DFT Based Image Enhancement and Steganography

Inderjit Singh[1], Sunil Khullar[2] , Dr. S.C. Laroiya[3]

[1]M-Tech Scholar, Department of Computer Science

[2]Assistant Professor, Department of Computer Science

[3]Professor & Director

[1, 2, 3] Rayat Institute of Engineering & Information Technology, Railmajra (Punjab), India

[1]Indersaini19@gmail.com, [2]sunilkhullar222@yahoo.co.in, [3]drsclaroiya@gmail.com

***Abstract*— The main purpose of steganography is to hide the presence of communication. While most methods in use today are invisible to an observer's senses, mathematical analysis may reveal statistical anomalies in the stego medium. These discrepancies expose the fact that hidden communication is happening. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Discovering and rendering useless such covert messages is a new art form known as steganalysis. In this Paper, we provide an information about hiding methods of Image steganography such as LSB and DFT that direct the steganalyst to the existence of a hidden message and identify where to look for hidden information.Further we In this paper we have proposed a method to combine the features of image enhancement and Steganography. Various still images we have to be used on which the tests have been implemented.**

Keywords — Image **enhancement, Steganography, LSB, DFT.**

I. Introduction

Removing and reducing impulse noise is very active research area in image processing. Present day applications require various kinds of images and pictures as sources of information for interpretation and analysis. Whenever an image is converted from one form to another, some form of degradation occurs at the output. The output image has to undergo a process called image enhancement. An effective method for image enhancement was presented by Russo, which was controlled by tuning of one parameter.

Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. Two techniques are available to achieve this goal: one is cryptography, where the sender uses an encryption key to scramble the message; this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is steganography, where the secret message is embedded in another message. Using this technology even the fact that a secret is being transmitted has to be secret. Our method is to combine these two techniques. First method is image enhancement and second method is image stegangraphy based on LSB and DFT.

II. Proposed Work

Image Enhancement and steganogrphy are the two broad categories in the field of image processing. Image Enhancement and steganogrphy are the two broad categories in the field of image processing. We are tried to combine these two fields. The method is discussed here

Image Enhancement and steganogrphy are the two broad categories in the field of image processing. We are tried to combine these two fields. The method is discussed here.

When an image is processed for visual interpretation, the viewer is the ultimate judge of how well a particular method works. Visual evaluation of image quality is a highly subjective process, thus making the definition of a "good image" an elusive standard. The main goal is to combine the features of image enhancement and Steganography. Steganography is used to send the data secretly in the carrier. While sending this information, noise may get added and it will distort the message which is sent. For the removal of noise we require the features of image enhancement. Hence in our work these two important fields are combined together so that the receiver can get the image which is noise free and the message has been delivered.

We will implement steganography on noisy and low contrast images. We have opted LSB and DFT methods for the same.

LSB: Usually 24-bit or 8-bit files are used to store digital images. The former one provides more space for information hiding; however, it can be quite large. The colored representations of the pixels are derived from three primary colors: red, green and blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data, then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system. This simple method is known as *Least Significant Bit insertion*. Using this method it is possible to embed a significant

amount of information with no visible degradation of the cover image.

DFT: The Discrete Fourier Transform to get frequency component for each pixel value. The Discrete Fourier Transform (DFT) of spatial value f(x, y) for the image of size M x N is defined in equation for frequency domain transformation.

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\, e^{-i2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)}$$

Where u = 0 to M – 1 and v = 0 to N-1. Similarly inverse discrete Fourier transform (IDFT) is used to convert frequency component to the spatial-domain value, and is defined in equation for transformation from frequency to spatial-domain.

$$f(x, y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{i2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)}$$

The Fourier Transform produces a complex number valued output image which can be displayed with two images, either with the real and imaginary part or with magnitude and phase.

III. Implementation

To implement our work we will follow the following algorithms.

A. Algorithm to remove the noise from images and improve the contrast of image

Step 1: Read the noisy image
Step 2: Each pixel of the image is traversed and the value of pixel is checked whether it is noisy or not.
Step 3: If the is found to be noisy, its pixel value is changed according to a similarity function. It is implemented on each component of the image.
Step 4: The components are then concatenated to form the noise free image.
Step 5: When the noise is removed, next step is to improve the contrast of the image. For this the image component is taken and the image is overlapped with dark, gray and bright components. Then the contrast improved image is formed.

B. Algorithm for LSB Steganography

Step 1: Read the noisy image.
Step 2: Read the cover and the secret image which is to be hidden in the cover image.
Step 3: Convert the secret image to binary
Step 4: Add the bit set of the secret image to the cover image.
Step 5: Read the stego image. Get the bits from the image and retrieve the secret image.

