DATA DISGUISABLE MODUS

A Major Project report

Submitted in partial fulfillment of the requirement

For the award of the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

By

K. Srinivasa Rao **(R121842)**

P. Chandu **(R121743)**

Under the guidance of

Mr. A. Sreekanth Reddy

Lecturer

Department of Electronics and Communication Engineering

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

RK Valley – 513330

KADAPA

ACKNOWLEDGEMENT

We would like to take this opportunity to express our profound sense of gratitude to our guide **Mr. A. Sreekanth Reddy**, Lecturer, Rajiv Gandhi University of knowledge Technologies, for her constant guidance, supervision, motivation and encouragement all the way during the project, his annotations and criticisms are the key behind successful completion of this project work.

We also like to thank our beloved Head of the Department, Electronics and Communication Engineering, Assistant Prof. **M. Siva Rama Krishna** garu, for his cooperation and encouragement in completing this project by providing us proper lab facilities.

We, the members of the project, express thanks to the people who were directly or indirectly involved in this project for their overwhelming cooperation. Finally we would like to extend our heartfelt thanks to our beloved parents whose blessings and encouragement were always there as a source of strength and inspiration.

Project Associates

K.Srinivasa Rao (R121842)

P. Chandu (R121743)

CERTIFICATE

This is to be certified that Mr. K.Srinivasa Rao (R121842), Mr. P.Chandu (R121743), students of Final Year Engineering I semester of Electronics and Communication Engineering Dept., IIIT RKValley RGUKT-AP, have completed their Major Project entitled '**DATA DISGUISABLE MODUS'**.

They have submitted their Project Report for the partial fulfilment of the curriculum of the Degree of Bachelor of Electronics and Communication Engineering from IIIT RKValley RGUKT-AP.

(Head of the Department) (Project Guide)

CONTENTS

ABSTRACT

We propose a new method for strengthening the security of information through a combination of signal processing, cryptography and steganography. Cryptography provides the security by concealing the contents and steganography provides security by concealing existence of information being communicated. Signal processing adds additional security by compressing and transforming the information. The proposed method, viz. Steganography Based Information Protection Method (SBIPM), consists of scanning, coding, encryption, reshaping, cover processing and embedding steps.

We then turn to data-hiding in images. Steganography in images has truly come of age with the invention of fast, powerful computers. Software is readily available off the Internet for any user to hide data inside images. These software are designed to fight illegal distribution of image documents by stamping some recognizable feature into the image. The most popular technique is Least Significant Bit insertion, which we will look at. Also, we look at more complex methods such as masking and filtering, and algorithms and transformations, which offer the most robustness to attack, such as the Patchwork method which exploits the human eye's weakness to luminance variation.

We will take a brief look at stegonalysis, the science of detecting hidden messages and destroying them. We conclude by finding that steganography offers great potential for securing of data copyright, and detection of infringers. Soon, through steganography, personal messages, files, all artistic creations, pictures, and songs can be protected from piracy.

INTRODUCTION

Now a days, various modes of communication like LAN, WAN and INTERNET are widely used for communicating information from one place to another around the globe. Such communication networks are open which any one can access easily. They are regularly monitored and an intercepted.

Steganography, from the Greek, means covered or secret writing, and is a long-practiced form of hiding information. Although related to cryptography, they are not the same. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Stegranography include an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, streganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases.

STEGANOGRAPHY

Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method. Generally there are three different methods used for hiding information: steganography, cryptography, watermarking.

In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical.

Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e. its presence is undetectable by sight. Detection of steganography is called Steganalysis.

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

Steganography is of different types:

1 Text steganography

2 Image steganography

3 Audio steganography

4 Video steganography

History

Throughout history of Steganography has been used to secretly communicate information between people.Some examples of use of Steganography is past times are:

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.

2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.

