

COMPARISON OF PSNR OF DCT, DWT AND DTT USING TELENUCLEAR MEDICAL IMAGE

By

N. HARATHI *

V. MEENAKSHI **

C.H. SUNEETHA ***

*-** Assistant Professor, Department of EIE, Sree Vidyanikethan Engineering College, Tirupati.

*** Associate Professor, Department of ECE, Vignana Bharathi Institute of Technology, Aushapur.

ABSTRACT

The proliferation of digitized media due to the rapid growth of networked multimedia systems has created an urgent need for copyright enforcement technologies that can protect copyright. In this paper implementation of three different watermarking algorithms in the frequency domain is presented. The first algorithm is based on the Discrete Cosine Transform (DCT), the second one is based on the Discrete Wavelet Transform (DWT) and the third algorithm is based on the Discrete Tchebichef Transform (DTT). Embedding the watermark is done by modifying the coefficients of the middle frequency band so that the visibility of the image and diagnosis capability will not be affected. All schemes are tested using images and the simulation results are compared and the comparison shows the best scheme.

Keywords: DCT, DWT, DTT, PSNR, Image watermarking.

INTRODUCTION

The development of effective digital image copyright protection methods have recently become an urgent and necessary requirement in the multimedia industry due to the ever-increasing unauthorized manipulation and reproduction of original digital objects. The new technology of digital watermarking has been advocated by many specialists as the best method to such multimedia copyright protection probe. It's expected that digital watermarking will have a wide-span of practical applications such as digital cameras, medical imaging, image databases, and video-on-demand systems, among many others.

One of the most important topics in digital watermarking community is robust watermarking, which aims at achieving robustness, imperceptibility and high capacity simultaneously. These three objectives, however, are Contradictory to each other, and thus a good design is required to achieve an appropriate tradeoff between them. Digital watermarking systems are closely related to the problem of communication with side information at the encoder. The data hiding techniques are Cryptography, Steganography, and watermark. The modern field of cryptography can be divided into several areas of study.

Symmetric-key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key or less. Commonly in which their keys are different, but related in an easily computable way. This was the only kind of encryption publicly known until June 1976. Symmetric key ciphers are implemented as either A block cipher or stream cipher. A block cipher enciphers input in blocks of plain text as opposed to individual characters, the input form used by a stream cipher.

Public-key Cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. The very significant disadvantage of symmetric ciphers is the key management necessity to use them securely. Each distinct pair of communicating parties must ideally share a different key, and perhaps each cipher text exchanged as well. The number of keys required increases, as the square of the number of network members, very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure

channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

Steganography

It is the art of science of writing hidden messages in such a way that no one apart from the sender and intended recipient suspects the existence of the message a form of security through obscurity. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Watermarking

"Watermarking" is the process of hiding digital information in a carrier signal, and the hidden information does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing the copyright infringements and or banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, that is after using some algorithm and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable it is of no use. Traditional watermarks may be applied to visible media like images or video whereas in digital watermarking the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal a digital watermark does not change the size of the carrier signal.

In order for a digital watermarking method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, scaling cropping, and collusion attacks among many other

digital signal processing operations. Current digital image watermarking techniques can be grouped into two major classes: spatial-domain and frequency-domain watermarking techniques.

Compared to spatial domain techniques, frequency-domain watermarking techniques prove to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms. Watermarking adds the additional requirement of robustness. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. So, watermarking is mainly to prevent illegal copy or claims of the ownership of digital media. There are four essential factors which make watermarking effective Robustness: Watermark should be difficult to remove or destroy. It is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, collision attacks, resizing, cropping etc. Imperceptibility: quality of host image should not be destroyed by presence of watermark. Capacity: It includes techniques that make it possible to embed majority of information. Blind watermarking: Extraction of watermark from watermark image without original image.