C. Algorithm for DFT Steganography

Algorithm Insertion: In this algorithm all insertion is done in frequency domain. DFT is applied on source image. To convert from spatial domain to frequency domain. Each pixel (8 bits) in spatial domain is transformed into two parts one part is real and another is imaginary part. The authenticating bits are inserted in real part (excluding 1st pixel) of frequency domain .The process is repeated for whole image matrix in the same manner. After embedding IDFT is performed to convert from frequency domain to spatial domain.

1. Read the source image.
2. Read the image.
3. Apply DFT.
   - Embedded the image in the real part of frequency domain excluding 1st pixel.
4. Insert the image bit one by one.
5. Apply Inverse DFT.
6. Repeat steps 3 to 5 for the whole embedding process.
7. Stop.

2) Algorithm Extraction: During decoding the embedded image has been taken as input in spatial domain .To convert from spatial domain to frequency domain.DFT is applied on stego image. Apply the extraction algorithm to extract the authenticating message or image from transformed image. The process is repeated for whole embedded image matrix in the same manner.DFT is performed to transform from frequency domain to spatial domain to generate the original source image or message.

1. Read the noisy embedded image.
2. Apply DFT.
3. Extract the image from real part of frequency domain.
4. Repeat steps 2 to 3 for complete decoding of as per image size.
5. Apply Inverse DFT.
6. Stop.

IV. Results

We have implemented LSB using median filter and DFT using proposed filter. The test images are operated on different intensities of noise as 10%, 20%, 30%, 40% and 50%.Different PSNR values are calculated of each images using LSB with median filter and DFT using proposed filter.
Performance evaluation for test images:

The performance evaluation is done on the basis of PSNR.

TABLE I

Noise % / Images	10	20	30	40	50
Image 1	54.257	54.723	64.780	44.883	54.922
Image 2	48.342	64.503	44.621	54.697	54.998

Image 3	57.716	48.658	48.673	48.678	48.706
Image 4	51.389	65.652	55.653	55.654	65.655

PSNR ratio for test images with median filter using LSB

TABLE III

Noise % images	10	20	30	40	50
Image 1	32.139	44.723	44.780	43.883	44.922
Image 2	41.437	44.503	40.621	51.697	52.998
Image 3	37.781	38.658	42.673	41.678	45.706
Image 4	54.889	45.652	45.653	45.654	55.655

PSNR ratio for test images with proposed filter using DFT

The results clearly showed that the proposed filter (Image Stegnography with DFT) shows better results as compared to the LSB with median filter. Median filter only removes the noises from the image on the other hand the proposed filter not only removes the noise but also improve the contrast of the image.

V. Conclusion

The main purpose of combining two fields image enhancement and Steganography work together. The main goal is to combine the features of image enhancement and Steganography. Steganography is used to send the data secretly in the carrier. While sending this information, noise may get added and it will distort the message which is sent. For the removal of noise we require the features of image enhancement . Hence in our work these two important fields are combined together so that the receiver can get the image which is noise free and the message has been delivered.

References

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] József lenti, steganographic methods, periodica polytechnica ser. el. eng. vol. 44, no. 3–4, pp. 249–258 (2000).

[3] K.T.Talele, Dr.S.T.Gandhe,Dr.A.G.Keskar, International Journal of Computer and Network Security,Vol. 2, No. 4, April 2010

[4] Tanenbaum Andrew S., Computer Networks, 3rd edition, PHI

[5] Forouzan Behrouz A., Data Communication and Networking, 2nd edition, TATA McGraw Hill Publishing Company Ltd.

[6] Pressman Roger S., Software Engineering A Practitioner's Approach, 4th edition, TATA McGraw Hill Publishing Company Ltd.

[7] Jalote P mnb vmbankaj, An Integrated Approach to Software Engineering, Second Edition, Narosa Publishing House

[8] Jalote P mnb vmbankaj, An Integrated Approach to Software Engineering, Second Edition, Narosa Publishing House

[9] Schildt Herbert, JAVA The Complete Reference, 3rd Edition, TATA McGraw Hill Publishing Company Ltd.

[10] Gonzalez, R.C., Woods, R.E., Book on "Digital Image Processing", 2nd Ed, Prentice-Hall of India Pvt. Ltd.

[11] Johnson Neil F, Duric Zoran, Jajodia Sushil Information Hiding Chapter 1. "Steganography and Watermarking - Attacks and Countermeasures", Academic Publishers.

[12] Elke Franz, others, University of Dresden, January 6, 1996, "Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best"

[13] Johnson Neil, Steganography seeing the unseen, February 1998 IEEE paper, 26-34.

[14] Debnath Bhattacharyya ,Tai-hoon Kim; " Image Data Hiding Technique Using Discrete Fourier Transformation" ,Ubiquitous Computing and Multimedia Applications Communications in Computer and Information Science, 2011.

[15] Nabin Ghosal; J.K.Mandal; "Controlled Data Hiding Technique for Image Authentication in Frequency Domain", 2011 2nd international conference on Emerging Applications of information Technology.

WEBSITES

[1] http://world.std.com/~franl/

[2] http://www.jjtc.com/neil/