STEGANOGRAPHY METHODS

Submitted in partial fulfillment of the Degree of

Bachelor of Technology

May – 2012

Name of Student	Arpit Kishore Raizada	(081068)
	Harsh Sehrawat	(081088)
	Vipul Sharma	(081089)

Name of supervisor Dr. S.V. Bhooshan

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

CERTIFICATE

This is to certify that project report entitled "Steganography Methods", submitted by Arpit, Harsh and Vipul in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date: 19th May 2012

Supervisor's Name : Dr. S.V. Bhooshan

Designation: Head of Department

ACKNOWLEDGEMENT

We are grateful to our project guide Mr. S.V. Bhooshan, H.O.D., Dept of ECE JUIT, for his guidance, inspiration and constructive suggestions that helped us in the preparation of this project. He was always there guiding us, correcting us with attention and care. He took immense pain going through the project and made necessary correction as and when required.

We would also take this opportunity to thank our Institution and other faculty members without whom this project would be a distant reality.

Date : 1st June 2012

Arpit Kishore Raizada (081068)

Harsh Sehrawat (081088)

Vipul Sharma (081089)

TALBLE OF CONTENTS

LIST OF FIGURES

SUMMARY

Steganography is an art of hiding secret message in a cover media so that no one apart from intended recipient suspects the presence of hidden message. Think of all those pixels in an image file and each pixel is made up of different intensity values of red, green and blue colour. There are millions of pixels in an image. If we change a few of these intensity values the resulting picture would be almost similar to the original image. In fact, with naked eyes, no one can't detect that we have changed the image. In this project, data hiding in image and audio is proposed to embed high volume of data and facilitate secret and secure communication by using steganography techniques. An effective algorithm for this process has been presented, which hides the information in an audio and image file without producing any noticeable distortions. The coding is done using MATLAB.

CHAPTER 1

STEGANOGRAPHY

1.1 Introduction to Information Hiding

As audio, video and other works become available in digital form, the ease with which perfect copies can be made, may lead to large-scale unauthorized copying which might undermine the music, film, books and software publishing industries. These concerns over protecting copyright have triggered significant research to find ways to hide copyright messages and serial numbers into digital media; the idea is that the later can help to identify copyright violators, and the former to prosecute them, thus came the need of information hiding. The needs to embed information into such data aroused and give birth to digital watermarking. Watermarking was already in existence at that time.

At the same time, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. Techniques used in digital watermarking and other techniques were used so that data could be hidden in these cover messages. The field dealing with these techniques is called steganography.

Steganography is an important sub discipline of information hiding. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. This modern adaptation of steganographia (Trithemeus, 1462-1516), assumed from Greek σγεγαύμγ ,ьφραεζ literally means "covered writing"[1], and is usually interpreted to mean hiding information in other information.

1.2 A Brief History of Information Hiding (Steganography)

The first description of the use of steganography dates back to the Greeks.

- Herodotus [2] tells how a message was passed to the Greeks about Xerses' hostile intensions underneath the wax of a writing tablet, and describes the technique of dotting successive letters in a cover text with a secret ink, due to Aeneas the Tactician.

- Pirate legends tell of the practice of tattooing secret message, such as a map, on the head of someone, so that the hair would conceal it.

- Kahn tells of a trick used in China of embedding a code ideogram at a prearranged position in a dispatch; a similar idea led to the grille system used in medieval Europe, where a wooden template would be placed over a seemingly innocuous text, highlighting an embedded secret message.

- During WWII the grille method or some variants were used by spies. In the same period, the Germans developed microdot technology, which prints a clear, good quality photograph shrinking it to the size of a dot.

- More obscurely, during World War 2 a spy for the Japanese in the New York city, Velvalee Dickinson, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed how many of this or that doll to ship. The stego text in this case was the doll orders; the plain text being concealed was itself a code text giving information about the ship movements, etc. her case become somewhat famous and she became known as the DOLL WOMAN.

- There are rumors that during 1980's that Margareth Thatcher, then Prime Minister in UK, became so irritated about press leaks of cabinet documents that she had the word processors programmed to encode the identity of the writer in the word spacing, thus being able to trace the disloyal ministers.

- During the "Cold War" period, US and USSR wanted to hide their sensors in the enemy's facilities. These devices had to send the data to their nations, without being spotted.

Today Steganography is researched for both legal and illegal reasons.

- Among the first ones there is war telecommunications, which use spread spectrum or meteor scatter radio in order to conceal both the message and its source.
- In the industry market, with the advent of the digital communications and storage, one of the most important issues is copyright enforcement, so digital watermarking techniques are being developed to restrict the use of copyright data.
- Another important use is to embed data about medical images, so that there are no problems with matching patient's records and images.
- Among illegal ones is the practice of hiding strongly encrypted data to avoid controls by cryptography export laws.

1.3 Wisdom for Cryptography

Although steganography is different from cryptography, we can borrow many of the techniques and much practical wisdom from the later, more thoroughly researched disciples.

In 1883, Auguste Kerckhoffs enunciated the first principles of cryptographic engineering, in which he advises that we assume the method used to encipher data is known to the opponent, so security must lie only in the choice of key [3].

Applying this wisdom we obtain the tentative definition of a secure stego-system: one where an opponent who understands the system, but does not know the key, can obtain no evidence (or even ground for suspicion) that a communication has taken place. It will

remain a central principle that steganographic processes intended for wide use should be published, just like commercial cryptographic algorithms and protocols.

So one might expect that designers of copyright making systems would publish the mechanism they use, and rely on the secrecy of the keys employed. Sadly, this is not the case; many purveyors of such systems keep their mechanisms subject to nondisclosure agreements, sometimes offering the rationale that a patent is pending.

Any of these security-by-obscurity systems ever worked was a matter of luck. Yet many steganographic systems available today just embed the "hidden" data in the least significant bit of an image or audio file ——which is trivial for a capable opponent to detect and remove.

1.4 Principles of Steganography

The "classic" model for invisible communication was first proposed by Simmons [4] as the "prisoners' problem". Alice[1] and Bob are arrested for some crime and are thrown in two different cells. They want to develop an escape plan, but unfortunately all communication between them is arbitrated by a warden name Wendy. She will not let them communicate through encryption and if she notices any suspicious communication, she will place them in solitary confinement and thus suppress the exchange of all messages. So both parties must communicate invisibly in order not to arouse Wendy's suspicion; they have to develop a subliminal channel. A practical way to do so is to hide meaningful information in some harmless message: Bob could, for instance, create a picture of a blue cow lying on a green meadow and send this piece of modern art to Alice. Wendy has no idea that the colors of the objects in the picture transmit information.

1 In the field of cryptography, communication protocols usually involve two fictional characters named Alice and Bob.The standard convection is to name the participants in the protocol alphabetically or with a name whose first character matches their role.

