

Compare Between DCT and DWT for Digital Watermarking in Color Image

Khalid K. Jabbar* Munthir B. Tuieb
College of Education, Computer Science Department, University of Al Mustansiriya, Baghdad-Iraq

Abstract
In This paper we compare between Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) in the field of image authentication and digital watermarking. Our proposed method depending on the embedding stage and extraction stag that presented in [1] but our scheme embeds the logo bits inside the low frequency domain because DWT gives optimal results with LL domain, while [1] used middle frequency domain with DCT. Our improvement by using a secrete K called user key (int. K=1, K<=N) where N=10, is used to generate a random vectors for the selected coefficient, this attempt is made to increase the security and robustness for the proposed scheme to compare between DCT that illustrated in [1] with middle frequency domain and DCT, DWT in the existing paper that used low frequency domain, it used block based technique with embedding stage, the development that illustrated in the existing paper by using DWT transform on the recovered of binary watermark for the purpose of image authentication in frequency domain using DWT, and DCT transforms with true color image. The method focused on the objective quality after embedding stage and the recovered watermark after extraction stage. With DWT in the first step, the cover image is decomposed into three levels by DWT transform. Then the hiding site was LL sub band of the DWT coefficients. Furthermore, our proposed method deal with true color image without converting its color space into other color space with various image texture all of them with size of 256*256 Bit map image file format, the proposed scheme deal with three sub-bands (Red, Green, and Blue) at the same time to hide logo bits inside the host by using Patchwork technique with embedding stage, so if one is destroyed the other may survive, it provide optimal security whenever any sub-bands color destroyed. With our proposed method a secret watermark in the form of binary (o, 1) pattern is embedded inside the host under DCT, DWT, one bit from the watermark will be embedded inside the selected coefficient from the selected block of the host. Our proposed method was evaluated with different types of intended attacks such as: salt and pepper noise, Poisson noise, and speckle noise. Moreover, unintended attacks consider by spatial enhancement filter such as median filter that used to improve the quality for the watermarked image after unintended attack. After experiments, it was found that our proposed method provides security and high performance with low computational complexity and good objective quality. Our scheme evaluate the imperceptibility for the watermarked image after embedding stage by using Peak signal to Noise Ratio (PSNR), while the recovered watermark evaluated by some types of metrics such as Mean Square Error (MSE), Normalized Correlation (NC), and correlation factor (SIM). Our proposed method has ability to deal with different image texture and format such as (BMP), Portable Network Graphics (PNG), and Tagged Image File Format (TIFF).
Keywords: Authentication, Objective, Subjective.

1. Introduction

With onset of the World Wide Web, authors of digital media can easily distribute their works by making them available on Web pages or other public forums. Anyone having access to those forums can copy the author's media. By the nature of digital media, a copy is an exact, perfect duplicate of the original. This brings to front a potential problem. How do authors claim ownership a right of such digital media if multiple persons have exact copies, one method is to embed additional information and only distribute the media that contains this additional information. The embedded information is known as a watermark can provide, for example, information about the media, the author, copyright, or license information. Interest in digital watermarks has grown out of an increasing interest in intellectual property and copyright protection. Digital watermarks may be perceptible (visible) or imperceptible (invisible) to human vision. Visible watermarks, by nature, are more intrusive to the media and act to deter theft of the media, such as a warning sign announces an alarm system even if one does not exist. Examples of such watermarks can be seen easily on most network television stations by the station's logo in the corner of the viewable screen. These watermarks are typically confined to an area of the image, which is less intrusive to the overall image. Attackers have a visible target and can remove the watermark by cropping the image [2, 3]. For the watermarking method to be effective, it should be imperceptible and robust to various image processing attacks. The commonly technique used frequency-domain transforms are the (DWT), (DCT) and Discrete Fourier Transform (DFT). However, Using DCT is simple, fast and is mainly for its similarity to BMP image file type. The DCT can be applied to transform the whole image or image blocks. Moreover, DCT allows an image to divide into different frequency domains to determine the best hiding domain later; these properties make DCT more suitable with image authentication and digital watermark with true image. DWT has

been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system (HVS) [4]. In [5] DCT and DWT are used for embedding and extraction of watermark. DWT and DCT are compared with respect to peak signal to noise ratio (PSNR) at a different threshold values. DWT gives better Image quality then DCT. A subsampling based watermarking scheme has been investigated in [6] for digital images. The algorithm utilizes the wavelet multi-resolution structure and subsamples the individual sub- band coefficients in order to embed the watermark information respectively. The proposed method compared with the similar approach by discrete cosine transform based approach, the wavelet based algorithm apparently preserves superior image quality and robustness under various attacks.

