Comparative Analysis of DCT and DWT based novel methods for Watermarking

Arshad Hassan Lone[1], Reena Chauhan[2]

[1]Research Scholar, Dept. of ECE, SDDIET college, Panchkula, Haryana , India
[2]Assistant Professor, Dept. of ECE, SDDIET college, Panchkula, Haryana , India

---***---

Abstract - *Present age is the age of information and digital multimedia plays a very vital role in the representation, expression and propagation of the information. Equally important is to secure the information from being duplicated, altered and mutilated. Digital watermarking, hence has become a hot research topic to safeguard the copyright of the content. This work provides an innovative image watermarking scheme in two transform domains – Discrete Cosine Transform and Discrete Wavelet Transform. It is proved that DWT is more suited for Human Visual System. DWT is better than DCT in various aspects and becomes better as embedded factor is increased at the expense of imperceptibility and fidelity because, as the embedded factor is decreased below 10, the watermark becomes visible in the watermarked image. We also study various issues – robustness, fidelity, capacity and reliability in a proper manner and concluded that these are inter-related and a good watermark technique should take this into consideration. As we increase robustness, by making watermark strongly entrenched with the image, then the perceptibility and fidelity suffers. For increasing capacity, if we embed a larger watermark, then also the perceptibility and fidelity suffers. Thus there is a trade-off among the parameters. From the study, it is obvious that DWT is better technique than DCT for the application of watermarking. When embedded factor is chosen to be small, it results in better robustness but perceptibility and fidelity suffers. When embedded factor is chosen to be large, it results in better perceptibility and fidelity but robustness and reliability suffers. We have concluded that a medium value (k = 10) is a better pick for our case, which takes into consideration all the parameters simultaneously.*

***Key Words*: Digital Watermarking, Discrete Cosine Transformation, Discrete Wavelet Transform, Robustness, Fidelity, Capacity, Reliability.**

1. INTRODUCTION

Recent years have witnessed a rapid growth of digital media, and their propagation, especially images. This makes protecting multimedia information more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest and gradually has become a research hotspot in the field of information security [1]. The idea of robust watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations [10,12]. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary [2]. Some of the applications of watermarking are broadcast monitoring, copy protection, data authentication and data hiding. Watermarks are classified after watermark embedding operation, whether they are visible to human visual system or not; visible watermarking and invisible watermarking. In real life, shading examples visible digital watermarking is the most common is to add "confidential" words in the word document, the visible watermarking is equivalent to a statement. Without visible digital watermarking is required in the visual perception cannot be aware of its existence, it is normally hidden embedded into the carrier, when the need to be extracted from the carrier. Unless there is a special statement, the objective of study of digital image watermarking is invisible watermark.

This study presents a novel scheme of watermarking of digital images for copyright protection and authentication. In this study, we proposed methods of watermarking in frequency transformed techniques; Discrete Wavelet Transform (DCT) and Digital Wavelet Transform (DWT) respectively. In DCT, we embedded in the medium frequency region. It is a blind technique where we do not use the original image for extraction. In DWT, we embed in the LL region [3,4]. Although, it is the most sensitive region, but embedding in this region proves resistance to various attacks especially compression. For DWT, non-blind technique is used [5,8,9,11].

2. THREATS AND SECURITY REQUIREMENTS

Threats are the conditions of possible specific actions that are enforced over the document that makes it counterfeit and illegal as against the wishes of the owner or creator. The most important threats which ought to be handled to ensure the security of the multimedia system are [1]:

2.1 THREAT OF CONFIDENTIALITY: This threat represents the possibilities of accessing the data or document via unauthorized channels, with the growing usage of Internet, the chance of its occurrence is highly likely and is hard to get it dispelled out, unless effectively addressed.

Security Requirement: This requirement emphasizes the permit of only authorized access to the document or content and prevents the unauthorized access of resources [6,7].

2.2 THREAT OF INTEGRITY: This is a threat to the content of the document by unauthorized entities, where the resource can be altered without any detection.

Security Requirement: It is required by this security requirement that the data be identically maintained from its source to destiny, and has not been accidentally or modified, altered, or destroyed, and remain unchanged right throughout the operations such as transfer, storage, and retrieval.