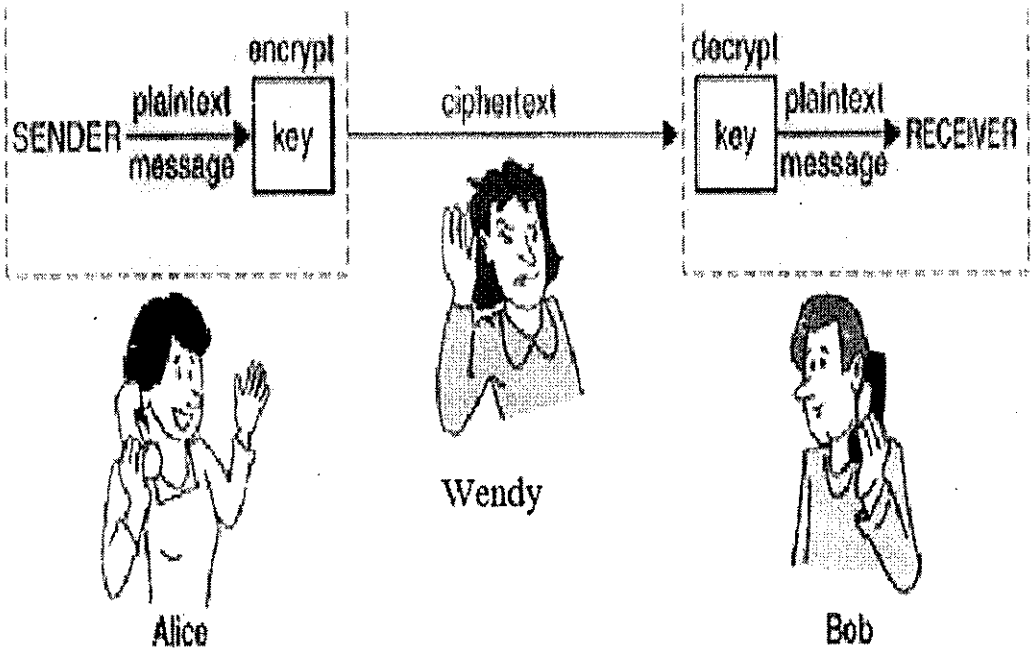


Fig. 1-1 The Prisoners' Problem [5]

Unfortunately there are other problems which may hinder the escape of Alice and Bob, Wendy may alter the message Bob has sent to Alice. For ex, she could change the color of Bob's cow to red, and so destroy the information; she then acts as an active warden. Even worse, if she acts in a malicious way, she could forge messages and send a message to one of the prisoner through the subliminal channel while pretending to be the order.

The above model is generally applicable to many situations in which invisible communication- steganography takes place. Alice and bob represented two communication parties, wanted to exchange secret information invisibly. The warden Wendy represents an eavesdropper who is able to read and probably alter the messages sent by the communication partners (see figure 1-1).

Whereas cryptographic techniques try to conceal the contents of a message, steganography goes yet a bit finder: it tries to hide the fact that a communication even exist. Two people can communicate covertly by exchanging unclassified messages

containing confidential information. Both parties have to take the presence of a passive, active or even malicious attacker into account.

1.5 Frameworks for Secret Communication

Most application of steganography follow one general principle, illustrated in figure1.2. Alice who wants to share secret message m with Bob, randomly chooses(using the random source r) a harmless message c, called cover object, which can be transmitted to Bob without rising suspicion, and embeds the secret message into c, probably by using a key k, called stego-key. Alice therefore changes the cover c to a stego-object s. This must be done in a very careful way, so that the third party, knowing only the apparently harmless message s, cannot detect the existence of the secret message. In a "perfect system", a normal cover should not be distinguishable from the stego-object, neither by a human nor by a computer readable data such as image file, digital sound, or written text.

Alice then transmits s over an insecure channel to Bob and hopes that Wendy will not notice the embedded message, Bob can reconstruct m since he knows the embedding method used by Alice and has the access to the key k used in the embedding process. This extraction process should be possible with the original cover c.

Thus the secrecy of the invisible communication lies mainly in the invisibility to distinguish cover-object from stego-objects.

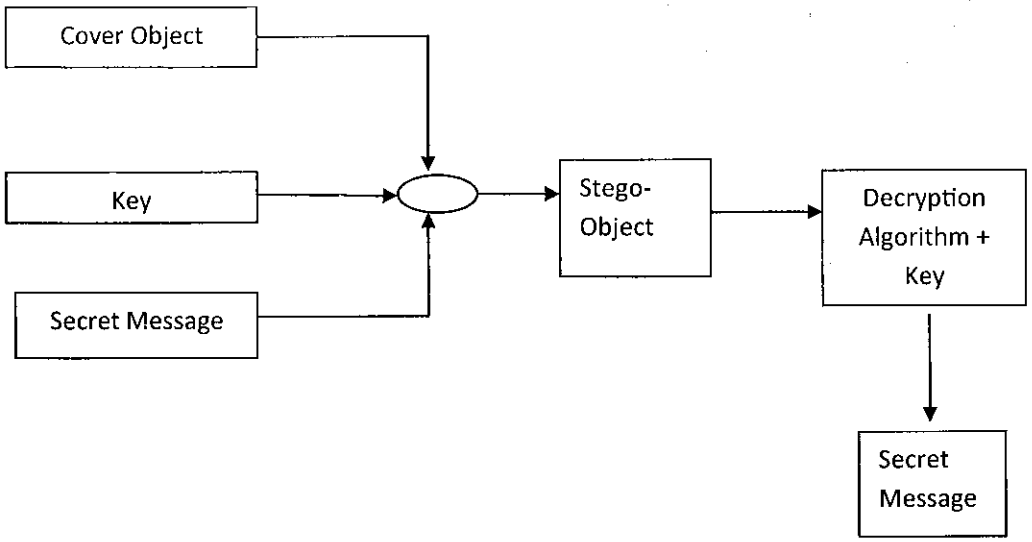


Fig. 1-2 Schematic description of Steganography

In practice however, not all data can be used as cover for secret communication, since the modifications employed in the embedding process should not be visible to any one not involved in the communication process. This fact requires the cover to contain sufficient redundant data, which can be replaced by the redundant data. In fact, it turns out that noisy data has more advantageous properties in most steganographic applications. Obviously a cover should not be used twice, since an attacker who has access to two "versions" of one cover can easily detect and possibly reconstruct the message. To avoid accidental reuse, both sender and receiver should destroy all covers they have already used for the information transfer.

1.6 Types of Steganography

Figure 1-3 shows how information hiding can be broken down into different areas. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent the message being detected by any other party. The other major area of steganography is copyright marking, where the message to be inserted is used to assert a copyright over a document. This can be further divided into watermarking and fingerprinting which will be discussed later.

