WATERMARKING OF TELE-MEDICINE IMAGES USING DISCRETE COSINE TRANSFORM WITH ATTACKS

[1]M.Gowthami Reddy, [2] K. Pradeep Kumar
[1] (M. Tech., E.C.E.), [2](M. Tech. ,E.E.E.)
College of Engineering, S. V. University, Tirupathi-517502
Email : mummadigowthami@gmail.co

***Abstract*-Watermarking provides authentication, copyright protection and encryption etc., Nuclear images are low resolution images so they have special requirements for image watermarking as watermarked images should not differ from their original images because of the clinical reading of the images. Nuclear images are not only for authentication, but also for protection against malicious intentions to change or even use it for other person for any reason.**

Watermarking algorithm operating in the Discrete Cosine Transform is presented. In the frequency-based watermarking technique the watermark is added to the low and the high frequency values of the DCT coefficients. In this Paper the watermarking is accomplished by embedding the watermark into mid frequency range according to the characteristics of the human visual system (HVS).PSNR for host image, Watermarked images along with Embedded watermark, Retrieved watermark are compared. The PSNR values are compared for different kinds of malicious attacks. In almost all the transformed domain watermarking techniques, there is a trade-off between robustness and imperceptibility.

I. INTRODUCTION

a] Introduction to Tele-Medicine

Telemedicine is an upcoming field in health science arising out of the effective fusion of Information and Communication Technologies (ICT) with Medical Science having enormous potential in meeting the challenges of healthcare delivery to rural and remote areas. There are several definitions of telemedicine. According to World Health Organization, telemedicine is defined as, “The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities”

b] Advantages of Telemedicine

The main objective of telemedicine is to cross the geographical barriers and provide healthcare facilities to rural and remote areas (health for all) so it is beneficial for the population living in isolated communities, other advantages telemedicine are

- Applications of Telemedicine are Disaster Management, Tele-home health care, Tele-health care, Tele-education
- Eliminate distance barriers and improve access to quality health services
- In emergency and critical care situations where moving a patient may be undesirable and/or not feasible
- Facilitate patients and rural practitioners’ access to specialist health services and support
- Lessen the inconvenience and/or cost of patient transfers
- Reduce unnecessary travel time for health professionals
- Reduce isolation of rural practice by upgrading their knowledge through Tele-education.

II. DISCRETE COSINE TRANSFORM

Discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering from lossy compression of audio and images (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as explained below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data.

The Discrete Cosine Transform (DCT) is the most popular used transform. It is a technique for converting a signal into elementary frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. DCT decorrelates the image data to reduce redundancy between neighboring pixels. The 2-D DCT can be expressed as

$$Y[u,v] = 2C_u C_v / N \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} X[m,n] \cos\left[\frac{(2m+1)u\pi}{2N}\right] \cos\left[\frac{(2n+1)v\pi}{2N}\right] \quad (2.1)$$

Where: u, v = discrete frequency variables (0,1,2.. N - 1)

X [m, n] = N by N image pixels (0, 1, 2… N - 1)

Y [u, v] = the DCT coefficients

C_u, C_v = 1 / Sqrt (2) when u, v = 0

= 1 Otherwise

And the matrix form

$$Y = C.X.C^T \quad (2.2)$$

Where

X is an NxN image block

Y contains the NxN DCT coefficients

C is an NxN matrix defined as:

C_{mn} = K * Cos [(2m+1)* n * π /2*N] (2.3)

Where

K = 1 / Sqrt (2) when n = 0

K = 1 Otherwise

III. ATTACKS

According to the watermarking jargon, an attack is any processing that may mess up detection of the watermark or communication of the information provided by the watermark. The processed, watermarked data is then called attacked data. Robustness against attacks is an important issue for watermarking schemes. Attacks are generally occur during transmission of the watermarking image. There are many major attacks and they are tested in the proposed work. Some of the attacks are explained bellow in brief.

a] Salt and pepper noise

Salt and pepper is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels. An effective noise reduction method for this type of noise involves the usage of a median filter or a contra harmonic mean filter. Salt and pepper noise creeps into images in situations where quick transients, such as faulty switching, take place.

