International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7442-7448

Tool for Different Watermarking Applications Using Low and High DCT Frequencies

Ahmed M.N. Al-Gindy
School of Engineering and Information Technology,
AlDar University College, Dubai, United Arab Emirates.

Orcid ID: 0000-0002-0097-5743 & Scopus Author ID: 24821768600

Abstract

This paper presents a tool for different applications digital watermarking of still colour images. The aim of the scheme is to protect the copyright information or to proof the identity by authenticating the image. In general, all watermarking schemes satisfy only one application. However, the proposed algorithm permits users to use the system for both copyright protection and authentication purposes, even though, both purposes have opposing functions. For instance, watermarking techniques used for copyright protection are meant to be robust and strong against watermark impairment even with massive alterations, whereas watermarking techniques utilized for authentication purposes should be fragile and easily impaired via simple modifications. Nevertheless, any of the aforementioned applications can be selected through one system depending on user's protection means.

Keywords: watermarking, digital image processing, discrete cosine transform, copyright, authentication, medical images

INTRODUCTION

The Process of Embedding information into another object/signal is called watermarking. Watermarking of digital data is one of the solutions for unauthorized replication problem which caused many copyright ownership disputes regarding the originality of the digital contents. Digital watermarking methods describe the technologies that allow hiding of information in digital media, such as images, video and audio. Watermarking techniques embed information in images by introducing changes that are imperceptible to the human eye but recoverable by a computer program. Generally, the watermark is a code to identify the owner of the image. The locations in which the watermark is embedded are determined by a secret key. Doing so prevents possible pirates from easily tamper the watermark.

Watermark can be used in a wide variety of applications such as, copyright owner identifications and data Authentications. For the copyright identifications, the data owner can embed a watermark representing copyright information in his/her data. This watermark can prove the ownership in court when someone has infringed on the copyright. Digimarc's watermark for images [1] was designed for this type of application. It detects a watermark; it contacts a central database over the Internet and uses the watermark message as a key to find contact information for the image's owner.

Fragile watermarks [2] can be used to check the authenticity of the data. A fragile watermark indicates whether the data has been altered and supplies localization information as to where the data was altered. For example, this can be useful in legal investigations.

Digital watermarking has recently become an important field of research. Many researchers produced papers covering digital watermarking techniques, attacks, applications and analysis. Digital watermarking challenges include design considerations, requirements, robustness, tradeoffs involved and speed. One of the major digital watermarking challenges is to design an embedding-extraction system that would not affect the quality of the image while at the same time, would satisfy the conditions of security and high robustness. Efficient watermarking system must fulfill the common requirements of transparency and robustness. A new challenge arises when a speedy embedding technique is needed so that users do not face unacceptable delays before they download their marked content. Another challenge is to make the watermarking system deal easily with different file formats, different colour formats, different sizes and types of images, different sizes and types of watermarks and different applications. Data capacity which is defined as how much data can be added before disturbing the quality of the image is yet another challenge for digital watermarking systems. The capability of any watermarking system to hide large or small amounts of data while maintaining the robustness and quality is also an important challenge in watermarking.

THE PROPOSED SYSTEM

The proposed GUI system embeds decimal numbers onto the image. Personal decimal numbers such as Id's, mobile phone numbers, passwords or file number with entry date in hospitals can be used as watermarks since they are practical and more informative for representing one's identity. Each bit of the decimal digits is inserted onto one low frequency or high frequency coefficient of one of the DCT blocks of the host image depending on the application selected by the user. For

copyright protection, the low frequency components of the DCT are utilized whereas for authentication applications the high frequency components of the DCT are utilized. A Friendly Graphical User Interface (GUI) has been developed to ease user's selections as shown in the GUI system Figure 1 for embedding and Figure 2 for Extraction. The implemented tool is comprised of two embedding systems one is used for copyright protection and the other for authentication purposes. They are presented in more details at sections IV and V. The user will be able to evaluate the perceptible changes in the system using Peak Signal to Noise Ratio (PSNR) and the structural similarity index measurement (SSIM) [3] to compare between the host image and the watermarked image.