The primary goal for our proposed method is focused on the invisibility for the embedded watermark and the quality for the watermarked image after embedding stage and the recovered watermark after extraction stage to compare the fidelity for the proposed method between DCT, DWT.

2. Discrete Wavelet Transform

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension.

The filters divide the input image into four non-overlapping multi-resolution sub bands, a lower resolution approximation image (LL1), horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. The process can be repeated to obtain multiple scale wavelet decomposition. The information of low frequency district is an image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image. According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Embedding the watermark in the higher level sub bands increases the robustness of the watermark. However, the image visual fidelity may be lost, which can be measured by PSNR. With the DWT, the edges and texture can be easily identified in the high frequency band .Therefore it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then it can carry more watermark signal and has good concealing effect [7].

3. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) is a way to transform a signal into elementary frequency components. Two dimensional DCT is used in image compression. In which the 2-D DCT of a given matrix gives the frequency coefficients in form of another matrix where vertical and horizontal dimensions are considered. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks [8].

4. The Proposed Method

The important fact with the field of image authentication is the imperceptibility. Other hand, the host different form one to another and its texture different, few attempts have been made with true image authentication, the color image watermarking schemes for digital watermark and image authentication that have been relatively developed without converting the original image color space into other color space such as: [1,4,9, and 10], but other attempts in field of digital watermark that deal with color image converts the original image from R, G, and B to other color space such as: YIQ, YC_bC_r, YUV, and Index image, this attempts found in [13, ,14,15,16, and 17], While most color image watermarking schemes concentrate on the efficiency of tamper detection, but the improvement of visual quality of the recovered watermark that used for blind tamper proofing with color image is not discussed.

Our proposed method deal with color image with different texture without converting its color space into other color space, and it focused on the quality for the watermarked image after embedding stage and recovered watermark after extraction stage. Our proposed method embedding original watermark in the binary patterns into the color image under DCT, and DWT domain by modifying the selected coefficients for low frequency domain, to achieve perceptual invisibility of the watermarked during embedding stage that adapted in [1] by using only DCT, while the existing paper deal with the same embedding algorithm but with two transforms DCT, and DWT.

A binary watermark bits are embedded in certain sub-bands of a 3-level DWT transformed of a host image. Then, DWT transform of each selected DWT sub-band then the watermark bits are embedded in the selected coefficients of the selected corresponding DWT block in low frequency (LL) domain. In the extraction stages, the watermarked image, which may be attacked or processed by any types of mild processing, is first

preprocessed by median filter without effective for the quality of the recovered watermark, this preprocessing enhanced and reduced the effectiveness that accorded after mild processing such as noise with different types. Then, the same approach as the embedding stage is used to extract the DWT coefficients form low frequencies of each sub-band. The following figure shows the global diagram of our proposed method:

