DELHI TECHNOLOGICAL UNIVERSITY
(formerly Delhi College of Engineering)

Electronics and Communication Department

PROJECT REPORT

Image Steganography based on analysing connected objects and image blocks

MENTOR : Dr Sudipta Majumdar

Submitted by:

Aakriti Yadav	(2K10/EC/002)
Bhuvi Chopra	(2K10/EC/045)
Dhwani Kapoor	(2K10/EC/053)
Ekta Sengar	(2K10/EC/056)

CONTENTS

CERTIFICATE

This is to certify that the under mentioned students have carried out the project '**Image Steganography using connected objects and image blocks**' in partial fulfillment of the degree of B.TECH in Electronics and Communication Engineering from Delhi Technological University during 2013-2014. They completed the project under my guidance.

Aakriti Yadav	(2K10/EC/002)
Bhuvi Chopra	(2K10/EC/045)
Dhwani Kapoor	(2K10/EC/053)
Ekta Sengar	(2K10/EC/056)

Dr. Sudipta Majumdar

(Assistant Professor)

Electronics and Communication Department

ACKNOWLEDGEMENT

O MY GOD, TO WHOM I PRAY,
INCREASE MY KNOWLEDGE DAY BY DAY.

After this little prayer to almighty, I extend my utmost, heartfelt acknowledgement to my respected teachers and Guides, who embody vast knowledge and experience & perform the task of God by imparting knowledge to me & moulding my future. One is confronted with great difficulty when words find themselves unable to express what one feels in the depth of heart.

We would like to thank our mentor Dr Sudipta Majumdar(Department of Electronics and Communication, Delhi College of Engineering) for giving us an opportunity to research on the topic 'Steganography' with constant guidance, help and support.

We would like to thank Delhi Technological University for providing us excellent facilities needed to complete our project.

Objective

Implementing Image Steganography using Connected Objects approach and image blocks in MATLAB.

Project Overview

Image steganography is the technique of hiding secret messages in a digital image. It exploits the weakness of Human Visual System (HVS).

Over the past few years, numerous 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.

Problem with steganography is the once it is realised that there is a hidden message within the media that is used for communication, it is normally relatively easy to extract the message. The only solution is to create new steganographic methods that cannot be easily detected. We have proposed two such methods.

The first method is based on dividing the image into blocks and identifying the optimum block for data hiding.
The second approach is based on finding connected objects and identifying the optimum object for data hiding while maintaining the image quality.

Software used:

MATLAB language is used in the implementation of the concept. The language is chosen due to its fast compilation time and its powerfulness in handling the concept of the program. Further the ease of programming and the interactive graphics environment lead to this decision of choosing MATLAB as the developing tool in this project.

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

Steganographic messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stego text. For example, the letter size, spacing, typeface, or other characteristics of a covertext can be manipulated to carry the hidden message; only the recipient (who must know the technique used) can recover the message and then decrypt it. Steganography uses in electronic communication include steganographic coding inside of a transport layer, such as an MP3 file, or a protocol, such as UDP.

The project 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

Encryption is the process of encoding a message in such a way as to hide its contents. Modern Cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called ***keys.*** A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key.

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injected payload (the signal to covertly embed) are visually (and ideally, statistically) negligible; that is to say, the changes are indistinguishable from the noise floor of the carrier.

An overview of Internet Security

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Everyday tons of data are transferred through the Internet through e-mail, file sharing sites, socialnetworking sites etc to name a few. As the number of Internet users rises, the conceptof Internet security has also gain importance. The fiercely competitive nature of thecomputer industry forces web services to the market at a breakneck pace, leavinglittle or no time for audit of system security, while the tight labour market causesInternet project development to be staffed with less experienced personnel, who may have no training in security. This combination of market pressure, low unemployment, and rapid growth creates an environment rich in machines to be exploited, and malicious users to exploit these machines.

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 including 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. The advantage of LSB-based method is easy to implement and high message pay-load.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

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 variant.