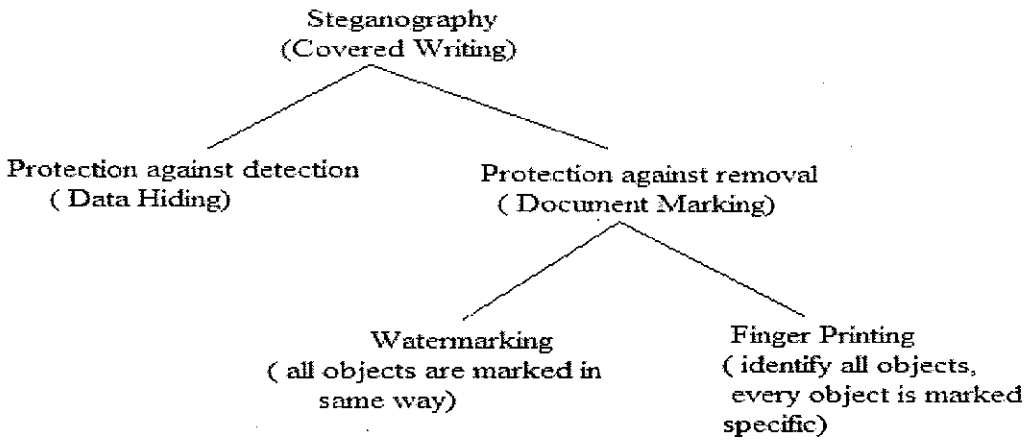


Fig. 1-3 Types of Steganography

Steganography and encryption are both used to ensure data confidentiality. However, the main difference between them is that with encryption anybody can see that both parties are communicating in secret.

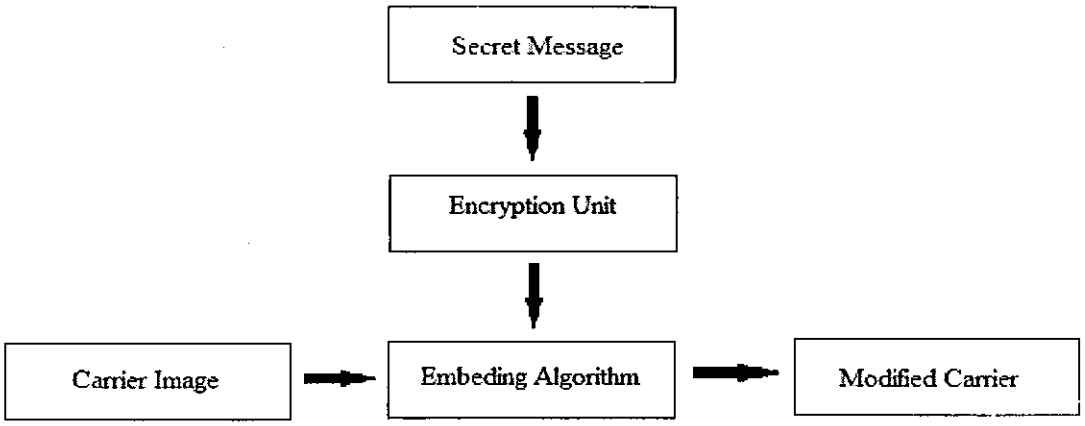


Fig. 1-4 Steganograhy with Encryption

Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for

some tasks for which encryption aren't, such as copyright marking. Figure 1-4 shows a comparison of both techniques for communicating in secret. Encryption allows secure communication requiring a key to read the information.

1.7 Properties of Hiding Schemes

Robustness

The ability to extract hidden information after common image processing operations: linear and nonlinear filters, lossy compression, contrast adjustment, recoloring, re-sampling, scaling, rotation, noise adding, cropping, printing, copying, printing, scanning.

Undetectability

Impossibility to prove the presence of a hidden message. This concept is inherently tied to the statistical model of the carrier image. The ability to detect the presence does not automatically imply the ability to read the hidden message. Undetectabilty should not be mistaken for invisibility- a concept related to human perception.

Invisibility

Perceptual transparency. This concept is based on the properties of the human visual system or the human audio system.

Security

The embedded information can't be removed beyond reliable detection by targeted attacks based on the knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message.

1.8 Applications

1. Most of the applications use steganography like a watermark to protect a copyright on information. Photo collection, sold on CD often have hidden message in photos which allow detection of unauthorized use. The same technique applied to DVDs is even more effective, since the industry build DVD recorders to detect and disallow copying of protected DVDs.

2. Even biological data, stored on DNA, may be a candidate for hidden messages as biotech companies seek to prevent the unauthorized use of their genetically engineered material. The technology is already in place for this: three New York researches successfully hide a secret message in a DNA sequence and sent it across the country. Sound like science fiction? A secret message in a DNA provides Star Trek's explanation for the dubious fact that all aliens seem to be human in prosthetic makeup.

3. Unobtrusive communication-Military and intelligence agencies.

4. Plausible deniability- Fair voting, personal privacy, limitation of liability.

5. Anonymous Communication- Vote privately, make political claim, access censored material, and preserve free speech.

1.9 Advantages and Disadvantages

Steganography is beneficial for securely storing sensitive data, such as system passwords or keys within other files. However, it can also pose serious problem because it's difficult to detect. Network surveillance and monitoring system will not flag message or files that contain steganographic data. Therefore, if someone attempted to steal confidential data, they could conceal it within another file and sent it in an innocent looking email.

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide.

Further steganography can be used to tag notes to online images (like post-it notes attached to paper files).

However, steganography has a number of disadvantages as well.Unlike encryption it generally requires a lot of overhead to hide a relatively few bits of information. However, there are ways around this. Also, once the steganographic system is discovered, it is rendered useless. This problem, too, can be overcome if the hidden data depends on some sort of key for its insertion and extraction.

Another limitation is due to the size of the medium being used to hide the data. In order for steganography to be useful the message should be hidden without any major changes to the object it is being embedded in. This leaves limited room to embed a message without noticeably changing the original object. This is more obvious in compressed objects where many of the obvious candidates for embedding data are lost. What is left is likely to be the most perceptually significant portions of the file and although hiding data still possible it might be difficult to avoid changing the file.

Although many of the uses of steganography are perfectly legal, it can be abused by certain group. The potential exists for terrorist groups to communicate using these techniques to hide their messages and rumor persists that Al-Qaeda have used it to communicate. Also of concern is that these techniques are used by pedophiles to hide pornographic images within seemingly innocuous material.

As a result the need for detection of steganographic data has become an important issue for law enforcement agencies. Attempting to detect the use of steganography is called steganalysis and can be either passive, where the presence of the hidden data is detected, or active, where an attempt is made to retrieve the hidden data.

CHAPTER 2

The Project Theory

2.1 Outline

The project aimed on implementing a simple steganographic method on image and audio files using Graphical user interface for inputs and outputs. The Least Significant Bit (LSB) substitution method was implemented with some modifications on uncompressed BMP images so that the embedding becomes secure and makes use a key which must be mutually shared between the participants of the communication.