1. Theoretical Background

A. General Model of Digital Watermarking

Digital watermarking can be defined as the process of embedding a certain piece of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams, such that the watermark can be detected or extracted later to make an assertion about the data. A generalized watermark model consists of watermark encoding and detection processes as shown in Figure 1. Figure 2 shows the General watermarking system and Figure 3 presents the Taxonomy of watermarking Techniques. The inputs to the embedding process are the watermark, the cover object and a secret key. The key is used for security and to protect the watermark. The output of the watermarking scheme is the watermarked data. The output of the

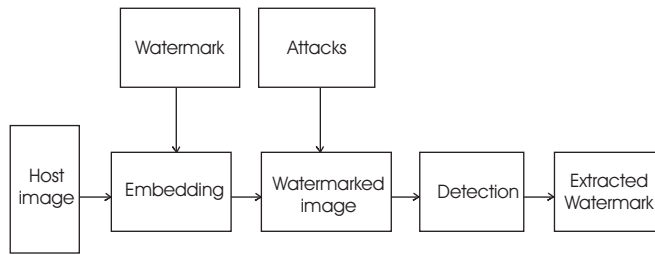


Figure 1. Block diagram of general watermarking system

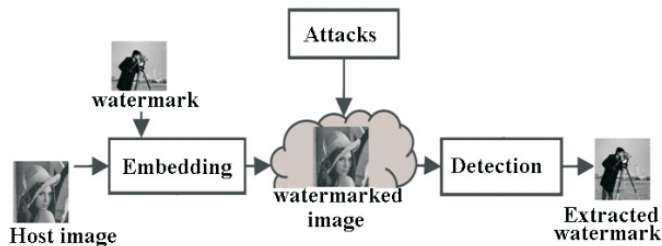


Figure 2. General watermarking system

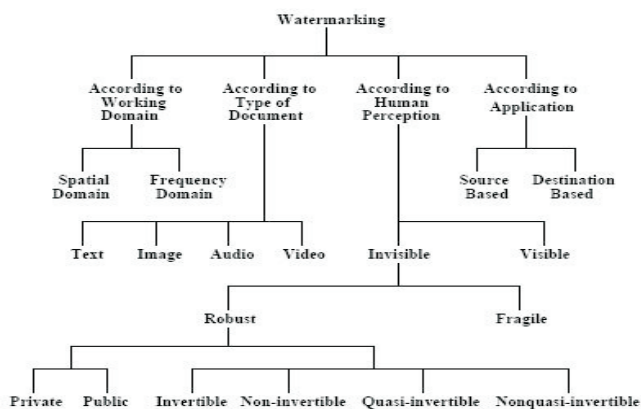


Figure 3. Taxonomy of watermarking Techniques

watermark recovery process is the recovered watermark. Figure 4 shows the Watermarking system classification.

B. Types of Digital Watermarking

An analogy of digital watermark is the paper watermark. Paper watermarks on currency notes and corporate letterheads are used to prove their authenticity. Similarly, digital watermark is embedded into digital media to validate their contents.

2. Application of Digital Watermarking

There is a wide variety of applications for watermarking.

- 1) Owner identification: It is similar to copyright protection to establish ownership of the content.
- 2) Copy protection: It prevents people from making illegal copies of Copyrighted content.

- 3) Content authentication: To detect modifications of the content, as a sign of invalid authentication.
- 4) Fingerprinting: To trace back illegal duplication and distribution of the content.
- 5) Broadcast monitoring: Specifically for advertisements and in entertainment industries, to monitor content being broadcasted as contracted and by the authorized source.
- 6) Medical applications: Used to provide both authentication and Confidentiality in a reversible manner without affecting the medical image in any way.

2.1 Watermarking 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. The usefulness of an attacked data can be measured by its perceptual quality and the amount of watermark destruction can be measured by criteria such as miss probability, probability of bit error, or channel capacity. An attack may succeed in defeating a watermarking scheme if it distorts the watermark beyond tolerable limits while maintaining the perceptual quality of the attacked data.

3. Implemented Algorithms

Algorithms for Biomedical image processing:

P.Tay and Havlicek proposed "Image Watermarking Using Wavelets", a novel image watermarking technique in wavelet domain that inserts a scaled image into a mid-frequency channel of a three level 2-D wavelet transform.