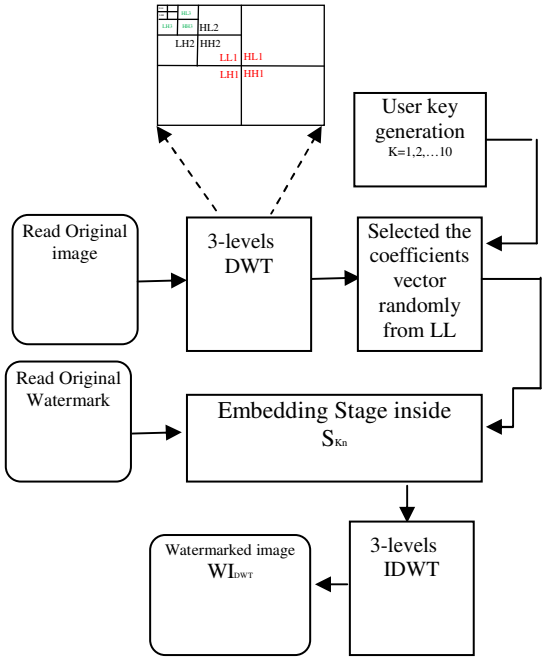


Figure 1. General Diagram for Embedding Stage under DWT

4.1 Algorithm: Embedding Stage Under DWT

Input: O as Original Image.
W as Original Watermark.
Output: WIDWT as watermarked image after DWT.

Step 1: Read the original image O.
Step 2: Read the original watermark W.
Step 3: Perform DWT on the O to decompose it into three non-overlapping (3-level) coefficient sets: LL1, HL1, LH1 and HH1 to produce ODWT'.
Step 4: Perform DWT again HL1 sub-bands to get smaller sub-bands and choose randomly the coefficient sets.
Step 5: According to key generation K (k=1, k<=N), selects the coefficients SKn randomly from LL1. Where N=10.
Step 6: Perform the embedding stage to hide the watermark bits inside the transformed image O' in the selected coefficients SKn, after DWT performed by modify the selected coefficients SKn value.
Step 7: Perform the inverse DWT (IDWT) on the ODWT', including the modified coefficient sets, to produce the watermarked image WIDWT.
Step 8: END.

After embedding stage completed and the watermarked image under DWT produced, the extraction stage produced to extract the watermark from the watermarked image, this process with its activities illustrated in the following algorithm:

4.2 Algorithm: Watermark Extraction after DWT

Input: WIDWT as Watermarked image.
Output: RDWT' as Recovered watermark.

Step1: Read WIDWT.
Step2: Apply DWT (3-level) to decompose WIDWT into four sub-bands LL', HL', LH' and HH'.
Step3: Perform DWT (3-level) again over the low frequency domain represented by LL1' sub-bands to get another sub-bands.
Step4: Choose the selected coefficients SKn randomly from LL1' sub-band by using K'.
Step8: Perform the same extraction process that illustrated in [1] embedding process.

Step9: Extracted Watermark, RDWT'.
Step10: END.
The following diagram illustrates the extraction stage in our proposed method:

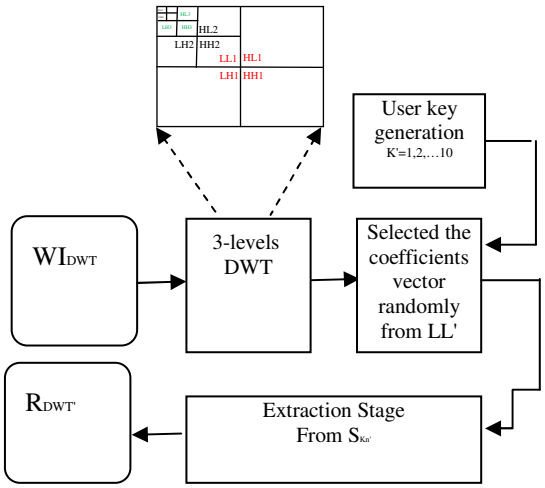


Figure 2. General Diagram for Extraction Stage under DWT

5. Performance Measures

Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. The performance of any watermarking scheme can be evaluated on the basis of its robustness and imperceptibility. The imperceptibility can be measured by using (PSNR). The PSNR has been utilized to calculate similarity between the original image and the watermarked image by using equation 1.

$$PSNR = 10 \log_{10} \frac{(R)^2}{MSE} \tag{1}$$

Where the performance measure (MSE), which used to assess the extent of tampering. A tamper assessment function MSE that used in the existing work computed between the original watermark W and the recovered watermark R′, to determine the refined value between of them, MSE computed by using equation (2) to find the competency of W under unintended attack [16]**.**

$$MSE = \frac{\sum_{x,y} [O(x,y) - R(x,y)]^2}{W*H} \tag{2}$$

Robustness is a measure of the immunity of the watermark against attempt to remove it by different types of attacks. We measure the similarity between the original watermark and the extracted watermark from the attacked image by utilizes the Normalized Correlation (NC) factor that computed from the following equation [17].