Figure 3.1 Salt and pepper noise image

b] Speckle noise

Speckle noise is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images. Speckle noise in conventional radar results from random fluctuations in the return signal from an object that is no bigger than a single image-processing element. It increases the mean grey level of a local area.

Speckle noise in SAR is generally more serious, causing difficulties for image interpretation. It is caused by coherent processing of backscattered signals from multiple distributed targets. In SAR oceanography, for example, speckle noise is caused by signals from elementary scatterers, the gravity-capillary ripples, and manifests as a pedestal image, beneath the image of the sea waves.

Several different methods are used to eliminate speckle noise, based upon different mathematical models of the phenomenon. One method, for example, employs multiple-look processing, averaging out the speckle noise by taking several "looks" at a target in a single radar sweep. The average is the incoherent average of the looks.

Figure 3.2 Speckle noise image

c] Gaussian noise

Gaussian noise is statistical noise that has its probability density function equal to that of the normal distribution, which is also known as the Gaussian distribution. In other words, the values that the noise can take on are Gaussian-distributed. A special case is white Gaussian noise, in which the values at any pairs of times are statistically independent (and uncorrelated). Gaussian noise is properly defined as the noise with a Gaussian amplitude distribution. Labeling Gaussian noise as 'white' describes the correlation of the noise. It is necessary to use the term "white Gaussian noise" to be precise. Gaussian noise is sometimes misunderstood to be white Gaussian noise, but this is not the case.

Figure 3.3 Gaussian noise image

IV. THE PROPOSED ALGORITHM

The Discrete Cosine Transform (DCT) Watermarking Algorithm

Nuclear image contains very less information in mid-frequency range as compared to normal set of images, so the patient details which are to be kept confidential is used as watermark and is embedded in the mid-frequency range. Patient details are embedded in mid frequency of host image for better PSNR.

a] Embedding process

A 256x256 nuclear image is considered as the host image. The patient records are used as watermark image to hide the data.DCT is applied to host image and coefficient matrix 'A' is obtained. Coefficient matrix 'B' of the watermark image is obtained by applying DCT on watermark image separately. Singular values are calculated for each obtained matrixes 'A' and 'B' separately. Singular values of matrix 'A' are modified by adding singular values of matrix 'B' in mid-frequency . The proposed embedding algorithm is given by block diagram in Figure 3.1.

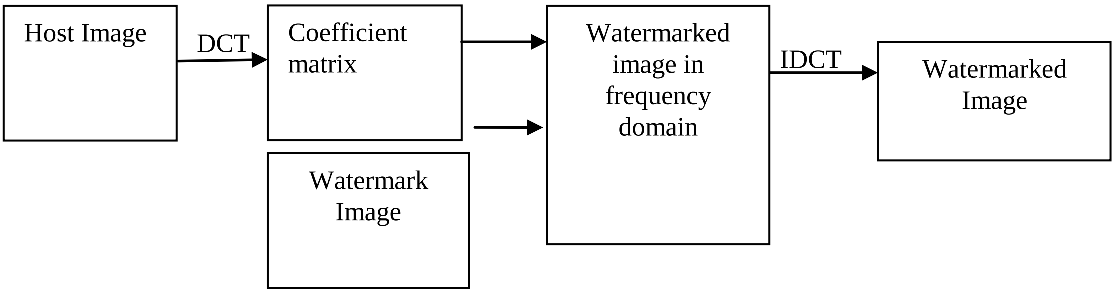


Figure 4.1 Embedding watermark using DCT

Digital watermark embedding process is divided into 4 steps and described as given below