3. Another method used in Greece was where someone would peel wax off a tablet.

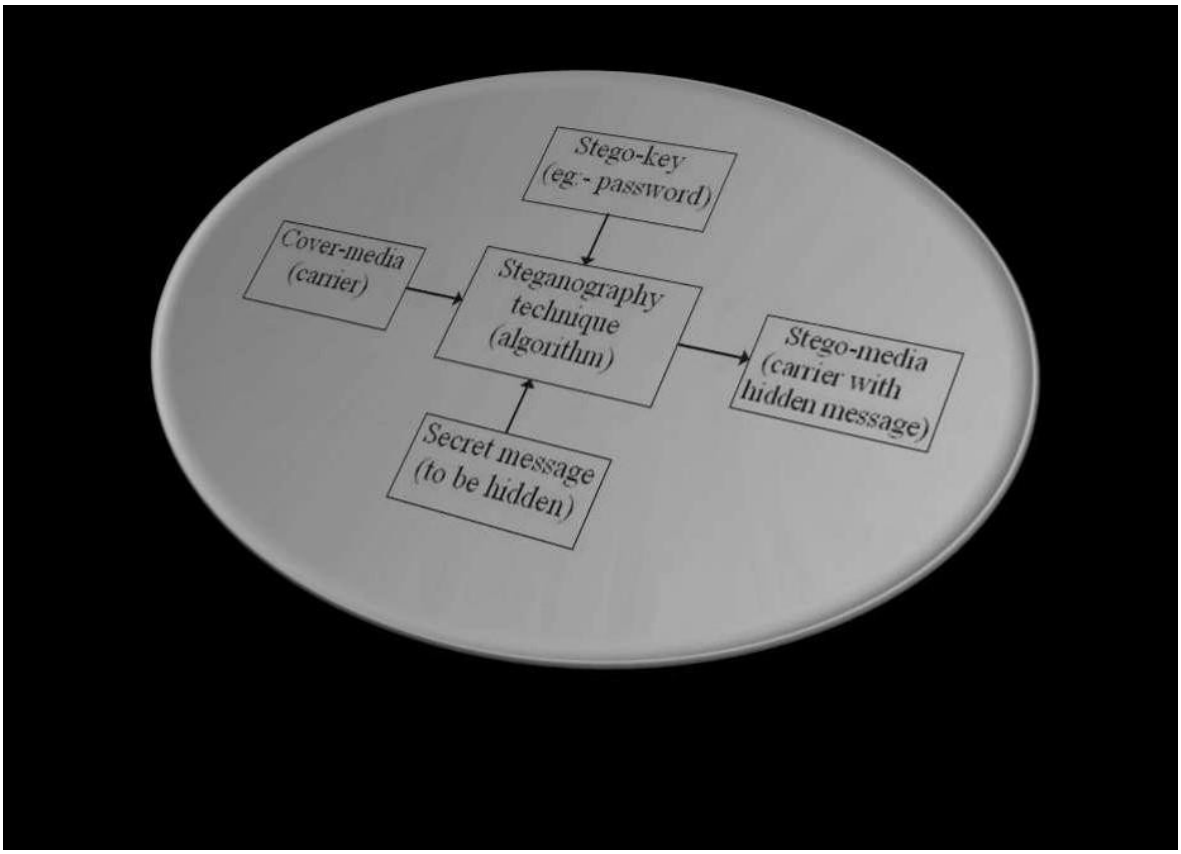
Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.

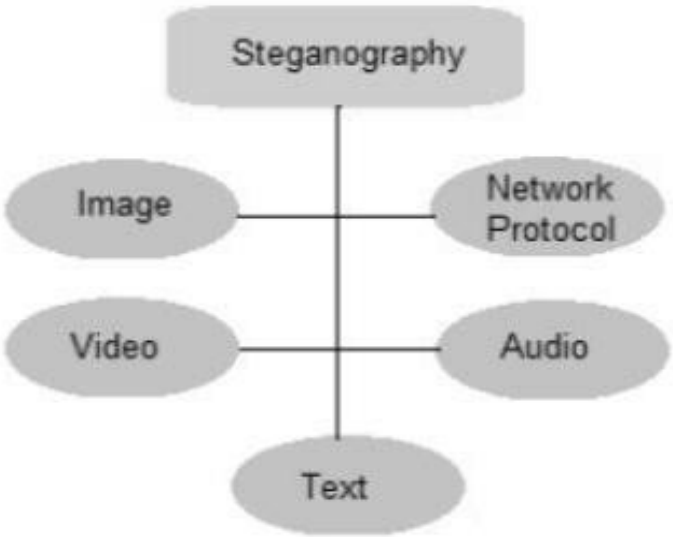
Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

