Steganography using lsb insertion technique computer science essay

Technology, Computer

Steganography is a method used for hiding a message by fixing in a carrier data. There are two types of data. They are internal data and external data . The external information contains visible part or audible part of data which is not useful for data owner and the internal information contains embedded data.

The techniques used in Steganography makes hard to detect hidden message within an image file. By this technique we are not only sending a message but also we are hiding the message. Steganography system is designed to encode and decode a secret file embedded in image file with a random Least Significant Bit (LSB) insertion technique. By using this technique the secret data are spread out among the image data in a random manner with the help of a secret key. The key generates pseudorandom numbers and identifies where and in which order hidden message is laid out. Steganography includes cryptography which is an advantage for Steganography . In cryptography, diffusion is applied to secret message. A

INTRODUCTION:

The Data transmitted comes in many forms and it is used for more than one application. Communications should be done secretly. Secret communication varies from bank transfers, corporate communications and credit card purchase. Steganography is an art of embedding a secret message into a normal message. Steganography is used in watermarking for protecting data copyrights . Unsurprisingly, methods of Steganography change because innocuous spam contents are growing frequently by embedded texts

Cryptography is technique used to make secret message scribbled for third party and are normally used in internet. The encrypted message is targeted by attackers in cryptography because it hides the message content. An another data hiding technique known as watermarking used for embedding and hiding, some symbol data or digital manifest in the digital valuable data like photo picture, digital movie, musical sound etc. Watermarking purpose is mainly used to protect ownership or copyrights of the data. In this technique, hardness of embedded evidence and hidden evidence are very small and is important. In this technique the important information is present in external information which is visible or audible.

In the Steganography technique, confidential information is made invisible to a human eye by embedding it as a dummy data such as a speech sound and a digital image. Steganography contains another research topic called as steganalysis which is used to find a stego file from the available files. Steganalysis is used in detecting suspicious image file. The suspicious image files are embedded with the crime associated information

All traditional Steganography techniques have limited information-hiding capacity. These techniques can hide 10% or less than 10% data of a carrier data. The principle of these techniques is to replace frequency components of carrier or to replace LSB bits of multivalued image with secret information. Steganography uses image as a carrier data and it embeds secret information in bit planes . We can replace all noise like regions in the bit planes without disturbing the quality of image and is termed as B. P. C. S

Steganography . BPCS Steganography is known as Bit plane complexity segmentation Steganography.

BACKGROUND HISTORY:

Steganography is derived from a Greek word which means as a “ covered writing or hidden writing”. In Steganography stegos means cover and grafia means writing.

THEORY:

Steganography is used to hide confidential information from human eyes by embedding it in a carrier data such as digital image or speech sound. A carrier data is a color image having RGB color components in a multi-bit data structure. The embedded information is extracted using special extracting program and key . The techniques of Steganography are different from “ file camouflage” or file deception technique.

File deception is a technique used for hiding secret data in computer file and it almost looks like a Steganography. But, it is an trick to disguise a secret-data file as a normal file and is possible in files which have don’t care option. For example, Word file or JPEG image OR MPEG will allow for adding an “ extra” data (extension) at the end of a regular file. Even an extra data (which can be encrypted) are added, the JPEG image, word file or MPEG looks like the original image and original sound, or document on the computer. People may think this is due to Steganography. The lengthy files are easily detected by engineers. So, file deception and Steganography are different.

The Steganography software’s that are available in the market are based on file deception. In Steganography, if output file size is increased by embedding the information then the program is called as File deception. A secret data can be made unreadable by encrypting the data. The secret data should be encrypted to make it unreadable for third party. With the help of data encryption, secret data can be safe. Data encryption is based on data scrambling and it uses a secret key. Data encryption can create a doubt to the people that owner of the data is hiding something in an image. In data encryption we can find easily that he is hiding something in a image. Therefore encryption of data is not enough. Steganography is the solution for data encryption.