PSNR penalizes the visibility of noise in an image. Thus, two images that are the same will produce an infinite PSNR value. While, higher SSIM percentage translates to greater similarity between the compared images. The user will also be able to select the watermarking strength Δ. Higher watermarking strength will increase the robustness and reduce the invisibility quality of the watermarked images, this is more suitable for copyright protection. In the authentication purposes, lower watermarking strength will be utilized in the higher frequencies of the DCT transformation to increase the sensitivity for any tampering. In general, the GUI system will allow the users to open, browse, select, evaluate, save and display the results of both the original and watermarked image.

Additionally, the user will be able to verify the robustness or fragileness of the system using various common signal processing and geometric attacks when applying them to the watermarked images. The Implemented GUI system is equipped with evaluation tool for generating attacks on watermarking algorithms [4] as shown in Figure 3.

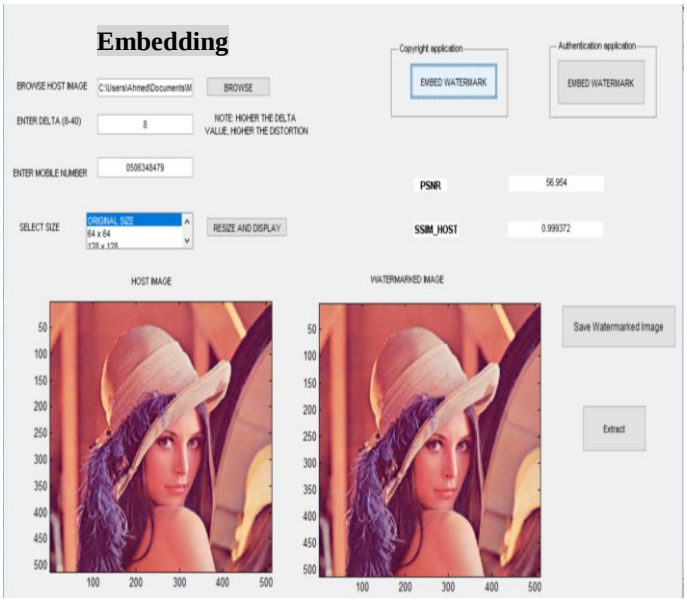


Figure 1. The GUI for the Proposed System- Embedding

Figure 2. The GUI for the Proposed System- Extraction

Figure 3. Attachmark Tool

LOW DCT FREQUENCIES VS. HIGH DCT FREQUENCIES

A coefficient selection process has been applied to find the coefficient with the maximum magnitude in the upper left 16 low frequency coefficients (excluding the DC value) or coefficients with minimum magnitude in the lower right 16 low frequency coefficients in the 8×8 DCT block depending on the application required as shown in Figure 4. This has a direct influence to increase the robustness or fragileness of the system. For the copyright applications, placing the watermark in the low DCT coefficients increases the robustness and maximizes the chances of reconstructing the watermark even after common signal distortions. Furthermore, any modifications to these components will result in severe image degradation, long before the watermark itself is destroyed. An attacker would have to add very large noise energy to sufficiently remove the watermark and this process would destroy the image fidelity. On the other hand, for the authentication applications, placing the watermark in the high DCT coefficients increases the fragility and maximizes the sensitivity of the proposed method against any modification. The watermark information will be embedded using Equation 1. Assume that *f(i,j)* represents the pixel of the

medical image, *w(i,j)* represents the binary pixel of the watermark and

$$F_k(u,v) = DCT\{f_k(i,j)\},$$

If w(i,j)=1 then

$$F_k(x,y) = \begin{cases} \Delta Q_e\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases}$$

If w(i,j)=0 then

$$F_k(x,y) = \begin{cases} \Delta Q_o\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases} \quad (1)$$