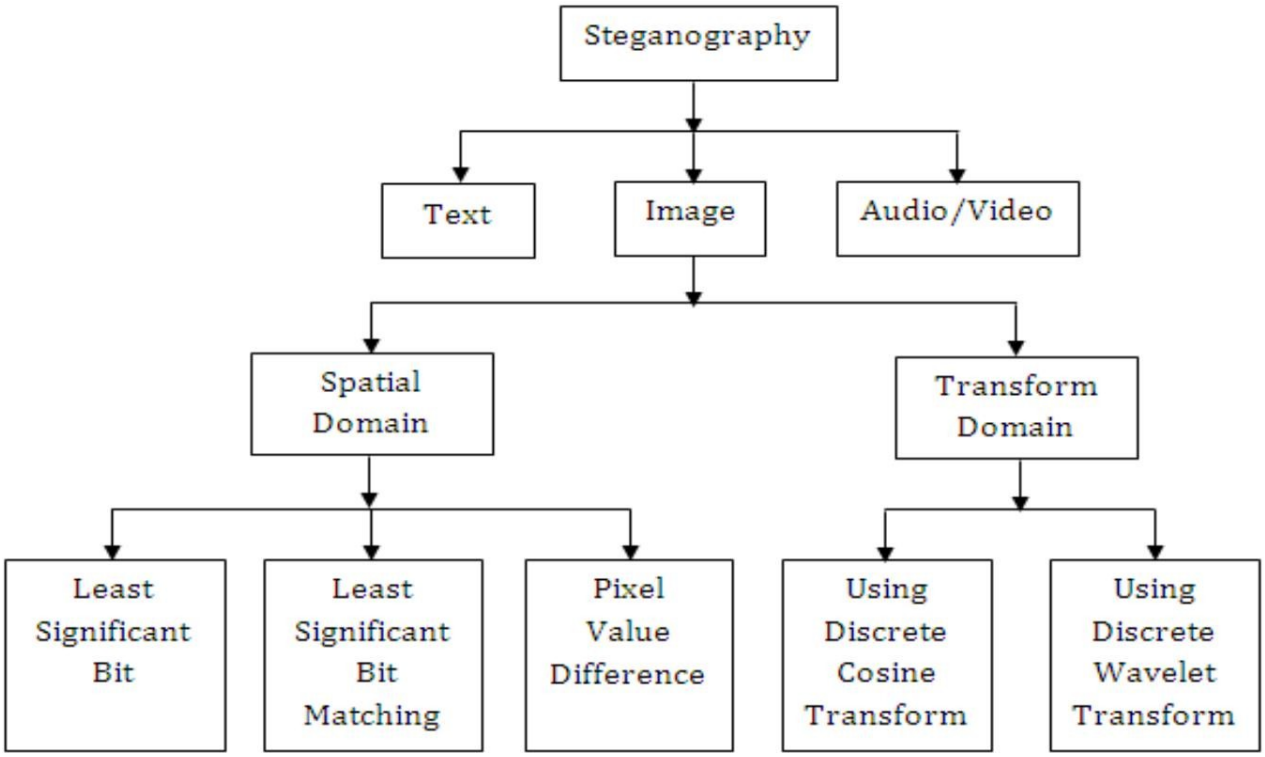
BLOCK DESIGN OF STEGANOGRAPHY:



STEGANOGRAPHY TYPES:

There are different type of sources and carriers are present that can be used for steganography. Mainly those are divided into following types.




Steganography
Text
Image
Audio/Video
Spatial Domain
Transform Domain
Least Significant Bit
Least Significant Bit Matching
Pixel Value Difference
Using Discrete Cosine Transform
Using Discrete Wavelet Transform