$$NC = \frac{\sum_{j=0}^{j-1} \sum_{k=0}^{k-1} W1(j,k) W2(j,k)}{\sum_{j=0}^{j-1} \sum_{k=0}^{k-1} W1(j,k)^2} \tag{3}$$

Another performance measure that used to measure the similarity between the original watermark and the extracted watermark using the correlation factor **sim** given below:

$$Sim = \frac{\sum_{I=1}^{N} W_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \hat{w}_i^2}} \quad (4)$$

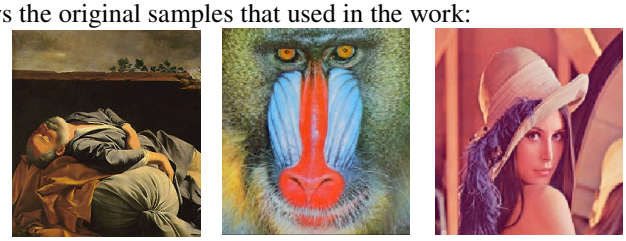
Where N is the number of pixels in watermark, w and $w\hat{}$ are the original and extracted watermarks respectively. The correlation factor *sim* may take values between 0 to1. If exact matches occurs, then sim=1[18].

6. Results

The experiments are carried out on the 3 images with different types and texture such as: standard given by Lena, high texture that given by Baboon, and low texture that given by Poor, but all of them have the same following properties:

- Image of size: 256 × 256 pixels.
- Color format: BMP – 24 bits.
- The wtermark used is a binary logo of size 128 × 128 pixels.

The following figure shows the original samples that used in the work:



a b c

Figure 3. Original Image with Different textures, (a) low texture as poor, (b) high texture as baboon, (c) smoothed as lean

One of the importants expirement results that presented in our proposed method is made by processing the watermarked image for some type of noise such as salt and pepper, piossion noise, and speckly noise, then the attacked image was treatments by using median filter, the aim of the previouse activites is to assessment the ability of proposed method (DCT, DWT) in resistance of attacks. For the experimental purpose the results that represent the quality of the watermarked image by using PSNR after embedding stage that taken without any pre-processing obtained from the following tables, While MSE that computed between the original watermark and the recovered watermark illustrated in the same table:

Table 1. PSNR, MSE for the Watermarked Image After DCT.

DCT (db units)	Lena	Baboon	Poor
PSNR	47.1225	47.0003	45.9991
MSE	0.0020	0.0155	0.1155

The next table illustre the value for PSNR for the watermarked image after embedding process completed after DWT.

Table 2. PSNR, MSE for the Watermarked Image After DWT.

DWT (db units)	Lena	Baboon	Poor
PSNR	41.1225	40.0003	39.9991
MSE	0.9995	1.1020	1.1150

The next figure shows the watermarked image with its histogram after DCT transform:

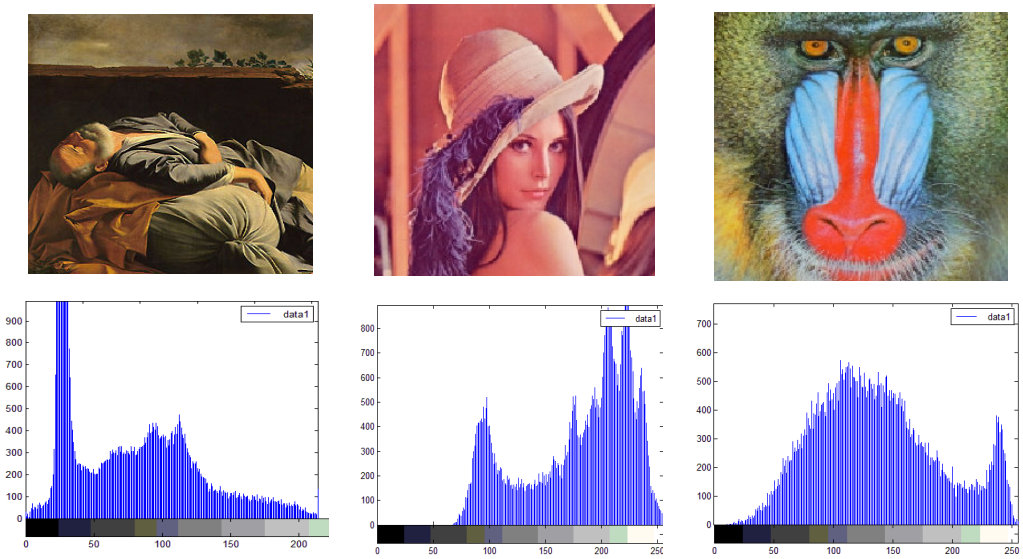


Figure 4. Watermarked Image after DCT with Histogram

While figure 5, shows the objective quality after embedding process completed under DWT:

Figure 5. Watermarked Image after DWT with Histogram

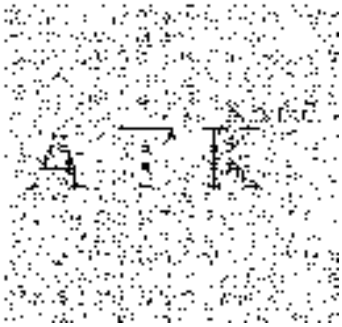


Figure 7. The Recovered Watermark After DWT

Figure6. The Recovered Watermark After DCT

Figure 6 shows the recovered watermark after DCT, while figure 7 shows the recovered watermark after DWT. Our proposed scheme was exposed for intended attack such as salt and pepper noisy, then we enhanced the noised watermarked image with spatial filter such as median filter that illustrated in figure 8 under DCT and figure 9 under DWT, to see how noises are effect on the objective quality under DCT, and DWT for our human eyes, figure 10 shows the watermarked image under DCT after passion noise, while figure 11 shows the watermarked image with the same noise but after DWT. While Table 3 shows the results that gained after computed (NC) values between the original watermark and recovered watermark under DCT, the results under DWT illustrated in table 4. And SIM results illustrated in table 5 after DCT, to see the similarity between the original watermark and recovered watermark, while the results after DWT illustrated in table 6.

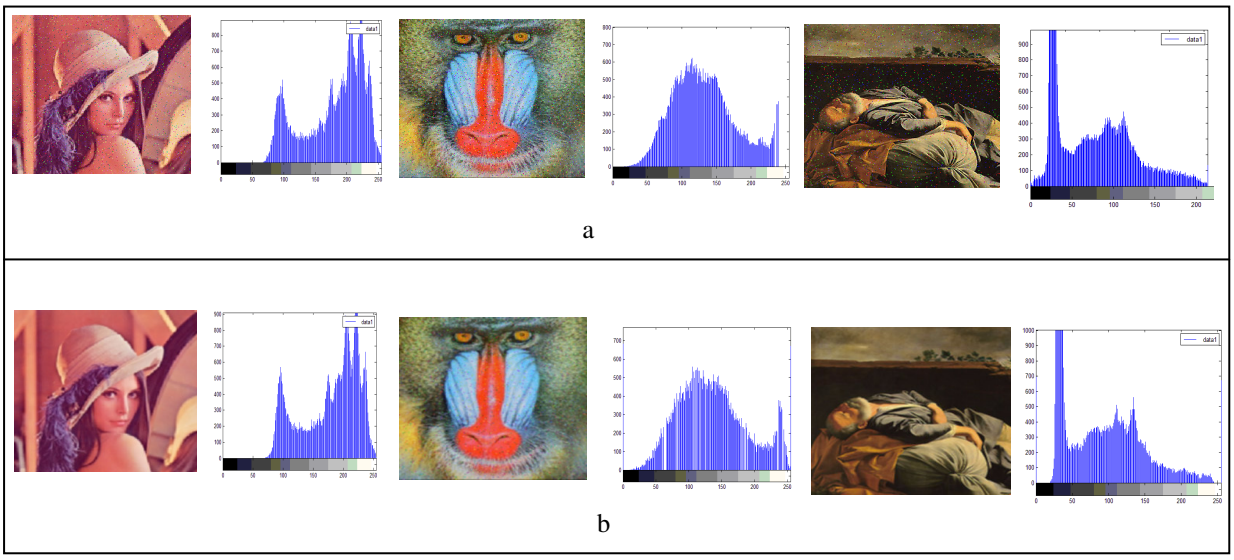


Figure 8. Watermarked Image after DCT
Group (a): Watermarked Image after Salt and Pepper with Histogram, Group (b): Watermarked after Median Filter with Histogram