3. PROPOSED METHODS

3.1 DCT BASED

The Algorithm for DCT based Digital Watermarking Embedding is proposed as below:

a) Read the watermark and the original image.
b) Make the watermark image information into the 1-Dimensional sequence.
c) Input the original image into 8 x 8 sub-blocks, then do the DCT transform.
d) Sort the coefficients of each sub-block after the DCT transforming, find two coefficients in the middle energy and record their locations. In the 8 x 8 blocks, the sequence has length of 64 according the sorting result and the middle energy locations are the 32nd (coefficient P) and 33rd (coefficient Q). Record the initial positions of these two coefficients in the sequence before sorting. Here we have used two mid-band locations viz. P as (5,2) and Q as (4,3).
e) According the principle above, compare the watermark information, exchange the coefficients if the relative doesn't match the watermark information

   If i = 0;
      Make |P| > |Q|;
   Else
      Make |P| < |Q|;

f) Do the inverse DCT and form the watermark image.

The Algorithm for DCT based Digital Watermarking Extraction is proposed as below:

a) On each 8 x 8 block of the watermarked image DCT is performed.
b) Compare the middle frequency coefficients, i.e. the coefficient values at locations ((5,2) and (4,3) are compared.)
c) If coefficient value at (5,2) is greater than (4,3), then the message bit is 1; otherwise it is 0. Then form the 1_D sequence
d) Re-organize the 1-D sequence into 2-D sequence and form the recovered watermark image.

3.2 DWT BASED

The Algorithm for DWT based Digital Watermarking Embedding is proposed as below:

Given a watermark, host image, watermark embedding inserts the watermark into the target area of the host image. The cover image is decomposed into 1-level using DWT as the transform domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. Here, we are using the Haar wavelet (db1). The embedding is done in the LL region. So the altered host image i.e. watermarked image (LL) region (LL1) is

$$LL1 = LL + k*w;$$

Where w is watermark, and k is the embedding factor/strength. As watermark is directly embedded into some region, so far matrix addition to be feasible; we can concatenate zeros to watermark (in case watermark image is smaller than size if LL band). The cover images further reconstructed using inverse discrete wavelet transform.

The Algorithm for DWT based Digital Watermarking Extraction is proposed as below:

The watermarked image is decomposed into level 1 using DWT as the transform domain at the receiver end. The extraction part is simply the inverse of the embedding procedure. Using the embedding strength (k) and the original image, we can recover the watermark. After receiving the final watermarked image (may/may not be altered by attacks). The below mentioned steps are followed to extract the watermark:

a) Obtain the 1-level DWT of the watermarked image.
b) The extraction part is as follows

$$W_{rec}(i,j) = (LL_{wi}(i,j) - LL(i,j))/k;$$

Where $W_{rec}(i,j)$ is the recovered watermark, $LL_{wi}(i,j)$ is the LL component of the watermarked image, LL(i,j) is the LL component of host image and k is the embedding factor. If concatenation is done in the embedding part, the de-concatenation is required here to retrieve the watermark.

4. IMPLEMENTATION RESULTS

Different images have been taking while analyzing various noise attacks and their effects on the original images and the recovered watermarks. It is not possible to display here all the results for all images. Fig-1 shows the original Lena image analyzed and the corresponding watermark.

Fig-1: Original image (Lena) and corresponding watermark

We use the standard Lena image (512 x 512) and watermarks of different sizes. The results have been simulated on MATLAB. The attacks performed are 'Salt & Pepper', 'Gaussian' and 'Compression'. Also region based attacks have been analyzed on the images. Fig-2 and Fig-3 show the recovered watermark when 'Salt & Pepper' and 'Gaussian' noise attacks were performed on DCT and DWT based watermarked image respectively. Fig-4 shows the recovered watermark which experienced region-based attack.

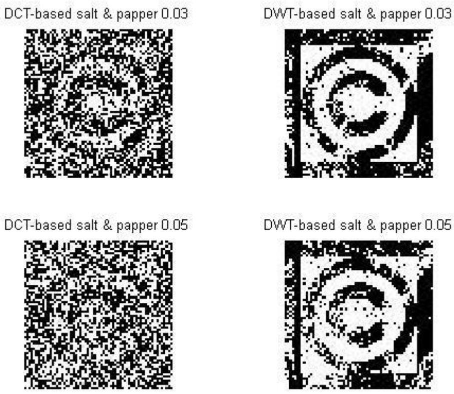

Fig-2: Comparison of recovered watermarks on basis of 'Salt & pepper' noise

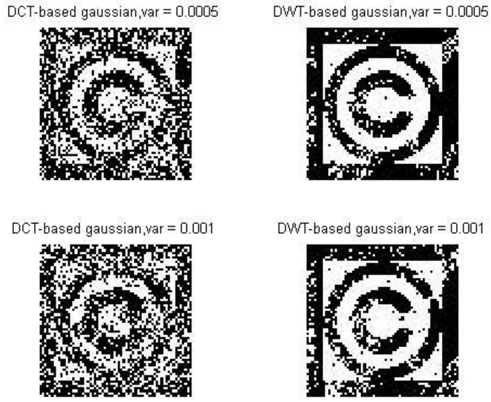

Fig-3: Comparison of recovered watermarks on basis of 'Gaussian' noise

Fig-4: Region based tempering and corresponding recovered watermarks in DCT and DWT domain respectively