There are two types of data in Steganography . they are secret data and carrier data. Secret data is very valuable when compared to the carrier data. Carrier data is a type of dummy data which is not so important but it is needed. The data which is embedded is called as stego data. If we want to recover the secret data , we can extract that data from stego data. We need a special program or a key for data extraction..

The carrier is image data which has color components of red green and blue colors in 24 bit pixel structure. The figure below shows an example of carrier image and stego image. The secret data is embedded in stego image.

Steganography is a method of hiding the secret data by fixing it in media data . For example in the figure a secret data is embedded but we can’t find in which place the secret data is embedded. The Embedded data will be very

safe in the Steganography because it will hide content of the message and location of hidden image. There are many methods to embed the data . but; it is very hard to find about the method used in embedding the message.. Steganography can co-operate with cryptography to embed the encrypted data safely. In Steganography , Stego data will not have any evidence about the embedded data.

The Steganography user should discard the original carrier data after embedding such that it will not allow comparison of stego and original data. Embedded capacity should be larger. BPCS method is the method available method for image Steganography. If anyone detect the Steganography image, it is very difficult for him to retrieve the hidden image. There are three basic ways to hide a message in image. They are Injection, substitution and generation. Using Injection method we can find in which place data to be inserted and using substitution we can find least significant bits for hiding the message. Using generation method we can create a new file based on the hidden information.

Method of implementation:

Least significant bit insertion is one of the important methods of implementation. In this method, the LSB bits of byte are altered so that it form bit string and represents an embedded file. By changing the LSB bits, it will cause some small differences in color which are not noticeable to human eye. After that an image is compressed and a text message is hidden in image . In LSB method, LSB bits of the covered image is altered such that

they form embedded information. Embedding a message into cover image will result a stego image. For normal vision, stego image looks identical as cover image; this is because of only small changes of pixel values. Therefore there is no significant difference. The embedded message is sequentially embedded in covered image so that it is easy for a third party to recover the message by retrieving the pixels sequentially starting from the first pixel of the image. Steganography uses a key which as a better security. It is difficult to recover the embedded image without valid key.

LEAST SIGNIFICANT BIT INSERTION

Least significant bit insertion is the common technique used in Steganography. In LSB method, an image is used. An image is more than strings and string of bytes. Each byte in an image represents different colors. The last few bits in a color byte do not hold much significance as the first few bits. Therefore only two bits differ in last few bits that represent a color which is undistinguishable to human eyes. In LSB method, least significant bits of a cover image are altered such that we can embed information. The example shows how letter A is hidden in first 8 bytes of 3 pixels in a 24 bit image. Since the 8 bit letter A requires only 8 bytes to hide it, ninth byte of the 3 pixels used to hide the next character of the hidden message.

Example shows that in a 24 bit image, letter A can be hidden in first 8 bytes of 3 pixels

Pixels: (00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

A: 01000010

Result: (00100110A 11101001 11001000)

(00100110A 11001000 11101000)

(11001001A 00100110A 11101001)

The five underlined bits are the 5 bits which were altered. With LSB insertion technique, on an average half of the bits of an image are changed. ‘ A’ is a 8 bit letter and requires 8 bytes for hiding. The ninth byte of 3 pixels is used for hiding next character of secret message.

The slight variations of this technique allows a message to embed into two or more least significant bits per bytes, and increases the information hidden capacity of the cover object . but cover object is degraded and easily detectable. LSB insertion is easy to implement and is also easily attacked if the modifications are done wrongly. Improper modifications in color palette and simple image calculations will destroy hidden message. Image resizing and image cropping are some examples of image manipulations.

Applications of Steganography:

Steganography is applicable the following areas.

1). Private communication and secret data storing.

2). Security of data.

3). Accessing the control system for distributing the digital content

4). Media data base systems.

The application area of Steganography differs based on the features utilized in a system.