Diagramatically, the process of Steganography as we've implemented

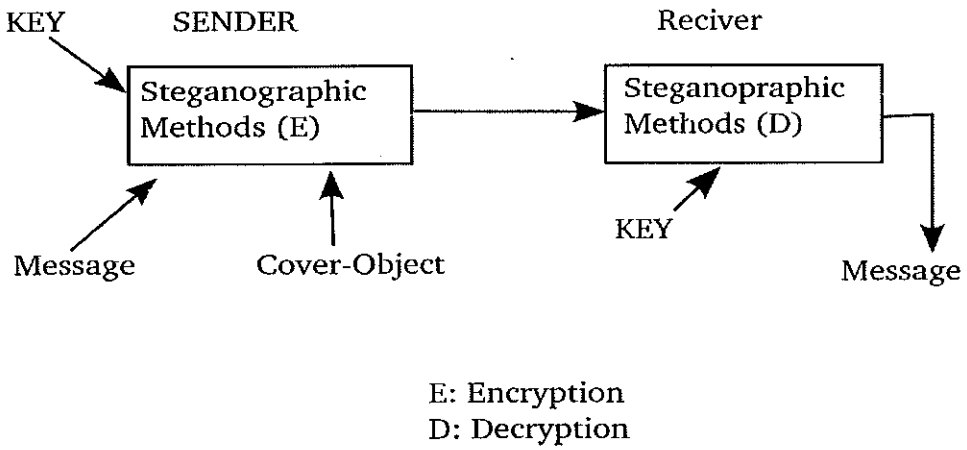


Fig. 2-1 Process of Steganography

2.2 Algorithm Used

Briefly, the key used and message bits are embedded after suitable gap depending on the algorithm used in the bit map image. This makes it a secret key steganographic technique.

2.2.1 Algorithm for Embedding

1. •Import the cover image .
2. •Import the message to be embedded.
3. •Ask user for the desired key.
4. •Convert the elements of image matrix and message matrix into 8-bit binary code.
5. •Embed the key and the secret message into the 2 LSb's of the layer 1 of the three dimesional image matrix.
6. •Combine back all the 3 layers of the cover image and save the image is some uncompressed format .
7. • The message is successfully embedded.

2.2.2 Algorithm for Extraction

1. • Import the Stego-object.
2. • Extract the key from the image.
3. • Ask user to enter the key.
4. • Compare the extracted password and the entered password.
5. • If key entered is correct , extract the message from the LSB of the layer 1 of the image matrix otherwise return the error message.
6. • Message is Extracted.

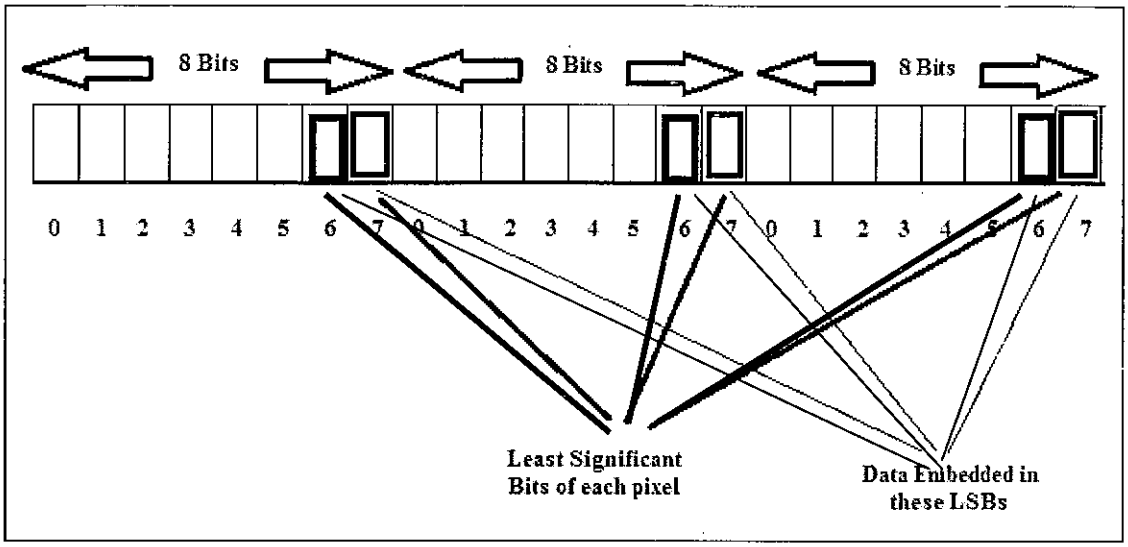
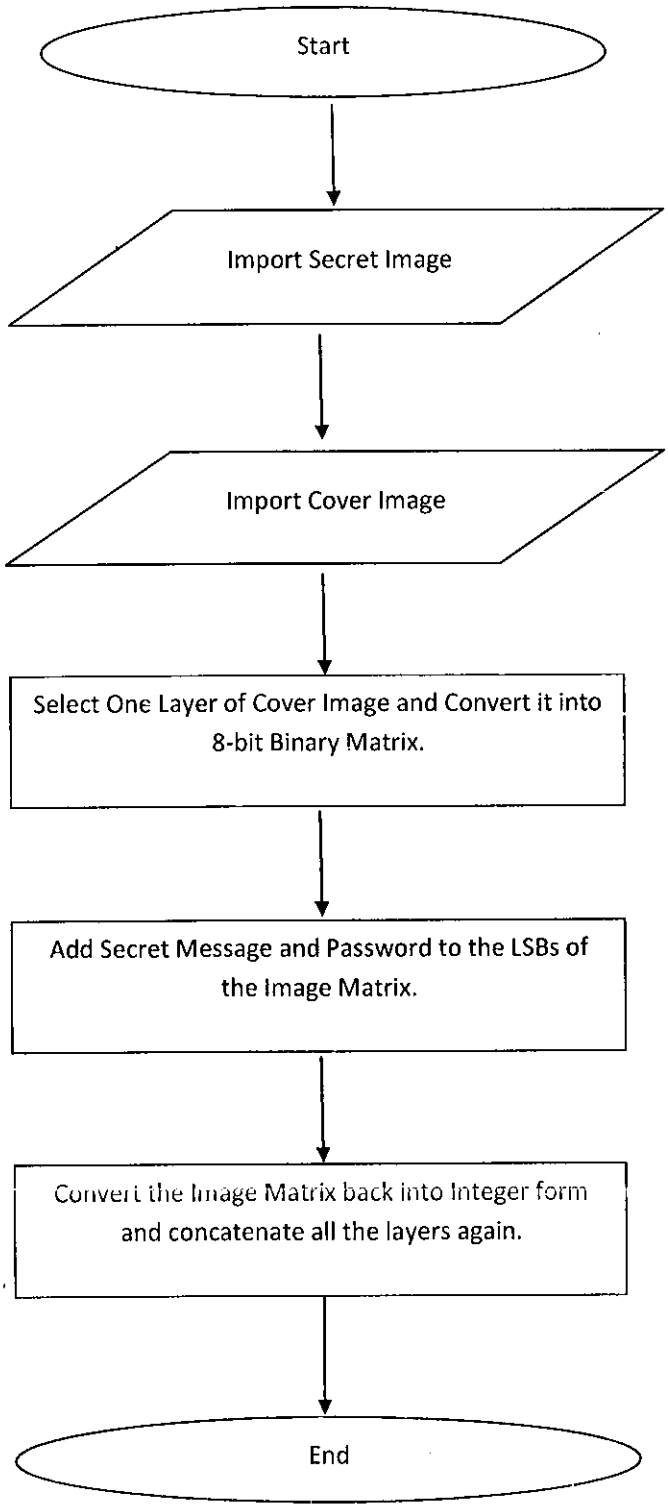