The watermark embedded image is produced by

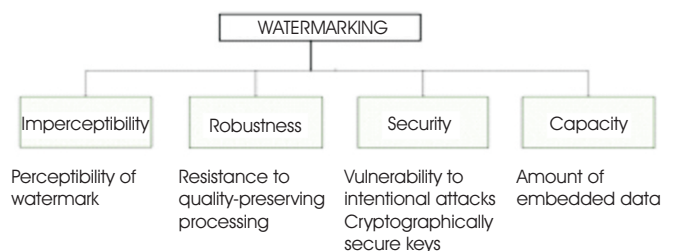


Figure 4. Watermarking system classification

applying the inverse three level 2-D wavelet transform. Multiplication by a non-zero scaling parameter 'g' to the watermark image before inserting into the wavelet channel allows to adjust the image quality albeit resistance to attacks to remove the watermark. The extraction of the watermark requires the correct security key, namely the image size NXN, and the parameter 'g', the channel in which the watermark is inserted, and the filters used in the embedding process. If the security key is correct, the extraction process is straightforward. A binary image was watermarked into the Lena image which indicated that this watermark embedding technique is resilient to attacks by JPEG compression, 3 x 3 median filtering and image cropping. In all cases the watermark was successfully recovered which supports the robustness of this image watermarking scheme.

3.1 Discrete Cosine Transform (DCT)

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 neighbouring pixels. The 2-D DCT can be expressed as

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

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

$C_u, C_v = 1 / \text{Sqrt}(2)$

when $u, v = 0$

= 1 Otherwise

And the matrix form

$$Y = C.X.CT \quad (2)$$

Where X is an NxN image block

Y contains the NxN DCT coefficients

C is an NxN matrix defined as:

$$C_{mn} = K * \text{Cos}[(2m+1)*n*\pi/2*N] \quad (3)$$

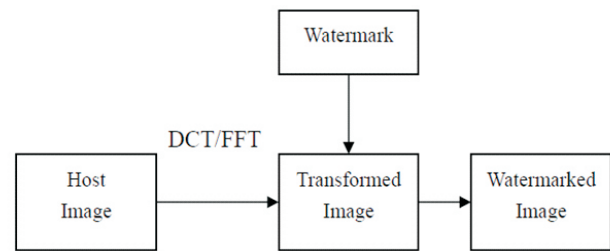


Figure 5. Embedding watermarking using DCT

Where $K = 1 / \text{Sqrt}(2)$

When $n = 0$ $K = 1$ Otherwise

Proposed Watermarking Algorithm for Tele-Nuclear Medicine Images using DCT.

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 Figure 5.

The same can be divided into 4 steps and described as given below.

1. Nuclear image of size 256X256 is considered as host image. DCT is applied to host image and coefficient matrix 'A' is obtained.
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.

The disadvantage of DCT is when the image is compressed, blocks are visible in discrete wavelet transform DCT, which is called blocking effect (Figures 6,7).

3.2 Discrete Wavelet Transform

Wavelets isolate and manipulate specific types of patterns hidden in masses of data, as much the same way as eyes pick out the trees in a forest; and ears pick out the flute in symphony. For example to understand the difference between two kinds of sounds, Human voice and a tuning fork, by contrast spoken word lasts for a second. Figure 8 shows the Discrete Wavelet Transform

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere.



Figure 6. Original image applied DCT



Figure 7. Compressed image applied DCT

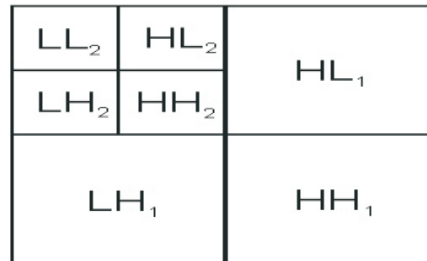


Figure 8. Discrete Wavelet Transform

The Daubechies D4 transform has four wavelet and scaling function coefficients. The scaling function coefficients h₀, h₁, h₂ and h₃ are shown in below equations respectively.