1). Private communication and secret data storing:

The secrecy of embedded data is important in this area. Steganography provides capacity for hiding the existence of secret data and Steganography makes very hard to detect the embedded data in a image and Steganography strengthens the encrypted data.

In Steganography, select a carrier data according to the size of embedded data. Carrier data should not be effective. Now embed the secret data using an embedding program with the help of a key. To recover the embedded data, an extracting program is used with a key. Before starting the communication in this case, Key negotiation is used

2). Security for a data:

Steganography is used in military applications for maintaining the secret data . In military secret information should be very secure to avoid sudden attacks on them from enemies. Steganography can hide the existence of contents of data but it cannot hide the presence of data. Data should not be larger than carrier image . Steganography strengthens the secrecy of the

data. Fragility of the embedded data is advantage for this application area. Embedded data can be rather fragile than robust. But embedded data is fragile in most of the Steganography programs. No one can change or tampered the data . If anyone changes or tampers the data, and then it can be easily detected by the extraction program.

3). Accessing the control system for distributing the digital content :

In this application, embedded data is explained to publicize the content. Here embedded data is hidden data. Digital contents are being commonly distributed by internet. Some music companies release the music for free in some web sites and in some sites it charges for the music downloads. Digital contents are equally distributed to user who accesses the web pages. Even it is possible to send digital content to e-mail messages it takes more time. We can to upload any content on the web page; we can issue a special access key to extract the content. In Steganography a prototype of an access control system is developed for distributing the digital content through internet. This can be explained by following steps.

1). The content owner will classify his digital content in a folder and embeds the folder according to Steganography method by accessing the folder access key and uploads embedded content on web page.

2). On the web page, owner will explains the contents clearly and publicises it worldwide and gives his contact information on web page.

3). The owner will receive access request from the customer who visited that web page. Then owner creates an access key and provides it to the customer for free or charge.

4). Media database systems:

In this type of application secrecy of data is not important, converting two types of data into one data is important. Photos, Pictures, movies and music will come under media data. For example the media data for a photograph will contain about the title of the photo and date and time of a photo and it also contain about the camera used to take that photograph.

A? a,¬a,¬

Data hiding in . bmp images:

There are several formats exists for an digital image. . BMP, JPG, GIF are some formats . Each format is associated with advantage and disadvantages. Because of its simplicity, windows BMP file offers more advantages. It has an advantage of widely spreader and the information contained is minimum . Bmp file is a binary file. bmp file is divided into four sections such as file header, image header, color table and pixel data. The file header is used to know about size of the image and to learn where actual image data is located within the file. The Image header gives information about the image and its data format such as width and height of the image. Image header also gives information such as how many bits are used per pixel and checks whether the image data is compressed data or

uncompressed data. Depending on the image data, color table will be present. When color table is not present, a set of bit masks are used to extract the color information from the image data. When dealing with 24-bit image, color table is not present. When dealing with 8-bit image, color table consists of 256 entries. Each entry consists of four bytes of data. In these four bytes of data, first three bytes are blue, green and red colors values . The fourth byte must be equal to zero because it is not used. In 8-bit format, each pixel is represented by single byte of the data which is index in to color table. In 24-bit format, each pixel I represented by RGB component values . The pixel data holds entire hidden data and there are changes by one pixel value either positive or negative.

MATLAB:

The MATLAB is a language for technical computing. MATLAB integrates computation, visualization and programming in a easy way in which problems and solutions are expresses in mathematical notation. Typical uses include

Math and computation

Data acquisition

Algorithm development

Modelling, simulation and protyping

Data analysis, exploration and visualization

Application development

MATLAB is a system whose data element is an array without dimensions. It allows in solving computing programs such as Matrix and vectors formulations. It writes program in a scalar language such as FORTRAN within a fraction of seconds.