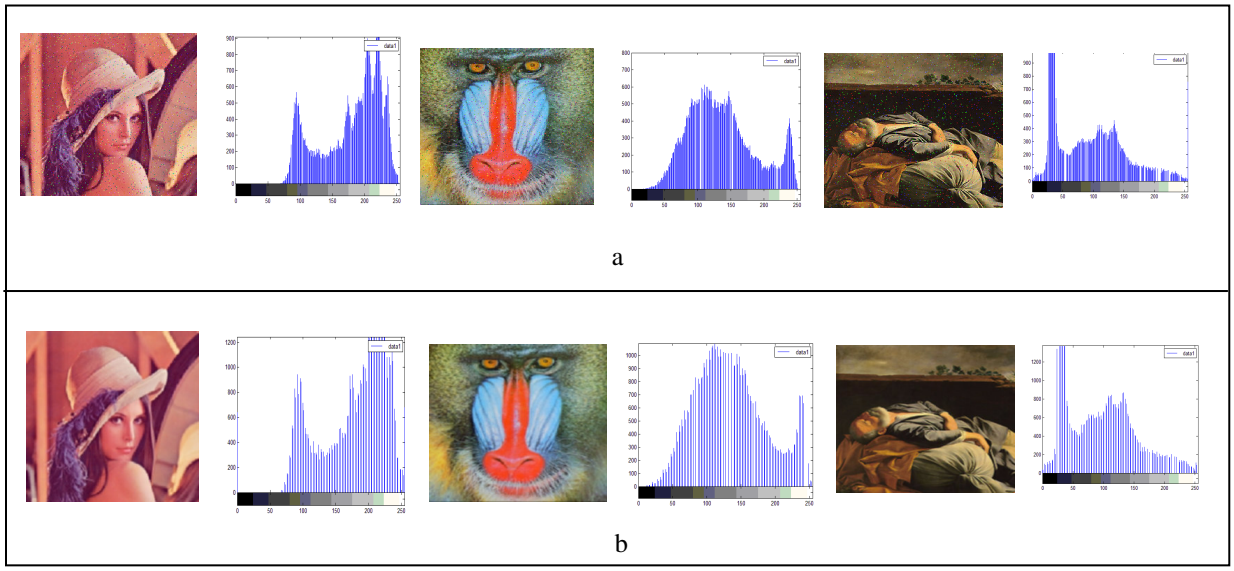


Figure 9. Watermarked Image after DWT
Group (a): Watermarked Image after Salt and Pepper with Histogram, Group (b): Watermarked after Median Filter with Histogram

Table 3. NC for the Watermarked Image After DCT.

DCT / NC	Salt & Pepper	Poisson noise	Speckle noise
Lena	0.9970	----------	----------
Baboon	0.8910	0.9601	0.9111
Poor	0.7774	0.8654	0.8774

Table 4. NC for the Watermarked Image After DWT.

DWT / NC	Salt & Pepper	Poisson noise	Speckle noise
Lena	0.9794	0.9981	0.9981
Baboon	0.7955	0.8770	0.6543
Poor	0.7689	0.9934	0.5543

The following fugure shows the objective quality (watermarked image) after poisson noise with DCT, and DWT.