$$h_0 = \frac{1+\sqrt{3}}{4\sqrt{2}} \quad (4)$$

$$h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}} \quad (5)$$

$$h_2 = \frac{1-\sqrt{3}}{4\sqrt{2}} \quad (6)$$

$$h_3 = \frac{3-\sqrt{3}}{4\sqrt{2}} \quad (7)$$

Each step of the wavelet transform applies the scaling function to the data input. If the original data set has N values, the scaling function will be applied in the wavelet transform step to calculate N/2 smoothed values. In the ordered wavelet transform the smoothed values are stored in the lower half of the N element input vector.

The wavelet function coefficients and scaling coefficient functions coefficients are related as shown in equations below.

$$g_0 = h_3 \quad (8)$$

$$g_1 = -h_2 \quad (9)$$

$$g_2 = h_1 \quad (10)$$

$$g_3 = -h_0 \quad (11)$$

Each step of the wavelet transform applies the wavelet

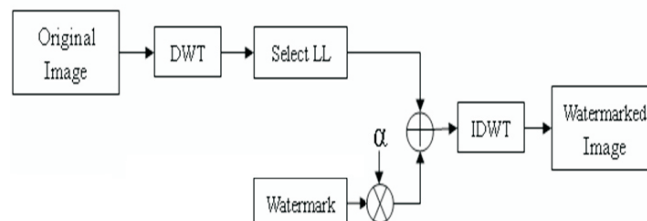


Figure 9. Embedding and Extraction of watermarking using DWT

function to the input data. If the original data set has N values, the wavelet function will be applied to calculate $N/2$ differences (reflecting change in the data). In the ordered wavelet transform the wavelet values are stored in the upper half of the N element input vector. The scaling and wavelet functions are calculated by taking the inner product of the coefficients and four data values. Each iteration in the wavelet transform step calculates a scaling function value and a wavelet function value. The Proposed Watermarking Algorithm for Tele-Nuclear Medicine Images is using DWT.

General images contain maximum information in low frequency and considerable in mid frequency and little information in high frequency components of image in frequency domain. On the other hand, the nuclear medical images provide an additional space for watermarking as the content is stored more in low frequency components of image. So watermark (patient record) is embedded into mid and low frequency components of host image. Wavelet transform is applied to the host image and watermark is embedded into the mid frequency range. The watermark embedding and extraction process are explained using block diagram as shown in Figure 9.

(a) Watermark Embedding Process

Digital watermark embedding process is divided into '6' steps and described as given below.

1. The intensity values of original image or Host image which is Nuclear Tele-Medicine image of size 256×256 (MXN) are obtained into matrix I .
2. DWT is applied to host image ($I \times N$) to obtain LL low frequency sub band and three LH, HL and HH high frequency sub bands of the host image.
3. The gray level values of watermark image (patient record) to be hidden are obtained into the matrix $W_{m \times n}$ of size 64×64 (m \times n).
4. The watermark is scaled with the scaling factor 'k'. The value of scaling factor is decided by the content of watermark and the Host image gives a tradeoff between watermark strength and visible distortion.
5. The intensity values of scaled watermark are placed

into the Mid frequency sub band of the Host image i.e HL sub band of host image is replaced with $W_{m \times n}$ (64×64). These four sub bands LL, LH of Host image, $W_{m \times n}$ the watermark and HH of host image, are nothing but the transform domain image of watermarked image.

6. Inverse DWT is applied to these sub bands LL, LH, $W_{m \times n}$ and HH to obtain the Watermarked image.

(b) Watermark Extraction Process

In order to recover the watermark, reverse process of embedding process is applied. The DWT decomposes the watermarked image into single Low and three High frequency sub bands where in the watermark intensity values are the one of the LH, HL and HH sub band of the watermarked image. The sub band where the watermark is embedded is to be divided with the scaling factor 'k' to obtain the watermark.