1. The intensity values of original image or Host image which is Nuclear Tele-Medicine image of size 256X256 (MXN) are obtained into matrix I .
2. A patient record to be hidden is considered as watermark image of size 64x64. Coefficient matrix 'B' is obtained.
3. Mid frequency values of coefficient matrix 'A' are replaced with intensity values of 'B' to obtain watermarked image in frequency domain.
4. Watermarked image is obtained by applying inverse DCT to the coefficient matrix 'A'.

b] Extraction Process

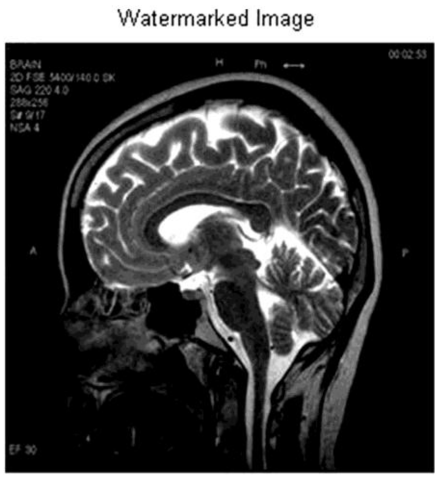
Digital watermark extraction process is divided into 2 steps and described as given below

1. DCT is applied to the watermarked image
2. Mid frequency values of coefficient matrix 'A' are taken out into matrix B

c] Experimental Results.

For evaluation of the developed algorithm, experiments are conducted using gray scale nuclear images. The host image used as shown in the Figure 3.2(a) of size 256x256 and patient information is used as watermark as shown in Figure 3.2(c) of size 64x64. Proposed algorithm is also tested for various attacks and results are shown in Table 3.1.

Figure 4.2(a) Host image



4. 2(b) Watermarked image

Figure: 4.2(c) Used Watermark

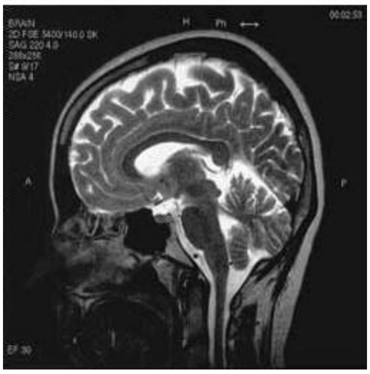
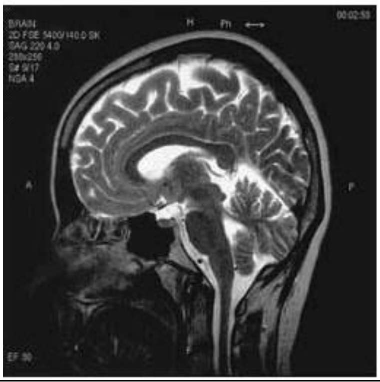
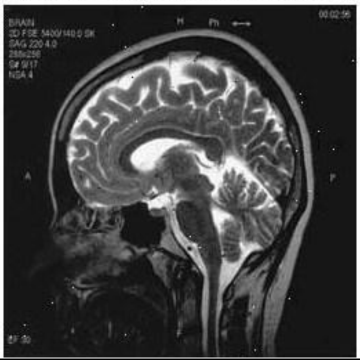
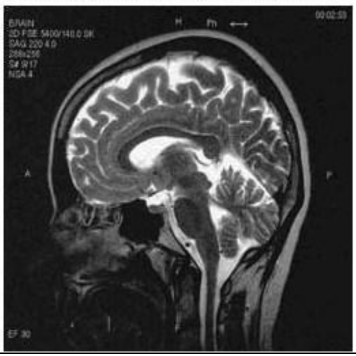
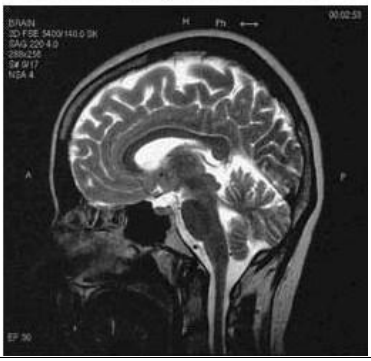
Figure:4.2(d) Retrieved Watermark