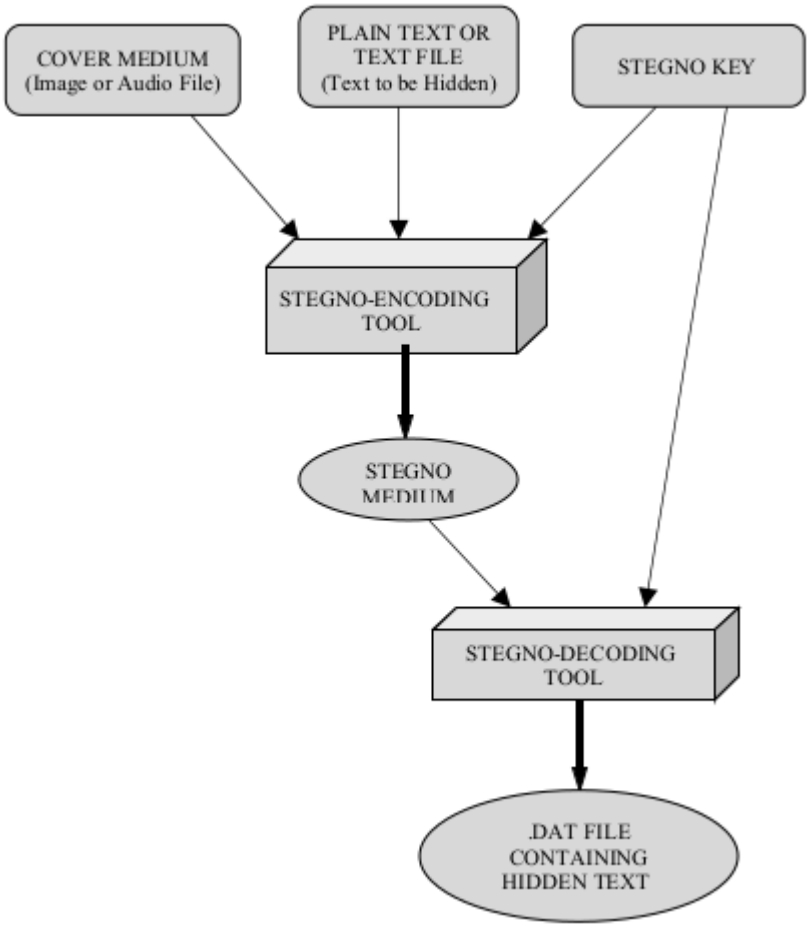


IMAGE STEGANOGRAPHY

In this section we deal with data encoding in still digital images. In essence, image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image.

When embedding data, it is important to remember the following restrictions and features:

1.The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible. (This does not mean the embedded data needs to be invisible; it is possible for the data to be hidden while it remains in plain sight.)

2.The embedded data should be directly encoded into the media, rather than into a header or wrapper, to maintain data consistency across formats.

3.The embedded data should be as immune as possible to modifications from intelligent attacks or anticipated manipulations such as filtering and resampling. Some distortion or degradation of the embedded data can be expected when the cover data is modified. To minimize this, error correcting codes should be used.

4. The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can still be extracted when only a portion of the cover data is available. For example, if only a part of image is available, the embedded data should still be recoverable.

IMAGE COMPRESSION

Image compression offers a solution to large image files. Two kinds of image compression are lossless and lossy compression. Both methods save storage space but have differing effects on any uncompressed hidden data in the image.

Lossy compression, as typified by JPEG (Joint Photographic Experts Group) format files, offers high compression, but may not maintain the original image's integrity. This can impact negatively on any hidden data in the image.

This is due to the lossy compression algorithm, which may "lose" unnecessary image data, providing a close approximation to high-quality digital images, but not an exact duplicate. Hence, the term" Lossy" compression. Lossy compression is frequently used on true-color images, as it offers high compression rates.

Lossless compression maintains the original image data exactly; hence it is preferred when the original information must remain intact. It is thus more favoured by steganographic techniques. Unfortunately, lossless compression does not offer such high compression rates as lossy compression. Typical examples of lossless compression formats are CompuServe’s GIF (Graphics Interchange Format) and Microsoft's BMP (Bitmap) format.

Image Encoding Methods:

- PI (Pixel indicator)
- SCC (Stego Color Cycle)
- Triple-A
- Max-Bit
- LSB (Least Significant Bit)

LEAST SIGNIFICANT BIT METHOD:

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. This method is exactly what it sounds like; the least significant bits of the cover-image are altered so that they form the embedded information. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (00100111 11101001 11001000)

(00100111 11001000 11101001) (11001000 00100111 11101001)

A*:* *10000001*

Result: (00100111 11101000 11001000)

(00100110 11001000 11101000) (11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to hide the next character of the hidden message.

A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object degrades more statistically, and it is more detectable. Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. Changes in