Where Q_e is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either to an even or an odd number. It is important to note that the watermark is embedded in the first 64 host blocks in the host image (i.e. the required N_{HB} = 64). The predefined coefficient in each 8×8 sub block is represented by H_k, $1 \le k \le N_{HB}$. The recovery function is the inverse of the embedding function. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The extraction formula is defined as follows:

$$If \quad Q\left(\frac{F_k(x,y)}{\Delta}\right) is\ odd \quad then\ w(i,j)=0$$

$$If \quad Q\left(\frac{F_k(x,y)}{\Delta}\right) is\ even\ then\ w(i,j)=1 \quad (2)$$

Where Q is rounded to the nearest integer. Δ is the same as that used in the embedding process.

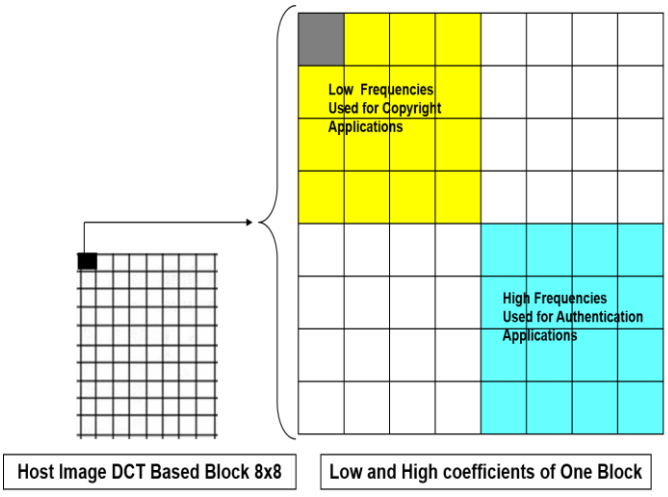


Figure 4. The Used Frequency Coefficients in each 8×8 Block

THE AUTHENTICATION TECHNIQUE

Several types of watermarking schemes have been proposed for handling content authentication applications [5-8] where any tiny changes to the content are not acceptable and the embedding distortion has to be reversed.

The authentication part of the proposed system is carried out in the frequency domain. A DCT block based-approach has been applied and tested on medical images for authentication purpose. Medical images are usually stored in archiving and communication systems that are accessed by the radiologists for diagnosis. The authentication part insures the integrity of the medical image data that is being transferred over public network. The signature which contains 14 decimal digits number representing patient's entry date and file ID embedded inside the patient's medical image in an imperceptible way without increasing the data size that need to be transferred. This signature can be extracted at the radiologist viewer work stations and used for the authentication while the modified data is restored back to original if the image found to be authentic.

Each bit from the signature digits is embedded in one of the high frequency DCT coefficients of the host image. Checksum error detection encoder is used in the technique where a numerical value representing the sum of the signature digits is added to the embedded numbers. This is useful to check that(if) the extracted number is correct or not. A special procedure is applied if the summation exceeds 99. It's worth mentioning that the maximum summation that can be achieved is 126 when a signature with 14 digits and all nines is entered. In such a case, the check sum digits will hold 12 and 6. Then each one of the 16 decimal digits is encoded to a 4-bit binary number. Therefore, we will end up with 64 binary bits. Any modification to the watermarked image can be detected using the proposed watermarking method. This kind of erasable embedding process would ensure medical image retrieval without any modification to the image data after the authentication process. The proposed frequency domain watermarking method go along with the unique need of medical images for diagnosis. A visual representation for the embedding process is shown in Figure 5. The extraction-restoration process is shown in Figure 6, if the watermark is authentic and successfully extracted, the restoration process will be applied to the previously modified coefficients during the embedding process. The secret key 2 has been used to restore the original medical image data.