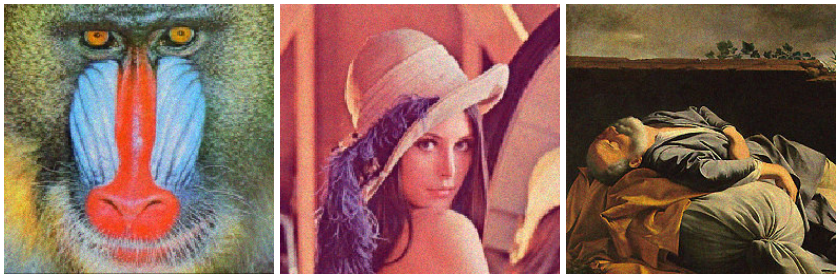


Figure 10. The Watermarked Image after Poisson Noise after DCT

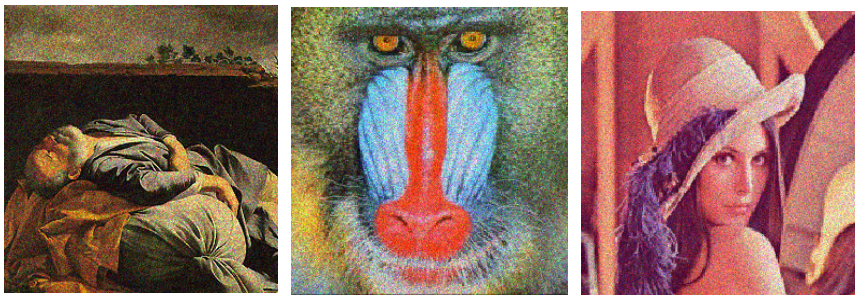


Figure 11. The Watermarked Image after Poisson Noise after DWT

Futhermore, the similarity between the original watermark and the recocered watermark illustrated in the following tables after DCT, and after DWT:

Table 5. SIM for the Watermarked Image After DCT.

DCT / SIM	SIM
Lena	0.9905
Baboon	0.9743
Poor	0.94430

Table 6. SIM for the Watermarked Image After DWT.

DWT / SIM	SIM
Lena	0.58036
Baboon	0.45610
Poor	0.45010

7. Conclusion

In this paper, we attempted to hide the watermark bits that considered as logo pattern inside the host with BMP color image format fewer than two transforms such as DCT, and DWT to obtain the objective quality after embedding stage and to compare between of them to gain the results after numbers of tests illustrated inside intended and unintended attack. Our proposed method focuses on the invisibility for the embedded watermark under DCT, DWT, and the quality for the watermarked image after embedding stage; furthermore it focuses on the quality for the recovered watermark after embedding stage performed under DCT, DWT. So, in the field of objective with invisibility, it was found that the watermarked image after embedding stage under DCT, DWT has good objective quality, and the watermark bits are not visible for human eye, but with subjective, it was found that the PSNR value was high with DCT rather than DWT such as: the PSNR for watermarked image after DCT has 47.1225 Db with lena sample while PSNR for the same sample under DWT is 41.1225 Db. A high-quality for the recovered watermark can be achieved under DCT, but the recovered watermark under DWT was destroyed, such as: the value of MSR for the recovered watermark was 0.0020 for lena sample under DCT, but it is 0.9995 for afetr DWT. Furthermore, Our proposed method was exposed for some type of intended attacks such as salt and pepper noise with 0.02 degrees, Poisson noise, and speckle noise then we perform some type of preprocessing such as median filter to improve the watermarked image quality, after then the value of SIM was computed between the original watermark and the recovered watermark to gain the similarity between of them and it was found that the recovered watermark under DCT is the best rather than DWT. While NC that used to evaluate the robustness was used to evaluate the similarity between the original watermark and recovered watermark, it was found that noises are effect on the quality for the watermarked image. Where NC measure computed from the attacked image between original and recovered watermark, the recovered watermark from attacked image after DWT was destroyed while the recovered watermark after DWT survive, the important note that the previous results may be different with another embedding algorithm, our proposed scheme implemented by using MATLAB 10. The proposed watermarking algorithm is tested for the various image textures with color BMP, PNG, TIFF image file format with size of 256×256.

References

[1] Khalid K. Jabbar, 2014, "The Optimal Hiding Site with DCT", University of Al-Mustansiriya, College of Education, Computer Science Department, Baghdad-Iraq.

[2] Venkata R. and Rama K**.,** 2010, **"** Secure Image Watermarking in Frequency Domain using Arnold Scrambling and Filtering**"**, Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 3 Number 2 pp. 236–244.