MATLAB can be abbreviated as a matrix laboratory. MATLAB was developed to access matrix software. The matrix software was developed by linpack and eispack projectsdeveloped . MATLAB engine incorporates LAPACK and BLAS libraries by embedding the state of art in software for matrix computation.

Matlab has evolved over a period of years with input from many users. MATLAB has become a standard tool for advanced courses such as engineering, maths, and sciences . MATLAB is like a tool for high research productivity, analysis and development.

MATLAB SYSTEM:

MATLAB system consists of five main parts:

1). desktop tools and development environment

2). MATLAB Mathematical functions library

3). MATLAB language

4). graphics

5). MATLAB application program interface

1). Desktop tools and development environment:

MATLAB is a set of tools and facilities that helps to use and to become more productive with MATLAB function and files. In MATLAB most of the tools are graphical user interfaces and includes MATLAB desktop, command window, editor and debugger, code analyzer and browser for viewing help, workspace and folders.

2). MATLAB Mathematical functions library

MATLAB is a huge collection of computational algorithms ranging from elementary functions such as sum, sine, cosine and complex arithmetic to more sophisticated functions like matrix inverse, matrix Eigen values, Bessel functions and fast Fourier transforms

3). MATLAB language

MATLAB language is an high level matrix language with control flow statements, functions, data structures, and object-oriented programming features. It allows small and large programming . In programming in large is to create complete large and complex application programs and programming in small is to create quick and dirty throw away programs.

4). GRAPHICS:-

MATLAB is having extensive facilities to display vectors and matrices as graphs. It includes high level functions for two dimensional and three dimensional data visualization, image processing, and presentation graphics . MATLAB also includes low-level functions and allows in

customizing appearance of graphics to build complete graphical user interfaces on MATLAB application.

5). MATLAB Application program interface (API):-

It is a library which allows us to write C and FORTRAN programs to interact with MATLAB . It also includes facilities such as calling routines from MATLAB, calling MATLAB as a computational engine and for reading and writing MATA FILES.

MATLAB working environment:

MATLAB DESKTOP:-

It is the main application window in MATLAB. This window consists of five sub windows such as current directory, command history, workspace browser, command window, and a figure which is shown while displaying a graphic.

The User types commands in command window and expressions at the prompt. The output of these commands is displayed. In MATLAB, workspace is defined as a set of variables created by user in work session. These variables are shown in workspace browser. The workspace browser launches array editor by clicking on a variable. In array editor, we can edit properties of a variable and we can also get information about the variables.

In MATLAB, the current directory tab is above the workspace tab. The Current directory tab shows contents of current directory and its path is shown in current directory window. In windows operating system, the path c:

MATLABwork indicates work as a subdirectory and MATLAB as a main directory and is installed in c drive. In current directory window, click on an arrow button to see recently used paths. To change a current directory, click on a button on right side of a window.

To find M-files and other MATLAB files, MATLAB uses a search path that is organized in system files. The files that are to be runned in MATLAB should locate in the current directory or in directories available on search path . Math work related tools and files that are supplied by MATLAB are already exist in search path. On desktop from file menu select set path to modify or to add search path or to see which directories are existing on search path. To avoid repeated changing, the current directory adds a commonly used search paths to directory.

In MATLAB, the commands used by the user in current and earlier sessions are recorded in command history window. Using right click on command history window, we can select and re-execute previously entered MATLAB then it launches a menu. For execution of the commands select the options from menu. We can select various options from menu for execution of the commands which are useful in implementation of various commands.

MATLAB EDITOR TO CREATE M-FILES:

The MATLAB editor is used for creating M-files. The graphical window will appear in a separate window or a sub window. The M-files are represented as extension . m on desktop. MATLAB editor is having some options to debug a file and saving a file and to view the file. In differentiating various codes

MATLAB editor will perform some simple checking’s. In MATLAB, text editor is used to write and to edit M-functions. To edit a text in MATLAB, type as EDIT at prompt then it an M-file is opened with a filename. Therefore it is ready for editing. The files should be in a search path or in a current directory.