Though in DWT, we get very high compression ratio, we lose minimum amount of information. But if we do more than one level then we get more compression ratio but the reconstructed image is not identical to original image. MSE is greater if DWT apply more than one level. But that's not always true. This better result comes in cost of processing power.

3.3 Discrete Tchebichef Transform (DTT)

Discrete Tchebichef transform is based on a polynomial kernel derived from discrete Tchebichef polynomials. By performing DTT on an image, we transform the pixel intensity values in the spatial domain to the frequency domain. From the point of digital signal processing applications, the importance of DTT is evident. DTT and DCT share many common characteristics such as high energy compaction, near optimal decor relation and computational tractability. Due to these properties, DTT is useful for transform operations in image and video processing applications like feature extraction, image compression and video coding.

The basis function of the 1-DTT is defined as the following recurrence relation in polynomials $t_p(X)$ of degree p on a discrete domain $X=0, 1, \dots, N-1$

$$t_p(X) = (\alpha_1 X + \alpha_2) t_{p-1}(X) + \alpha_3 t_{p-2}(X) \quad (12)$$

$p=2, N-1$

Where

$$\alpha_1 = (2/p) * (4p^2 - 1 / N^2 - P^2)^{1/2} \quad (13)$$

$$\alpha_2 = (1 - N/p) * (4p^2 - 1 / N^2 - P^2)^{1/2} \quad (14)$$

The starting values of $t_0(x)$ and $t_1(x)$ are obtained from following equation

$$t_0(x) = N^{-1/2} \quad (15)$$

$$t_1(x) = (2x + 1 - N) * (3 / N(N^2 - 1))^{1/2} \quad (16)$$

The 2-D DTT transformation equation can be expressed as

$$T_{pq} = \sum_x \sum_y \alpha_1 \alpha_2 t_p(x) t_q(y) f(x, y) \quad (17)$$

$$p, q, x, y = 0, 1, 2, 3$$

The first transformation coefficient is the average value of the sample sequence. This value is referred to as the DC coefficient. All other transformation coefficients are called the AC coefficients. DTT can be expressed using a series representation involving matrices as follows

$$f(i, j) = \sum_p \sum_q \alpha_1 \alpha_2 T_{pq} G_{pq}(i, j) \quad (18)$$

$$p, q = 0, 1, 2, 3$$

Where G_{pq} is a 4x4 matrix called a basis images and is defined as

$$G_{pq} = \begin{bmatrix} t_p(0)t_q(0) & t_p(0)t_q(1) & t_p(0)t_q(2) & t_p(0)t_q(3) \\ t_p(1)t_q(0) & t_p(1)t_q(1) & t_p(1)t_q(2) & t_p(1)t_q(3) \\ t_p(2)t_q(0) & t_p(2)t_q(1) & t_p(2)t_q(2) & t_p(2)t_q(3) \\ t_p(3)t_q(0) & t_p(3)t_q(1) & t_p(3)t_q(2) & t_p(3)t_q(3) \end{bmatrix} \quad (19)$$

4. Evaluation Standards

In this work the results are evaluated based on Correlation and PSNR for the resultant images. Correlation is watermark image. PSNR and Correlation are the measurements between host image and watermarked image.

A. Correlation

$$NC = \frac{\sum_i \sum_j (x_{ij} - \bar{x})(x'_{ij} - \bar{x}')}{\sqrt{\left[\sum_i \sum_j (x_{ij} - \bar{x})^2 \right] \left[\sum_i \sum_j (x'_{ij} - \bar{x}')^2 \right]}} \quad (20)$$

Correlation (CORR) is defined as the degree through which two images relate to each other. It is calculated between used water mark and the extracted watermark. The normalized Correlation is given by the equation (21).