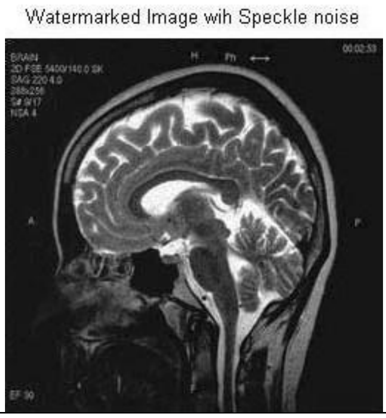
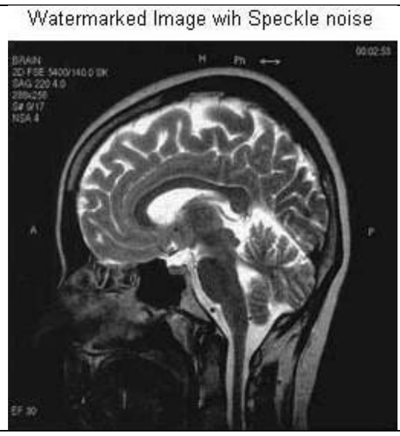
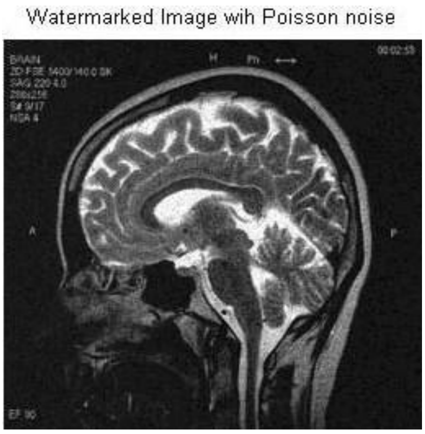
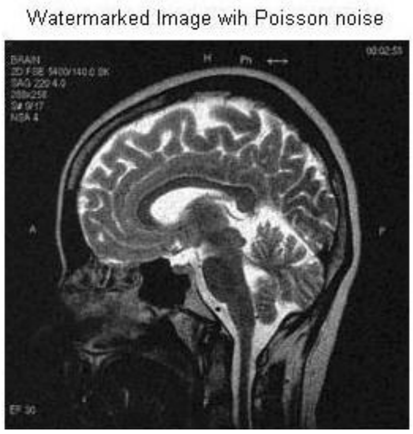
Table 4.1 PSNR Values for Nuclear Images of 256 x256 Size

ATTACK	Proposed Method 256 X 256 High Frequency	Proposed Method 256 X 256 Mid Frequency
	PSNR	PSNR
NO ATTACK	42.117	40.9821
Gaussian	37.8759	37.4242
Salt & Pepper	32.9174	33.4515
Poisson	30.4939	30.4047
Speckle	38.1236	37.6631

Proposed algorithm is also tested for various attacks and results are shown in Table 4.1. It is observed that PSNR are improved over DCT .

Table 4.2: Analysis of attacks using Proposed DCT Method

<table>
<tr><th colspan="2">Watermarked images of size 256x256</th></tr>
<tr><th>Mid Frequency</th><th>High Frequency</th></tr>
<tr><td>Watermarked Image
</td><td>Watermarked Image
</td></tr>
<tr><th colspan="2">Salt & Pepper</th></tr>
<tr><td>Watermarked Image wih Salt & Pepper noise
</td><td>Watermarked Image wih Salt & Pepper noise
</td></tr>
<tr><th colspan="2">Gaussian</th></tr>
<tr><td>Watermarked Image wih Gaussian noise
</td><td>Watermarked Image wih Gaussian noise
</td></tr>
</table>