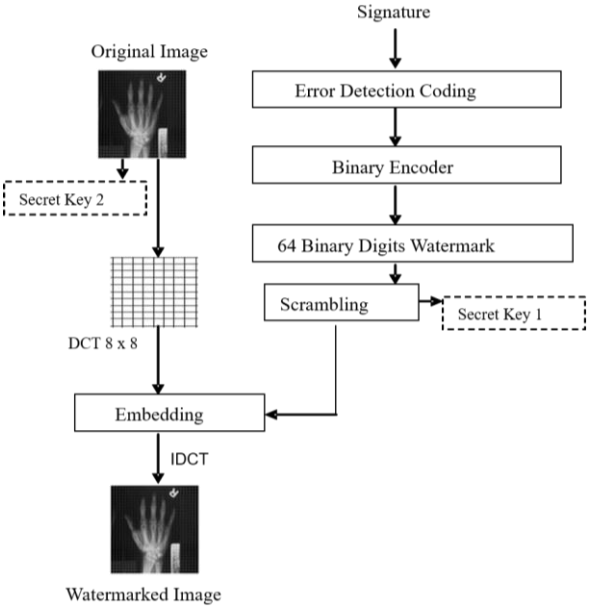


Figure 5. Authentication Process- Embedding

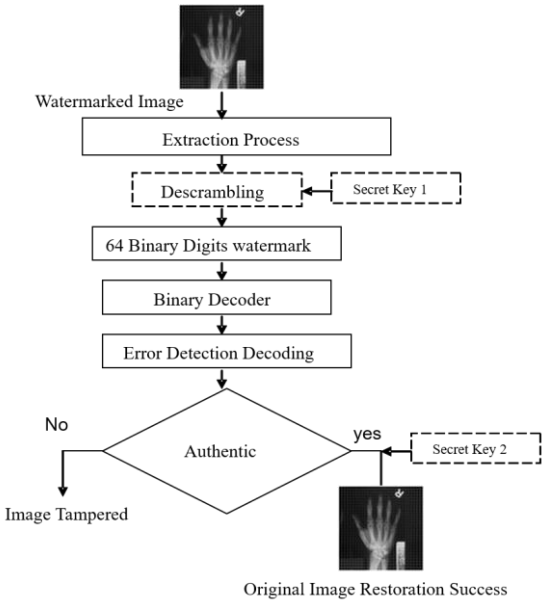


Figure 6. Authentication Process- Extraction

THE COPYRIGHT TECHNIQUE

The copyright part of the proposed system is carried out in the frequency domain. The watermark data is embedded in the very low-DCT frequency component obtained from the coefficient selection process. This range of frequencies is chosen because the high frequency components may be discarded in some image processing operation such as JPEG compression.

Colour images are used for testing the copyright part of the proposed system. The colour image is decomposed into three components R, G and B. The watermark information is embedded in the G plane [8] to produce G` after embedding.

The 16 digits signature are randomly scrambled using a secret key. This scrambling process is essential to reduce the spatial correlation between the host image and the embedded watermark. Shuffling process is also applied to increase robustness against cropping attacks.