Fig. 2-2 Embedding Message Bits in the LSB of Pixels

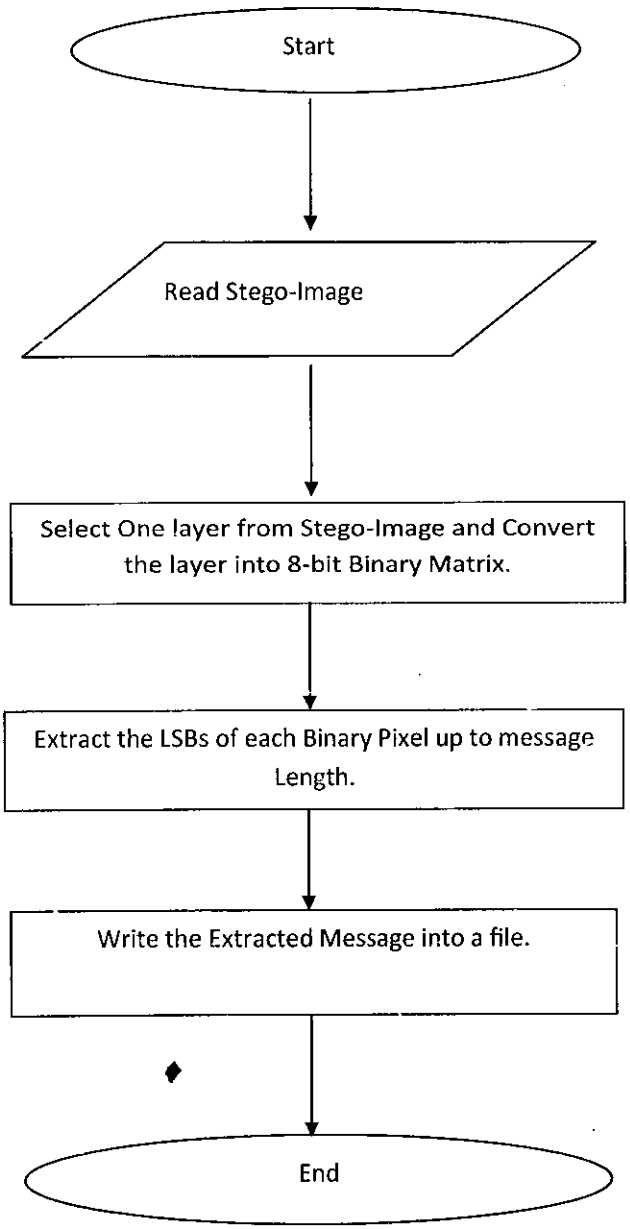
The process of LSB steganography deals with the embedding of the message bits in the LSBs of the image's pixel values. As shown in above figure 7^{th} and 8^{th} bit of the pixel is replaced by the secret message bits. In this way the secret message is embedded into the image without making a significant change in the pixel value of the original image.

2.3 Flow Charts

Encoding



Decoding


Start
Read Stego-Image
Select One layer from Stego-Image and Convert the layer into 8-bit Binary Matrix.
Extract the LSBs of each Binary Pixel up to message Length.
Write the Extracted Message into a file.
End

The process of Steganography used by use is briefly explained by the flow chart shown below. In this chart plain text is embedded into a carrier image by using suitable encryption algorithm. This embedding process generate a stego-image (1.0), which is then transmitted over a medium i.e. a wired or a wireless medium(2.0) to its destination. At the destination the decryption (3.0) of the message is done from its stego–image by using certain decryption algorithms, and then the text or secret message is decrypted from the stego-image. This provides a secure and covert transmission of data i.e. secret plain text or image files over a transmission medium with high security.

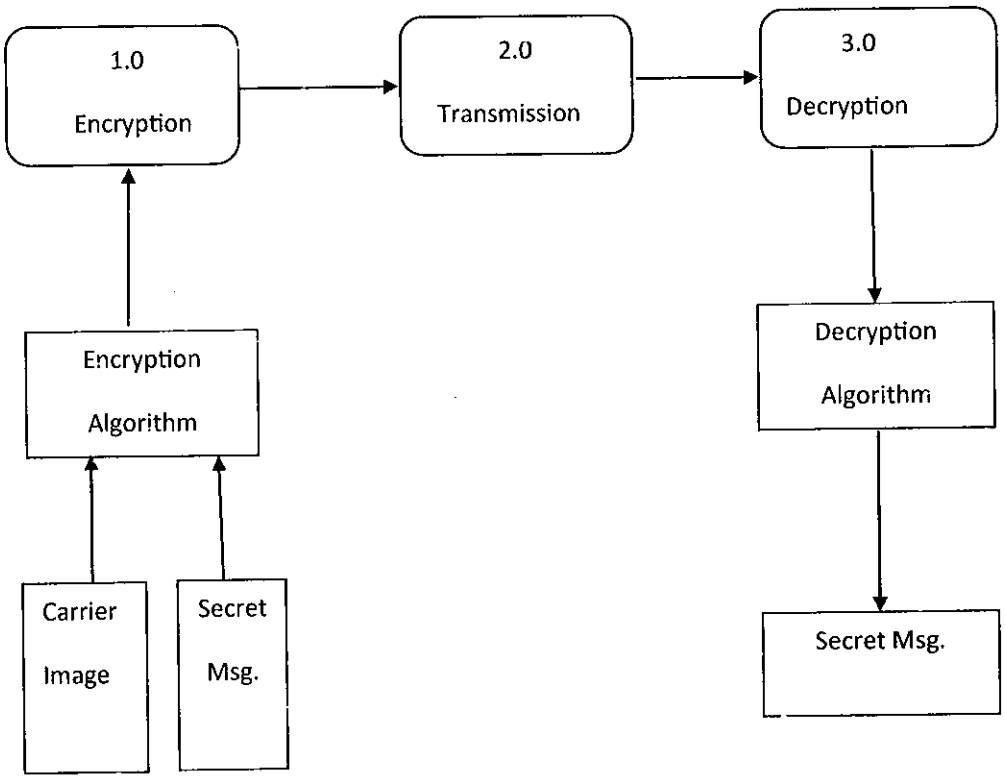


Fig. 2-3 Flow Chart of Process of Steganography

2.4 Code:

Code for Hiding Text Message in an Image File:

Encoding:

```
clearall;
password=input('enter the password:','s');
% desired password for security
numpass= uint8(password);
% converts the password from string to unsigned integer with ASCII values
bipass= de2bi(numpass',8);
% converts the integer into binary 8-bit code
ps=size(bipass);
ps1=ps(1,1);
% ps1 stores the password length(password lenght will be used in decoder)
passlen=de2bi(ps1,8);

msg=input('enter the message:','s');
% for entering the desired message to be encoded
nummsg= uint8(msg);
% converts the message from string to unsigned integer with ascii values
bimsg= de2bi(nummsg',8);
% converts the integer into binary 8-bit code
b=size(bimsg);
b1=b(1,1);          % b1 stores the message length

k=imread('cover.jpg');              % for importing the image
a=size(k);
a1=a(1,1);
a2=a(1,2);
y=k(1:a1,1:a2,1);                   % selects layer 1 of the three dimensional image matrix
y2=k(1:a1,1:a2,2);
y3=k(1:a1,1:a2,3);
z=de2bi(y',8);

 i=1;
%loop for embedding the password length into layer 1 of three dimensional image matrix
l=1;
m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
```

```
z(i,j)=passlen(l,m);
        m=m+1;
end
end
  i=i+1;
end

%loop for embedding the password into layer 1 of image matrix
for l=1:1:ps1
  m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
z(i,j)=bipass(l,m);
          m=m+1;
end
end
     i=i+1;
end
end

%loop for embedding the message into layer 1 of image matrix
for l=1:1:b1
  m=1;
while m<=8

if z(i,8)==0 && z(i,7)==0
for j=1:1:2
z(i,j)=bimsg(l,m);
          m=m+1;
end
end
     i=i+1;
end
end

fp=bi2de(z);          %converts 'z' into decimal form
x=0;

%loop for arranging the dimension of 'fp' matrix same as the dimensions of image matrix
for i=1:1:a1
for j=1:1:a2

     x=x+1;
s(i,j)=fp(x);
```

```
end
end

sf=cat(3,s,y2,y3);
% concatenates the altered layer s with y2 and y3 to get the colored image

imwrite(sf,'encoded.bmp');      % writes the image in uncompressed 'bmp' format
imshow(sf);                     % for displaying the image
```

Decoding:

```
clearall;
pass1=input('Enter the password: ','s');   % enter password to decode the message
numpass1= uint8(pass1);
% converts the entered password into unsigned integer form using ASCII values
bipass1=de2bi(numpass1',8);
% converts the password into binary 8-bit binary code

k=imread('encoded.bmp');                    % for reading the encoded image
a=size(k);
a1=a(1,1);
a2=a(1,2);
y=k(1:a1,1:a2,1);                           % selects layer 1 of the encoded image
z=de2bi(y',8);

i=1;

%loop for extracting the password length
l=1;
m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
binpasslen(l,m)=z(i,j);
        m=m+1;
end
end
  i=i+1;
end

passlen=bi2de(binpasslen);

%loop for extracting the password
for l=1:1:passlen
```

```
   m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
pass(l,m)=z(i,j);
            m=m+1;
end
end
      i=i+1;
end
end

%comparing extracted password with entered password
if pass == bipass1

  x=input('enter message size');

% loop for extracting the hidden message
for l=1:1:x
      m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
hidden(l,m)=z(i,j);
               m=m+1;
end
end
         i=i+1;
end
end

   m1=bi2de(hidden);
   m2=m1';
message=char(m2)            % converts the message into character form

else
error('password entered is incorrect')

end
```

Code for Hiding Secret Image in an Image File

Encoding:

```
clearall;
password=input('enter the password:','s');          % desired password for security
numpass= uint8(password);
% converts the password from string to unsigned integer with ASCII values
bipass= de2bi(numpass',8);
% converts the integer into binary 8-bit code
ps=size(bipass);
ps1=ps(1,1);
% ps1 stores the password length(password lenght will be used in decoder)
passlen=de2bi(ps1,8);

 l=imread('message.jpg');      % for reading the message image
message=size(l);
c1=message(1,1);
c2=message(1,2);
l1=l(1:c1,1:c2,1);          % selects layer 1 of the three dimensional image matrix
bimsg=de2bi(l1',8);
b=size(bimsg);
b1=b(1,1);

 k=imread('cover.jpg');      % for reading the cover image
a=size(k);
a1=a(1,1);
a2=a(1,2);
y=k(1:a1,1:a2,1);                  % selects layer 1 of the three dimensional image matrix
y2=k(1:a1,1:a2,2);
y3=k(1:a1,1:a2,3);
z=de2bi(y',8);

 i=1;
%loop for embedding the password length into layer 1 of image matrix
l=1;
m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
z(i,j)=passlen(l,m);
        m=m+1;
end
end
   i=i+1;
end
```

```
%loop for embedding the password into layer 1 of image matrix
for l=1:1:ps1
   m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
z(i,j)=bipass(l,m);
            m=m+1;
end
end
      i=i+1;
end
end

%loop for embedding the message picture into layer 1 of image matrix
for l=1:1:b1
   m=1;
while m<=8

if z(i,8)==0 && z(i,7)==0
for j=1:1:2
z(i,j)=bimsg(l,m);
            m=m+1;
end
end
      i=i+1;
end
end

fp=bi2de(z);                    %converts 'z' into decimal form
x=0;
%loop for arranging the dimension of 'fp' matrix same as the dimensions of
image matrix
for i=1:1:a1
for j=1:1:a2

      x=x+1;
s(i,j)=fp(x);
end
end
sf=cat(3,s,y2,y3);
% concatenates the altered layer s with y2 and y3 to get the colored image

imwrite(sf,'encoded.bmp');   % writes the image in uncompressed 'bmp' format
imshow(sf);                  % for displaying the image
```

Decoding:

```
clearall;
pass1=input('Enter the password: ','s');          % enter password to decode the message
numpass1= uint8(pass1);
% converts the entered password into unsigned integer form using ASCII values
bipass1=de2bi(numpass1',8);

k=imread('encoded.bmp');                          % for reading the encoded image
a=size(k);
a1=a(1,1);
a2=a(1,2);
y=k(1:a1,1:a2,1);                                 % selects layer 1 of the encoded image
z=de2bi(y',8);

i=1;

%loop for extracting the password length
l=1;
m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
binpasslen(l,m)=z(i,j);
        m=m+1;
end
end
  i=i+1;
end

passlen=bi2de(binpasslen);

%loop for extracting the password
for l=1:1:passlen
  m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
pass(l,m)=z(i,j);
          m=m+1;
end
end
      i=i+1;
end
end
```

```
%comparing extracted password with entered password
if pass == bipass1

row=input('enter rows');          % rows of the message image matrix
col=input('enter column');        % columns of the  message image matrix

   x=row*col;

% loop for extracting the hidden message image
for l=1:1:x
      m=1;
while m<=8
if z(i,8)==0 && z(i,7)==0
for j=1:1:2
hidden(l,m)=z(i,j);
              m=m+1;
end
end
        i=i+1;
end
end

   m1=bi2de(hidden);
   m2=m1';
xi=0;

%loop for making the dimensions of the 'm1' matrix same as message image
for i=1:1:row
for j=1:1:col
x1=x1+1;
fin(i,j)=m2(x1);
end
end

imshow(fin)          % displays the message image

else
error('password entered is incorrect')
end
```