B. Peak Signal to Noise Ratio (PSNR)

Signal to noise ratio (SNR) effectively measures the quality of the watermarked image as compared to the original image. This difference is represented as an error function that shows how close the watermarked image is to the original image and it is written as shown in equation.

$$e(x, y) = I(x, y) - Iw(x, y) \quad (21)$$

The larger the value of $e(x, y)$ the greater is the distortion caused by the watermark and the attacks. One of the simplest distortion measures is the mean square error (MSE) function which is given by the formula as shown in equation

PSNR is given by

$$PSNR(Iorg, Iw) = 10 * \log \left(\frac{255^2}{MSE(Iorg, Iw)} \right) \quad (22)$$

Where MSE is mean square error between the original image ($Iorg$) and the watermarked one (Iw). The MSE is defined as

$$MSE(Iorg, Iw) = \frac{1}{N_x N_y} \sum_{i=0}^{N_x-1} \sum_{j=0}^{N_y-1} (Iorg(i, j) - Iw(i, j))^2 \quad (23)$$

Where N is image dimensions.

CORR is the two-dimensional Correlation coefficient.

Conclusion and Future Scope

Nuclear medicine is less expensive and may yield more precise information than exploratory surgery and using Tele-nuclear medicine can enable increased availability of nuclear medicine in underserved areas which will enhance health care. Transferred nuclear medicine images can suffer from malicious attacks so an image watermarking is needed to protect these images against attacks. A robust frequency domain image watermarking scheme have been implemented using the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Tchebichef Transform (DTT). (Figures 10(a), 10(b), 10(c)). A comparison between the proposed algorithms is presented in Table 1 and it is shown that the scheme based on using DTT has a better robustness than

Transforms	PSNR
Discrete Cosine Transform	38.12
Discrete Wavelet Transform	41.68
DiscreteTchebichef Transform	43.02