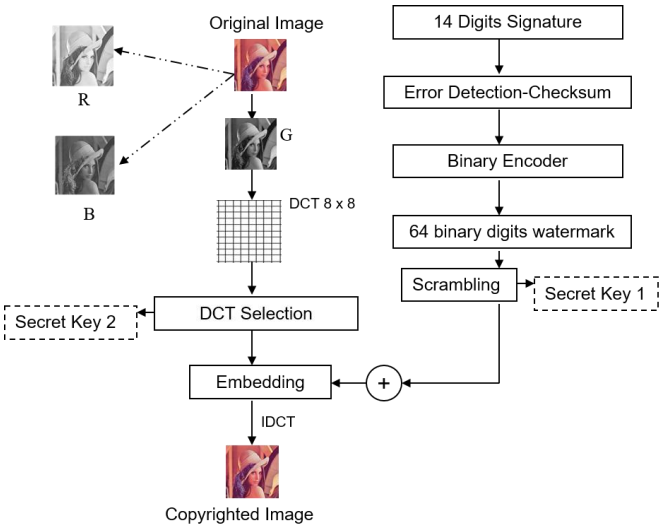


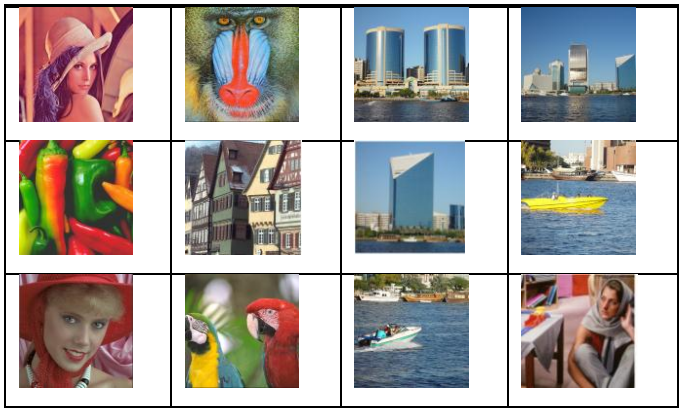
Figure 7. Copyright Process

The extraction process is performed without needing the original unmarked image. Simply the recovery function is the inverse of the embedding function. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The extraction formula is defined in Equation 2.

SIMULATIONS AND RESULTS

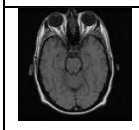
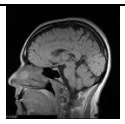
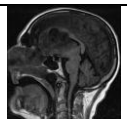
The system is examined in two different dimensions to evaluate the authentication and copyright applications. For the copyright applications, a library of several 512×512 colour images depicted using digital camera plus some standard images were used to test and evaluate the system as shown in table I. Mobile phone number plus the international country code is used as the watermark.

Table I: Copyright Applications Test Images



For the authentication technique, different medical images have been used as shown in table II. A unique 16 digits number that includes patient's entry date and ID is used as signature (watermark) because they are more practical and more informative for representing one's identity.

Table II: Authentication Applications Test Images

Authentication Application Test Images			
			

In order to prove that the changes in the watermarked image will not be perceptible to the normal eye, the watermarked images and the original images have been evaluated when using different watermarking strengths Δ. The evaluation is carried out by calculating the peak signal to noise ratio (PSNR) and Structural Similarity Index Measurement (SSIM) between the host image and the watermarked image. Table III and IV demonstrates the perceptual invisibility of the proposed system at different embedding strengths. The PSNR values between the watermarked and original images varies between 51.4 dB and 43.2 dB for watermarking strengths between Δ=16 and Δ=40, respectively. This can be a delicate balancing act, since the robustness and visibility of a digital watermark are directly related. An increase in the watermark embedding strength increases the visibility of the extracted watermarks. The second evaluation is carried out using the structural similarity index measurement (SSIM) between the host image and the watermarked image [3]. The higher the SSIM percentage is, the larger the similarity between the compared images. Table V demonstrates the perceptual invisibility of medical image authentication at different embedding strengths. The PSNR values between the watermarked and original images are varies between 74.9 dB and 71.4 dB for watermarking strengths Δ=8 and Δ=4, respectively. Lower embedding strengths will increase the sensitivity of the proposed method against any modification which in turn increase the fragility of the proposed method. It has been found that the performance achieved by the proposed method after running through attacks is very sensitive at Δ=4, which can be considered as a suitable value for the embedding strength, Higher embedding strength values such as Δ=8 will decrease the sensitivity of the proposed method against any modifications. SSIM values are shown in table VI. The perceptual quality at different embedding strengths for copyright applications and authentication applications are depicted in tables VII and VIII respectively.