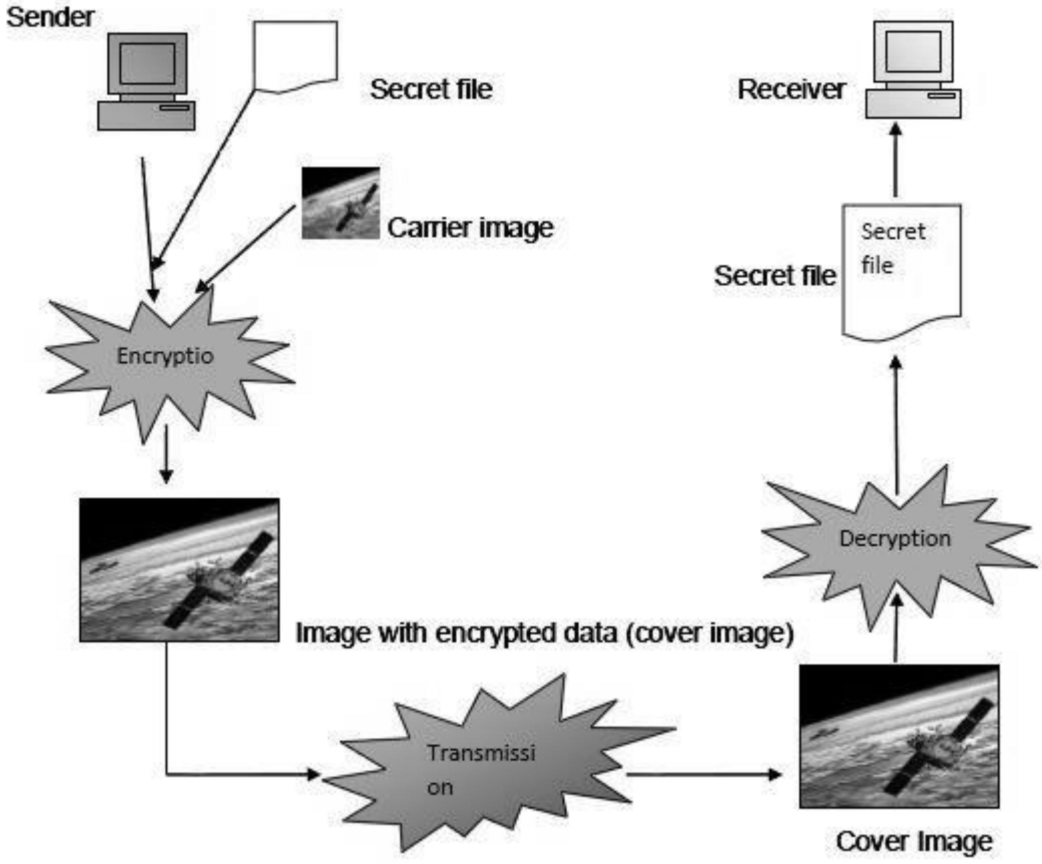
This project aims at the implementation of the concept of steganography. There are many methods of implementation of this concept available to us but the method I have used here is 'The LSB substitution method'. These techniques are based on modifying the least significant bits (LSBs), of the pixel values in the space domain.

In this project we mainly concentrated on embedding the data into an image. Normally, after embedding the data into the image, the image may lose its resolution. In the proposed approach, Image Steganography has been designed to embed information in images while maintaining/enhancing the image quality. Two separate codes were used based on analyzing block detection and object detection. The speed of embedding the data into the image is also high in the proposed approach. The image is protected and the data to the destination is sent securely.

The common modern technique of steganography exploits the property of the media itself to convey a message.

The following media are the candidate for digitally embedding message:

- Plaintext
- Still imagery
- Audio and Video
- IP datagram



Still imagery steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

For example: a 24-bit bitmap will have 8 bits, representing each of the threecolor values (red, green, and blue) at each pixel. If we consider just the blue there will be 28 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.

This technique can be directly applied on digital image in bitmap format as well as for the compressed image format like JPEG. In JPEG format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used as the carriers of the hidden message.

The details of above techniques are explained below:

Modification of LSB of a cover image in 'bitmap' format .

In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel. For example we will try to hide the character ‘A’ into an 8-bit color image.

