HIDING TEXT INFORMATION BEHIND IMAGE

BY

JYOTI GARG - 041016
NEHA VERMA - 041017
VARUN BANSAL - 041025

JAYPEE UNIVERSITY OF
INFORMATION TECHNOLOGY

MAY-2008

Submitted in partial fulfillment of the Degree of Bachelors of Technology

DEPARTMENT OF ELECTRONICS AND COMMUNICATION

CERTIFICATE

This is to certify that the work entitled "HIDING TEXT INFORMATION BEHIND IMAGE" submitted by JYOTI GARG (041016), NEHA VERMA (041017), VARUN BANSAL (041025) in partial fulfillment for the award of degree of Bachelor Of Technology in Electronics and Communication Engineering Of Jaypee University Of Information Technology has been carried out under my supervision. This work has not been submitted partially or wholly to any other university or institute for the award of this or any other degree or diploma.

Supervisor

Mr. Vinay Kumar
Senior Lecturer
Department Of Electronics and Communication Engineering
Jaypee University Of Information Technology
Waknaghat,Solan (H.P.)
India

ACKNOWLEDGEMENT

The work on the "HIDING TEXT INFORMATION BEHIND IMAGE" has taken lots of pains on our part to take the shape that it has taken finally. At the same time, we would like to express our deep gratitude to all those, without whom this project would have been extremely difficult to accomplish.

We are extremely grateful to Dr. Sunil Bhooshan and Mr. Vinay Kumar for guiding us through out the duration of the project. It was their vision which led us towards this practical work that will hopefully prove beneficial to the student community as well as the faculty of our college.

Jyoti Garg Neha Verma Varun.

JYOTI GARG(041016) NEHA VERMA(041017) VARUN BANSAL(041025)

Contents

List of Figures

LIST OF ABBREVIATION

a .....Image

b .....Text image

f1 .....fft of image

f2 .....fft of text image

f3 .....fft of merged image

m1 .....magnitude of image

m2 .....magnitude of text image

m3 .....magnitude of merged image

ang1 .....phase of image

ang2 .....phase of text image

ang3 .....phase of merged image

new .....variable containing the products of phase of image and magnitude of text image

new1 .....ifft of new

q .....merged image

im1 .....retrieved text image points

im2 .....retrieved image points

iftt .....variable containing the image which we got after the product.

iftt1 .....retrieved image

iftt2 .....retrieved text image

E .....Error matrix

A .....Image matrix

Q(A) .....Quantized image matrix

ABSTRACT

Text Information hiding behind image has been developed using the MATLAB(Image Processing Tool Box) as platform.The Application Interface provides basically two operations - hide, retrieve. The user can specify any bitmap image file of his preference to hide his message which can be of any data type. This text is hidden with no apparent visual change in the image. The image opens normally in any image viewer. The hiding operation has been used to hide the text data in the image file. The retrieve operation is used for decoding. At a time only one text file can be hidden in an image file.

Chapter 1

OVERVIEW OF THE PROJECT

1.1 Introduction

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Today, the term steganography includes the concealment of digital information within computer files[1, 2]. For example, the sender might start with an ordinary-looking image file,then adjust the color of every 100th pixel to correspond to a letter in the alphabet – a change so subtle that no one who isn't actively looking for it is likely to notice it.

We have implemented a project based on steganography in which we have used images in bmp format using matlab as the platform.Here text information has been hidden with no apparent visual changes. The retrieve process is used for decoding the hidden text.

1.2 Algorithm

The program has been[4] implemented using the Matlab Image processing toolbox as a platform. The program consist of following stages:

a)Hide

b)Retrieve

1.2.1 *Hide*

This operation comprises of the following steps:

1. Read the first image
2. Read the text information and convert it into image (text image).
3. Calculate the FFT (fast fourier transform) of both images.
4. Calculate the magnitude of text image and phase of images.
5. Now merge the phase of image and magnitude of the text image.
6. Finally the image dominates over text image as output and the required text image is hidden behind the image.

1.2.2 *Retrieve*

The output which we got after hiding are retrieved through this operation. Retrieving operation consist of following steps:

1.Read the image from which text has to be retrieved.

2.Resize the image if the output image size is not similar to the input image size.

3.Calculate FFT, magnitude and phase of the image.

4.Now retrieve the text from the image.