[3] N.F. Johnson, S. Jajodia, 1998, "Steganalysis of Images Created using Current Steganography Software," in [4], pp. 273-289.

[4] hang-Lin, I-Ju T. and Bin-Yuan H. 2008, "Protecting Copyright of Color Images Using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal of Multimedia, Vol.3, No.4.

[5] Rakhi D. , Roop S. and Sarita , R., 2011, " Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR", International Conference on Communication Systems and Network Technologies, IEEE, Gwalior, India.

[6] Min-Jen Tsai and Hsiao-Ying Hung, 2013, " DCT and DWT-based Image Watermarking by Using Subsampling", institute of Information Management National Chiao Tung University. China.

[7] Mohammad Ibrahim K., Md. Maklachur R. and Md. Iqbal Hasan Sa., 2013, " Digital Watermarking for Image AuthenticationBased on Combined DCT, DWT and SVD Transformation", 1Department of Computer Science and Engineering, Chittagong University of Engineering and Technology Chittagong-4349, Bangladesh.

[8] Abdul R., Olasebikan A and Periasamy K., 2009, "Digital Watermarking Of Still Images With Color Digital Watermarks**",** 978-1- 4244-3861- IEEE.

[9] Soumik D., Pradosh B., Monalisa B., 2011, " A Chip-Based Watermarking Framework for Color Image Authentication"**,** *ICCCS'11*, February 12–14, Rourkela, Odisha, India.

[10] Patchara S., Yun-Qing S., and Tieniu T., China, 2010, "New Developments in Color Image Tampering Detection", IEEE, Hong Kong and the National Science Foundation of Grant No. 60603011.

[11] Qian-chuan Z., and Qing-x., China, " A DCT Domain Color Watermarking Scheme Based on Chaos and Multilayer Arnold Transformation", International Conference on Networking and Digital Society, IEEE, Chengdu.

[12] Li Y. and Hao Y.," A Research on the Robust Digital Watermark of Color Radar Images", International Conference on Information and Automation June 20 - 23, Harbin, China, IEEE, 2010.

[13] Na W., and Chung-Hwa K., 2009, " Color Image of Tamper Detection and Recovery using Block-based Watermarking", Dept. Electronic Engineering of Chosun University Chosun University Gwangju, Korea, IEEE.

[14] SHI H., and LV F.," A Blind Digital Watermark Technique for Color Image Based on Integer Wavelet Transform", School of Software, East China Jiaotong University Nanchang，China, IEEE, 2010.
[15] Kuo-Cheng L., 2010, " Pattern-Based Fragile Watermarking For Color Images", European Signal Processing Conference (EUSIPCO), Taiwan.
[16] hang-Lin, I-Ju T. and Bin-Yuan H., 2008, "Protecting Copyright of Color Images Using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal of Multimedia, Vol.3, No.4.
[17] Kaushik Deb,1*Md. Sajib Al-Seraj,1 Md. Moshiul Hoque,2 and Md. Iqbal Hasan Sarkar1, 2012, " Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", International Conference on Electrical and Computer Engineering, Dhaka, Bangladesh, 20-22 December.
[18] Ali Al-Haj, 2007, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3(9):740-746.

First A. Author

Asst. Lec. Khalid Kadhim Jabbar, Baghdad-Iraq, date of Birth 3\ 4\ 1978. BSc. In Computer Science, Baghdad University, Baghdad-Iraq, 2001, HI-DUP in Data Security, ICCI, Baghdad-Iraq, 2002. MSc in Software Engineering Science, ICCI, Baghdad-Iraq, 2012. The major field of study is: information hiding (digital watermarking), image processing, and software engineering.
Khalid K. Jabbar was a Fellow to review the papers that submitted to IEEE-ICECCO' 2013.

Second A. Author

Asst. Lec. Munthir Bahir Tuieb, Baghdad-Iraq, date of Birth 29\ 4\ 1987, BSc. In Software Engineering, Immam Iaa'far Al-Sadiq, Baghdad-Iraq, 2009. MSc in Software Engineering Science, ICCI, Baghdad-Iraq, 2012. The major field of study is: Net Work and Communication, Computer Driven and Maintenance.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar