ISSN 2319-7080 International Journal of Computer Science and Communication Engineering
Volume 3 issue 2(May2014 issue)

A PROPOSED METHOD FOR STEGANOGRAPHY USING DISCRETE FOURIER TRANSFORMATION

Indu Ratti
Assistant Professor
Department of Mathematics, S.N. College, Banga, SBS Nagar, (Punjab) India
prof.induratti@yahoo.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 overview of some characteristics in information hiding methods 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 will be used on which the tests will be implemented.

Keywords—Image enhancement, Steganography.

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.

II. PROPOSED WORK

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

A. *Noisy Image*

The method we are going to develop will be for the noisy image. We assume that the image contain the salt and pepper noise.

1) *Removal of Impulse noise:* - We start from a gray scale image in order to better explain how the new algorithm is constructed. Let the grayscale image be represented by a matrix F of size N1×N2, F ={F(i, j)€ {0, . . . ,255}, i = 1, 2, . . . ,N1, j = 1, 2, . . . ,N2}. Our construction starts with the introduction of the similarity function $\mu : [0;\infty) \rightarrow R$. We will need the following assumptions for our construction starts with the introduction of the similarity function:

$\mu : [0;\infty) \rightarrow R$.

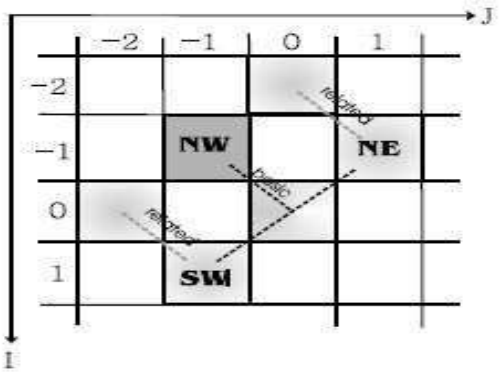
We will need the following assumptions for μ :

(1) μ is decreasing in $[0;\infty)$.

(2) μ is convex in $[0;\infty)$.

(3) $\mu(0) = 1$, $\mu(\infty) = 0$.

In the construction of filter, the central pixel in the window W is replaced by that one, which maximizes the sum of similarities between all its neighbors. Basic assumption is that a new pixel must be taken from the window W.



For each pixel (i, j) of the image (that isn't a border pixel) use a 3 X 3 neighborhood window. Each neighbor with respect to

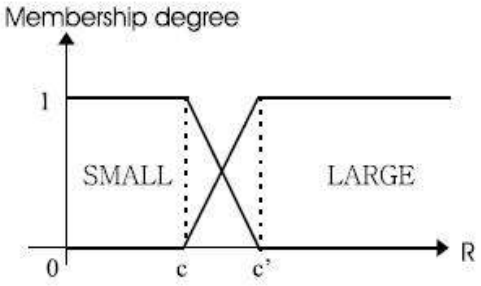
(i, j) corresponds to one direction {NW = North West, N = North, NE = North East, W = West, E = East, SW = South West, S = South, SE= South East}. Each such direction with respect to (i, j) can also be linked to a certain position.

INVOLVED GRADIENT VALUES TO CALCULATE THE FUZZY GRADIENT.

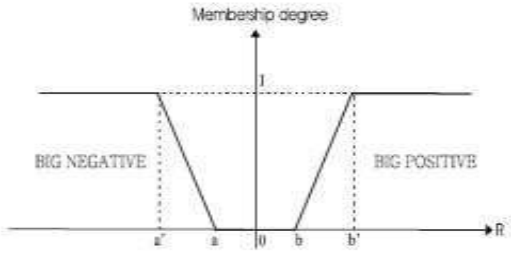
R	basic gradient	related gradients
NW	$\nabla_{NW}A(i,j)$	$\nabla_{NW}A(i+1,j-1), \nabla_{NW}A(i-1,j+1)$
N	$\nabla_{N}A(i,j)$	$\nabla_{N}A(i,j-1), \nabla_{N}A(i,j+1)$
NE	$\nabla_{NE}A(i,j)$	$\nabla_{NE}A(i-1,j-1), \nabla_{NE}A(i+1,j+1)$
E	$\nabla_{E}A(i,j)$	$\nabla_{E}A(i-1,j), \nabla_{E}A(i+1,j)$
SE	$\nabla_{SE}A(i,j)$	$\nabla_{SE}A(i-1,j+1), \nabla_{SE}A(i+1,j-1)$
S	$\nabla_{S}A(i,j)$	$\nabla_{S}A(i,j-1), \nabla_{S}A(i,j+1)$
SW	$\nabla_{SW}A(i,j)$	$\nabla_{SW}A(i-1,j-1), \nabla_{SW}A(i+1,j+1)$
W	$\nabla_{W}A(i,j)$	$\nabla_{W}A(i-1,j), \nabla_{W}A(i+1,j)$