Chapter 2

HIDING PROCESS

In the previous chapter we have explained the steps involved in hiding the text behind the image. In this chapter we will explain all the commands which had been used in hiding process.

2.1 Reading the image

To read the image imread command is used[6].

A = imread(FILENAME,FMT) reads a grayscale or color image from the file specified by the string FILENAME, where the string FMT specifies the format of the file.

2.2 Writing the image

Imwrite command is used to write the image[7].

imwrite(A,filename,fmt) writes the image in A to filename in the format specified by fmt.

2.3 Calculation of Fast Fourier Transform (FFT)

To calculate the fast fourier transform of images fft2 command is used. FFT2(X) returns the 2-dimensional discrete Fourier transform of the 2-D array X. If X is a vector, the output will have the same orientation.

2.4 Calculation of magnitude and phase of image

To calculate the magnitude[10] abs command is used and for the phase angle command is used.

abs(X) : abs(X) is the absolute value of the elements of X. WhenX is complex, abs(X) is the complex modulus (magnitude) of the elements of X.
magnitude = abs(X)

angle(H) : angle(H) returns the phase angles, in radians, of a matrix with complex elements Class support for input X:
float: double, single
phase = angle(X);

2.5 Merging the phase of image and mag of the text

This section demonstrates that the defining details of a picture are in the phase component of a 2D-Fourier Transform of an image.

Im2uint8 : Is used to form the image from the points that is in matrix form.

imagesc : It is used to scale the image.

2.6 Filtering

For further enhancing the merged image first of all we create a 2-D filter and then filtering[9] is done through the command imfilter.

B = imfilter(A,H) filters the multidimensional array A with the multidimensional filter H.

Figure 2.1: air1.bmp

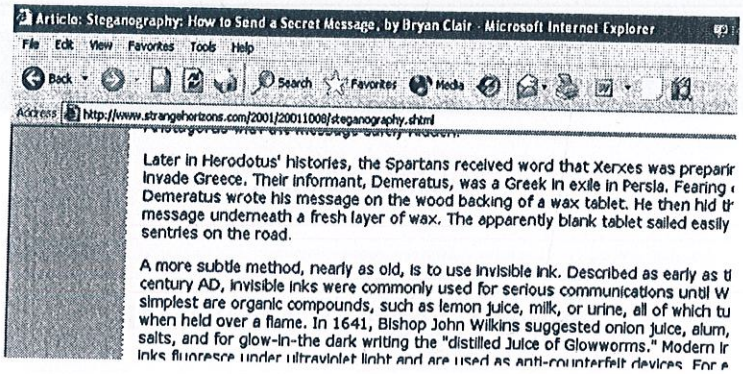

Figure 2.2: add1.bmp

Images taken as Inputs

Figure 2.3: D.bmp

Resultant Merged Image

2.7 Explanation of Hiding Procedure

Step 1: read the image and store its matrix variable a.

Step 2: resize the size of image from RGB to grayscale whose matrix is stored in variable a.

Step 3: similar to step 1 read the text image and store its matrix variable b.

Step 4: similar to step 2 resize the size of image from RGB to grayscale whose matrix is stored in variable b.

Step 5: calculate fast fourier transform of image and text image and that is stored in f1,f2.

Step 6: calculate phase of image and that is stored in variable ang1.

Step 7: calculate magnitude of text image and that is stored in m1.

Step 8: merging of phase of image and magnitude of text in matrix form and is stored in another variable new.

Step 9: calculate inverse fourier transform of matrix new and store its matrix in another variable new1.

Step10: now convert the new1 matrix in image form and merged image is obtained.

Chapter 3

RETRIEVING PROCESS

The functions and commands used in retrieving the merged image have already been explained in the previous chapters.

Resultant Retrieved Images

Figure 3.1: F.bmp

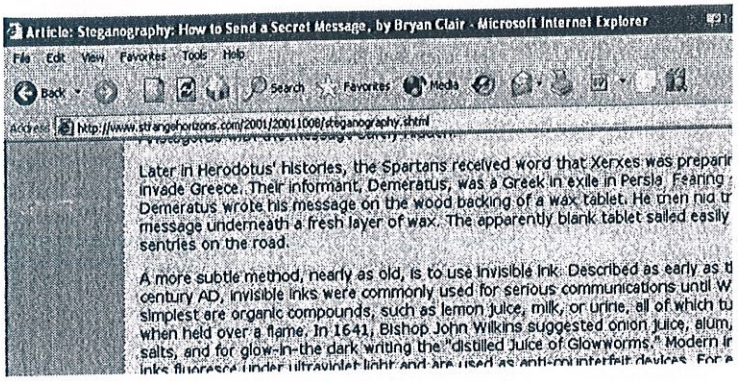

Figure 3.2: G.bmp

3.1 Explanation of Retrieving Procedure

Step 1 : read the merged image and store its matrix in a variable q.