To verify the fragility for authentication purposes and the robustness for copyright applications, attackmark system [4] has been used to general attacks on watermarked images as shown in Figure 8. In order to measure the sensitivity for authentications the attackmark parameters have been kept at minimum values (i.e. very small modifications) such as JPEG 95% quality, scaling up 1.0001 and scaling down 0.999 to ensure that the smallest modification will lead to unsuccessful recovery of the medical images. Table IX illustrate the effect of some attacks in the proposed technique. The performance achieved after running through attacks is very sensitive at Δ=4, which can be considered as a suitable value for the embedding strength, Higher embedding strength values such as Δ=8 will decrease the sensitivity of the proposed method against any modifications.

To verify the robustness of the system against copyright applications, various common signal processing and geometric attacks are applied to the watermarked images as shown in Figure 8. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark as shown in table X. Normalized correlation results less than one means that the algorithm has failed to restore the embedded data.

Table III: PSNR for the watermarked host image for Copyright Applications

Peak Signal to Noise Ratio			
Image	*Lena*	*Pepper*	*Baboon*
PSNR at Δ = 16	51.4395	50.6715	54.5712
PSNR at Δ = 24	47.8758	46.5765	49.1367
PSNR at Δ = 34	44.7981	43.1761	46.8171
PSNR at Δ = 40	43.2219	42.0291	45.7610

Table IV: SSIM for the watermarked host image for Copyright Applications

Structural Similarity Index Measurements			
Image	*Lena*	*Pepper*	*Baboon*
SSIM at Δ = 16	0.9979	0.9963	0.9993
SSIM at Δ = 24	0.9950	0.9918	0.9985
SSIM at Δ = 34	0.9902	0.9829	0.9970
SSIM at Δ = 40	0.9865	0.9778	0.9957

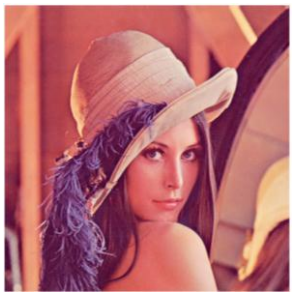
Table V: PSNR for the watermarked host image for Authentication Applications

Image	*Brian*	*Head*	*Hand*
PSNR at Δ = 4	73.0703	72.9095	74.9095
PSNR at Δ = 6	72.2230	72.3458	74.3458
PSNR at Δ = 8	71.4701	71.7939	73.7939

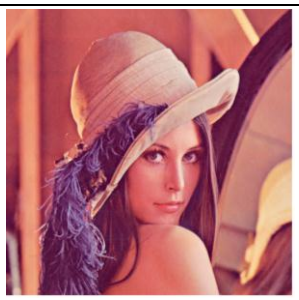
Table VI: SSIM for the watermarked host image for Authentication Applications

Image	*Brian*	*Head*	*Hand*
SSIM at Δ = 4	0.9992	0.9992	0.9997
SSIM at Δ = 6	0.9990	0.9991	0.9995
SSIM at Δ = 8	0.9988	0.9989	0.9993

Table VII: Perceptual quality at different embedding strengths for Copyright Applications



Original Unwatermarked Lena image



Watermarked image at Δ = 16

Watermarked image at Δ = 40

Table VIII: Perceptual quality at different embedding strengths for Authentication Applications