Table 1. Comparison between proposed algorithm

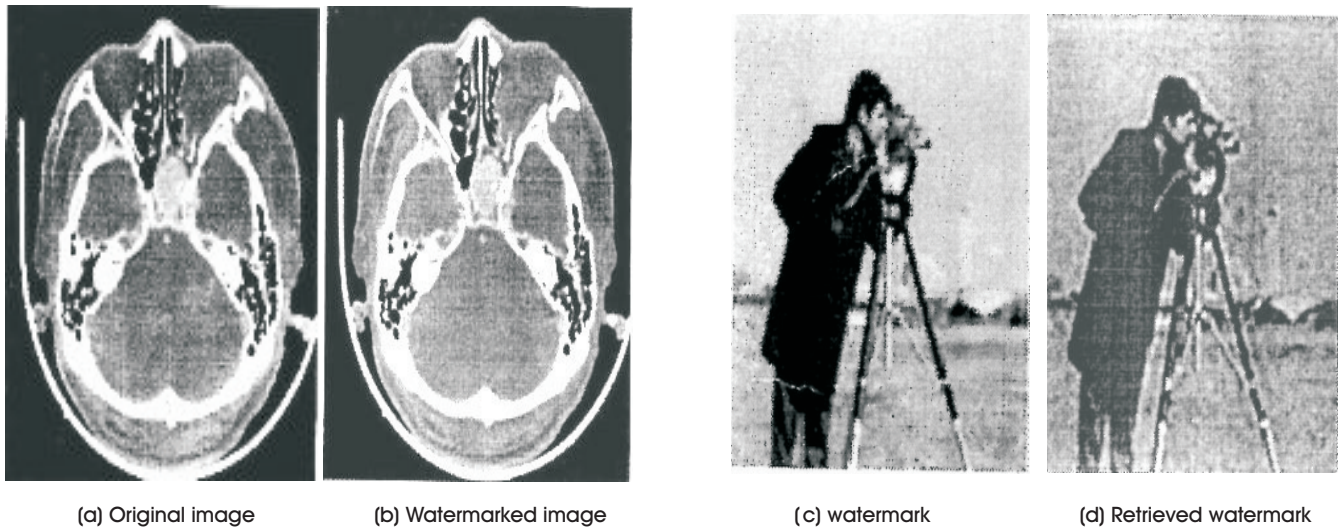


Figure 10(a). Discrete Cosine Transform (DCT) output

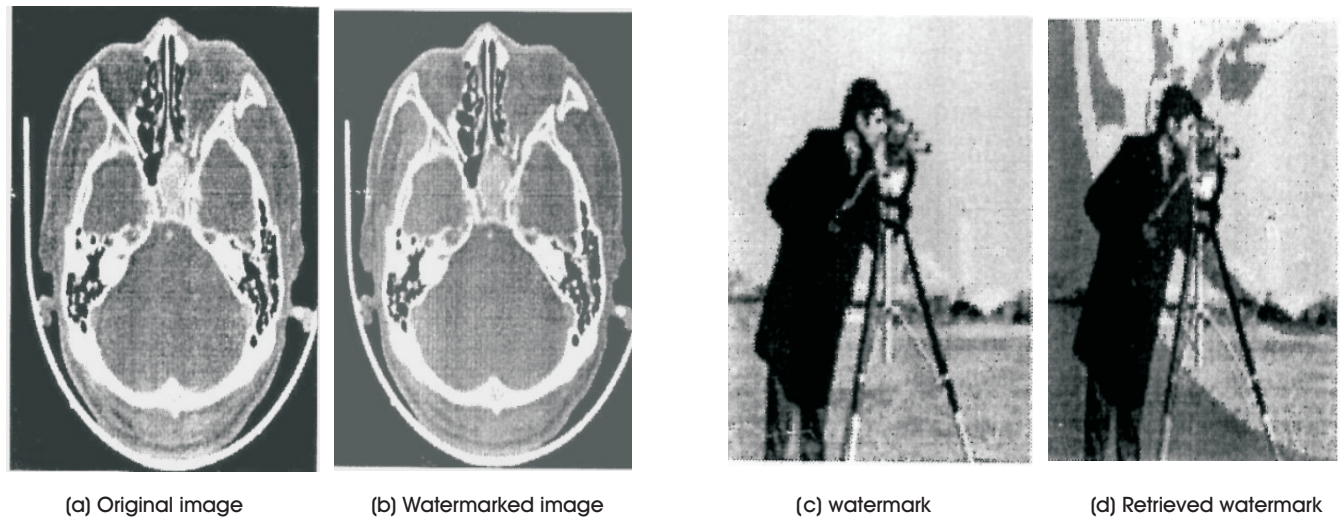


Figure 10(b). Discrete Wavelet Transform output

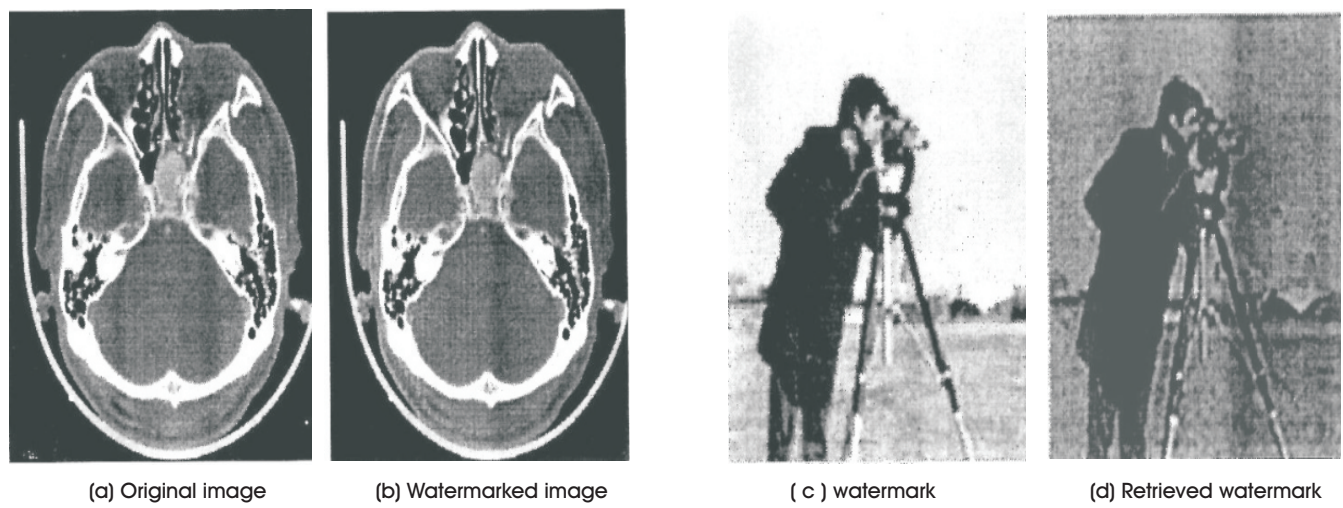


Figure 10(c). Discrete Tchebichef Transform output

that based on either DCT or DWT on 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 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 digital objects.

References

- [1]. Suzuki and M. Nakamura, (1997). "Internet in Nuclear Medicine", *Annals of Nuclear Medicine*.
- [2]. General Nuclear Medicine (<http://www.radiologyinfo.org>)
- [3]. R. Schyndel, A. Tirkel and C. Osborne, (1994). "A Digital Watermark", *Proceeding of IEEE International Conference on Image*, Vol.2.
- [4]. C. Wang, S. Tai and C. Shou, (2000). "Repeating Image Watermarking Technique by the Visual Cryptography", *IEICE Trans. Fundamentals*, Vol.E83.
- [5]. I. Cox, M. Miller and J. Bloom, (2001). "Digital Watermarking". New York: Morgan Kaufmann.
- [6]. A. Sakova, (2004). "DCT versus WHT for Fragile Image Watermarking", *Journal of Electrical Engineering*, Vol. 55.
- [7]. S. Maity and M. Kundu, (2009). "DHT Domain Digital Watermarking With Low Loss In Image Information", Science Direct, *AEU - International Journal of Electronics and Communications*.
- [8]. V. Licks and R. Jordan, (2000). "On Digital Image Watermarking Robust To Geometric Transformation", *Proc. IEEE Int. Conf. Image Processing*, Vol.3.
- [9]. A. Wakatani, (2002). "Digital Watermarking for ROI Medical Images by using Compressed Signature Image" *Proceedings of the 35th International Conference*, 2043 – 2048