Step 2 : resize the size of merged image whose matrix is stored in q.

Step 3 : calculate the fast fourier transform of the merged image and store its matrix in varaiable f3.

Step 4 : calculate the magnitude of image and phase of text image and store its matrix in variable m1 , ang2.

Step 5 : calculate the magnitude and phase of merged image and store its matrix in variable m3 , ang3.

Step 6 : now combine the magnitude of image and phase of retrieved image and store its matrix in variable im1 .

Step 7 : now convert matrix im1 in image form by taking its inverse fourier transform and image is retrieved.

Step 8 : similar to step 6 combine the magnitude of retrieved image and phase of text image and store its matrix in variable im2.

Step 9 : similar to step 7 convert matrix im2 in image form by taking its inverse fourier transform and text image is retrieved.

Chapter 4

PRECISION

To estimate how much the retrieved image differs from the original image in quantitative terms we calculated its mean square quantized error (MSQE)[3].which is dealt below in details.

4.1 MSQE

In statistics, the mean squared quantized error (MSQE) of an estimator is one of many ways to quantify the amount by which an estimator differs from the true value of the quantity being estimated. MSQE measures the average of the square of the "error." The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate[7].

4.2 Definition and Basic properties

Quantization error matrix(E)

$$E = A - Q(A) \tag{4.1}$$

$$MSQE = \sqrt{\frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (E(i,j))^2}{N * M}} \tag{4.2}$$

Percentage of MSQE calculated for various images :

MSQE of original image and merged image = 2.94

MSQE of original image and retrieved image = 1.35

MSQE of original text and retrieved image = 3.00

MSQE of original text and merged image = 3.07

MSQE of original image and enhanced merged image = 0.62

MSQE of original text and enhanced merged image = 2.72

Chapter 5

PROBLEMS FACED

While developing our project we faced the following problems :

1.When we merged the text and image, we were displaying the merged image through imagesc command but we cannot use imwrite command with imagesc directly. Therefore, we saved the image after normalizing the points of the merged image because after this process we can easily use imwrite command.

2.The merged image which we got after the above process was not so clear it was almost dark. so, inorder to enhance the merged image we did filtering to get the clear merged image.