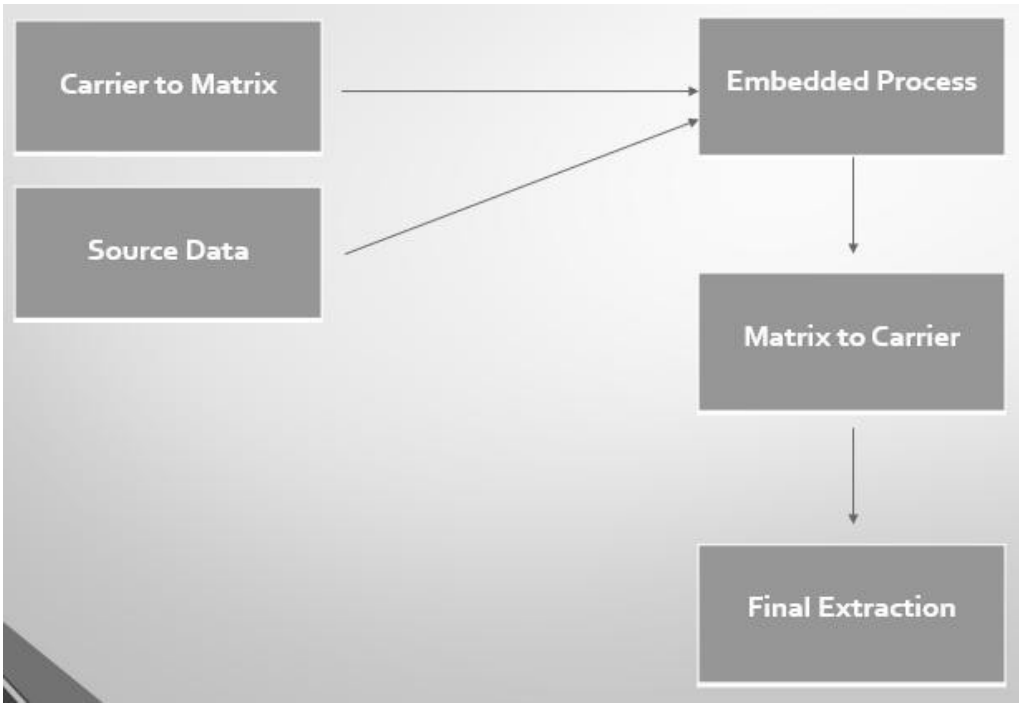
these pixels are then avoided because slight changes would cause noticeable variations in the area.

Advantages of LSB Insertion:

Major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software developed which work around LSB color alterations via manipulation.

LSB insertion also works well with gray-scale images. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity

DESIGN FLOW:



ALGORITHM:

Encryption:

- Select an appropriate message which is to be encoded.
- Select an image in which the message to be encoded.
- Convert the message into respective binary format.
- Choose even values of pixel data matrix
- Append the message binary number one by one to the pixel data.
- The appending data is to be transpose of the original message binary numbers
- Reproduce the output image (Stego Object) from the modified pixel data matrix.

Decryption:

- Select the Stego object (Encoded Image).
- Convert the image into its respective data matrix
- Select the data from the matrix from the even positions.
- Combine the sequence with 8 letters each
- Revert back to the ascii code from the binary
- Convert asci code into characters
- Club all the chatacter into a sequence
- The final message will be stored from the asci codes.

MATLAB IMPLEMENTATION

Encryption Panel:

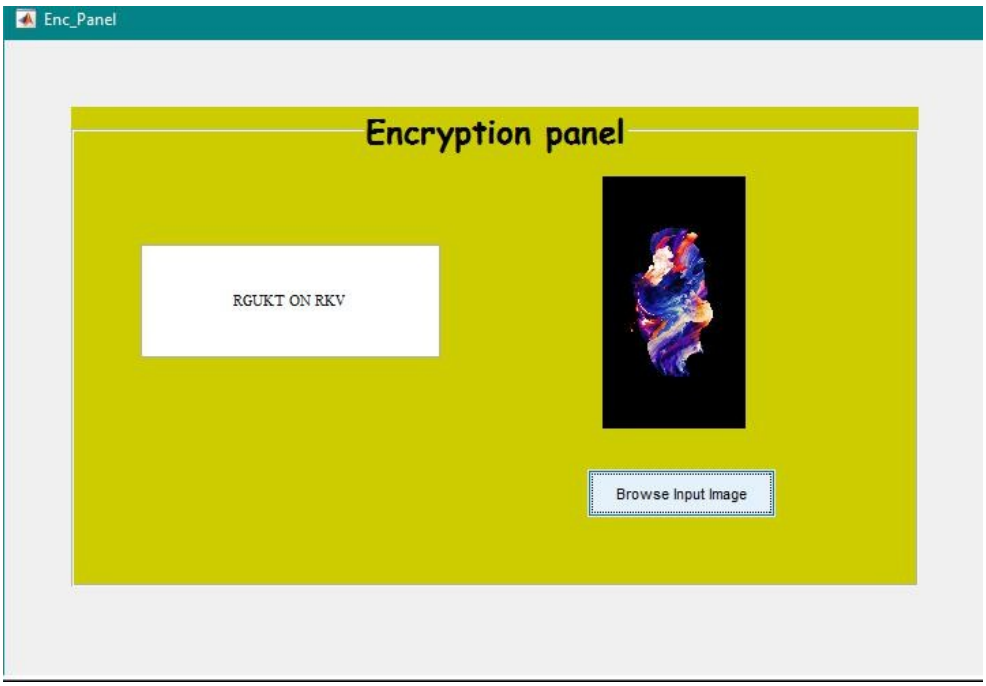
Enc_panel.m

```
function varargout = Enc_Panel(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Enc_Panel_OpeningFcn, ...
                   'gui_OutputFcn',  @Enc_Panel_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
   gui_State.gui_Callback = str2func(varargin{1});
end
if nargout
   [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
   gui_mainfcn(gui_State, varargin{:});
end
function Enc_Panel_OpeningFcn(hObject, eventdata, handles, varargin)
handles.output = hObject;
guidata(hObject, handles);

function varargout = Enc_Panel_OutputFcn(hObject, eventdata, handles)
varargout{1} = handles.output;
function pushbutton1_Callback(hObject, eventdata, handles)
[filename pathname]=uigetfile('File Selector');
fullpathname=strcat(pathname,filename);
global c;
c=imread(fullpathname);
axes(handles.axes1);
imshow(c);
```

```
fid = fopen('in.txt');
msg= fgetl(fid);
enc(msg,c);
function edit1_Callback(hObject, eventdata, handles)
    global message;
    message=get(hObject,'String');
    fileID = fopen('in.txt','w');
    fwrite(fileID,message);
    fclose(fileID);
function edit1_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end
```