We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this:

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this:

00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111

The only problem with this technique is that it is very vulnerable to attacks such as image compression and formatting.

Application of LSB technique during discrete cosine transformation (DCT) on cover image:

The following steps are followed in this case: -

1. The Image is broken into data units each of them consists of 8 x 8 block of pixels.

2. Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.

3. After applying DCT, one DCT Coefficient is generated for each pixel in data unit.

4. Each DCT coefficient is then quantized against a reference quantization table.

5. The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.

6. Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

If a stego or the modified image has good image quality, it can avoid being suspected during the transmission of the hidden secret.

Therefore, data hiding techniques should satisfy the following requirements:-

INVISIBILITY:-

The stego or the modified image should not appear to have gone under manipulation. This means that when one sees the image he must feel the image to be just an another image in transmission. This lets the image not being suspected in any reason .This characteristic of the stego or the modified image is desired to be in the highest grade or degree.

HIDING CAPACITY:-

The number of secret bits that can be hidden into the host image should be as large as possible. It is a desired thing that the size of the secret data file must be smaller then the host image or the original image file (in the project we have taken the host image to be at least 8 times larger then the secret data file).This is done so as to increase the size and the quantity of the data which can be hidden in the host or the original image. As large the size of the host image is, more the quantity of the data that can be hidden in the host image and thus more is the amount of secret information that can be sent via the host image.

DATA SECURITY:-

The embedded secrets must be secure. This simply means that the secret message cannot be extracted by the illegal user. When one sees the image he must feel the image to be just another image in transmission. Also the method which is used must be secret enough to accomplish the desired task. In this project we have used the LSB substitution method.

STEGNALYSIS

Steganalysis is the term used for decoding or attacking a steganographic message so as that the hidden message is revealed. There are several ways to go about attacking a steganographic message. These ways are based upon the assumption that there is a suspicion of a hidden message within the transmitted media, or the steganalyst has tools to detect such an event. A known stego attack is where the original cover-object and the stego-object are known along with the steganography algorithm tool. The stego-object could be an image with a message behind it. The original cover-object could be the original media that has not been altered. A stego-only attack is where only the stego-object is known. A chosen stego attack is when the availability of the steganographic tool and the stego object are at hand. A steganographic tool is used to implement and detect hidden information. A known message attack is the analysis of known patterns that correspond to hidden messages, which may help against attacks in the future. A known cover attack is when the original cover-object and the stego object are both available to decipher the message. The steganalyst generates a stego-object from some steganography tool or algorithm from a chosen message. The goal in this attack is to determine corresponding patterns in the stego-object that may point to the use of specific steganography tools or algorithms. (This is the most powerful attack)

Another problem with steganography is that once it is realised that there is a hidden message within the media that is used for communication, it is normally relatively easy to extract the message. The only answer is to create new steganographic methods that cannot be easily detected.

Project Details

Algorithm 1

1. A test image of size 32x32 pixels is taken as the cover image. The image is separated into its red, blue and green components. Blue component is chosen to embed the message.

2. Image is separated into 64 blocks of size 4x4 each and variance is calculated for each block and a variance matrix is formed.

3. Similarly, mean is calculated for each block and a mean matrix is formed.

4. A block with maximum value of mean and minimum value of variance is chosen for embedding the message bits. This will ensure least degradation and it enhances the image quality for human visual perception.

5. The least significant bits of the pixel values of that block are replaced with message bits.

6. Both the original image and stego image are displayed.

Algorithm 2

1. A test image of size 112x165 pixels is taken as the cover image.
2. The test image is converted into a binary image using a global threshold value.
3. Connected objects are identified, pixel values of each object are found.
4. Mean and variance of each object is calculated.
5. The object having maximum value of mean and minimum value of variance is chosen for embedding the message bits. This will ensure least degradation and it enhances the image quality for human visual perception.
6. The least significant bits of the pixel values of that object are replaced with message bits.
7. Both the original image and stego image are displayed.