<table>
<tr><th colspan="2">Speckle</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">Poisson</th></tr>
<tr><td>
</td><td>
</td></tr>
</table>

<table>
<tr><th colspan="2">Retrieved Watermark Images of Size 256X256</th></tr>
<tr><th>Mid Frequency</th><th>High Frequency</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">Salt & Pepper</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">Gaussian</th></tr>
<tr><td>
</td><td>
</td></tr>
</table>

<table>
<tr><th colspan="2">Speckle</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">Poisson</th></tr>
<tr><td>
</td><td>
</td></tr>
</table>

It is observed from Table 4.2 that the proposed DCT method is resilient for different types of attacks as the visual imperceptibility of the retrieved watermark is good.

V. CONCLUSIONS

Telemedicine is an upcoming field in health science arising out of the effective fusion of Information and Communication Technologies (ICT) with Medical Science having enormous potential in meeting the challenges of healthcare delivery to rural and remote areas.

A variety of imperceptible watermarking schemes have been proposed over the last few years. Most of the methods are said to be suitable for either copyright protection or authentication, i.e. for a single specific application with no investigation is done on the possibility of applying the same scheme to other applications as well. The proposed watermarking scheme provides the solution as

- Using the watermarking scheme proposed no additional file is sent, so storage and transmission overheads are reduced.
- The diagnosis made by the doctor and the prescribed medication is preserved in the medical image so as to provide security and proper transition to another doctor if required
- Legal prosecution against intentional and unintentional diagnosis mistakes made by the doctor can be done as the data saved in the image is un editable.
- As the patient information hidden is invisible and does not actually change the imperceptibility of the image, the watermarking scheme doesn't influence the diagnosis to be made by reducing the visual clarity of medical image.
- The diagnostic value of the medical images after watermarking is not lessened in any way.
- Efficient utilization of memory and efficient transmission time and cost.

PSNR is used to evaluate the perceptual quality of the watermarked image effectively and accurately, considering the effect of HVS. The algorithms are very much applicable for applications such as copyright protection, copy control and owner identification.

VI. FUTURE SCOPE

Because of the importance of the security issues in the management of medical information, it is suggested to use watermarking techniques to complete the existing measures for protecting medical images. The necessary requirements for such a system are to be accepted by medical staff and its complementary role with respect with existing security systems. Different scenarios can be considered like the amount of data to be embedded and availability of Space in the Host image, Authentication can be made robust by applying hybrid watermarking schemes i.e., combining both spatial domain and transform domain transformations to achieve the authentication and tracing of the images, the second to the integrity control of the patient's record. Visible text watermarks can be superimposed on images which can be used for explaining different parts of the image. A collateral and relevant use of watermarking is that it renders the watermark inaccessible without a decryption key while not changing the information content of the original image. With no change in the system configuration or software, the present methodology can be integrated with spatial domain technique to watermark other types of patient data such as EEG, PCG etc.

A breakthrough in theoretical research is required where in the schemes are to be implemented in DSP and DIP processors.

VII. BIBLIOGRAPHY

1. http://nptel.iitm.ac.in/courses/Webcoursecontents/IITKANPUR/Digi_Img_Pro/ui/ Course_home-1.htm

2. Cox.I., M.L. Miller, and J.A. Bloom, Digital watermarking. 2001, SanFrancisco, CA, USA: Morgan Kaufmann Publishers Inc.

3. R.C. Gonzalez, R.E. Woods, “Digital Image Processing”, Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002

4. N.F. Johnson, S.C. Katezenbeisser, “A Survey of Steganographic Techniques” in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75

5. S.C. Katzenbeisser, “Principles of Steganography” in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 2-40

6. M. Kutter, F. Hartung, “Introduction to Watermarking Techniques” in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 97-119.

◈◈◈