enc.m

```
function enc(message,c)
  message = strtrim(message);
    m = length(message) * 8;
    AsciiCode = uint8(message);
    binaryString = transpose(dec2bin(AsciiCode,8));
    binaryString = binaryString(:);
    N = length(binaryString);
    b = zeros(N,1); %b is a vector of bits
    for k = 1:N
        if(binaryString(k) == '1')
            b(k) = 1;
        else
            b(k) = 0;
        end
    end
    s = c;
    height = size(c,1);
    width = size(c,2);
    k = 1;v=1;
    for i = 1 : height
        for j = 1 : width
            if(k<=m && (mod(j,2)==0))
            s(i,j,v)=s(i,j,v)+b(k);
            k=k+1;
            end
        end
    end
     imwrite(s, 'encrypted.bmp');
end
```



Decryption Panel:

Dec_panel.m

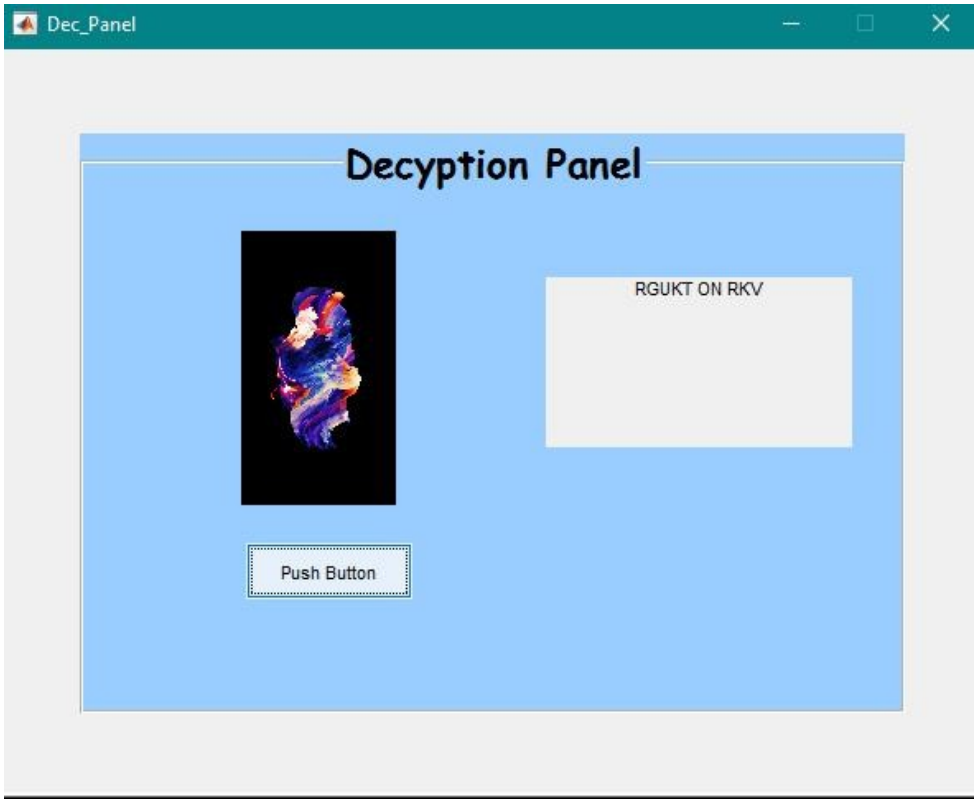
```
function varargout = Dec_Panel(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Dec_Panel_OpeningFcn, ...
                   'gui_OutputFcn',  @Dec_Panel_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end
if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end

function Dec_Panel_OpeningFcn(hObject, eventdata, handles, varargin)
handles.output = hObject;
guidata(hObject, handles);
```

```
function varargout = Dec_Panel_OutputFcn(hObject, eventdata, handles)
varargout{1} = handles.output;

function pushbutton1_Callback(hObject, eventdata, handles)
[filename pathname]=uigetfile('encrypted.bmp');
fullpathname=strcat(pathname,filename);
global s;
s=imread(fullpathname);
axes(handles.axes1);
imshow(s);
dec(s);
fid = fopen('out.txt');
msg= fgetl(fid);
msg=regexprep(msg,'ÿ','');
set(handles.final_msg,'String',msg);
```