Code 1:

```matlab
%loading a test image
%test image is of size 32x32 pixels

RGB=imread('testimage.png');

%separating the image into red, blue and green components
R=RGB(:,:,1);
G=RGB(:,:,2);
B=RGB(:,:,3);

%we've chosen the blue component to embed the message
K = B

%separating the image into 64 blocks of size 4x4 each and calculating
%variance of each block.
i=1;
j=1;

for x=[1:4:32]
    for y=[1:4:32]
B1 = K(x:x+3,y:y+3);
b = std2(B1);
u(i,j) = b^2;
j=j+1;
    end
    i=i+1;
    j=1;
end

variance2=u;
v2 = reshape(variance2.',1,[]);


subplot(1,2,1), imshow(B)
subplot(1,2,2), stem(v2)

variance2 %variance matrix

[v2_sort,IX] = sort(v2)
G1=IX
%calculating the mean for each block
i=1;
j=1;

for x=[1:4:32]
    for y=[1:4:32]
B1 = K(x:x+3,y:y+3);
a = reshape(B1.',1,[]);
m = mean(a);
w(i,j)=m;
j=j+1;
    end
    i=i+1;
    j=1;
end
```

```
mean2=w(1:8,1:8); % mean matrix

m2=reshape(mean2.',1,[])

temp=[1 1 1 1 1 1 1 1;1 1 1 1 1 1 1 1;1 1 1 1 1 1 1 1;1 1 1 1 1 1 1 1;1 1 1
1 1 1 1 1;1 1 1 1 1 1 1 1;1 1 1 1 1 1 1 1;1 1 1 1 1 1 1 1];

%taking reciprocal of the variance matrix and adding it to the mean matrix
%to get an index matrix(parameter matrix such that mean + inverse of
variance is maximum)
variance_reciprocal= temp./variance2;

variance_mean=variance_reciprocal + mean2;

maxm_variance_mean1=max(variance_mean);

maxm_variance_mean=max(maxm_variance_mean1); %matrix with maximum index
selected

% calculating the indices of the block wrt index matrix with optimum
% minimum value of variance and maximum value of mean.

 [i,j]=ind2sub(size(variance_mean),
find(variance_mean==maxm_variance_mean))

 %calculating the indices of block coresspoding to image matrix

        x=(i-1)*4+ 1;
y=(j-1)*4 + 1;

%setting the selected block as the cover image
cover= K(x:x+3,y:y+3)

coverzero=double(cover);

cover1 = std2(cover);
cover_var = cover1^2;
%setting lsb of cover block pixels to 0

coverzero=bitset(coverzero,1,0);
    %message bit stream
    message = [ 1 0 1 1; 0 0 1 0; 1 0 1 0; 1 1 1 1]
    %embedding the message bits into the lsb of cover block
    stego = uint8(coverzero+message);
subplot(1,2,1), imshow(stego);title('Stego image')
subplot(1,2,2), imshow(K(x:x+3,y:y+3,:))
L=K;

K(x:x+3,y:y+3)= stego;

K_stego= K;

subplot(1,2,1), imshow(K_stego);title('Stego image-blue comp')
subplot(1,2,2), imshow(L); title('original image-blue comp')

RGB1=RGB;
B= K
```

```
%displaying the original and stego images in both blue colour component and
%true colours.
subplot(2,2,1), imshow(K_stego);title('Stego image-blue comp')
subplot(2,2,2), imshow(L); title('original image-blue comp')
subplot(2,2,3), imshow(RGB);title('Stego image')
subplot(2,2,4), imshow(RGB1); title('original image')

block_selected=reshape(variance_mean.',1,[]);
[C,I] = max(block_selected);
variance2
mean2
variance_mean
index_value=C
block_number=I
```