How to get help in MATLAB:

Use the MATLAB help browser for any help in the MATLAB. The help browser will be opened in a separate window when we click on symbol (?) on desktop toolbar or in command window type as help. The Browser Help is displayed separately as a HTML document . HELP browser is incorporated into MATLAB desktop . HELP pane and DISPLAY pane are the two panes that are available in HELP browser. HELP pane is used in finding the information and display pane is used for viewing the information. To perform a search, Navigator pane is used.

CONCLUSIONS:

This project explains techniques for embedding a data in an color image and also some features are added which include file types excluding bitmap images and Steganography methods. Data extracted from cover image depends on pixel values of an image

CODING :

%I= imread(‘ sravs. bmp’); %%read an image

I= uigetfile(‘. bmp’,’select the iamge’);

I= imread(I);

b= 1;

disp(‘ orginal text to be embedded’);

%txt= textread(‘ message. txt’, ‘%c’, ‘ whitespace’ , ‘ ‘);

fid = fopen(‘ message. txt’);

A= fread(fid,’schar’);

fclose(fid);

A1= char(A);

disp(’embedding text’);

txt= A1;

txt’

N = 8*numel(txt); %%%%%%% to find out the total no of elements for the text

S = numel(I); %%%% total no of elements for the image

if N > S

warning(‘ Text truncated to be within size of image ‘);%%%%%%if text size is more than the image size

%%%%%% process block segmentation

txt = txt(1: floor(S/8));%%%%%% dividing into 8*8 blocks for the text

N = 8*numel(txt);

end

%%%%% initializing the total no of bits for the text and the image

p = 2^b;

h = 2^(b-1);

I1 = reshape(I, 1, S);%%%%% resize the elemnts for the new image size

%figure , imshow(I1,'truesize');

addl = S-N;%%%%%%%take the difference of the elments for the imagfe and the text

dim = size(I);

I2 = round(abs(I1(1: N)));%%%%%%take the complexity of each block

si = sign(I1(1: N));

for k = 1: N

if si(k) == 0%%%%%%%replace ment of the bits for the complexity blocks

si(k) = 1;

```
end

I2(k) = round(I2(k));

if mod((I2(k)), p) >= h

I2(k) = I2(k) – h;

end

end

bt = dec2bin(txt, 8);%%%%%%

bint = reshape(bt, 1, N);

d = h*48;

bi = (h*bint) – d; %%%%%%remove the complexity blocks of the image and replace with the non complexity blocksof image

I3 = double(I2) + bi;

binadd = [bi zeros(1, addl)];

I4 = double(si).*double(I3);

I5 = [I4 I1(N+1: S)];

intl = reshape(I5, dim);%%%%%%resize the image and display the stego cotents
```

```
figure, imshow(intl); title(‘ stegnograph image’);

%return

figure, imshow(I); title(‘ original image’);

I= im2bw(I);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%

%%%%%%%%%%%%%%%%%%%decoding%%%%%%%%%%%%%%%%%
%%%

siz= length(txt);

bsiz = 8*siz;

n = numel(intl);

if bsiz > n

error(‘ Size of text given exceeds the maximum that can be embedded in the image’)

return

end

dim = size(intl);
```

```
addl = n-bsiz;

I1 = reshape(intl, 1, n);

I2 = round(abs(I1(1: bsiz)));

p = 2^b;

h = 2^(b-1);

rb = zeros(1, bsiz);

for k = 1: bsiz

I2(k) = round(I2(k));

r = rem(I2(k), p);

if r >= h

rb(k) = 1;

end

end

rbi = (dec2bin(rb, 1))';

rbin = reshape(rbi, siz, 8);

rectxt = (bin2dec(rbin))';

disp(' retrived text from the steg image');
```

```
rextxt= char(rectxt)


return
```