Dec.m

```
function dec(s)
   height = size(s,1);
   width = size(s,2);
   m = 24000;
   k = 1;v=1;
   for i = 1 : height
      for j = 1 : width
         if (k<=m && (mod(j,2)==0))
            b(k) = mod(double(s(i,j,v)),2);
            k = k + 1;
         end
      end
   end
```

```
 binaryVector = b;
    binValues = [ 128 64 32 16 8 4 2 1 ];
    binaryVector = binaryVector(:);
    if mod(length(binaryVector),8) ~= 0
        error('Length of binary vector must be a multiple of 8.');
    end


 binMatrix = reshape(binaryVector,8,3000);
   % display(binMatrix);
    textString = char(binValues*binMatrix);
    fileID = fopen('out.txt','w');
    fwrite(fileID,textString);
    fclose(fileID);
end
```



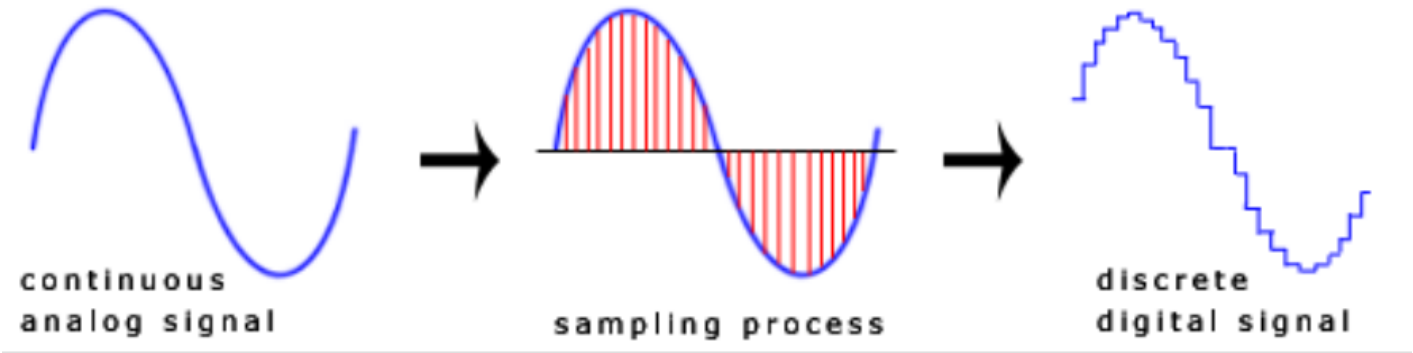
Steganography vs Cryptography:

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

ANALYSIS OF DIGITAL AUDIO

Digital audio differs from traditional analog sound in that it is a discreterather than continuous signal. A discrete signal is created by sampling a continuousanalog signal at a specified rate. For example, the standard sampling rate for CDdigital audio is about 44kHz. The following figure illustrates a continuous analogsound wave being sampled to produce digital audio. Note the sinusoidal nature of a sound wave.