Code for Hiding Text in an Audio (.wav) File:

Encoding:

```
[filename, pathname] = uigetfile('*.wav','Select a file');
[y,fs,nbits,opts]=wavread([pathname filename],[1 2]);

%open a wav file for hidding text
fid1=fopen([pathname filename],'r');

%first 40 bytes make wav header,store the header
header=fread(fid1,40,'uint8=>char');

%41st byte to 43rd byte,length of wav data samples
data_size=fread(fid1,1,'uint32');

%copy the 16 bit wav data samples starting from 44th byte
[dta,count]=fread(fid1,inf,'uint16');

%close the file only wav data samples are sufficient to hide the text
fclose(fid1);

lsb=1;

msg='Hello how are you?';     %text message

msg_double=double(msg);      %convert it to double
msg_bin=de2bi(msg_double,8); %then convert message to binary
[m,n]=size(msg_bin);         %size of message binary
msg_bin_re=reshape(msg_bin,m*n,1);  %reshape the message binary in a column vector
m_bin=de2bi(m,10)';
n_bin=de2bi(n,10)';
len=length(msg_bin_re);      %length of message binary len=m*n
len_bin=de2bi(len,20)';      %convert the length to binary

identity=[1 0 1 0 1 0 1 0]';              %hide identity in first 8 wav data samples.

dta(1:8)=bitset(dta(1:8),lsb,identity(1:8));

%hide binary length of message from 9th to 28 th sample
dta(9:18)=bitset(dta(9:18),lsb,m_bin(1:10));
dta(19:28)=bitset(dta(19:28),lsb,n_bin(1:10));

%hide the message binary starting from 29th position of wave data samples
dta(29:28+len)=bitset(dta(29:28+len),lsb,msg_bin(1:len)');

fid2=fopen('new2.wav','w');%open a new wav file in write mode
```

```
%copy the header of original wave file
fwrite(fid2,header,'uint8');
fwrite(fid2,data_size,'uint32');

%copy the wav data samples with hidden text
fwrite(fid2,dta,'uint16');
fclose(fid2);
```

Decoding :

```
[filename, pathname] = uigetfile('*.wav','Select a file');
[y,fs,nbits,opts]=wavread([pathname filename],[1 2]);

%open the file with hidden text
fid1=fopen([pathname filename],'r');
header=fread(fid1,40,'uint8=>char');
data_size=fread(fid1,1,'uint32');

%read the wave data samples
[dta,count]=fread(fid1,inf,'uint16');

%close the file,only wav data samples are sufficient for extracting the text
ans=fclose(fid1);

lsb=1;

identity=bitget(dta(1:8),lsb)';
if identity==[1 0 1 0 1 0 1 0]

%extract the length of text from first 9th to 28th wav data samples
len_bin=zeros(20,1);
m_bin=zeros(10,1);
n_bin=zeros(10,1);

m_bin(1:10)=bitget(dta(9:18),lsb);
n_bin(1:10)=bitget(dta(19:28),lsb);

%convert the length to decimallen=bi2de((len_bin)');
len=bi2de(m_bin')*bi2de(n_bin');
secmsg_bin=zeros(len,1);

%extract the lsb from wave data sample
secmsg_bin(1:len)=bitget(dta(29:28+len),lsb);
```

```
secmsg_bin_re=reshape(secmsg_bin,len/8,8);
secmsg_double=bi2de(secmsg_bin_re); %convert it to decimal
secmsg=char(secmsg_double)'  %convert to char(ASCII)
end
```

Chapter 3

Experiment

3.1 Experiment 1

Embedding Secret Text Message in Image File

Input File: Cover Image shown below:

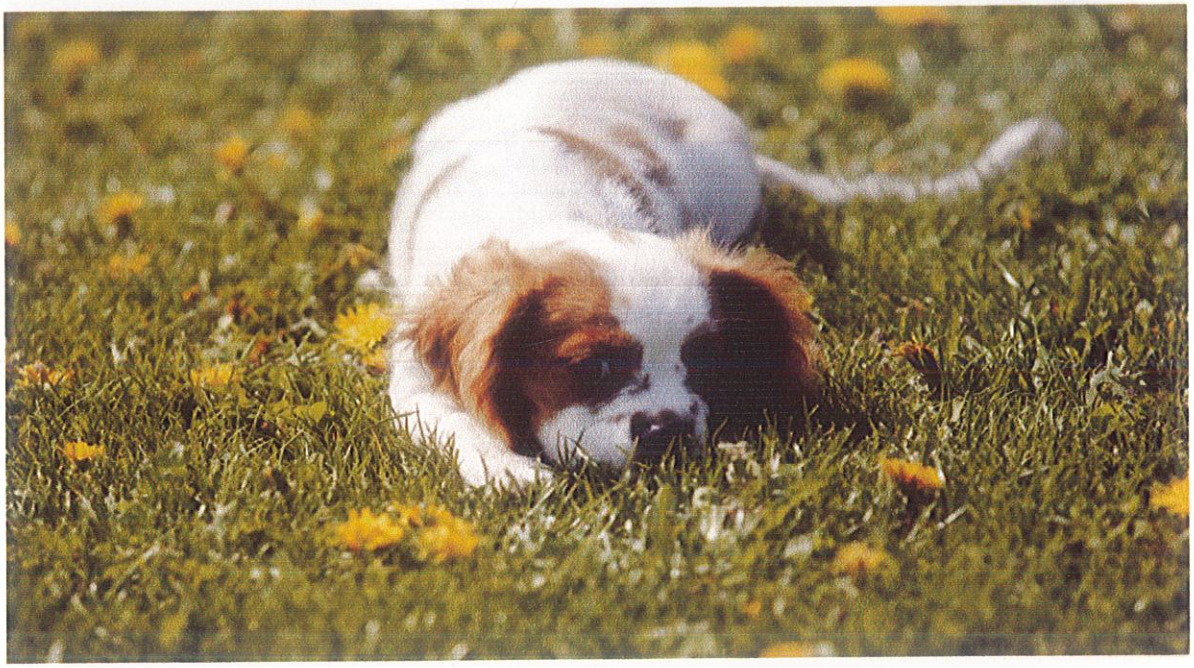


Fig. 3.1 Cover Image (Experiment 1)

Key: "abcd"

Secret Text : "Hello how are you ?"

