LSB data hiding included high embedding capacity and low computational complexity. The main disadvantages are the weaknesses with respect to robustness, tampering, geometric attacks, filtering, and compression.

**13**

I

**4.ARCHITECTURE**

**4.1** **BLOCK** **DIAGRAM**

**14**



**5.IMPLEMENTATION**

**SOURCE** **CODE:**

import cv2

import numpy as np

from PIL import Image

#converts data into binary

def data2binary(data):

if type(data)==str:

p = ''.join([format(ord(i),'88b')for i in data])

elif type(data)==bytes or type(data)==np.ndarray:

p=[format(i,'08b')for i in data]

return p

#hide data in given img

def hidedata(img, data):

data +="$$"

d\_index=0

b\_data=data2binary(data)

len\_data=len(b\_data)

#iterate pixels from image and upgrade

for value in img:

for pix in value:

r,g,b=data2binary(pix)

if d\_index < len\_data:

pix[0]=int(r[:-1] + b\_data[d\_index])

d\_index+=1

**15**

I

if d\_index <len\_data:

pix[1]=int(g[:-1] + b\_data[d\_index])

d\_index+=1

if d\_index <len\_data:

pix[2]=int(b[:-1] + b\_data[d\_index])

d\_index+=1

if d\_index >=len\_data:

break

return img

def encode():

img\_name=input("\n enter image name:")

image =cv2.imread(img\_name)

img=Image.open(img\_name,'r')

w,h=img.size

data=input("\n enter message:")

if data==0:

raise ValueError("Empty Data")

enc\_img=input("\n enter encoded image name:")

enc\_data=hidedata(image,data)

cv2.imwrite(enc\_img,enc\_data)

img1=Image.open(enc\_img,'r')

img1=img1.resize((w,h), Image.LANCZOS)

#optimize with 65%quality

if w != h:

img1.save(enc\_img, optimize=True, quality=65)

else:

img1.save(enc\_img)

#decoding

def find\_data(img):

bin\_data=""

for value in img:

**16**

for pix in value:

r,g,b=data2binary(pix)

bin\_data+=r[-1]

bin\_data+=g[-1]

bin\_data+=b[-1]

all\_bytes=[bin\_data[i:i+8] for i in range(0,len(bin\_data),8)]

readable\_data=""

for x in all\_bytes:

readable\_data+=chr(int(x,2))

if readable\_data[-2:]=="$$":

break

return readable\_data[:-2]

def decode():

img\_name=input("\n enter image name:")

image =cv2.imread(img\_name)

img=Image.open(img\_name,'r')

msg=find\_data(image)

return msg

def steganography():

x=1

while x!=0:

print('''\n Image Steganography

1.encode

2.decode''')

u\_in=int(input("\n enter your choice:"))

if u\_in ==1:

encode()

else:

ans=decode()

print("\n your message:"+ans)

x=int(input("\n enter 1 for continue otherwise 0:"

steganography() **17**





**6.RESULT**

**a.** **Original** **image** **in** **png** **format b.** **Encrypted** **image** **in** **png** **format**

**18**

I



22

|  |  |
| --- | --- |
| **7.** **CONCLUSIONAND** **FUTURE** **SCOPE**  **7.1** **CONCLUSION**  I conclude that Steganography has unique advantages for net-espionage agents. Even if a file is known or suspected to contain Steganographic software, it is almost impossible to extract the information until the correct password is obtained. Steganography is beneficial for securely storing sensitive data, such as hiding system passwords or keys within other files. In places where standard cryptography and encryption is outlawed, Steganography can be used for covert data transmission.  **7.2** **FUTURE** **SCOPE**  Still efforts have to be made to increase the embedding capacity and maintain secrecy. In this method we can hide text file equal to the size of the image. Efforts can be made to hide text files having more size than image size. The secret keys have to be known to both sender and receiver. Keys are not sent in cover-images but are distributed separately. A technique can be evolved so that these keys can be generated and distributed covertly. The Transform Domain method can be utilized if more security is required. If Steganography is used with Cryptography, it will prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques  **19** |  |
|  |  |
|  |  |



**8.REFERENCES**

Vasco Pereira and Tiago Sousa, “Evolution of Mobile Communications: from 1G to 4G”, in Proc. Of The 2nd International Working

Conference on Performance Modeling and Evaluation of Heterogeneous Networks, HET-NETs’04, West Yorkshire, U.K., July 2004

1. <http://studentweb.niu.edu/9/~Z172699/Description.html>

M. Pavani1, S. Naganjaneyulu, C. Nagaraju, ”A Survey on LSB Based Steganography Methods” International Journal Of Engineering And

Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467

Stuti Goel, Arun Rana, Manpreet Kaur,”A Review of Comparison Techniques of Image Steganography”, IOSR Journal of Electrical and

Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48

2.<http://dimabatenkov.info/ssis_project/methods.htm>

3. <http://dhsprojects.blogspot.in/2012/08/ieee-2012-separable-reversible-data.html>

A. I. Kahdum, ”IBN AL-HAITHAM Journal for pure & applied Science”, Vol.21(1) 2008

4. <http://studentweb.niu.edu/9/~Z172699/Description.html>

Diego De Luca Picione , Federica Battisti , Marco Carli ,Jaakko Astola , and Karen Egiazarian,”A FIBONACCI LSB DATA HIDING

TECNIQUE”,14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by

EURASIP

5. <http://imagelpcmatlab.blogspot.in/2013/12/matlab-implementation-of-steganography.html>

6. <http://www.asciitable.com/>

7. <http://www.viprefect.com/application-areas>

8. <http://studentweb.niu.edu/9/~Z172699/Conclusion.html>

**20**