- [10]. Yusuk Lim, Changsheng Xu, and David Dagan Feng, (2001). " Web based Image Authentication using Invisible Fragile Watermarking" *Pan-Sydney Area Workshop on Visual Information Processing*.
- [11]. Hemin Golpira and Habibollah Danvali (2009). "Reversible Blind Watermarking for Medical Images Based on Wavelet Histogram Shifting", *IEEE*, 31-36
- [12]. C.-T. Hsu, J.-L. Wu, (1999). "Hidden Digital Watermarks in Images", *IEEE Transactions on Image Processing*, Vol. 8, pp. 58-68.
- [13]. Jingbing Li, Huaiqiang Zhang, Yen-wei Chen, (2012). "Robust Zero-Watermarking for Medical Image Based on DCT" *Photonics and Optoelectronics (SOPO), Symposium*, 21-23 May 2012, 1-4.
- [14]. E. Ganic and A. M. Eskicioglu, (2004). "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," *ACM Multimedia and Security Workshop 2004*, Magdeburg, Germany, September 20-21.
- [15]. Akshya Kumar Gupta, Mehul S Raval, "A Robust and Secure Watermarking scheme based on Singular Value Decomposition" *Sadhana*, Volume 37, Issue 4 , pp 425-440.

ABOUT THE AUTHORS

Mrs. N. Harathi received B Tech degree from JNT University and her M.Tech degree from JNT University, Hyderabad. She has published in three International Journals and attended one National Conference. Her areas of interest include Signal & Image Processing and ARM Processors and PLCs. She is a life member of ISTE.



Mrs. V.Meenakshi received B Tech degree from Sri Venkateswara University and M.Tech degree from JNT University, Hyderabad. She has published in two International Journals and one International Conference and one National Conference. Her areas of interest include Signal & Image Processing and ARM Processor. She is a life member of IETE AND IETE.



Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.