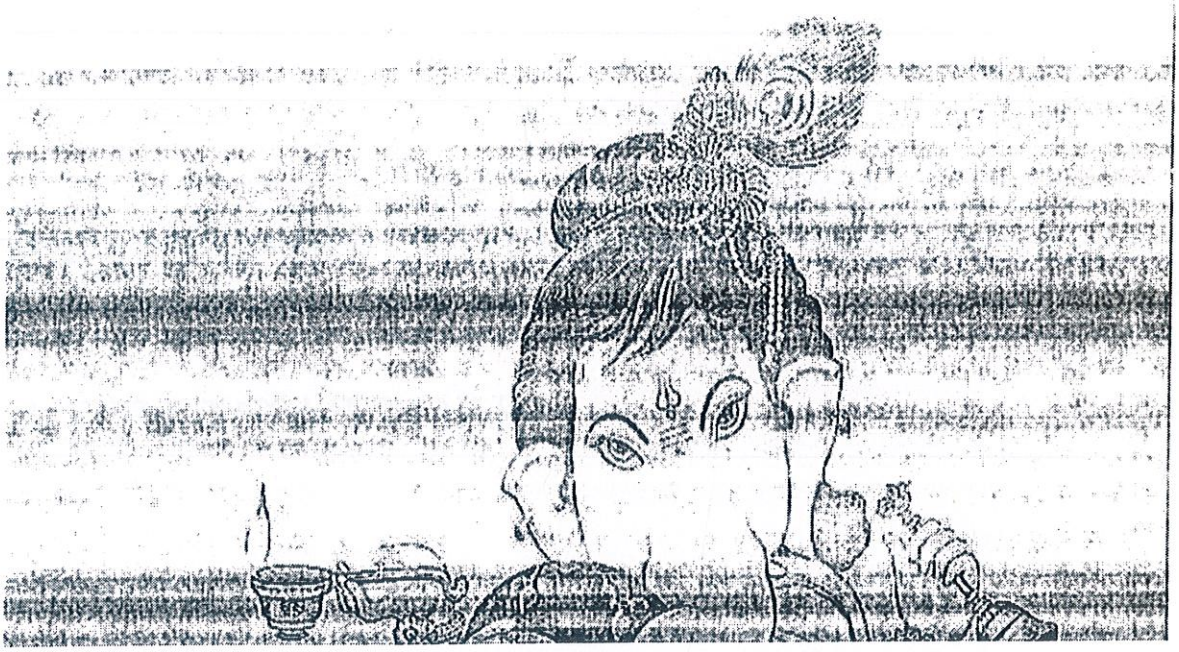

Figure 5.1: s.bmp

Filtered Merged Image

Chapter 6

APPLICATIONS

Steganography has vast applications in various fields illustrated below.

6.1 In the field of Digital Data Forensics

Digital data forensics, which gathers evidence of data composition, origin, and history. Although this new research field is still in its infancy stage[6], it has started to attract increasing attention from the multimedia-security research community.

In addressing digital data forensics, digital images are used as media for illustration while the principle should shed light to other media. Firstly, blind and passive image tampering detection is considered. After pointing out the urgency of this task, the state-of-the-art, including some newest technologies, is presented.

6.2 In the field of Semantics

Protocol steganography allows users who wish to communicate secretly to embed messages within other messages. These secret messages can be used for anonymous communication for purposes ranging from entertainment to protected business communication or national defense.

6.3 In the field of Defense

Given the growing threat of global terrorism, the potential use and exploitation of readily available information technology by our adversaries make it imperative thatour country continue to invest in technologies for the protection and authentication of digital information systems for the military and homeland defense[4]. The directorates work in such areas as information hiding, steganography, watermarking, steganalysis, and digital data forensics will greatly enhance war fighters ability to exploit enemy systems while providing greater security to ensure that an adversary does not have access to allied systems.

6.4 To keep a check on crime

Technology is rapidly changing the speed and manner in which people interact with each other and with the world. As technology helps criminals to operate more easily and quickly across borders, so law enforcement capability must continuously improve to keep one step ahead. Computer forensics has become a specialized and accepted investigative technique with its own tools and legal precedents that validate the discipline.Specially designed forensic software is also widely used for this.

Chapter 7

CONCLUSION

We have attempted to complete our project on hiding text information behind image to our fullest. The application basically consist of two operations, hide and retrieve. As per our expectation our project will be helpful for sending all the valuable informations to the recipients. It can be used by the officials for sending important and confidential details.

Since there is always a room for improvement, we feel that this project can be further improved. As in, the merged image which we get through our development can be further enhanced by processes that will be developed in the future and secondly, we can make this hiding and retrieving process password protected for data security.

Bibliography

[1] www.steganography.org

[2] www.electronics4u.com

[3] www.mathtools.net

[4] A.V.Oppenheim and J.S.Lim, *"The Importance of Phase in Signals,"* Proc. IEEE, 69, pp.529-541, 1981.

[5] R.C.Gonzalez and R.E.Woods, *"Digital Image Processing,"* Prentice Hall, Sec.Ed., 2002.

[6] M.J.Morgan and A. Hayes, *" the Relative Importance of Local Phase and Local Amplitude in Patchwise Image Reconstruction. Biological Cybernetics,"*65, pp.113-119, 1991.

[7] P.Cavanagh, *"Image transforms in the Visual System,"* Eds, New Jersey : Lawrence Erlbaum Associates, Figural synthesis, pp.185-218,1984.

[8] F.A.P.Petitocals,R.J.Anderson and M.G.Kuhn, *"Information Hiding - A Survey"*, proceedings of the IEEE,special issue on Protection of Hiding Data Contents, Vol 87, No. 7 July 1999, pp.1062-1078.

[9] W.Bender, D.Gruhl, N.Morimoto, and A.Lu , *"Techniques for Data Hiding,"* IBM Syst. Journal, Vol 35, pp 313-336,1996.