We emphasize the discrete nature of a digital signal in the diagram.However, standard sampling rates are usually set at a level where the resultantdigital signal is visually indistinguishable from the original analog signal.

Digital audio is stored on a computer as a sequence of 0's and 1's. With the right tools, it is possible to change the individual bits that make up a digital audio file. Such precise control allows changes to be made to the binary sequence that are not discernible to the human ear. The secret message is embedded by slightly altering the binary sequence of a sound file.

The key innovation in recent years was to choose an innocent looking cover that contains plenty of random information, called white noise. You can hear white noise as a the nearly silent hiss of a blank tape playing. The secret message replaces the white noise, and if done properly it will appear to be as random as the noise was. Thus the basic design principle of steganographic systems is "replacing high entropy noise with a high entropy secret transmission" .

SECURITY

A method, SBIPM, for providing the security of our important information is based on the techniques of signal processing, cryptography, and steganography. The security of information has been strengthened by applying scanning, coding, and encryption, cover processing and embedding techniques in the method. Reshaping step of the method provides robustness for detecting message correctly in such situation when stego image is distorted. The method developed is safe from various attacks. Simulation and stegonalysis results shown in this paper infer that one will not be able to distinguish between cover and stego images.

Thus we conclude that the strength of security achieved is very high and unauthorized receiver will not be able to get back the original message using even after exhaustive methods without the knowledge of key parameters.

Digital Steganography is interesting field and growing rapidly for information hiding in the area of information security. It plays a vital role in defense as well as civil applications. In future we will more of secure systems based on this technology. Several methods for hiding data in, images were described, with appropriate introductions to the environments of each medium, as well as the strengths and weaknesses of each method. The key algorithm for designing the steganography system has been dealt. Most data-hiding systems take advantage of human perceptual weaknesses, but have weaknesses of their own. We conclude that for now, it seems that no system of data-hiding is totally immune to attack.

However, steganography has its place in security. Though it cannot replace cryptography totally, it is intended to supplement it. Its application in watermarking and fingerprinting, for use in detection of unauthorized, illegally copied material, is continually being realized and developed.

FUTURE SCOPE

In this report many relevant issues were presented, from a technical point of view. However, little has been done to motivate these studies. A more detailed investigation of applications, and a comparison with current techniques in steganography would have been interesting. For example, a thorough evaluation of the advantages natural language-based techniques can offer over image-based techniques could have offered valuable insights.

An important contribution of this project to natural language steganography is the linguistic sophistication of the model for word-substitution put forward. The lexical models employed in current substitution-based systems were often criticized and their inadequate behavior usually described with respect to language theory. These phenomena could have been demonstrated by example, showing texts and inadequate replacements carried out by current stego-systems. A more detailed analysis of how common these critical situations really are in typical text could have given clues for the construction of such systems, to decide whether the additional complexity introduced by statistical word-sense disambiguation is worth the effort.

Other linguistic models have been studied, in addition to the lexical ones, and put in relation to each other, and to their use for steganography purposes. The steganography aspects were then covered by information-theoretic models. However, little has been done to justify this choice. It might have been fruitful to present other characterizations of steganography and to compare their suitability to natural language steganography.

A central part of the problem motivating this report was that there are no models formalizing the design and analysis of natural language stegosystems. Although the present report somewhat improves the situation, by providing a systematic investigation of the topic, there is still no system to build upon for making formal claims about security or robustness in the natural language scenario.

APPENDIX

KEYWORDS AND DEFINITIONS:

Steganography : The art and science of hidden writing.

Cryptography : The science of writing in secret codes.

Cover Medium : File in which we will hide the hidden_data

Plain Text : Data to be hidden.

Cipher Text : The encrypted data to be hidden.

Stego Key : Data is hidden by using this string

Stego Medium : The final resultant file after hiding data.

Bit Stream : The binary code generated from the string.

REFERENCES

[1] *B.Schneier, "Terrorists and Steganography", 24 Sep. 2001,* *http://www.zdnet.com/zdnn/stories/comment/0,5859,2814256,00.html*

[2] Y. Linde, A. Buzo, and R. M. Gray, "An Algorithm for Vector Quantizer Design," IEEE Transactions on Communications, pp. 84-95, January 1989

[3] Andersen, R.J., Petitcolas, F.A.P., On the limits of steganography. IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection 16 No.4 (1998)

[4] Johnson, Neil F. and Jajodia, Sushil. "Steganography: Seeing the Unseen." IEEE Computer February 1998, pp.26□34.