Code 2:

```
% Loading a test image
%test image is of size 448 by 660 pixels
image = imread('C:\Users\Twinkle\Desktop\abc.jpg');

% Resizing the test image to 112X165 pixels
test_image= imresize(image,0.25);
p= test_image;

%computing a global threshold (level) that will be used to convert the test
%image to a binary image
level=graythresh(p);
b=im2bw(p,level);
%finding connected objects
[L , num] = bwlabel(b,8);
num;
% L returns a matrix containing labels for the connected objects in binary
% image
%num returns the number of connected objects

%storing pixel values of objects in an array
for z=1:num
[r,c] = find(L==z);
rc = [r c];
si = size(rc)
n = si(1)
    for i= 1:n
      obj(z,i) = p(r(i),c(i));
    end

end

%isolating the pixel values and calculating mean and variance of each
%object
for i= 1:num
obj1 = obj(i,:)
obj2 = obj1(find(obj1 ~= 0))
st_dev=std2(obj2);
var(i)= st_dev^2;
obj_mean(i)=mean(obj2);
end
var;

obj_mean;

number_of_objects = num;

temp=ones(num)
temp1=temp(1,:)
var;

%taking reciprocal of the variance matrix and adding it to the mean matrix
%to get an index matrix(parameter matrix such that mean + inverse of
%variance is maximum)

var_reciprocal= temp1./var

var_mean= var_reciprocal + obj_mean
```

```
var_mean_maxm = max(var_mean)

%calculating the indices of the object with optimum minimum value of
%variance and maximum value of mean

obj_index = find(var_mean==var_mean_maxm)
 [r1,c1] = find(L==obj_index);
 rc1 = [r1 c1] ; % setting this object as the cover object

 si2 = size(rc1)
 hiding_capacity = si2(1);
n1 = si2(1)

% Generating a random sequence of message bits
n = n1;
numberOfOnes = n/2
indexes = randperm(n)
message = zeros(1, n);
message(indexes(1:numberOfOnes)) = 1;
message;

%embedding the message bits into the lsb of cover block
for i=1:n1
original(i) = p(rc1(i,1),rc1(i,2));
p(rc1(i,1),rc1(i,2))= p(rc1(i,1),rc1(i,2)) + message(i);
stego(i)=p(rc1(i,1),rc1(i,2));
end

stego_image= p;

subplot(1,2,2), imshow(p); title('Original Image')
subplot(1,2,1), imshow(test_image); title('Stego Image')

number_of_objects
var
obj_mean
var_reciprocal
var_mean
var_mean_maxm
rc1
hiding_capacity
message
original
stego
```

CONCLUSIONS

In the area of communication revolution, information has been an inevitable component. The attraction of web services is simplicity, firewall neutrality and lack of dependency on the implementation technology at the service end.

Efficient computing capabilities are therefore utilized. The availability of the required information at the press of a button is something favourable and therefore computers are used for this purpose. Thus, one way of potential taping is achieved.

The project "Steganography" after being tested and was found to be achieving what is meant for. But this system never provides a full proof solution for all their problems in the user point of view. The system is found to be 100% error free and ready for implementation.

The system has been designed in such a way that it can be modified with very little effort when such a need arises in the future. The system has been found to work efficiently and effectively. Due to its higher user friendliness, others may use these documents as a prototype for developing similar application.

References

- Abondoned Object Detection

  http://www.mathworks.in/help/vision/examples/abandoned-object-detection.html

- E. Franz, “Steganography preserving statistical properties,” in *5th International Working Conference on Communication and Multimedia Security*, 2002.

- Introduction to steganography, Brigitte Si Athabasca University, COMP607 Project, July, 2004

  http://io.acad.athabascau.ca/~grizzlie/Comp607/menu.htm

- Detecting a cell using Image Segmentation

  http://www.mathworks.in/help/images/examples/detecting-a-cell-using-image-segmentation.html

- Steganography and steganalysis-Robert Krenn, Internet Publication, March 2004 http://www.krenn.nl/univ/cry/steg/article.pdf

- Introduction to Object Detection http://www.cse.usf.edu/~r1k/MachineVisionBook/MachineVision.files/MachineVision_Chapter15.pdf

- Exploring Steganography: Seeing the Unseen Neil F. Johnson, Sushil Jajodia, George Mason University IEEE Computer, February 1998: 26-34. http://www.jjtc.com/pub/r2026.pdf

- Wikipedia

- Practical Data Hiding in TCP/IP - Kamran Ahsan and Deepa Kundur

  Multimedia and Security Workshop at ACM Multimedia,Juan-les-Pins, France, Friday, Dec 6th, 2002

  http://wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm02/ahsan_kundur.pdf