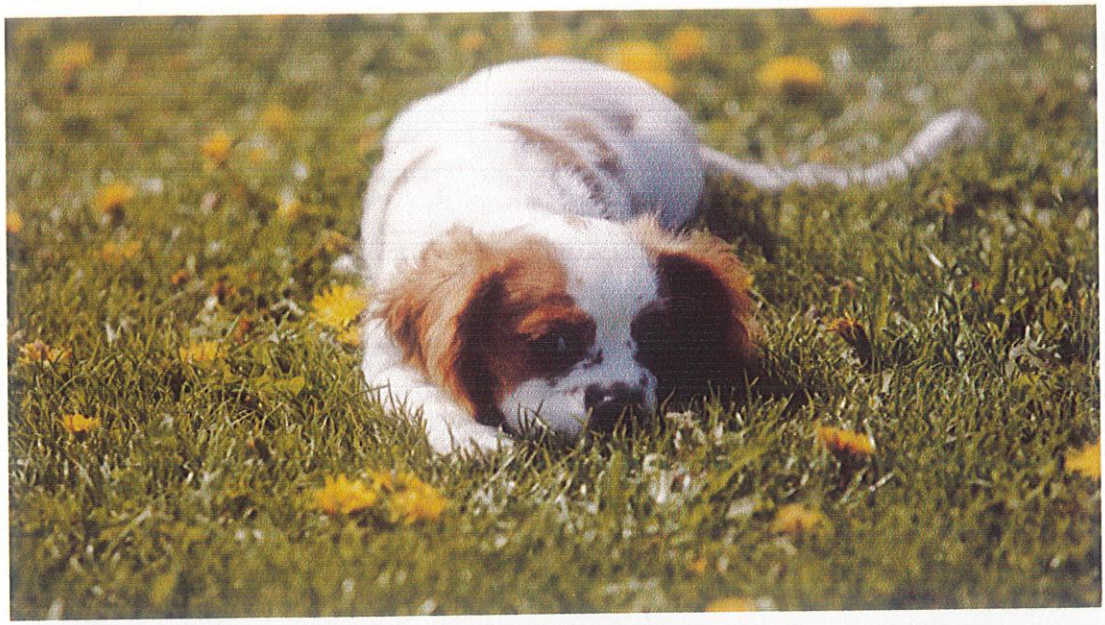


Fig 3.2 Output image

Extraction:

Input:Stego-object as shown above.

Key: "abcd"

Secret Message: "Hello how are you ?"

3.2 Experiment 2

Embedding Secret Image in an Image

Input File: Cover Image as shown below:

Fig. 3-3 Cover Image (Experiment 2)

Secret File: Message Image is as shown below.

Fig. 3-4 Message Object (Experiment 2)

Key: "abcd".

Output: Stego-object is as shown below:

Fig. 3-5Output image

Extraction:

Input File: Stego-Object as shown above.

Key: "abcd".

Fig- 3-6Message object as on Extraction

CHAPTER 4

Results and Conclusion

4.1 Results

The Stegenographic schemes which were present for more than 1000 years were studied and analyzed in details in this report. Various algorithms were analyzed, compared and implemented. For designing the steganographic application, we worked on different phases like encryption and decryption. An application for sending the personal data securely to the destination has been developed successfully. The design phase is the primary phase, which gives a brief idea about the different levels used for developing an application with the help of block diagrams. The software is designed in a user friendly manner. The most important phase in the project is the execution phase. The execution phase is developed with the help of design phase. For executing the application, we worked on two sections: one is encryption and another is decryption. As we designed the program using MATLAB, we faced some problems when writing the code, but at last we were successful in executing the program without errors.

In this project we mainly concentrated on embedding the data into an image and audio files. We have designed the steganographic application which embedded the data into the image. Normally, after embedding the data into the image, the image may lose its resolution. In the proposed approach, the image remains unchanged in its resolution as well in size. The speed of embedding the data into the image is also high in the proposed approaches such that the image is protected and the data to the destination is sent securely. For the decryption phase, we have used security keys like personal password for protecting the image from unauthorized modification, which improved the security level. There are many applications for image hiding but the proposed approach is easier for coding and the performance is better compared to other languages.

4.2 Conclusion

In the present world, the data transfer using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un-intended to him. The proposed approach in this project uses a new steganographic approach called image and audio steganograpgy.

The application creates a stego-object in which the personal data is embedded and is protected with a password which is highly secured. The main intension of the project is to analyze the various LSB steganography algorithms and develop a steganographic application using those algorithms such that it provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel. This project gave us good experience in dealing with the data security issues in theoretical as well as in technical domain. We did the project in a good manner with the help and guidance of our supervisor **Mr. S.V. Bhooshan.**

4.3 Future Work

The future work on this project will be to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg, .tif etc., in the future.

Further work could include developing a YASS (Yet Another Steganographic Scheme) and strong encryption algorithms.

REFERENCES

[1] Covered Writing Steganography: georgezapo.com/articles/covered-writing/

[2] History and Steganography: www.jjtc.com/stegdoc/sec202.html

[3]. Public Key Steganography: www.cs.cmu.edu/~biglou/pubkeystego.pdf

[4].Steganography for the Computer Forensics Examiner
www.garykessler.net/library/fsc_stego.html

[5]. Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[6]. Marvel, L.M. Boncelet Jr., C.G. &Retter, C., "Spread Spectrum Steganography", IEEE Transaction on image processing.

[7]. Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANSInstitute, January 2002

[8] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June2005

[9]. Johnson, N.F. &Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal,February 1998

[10]. Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[11]. Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[12]. Venkatraman, S., Abraham, A. &Paprzycki, M., "Significance of Steganography on Data Security",

[13]. http://www.jjtc.com/pub/r2026.pdf

[14]. www.ijcaonline.org/journal/number15/pxc387502.pdf.

[15]. Jamil, T., "Steganography: The art of hiding information in plain sight", IEEE Potentials,1999.

[16]. Alfred J, Met al., 1996. Hand book of applied Cryptography. First edition.

[17].Hide & Seek : An Introduction to steganography:Niles Provos and Peter Honeyman, IEEE Security & Privacy Magazine, May/June 2003.

[18]. Artz, D., "Digital Steganography: Hiding Data within Data", IEEE InternetComputing Journal, June 2001.

[19].S.William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50

[20]. Bloom,J. A. et al., 2008. Digital watermarking and Steganography.2nd edition.

[21]. Alfred J Metal., 1996. Hand book of applied Cryptography. First edition.

APPENDIX A

Steganography:It is the process of hiding digital data (text, image, audio or video) with in another digital data(text, image, audio, video).

Steganography Algorithms: These are the techniques by which we can hide a media within another media.

Steganalysis: Steganalysis is the art and science of detecting messages hidden using steganography.This is analogous to cryptanalysis applied to cryptography.

Cryptography: It is the process of encrypting a media so that it is not possible to understand without decrypting.

Internet Security: Internet security is a branch of computer security specifically related to the Internet. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Security Attacks: The data is transmitted from source to destination which is known as its normal flow. But the hackers might hack the network in order to access or modify the original data. These types of attacks are formally known as security attacks.