Various parameters have been evaluated against the quality of recovered image after the watermarked image was attacked with different types of attacks. Fig-5 to Fig-9 show various parameters being evaluated for the recovered watermark when under 'Salt & Pepper' noise image.

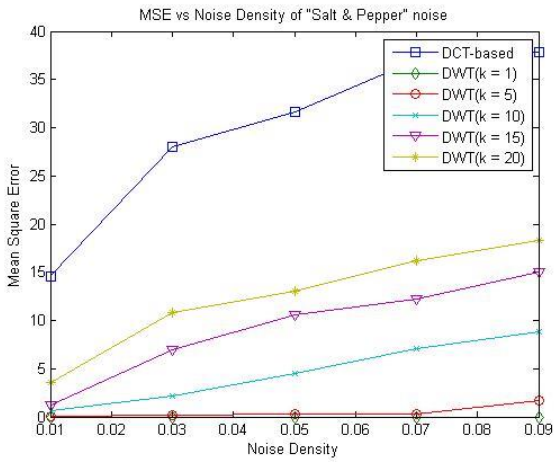

Fig-5: Comparison of received watermark; MSE vs Noise density

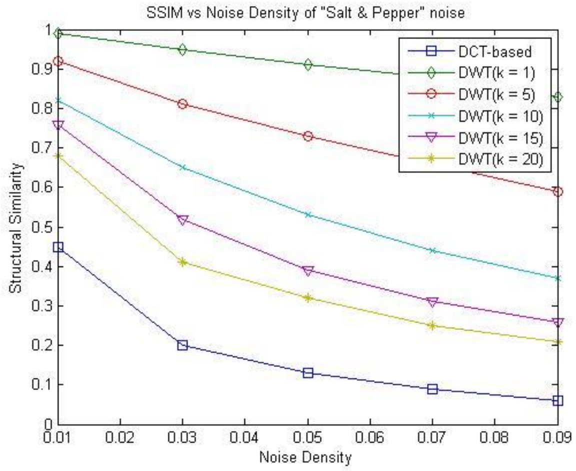

Fig-6: Comparison of received watermark; SSIM vs Noise density

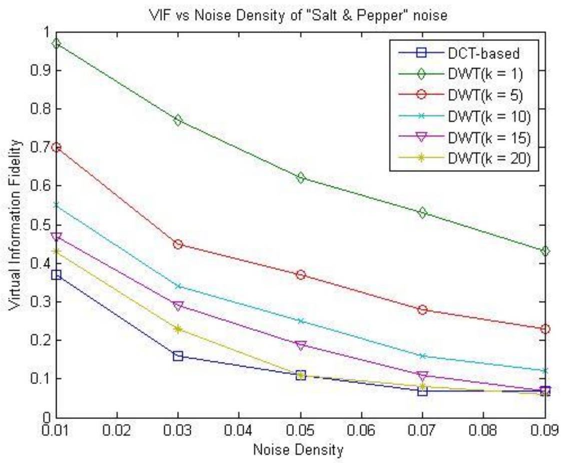

Fig-7: Comparison of received watermark; VIF vs Noise density

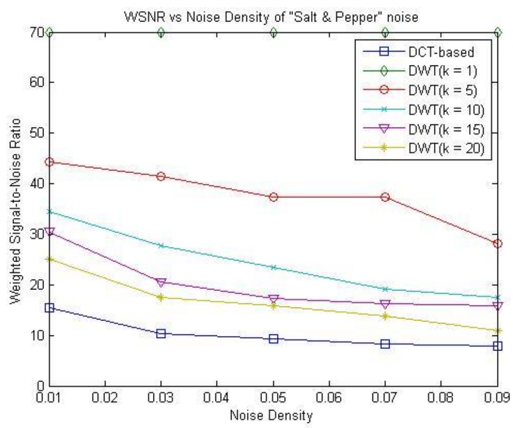

Fig-8: Comparison of received watermark; WSNR vs Noise density

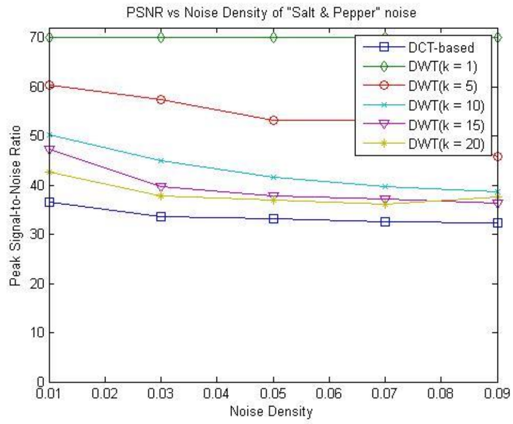

Fig-9: Comparison of received watermark; PSNR vs Noise density

From the results, following observations are made:

- MSE is comparatively higher in DCT than DWT. Also MSE decreases as the value of k (embedding strength) decreases from 20 to 1 in DWT.
- SSIM and VIF are higher in DWT as compared to DCT. Also SSIM and VIF has highest for k = 1 and decreases, as k increases.
- WSNR and PSNR are higher in DWT as compared to DCT technique. For k = 1, DWT provides highest value of WSNR and PSNR.

5. CONCLUSIONS

This work provides an innovative image watermarking scheme in two transform domains – DCT and DWT. Both the domains are good enough to resist various attacks. It is proved that DWT is more suited for Human Visual System. DWT is better than DCT in various aspects and becomes better as embedded factor is increased at the expense of imperceptibility and fidelity because, as the embedded factor is decreased below 10, the watermark becomes visible in the watermarked image. We also study various issues – robustness, fidelity, capacity and reliability in a proper manner and concluded that these are inter-related and a good watermark technique should take this into consideration. As we increase robustness, by making watermark strongly entrenched with the image, then the perceptibility and fidelity suffers. For increasing capacity, if we embed a larger watermark, then also the perceptibility and fidelity suffers. Thus there is a trade-off among the parameters. From the study, it is obvious that DWT is better technique than DCT for the application of watermarking. When embedded factor is chosen to be small, it results in better robustness but perceptibility and fidelity suffers. When embedded factor is chosen to be large, it results in better perceptibility and fidelity but robustness and reliability suffers. We have concluded that a medium value (k