Each direction R corresponds to central position. Column 2 gives the basic gradient for each direction; column 3 gives the two related gradients. The fuzzy gradient value for direction R is calculated by following fuzzy rule:

The membership function used are LARGE (for the fuzzy set large), SMALL (for the fuzzy set small), BIG POSITIVE (for the fuzzy set big positive) and BIG NEGATIVE (for the fuzzy set big negative).



The above graph shows the membership function for fuzzy set SMALL and LARGE.



The above graph shows the membership function for fuzzy set BIG NEGATIVE and BIG POSITIVE.

The pixels of the image are arranged in these membership functions. The noisy pixels are then sort out and form the member of the function more or less impulse noise. The noisy pixel values are then changed according to the following formula:

$$F(i,j) = \frac{\sum_{h=-1}^{1}\sum_{l=-1}^{1}[1-\mu(A(i+h,j+l))]A(i+h,j+l)}{\sum_{h=-1}^{1}\sum_{l=-1}^{1}1-\mu(A(i+h,j+l))}$$

2) *Improving contrast of the image:* - For improving the contrast of the image following steps are done: setting the shape of membership function (regarding to the actual image) setting the value of fuzzifier Beta calculation of membership values modification of the membership values by linguistic hedge generation of new gray-levels.

Using the notation of fuzzy sets, we can write,

$$X = \begin{pmatrix} \mu_{11}/x_{11} & \mu_{12}/x_{12} & \cdots & \mu_{1M}/x_{1M} \\ \mu_{21}/x_{21} & \mu_{22}/x_{22} & \cdots & \mu_{2M}/x_{2M} \\ \vdots & \vdots & & \vdots \\ \mu_{N1}/x_{N1} & \mu_{N2}/x_{N2} & \cdots & \mu_{NM}/x_{NM} \end{pmatrix}$$

Where $0 \leqslant \mu mn \leqslant 1$,m = 1, 2 . . . M,n = 1, 2 . . . N.

Contrast within an image is measure of difference between the gray-levels in an image. The greater the contrast, the greater is the distinction between gray-levels in the image. Images of high contrast have either all black or all white regions; there is very little similar gray-levels in the image, and very few black or white regions. High-contrast images can be thought of as crisp, and low contrast ones as completely fuzzy. Images with good gradation of grays between black and white are usually the best images for purposes of recognition by humans.

The object of contrast enhancement is to process a given image so that the result is more suitable than the original for a specific application in pattern recognition. As with all image-processing techniques we have to be especially careful that the processed image is not distinctly different from the original image, making the identification process worthless. The technique used here makes use of modifications to brightness membership value in stretching or contracting the contrast of an image.

Many contrast enhancement methods work as shown in the figure below, where the procedure involves primary enhancement of the image, denoted with an E1 in the figure, followed by a smoothing algorithm, denoted by an S, and a subsequent final enhancement, step E2.

B. *Steganography*

The The Steganography embeds a secret message in a cover message, this process is usually parameterized by a stego- key, and the detection or reading of embedded information is possible only having this key.

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

DFT: - A The discrete Fourier transform (DFT) is a basic but versatile algorithm that is very useful for digital the

signal level at various frequencies. The signal level at frequency k is equal to the sum of {the signal level at signal processing (DSP).

The DFT is a function that maps a vector of n complex numbers to another vector of n complex numbers. Using 0-based indexing, let x(t) denote the tth element of the input vector and let X(k) denote the kth element of the output vector. Then the basic DFT is given by the following formula:

$$X(k)=\sum t=0n-1x(t)e-2\pi itk/n.$$

The interpretation is that x represents the signal level at various points in time and X represents each time t multiplied by a complex exponential.

DFT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

C. *METHOD*

Firstly, we will take the noisy and low contrast images. At the sender end we will embed an image in the stego image.

Then, the noise will be removed from the image and the embedded image is extracted.

The stego image is extracted using algorithms DFT.

III. 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 Pankaj, An Integrated Approach to Software Engineering, Second Edition, Narosa Publishing House

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

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

[10] 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"

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

[12] The world.std website. [Online]. Available: http://world.std.com/~franl/

[13] The JJTC website. [Online]. Available: http://www.jjtc.com/neil/