Original Un-watermarked image

Watermarked image at Δ = 4

Watermarked image at Δ = 8

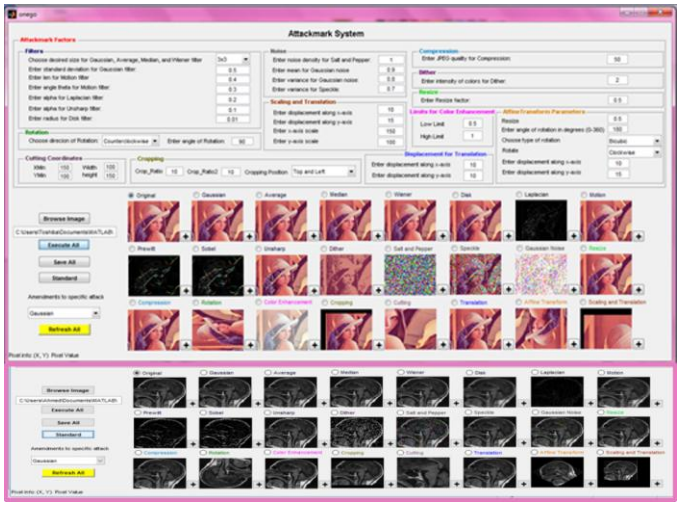


Figure 8. Generated attacks on the watermarked images

Table IX: Fragility Test for Authentication Applications

Experiments at Δ = 4.			
Attacks	**Condition**	**Attacks**	**Condition**
Wiener 3×3	Tampered	Low pass 3×3	Tampered
Median 3×3	Tampered	JPEG 95	Tampered
Scale 1.0001	Tampered	Scale 0.999	Tampered
Gauss. noise m=0,v=0.00005	Tampered	S&P noise, *d*=0.0005	Tampered
Stirmark_RML_100	Tampered	Contrast enhancements intensity=0.3, 0.9	Tampered

Table X: Robustness Test for Copyright Applications

NC values at Δ =24 mobile number = 97150634847900			
Attacks	**NC**	**Attacks**	**NC**
S&P noise, *d*=0.05+ Median 3×3	1	JPEG 18	1
Cropping 48% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 5×5	1
Cropping 50% V	Failed	Low pass 3×3	1
Gaussian noise m=0, v=0.002	Failed	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	1
Contrast enhancements intensity=0.3, 0.9		Scale 0.4	1

CONCLUSIONS

Dual watermarking applications has been presented. The system can embed watermarks in the low frequency coefficients

or high frequency coefficients depending on the application required by user. Graphical user Interface (GUI) has been implemented to ease the utilization of the proposed system. Medical images have been used to validate the authenticity of the proposed system. The original medical images were successfully restored if the transferred image found to be authentic. Satellite image transfers and topography image transfer can also be authenticated using the proposed system. For the copyright applications, the watermark has been placed in the low DCT coefficients which increases the robustness and maximizes the chances of reconstructing the watermark even after common signal distortions. The system has been examined using different colour and medical images. Two evaluation techniques were used in the experiments with different watermarking strengths between the host image and the watermarked image. Attacks have been applied with different sensitivity parameters using attackmark system for evaluation purposes.

REFERENCES

[1] A. M. Alattar, "Smart images using Digimarc's watermarking technology," in *SPIE Electronic Imaging '00, Security and watermarking of Multimedia content II*, San Jose, CA,, 2000, pp. 264-273.

[2] R. B. Wolfgang and E.J.Delp, "Fragile Watermarking using the VW2D watermark," in *Security and Watermarking of Multimedia Contents*, San Jose, CA, 1999, pp. 204-213.

[3] Z. Wang, A. Bovic, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," in IEEE Transactions on Image Processing, 2004, pp. 600-612.

[4] Ahmed -Al-Gindy, "Evaluation tool for generating attacks on watermarking Algorithms," IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.6, June 2016

[5] Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform, IEEE Transactions on Image Processing, Vol.13, No.8, Pp.1147-1156

[6] Tian, J. (2003) Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.8, Pp.890-896.

[7] Wang, F., Pan, J. and Jain, L.C. (2009) Digital watermarking techniques, Studies in Computational Intelligence, Springer Berlin / Heidelberg, Vol. 232/2009, Pp. 11-26.

[8] Zhang, X. and Wang, S. (2009) Fragile watermarking scheme using a hierarchical mechanism, Signal Processing, Vol. 89, Issue 4, Pp. 675-679.

[9] A. Al-Gindy, H. Al-Ahmad, R. Qahwaj, and A. Tawfik, "A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel " in Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA 2008). , Amman, Jordan, 2008.