= 10) is a better pick for our case, which takes into consideration all the parameters simultaneously.

REFERENCES

[1] Ashdown M., Flagg M., Sukthankar R., and Rehg J.M., A Flexible Projector-Camera System for Multi-Planar Displays, Computer Vision and Pattern Recognition (CVPR), pp. II-165 -II-172, 2014.

[2] Brown M.S. and Seales W. A Practical and Flexible Tiled Display System 10th Pacific Conference on Computer Graphics and Applications (PG'02), pp. 194 –203, 2002.

[3] Panyavaraporn, J.; Horkaew, P.; Wongtrairat, W., "QR code watermarking algorithm based on wavelet transform,"Communications and Information Technologies (ISCIT), 2013 13th International Symposium on , vol., no., pp.791,796, 4-6 Sept. 2013

[4] Naderahmadian, Y.; Hosseini-Khayat, S., "Fast Watermarking Based on QR Decomposition in Wavelet Domain," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.127,130, 15-17 Oct. 2010.

[5] Zhaoshan Wang, Shanxiang Lv,Yan Shna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform", 2012

[6] M. Nithya, "Multimedia Security", IIT Bombay, 2005.

[7] Bo Chen and Hong Shen, "A new robust-fragile double image Watermarking algorithm", Third international conference on multimedia and Ubiquitous Engineering, IEEE-2009.

[8] Ashish Kothari and Ved Vyas Dwivedi, "Transform Domain Video Watermarking: Design, Implementatiojn and performance and analysis", International conference on Communication and Network Technologies, Rajkot, Gujrat, India, ISBN: 978-0-7695-4692-6, may 11-13, 2012.

[9] Akhil Pratap Singh and Agya Mishra, "Wavelet based Watermarking on Digital image", Indian journal of Computer Science and Engineering, vol. 1, no. 2, 86-91, 2009.

[10] Del Colle et.al, "DWT based Digital Watermarking fidelity and robustness evaluation", Journal of Computer Science and Technology, 4-1-2008.

[11] Manzoor Ahmad Bhat, et.al, "Audio watermarking in images using wavelet transform", IJCST, vol.2, issue 4, Oct-2011.

[12] Say Wei Foo and Qi Dong, "A normalization based robust image watermarking scheme using SVD and DCT", IJICE, 2010.