Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain

Pooja Dabas , Kavita Khanna
Computer Science & Engineering,
M.D.U., Haryana , India

Abstract*— Availability of digital data such as images, audio and video has increased by the rapid expansion of internet. Public can easily access and share files on internet. With this availability, the technology also needs to enhance to protect data from unauthorized user. To protect infringement of the intellectual property digital watermarking becomes very important. Digital Watermarking is the process of embedding a secret information into a digital data. A methodology for comparing robustness of watermarking techniques is proposed. The techniques are used into a standard form to make comparison possible. In this paper, I will implement three different digital watermarking techniques each from Spatial Domain (LSB) and Transform Domain (DCT and DWT) evaluate their performance using various parameters such as PSNR, MSE, similarity ratio(SR), correlation(CORR) and BCR against robustness for attacks.

***Keywords*— Digital Watermarking, , Robustness, LSB, DCT, DWT, PSNR, MSE, SR, BCR, Attacks**

I. INTRODUCTION

Digital data like audio, images and videos are easily available to the public user by the boon of internet. The drawback is attack on the copyright owner's data. Thus, to provide security to multimedia data files and to save them from getting duplicated, various process can be used to protect intellectual property of the owners [1]. One of the important processes is the digital water marking. Digital Watermarking technique includes the process of embedding watermark and extraction of given watermark into the data file. A general definition can be as, "Hiding of a secret message or information within an ordinary message and extraction of it as its destination". Digital Watermarking consists of three major activities: Embedding, Attack and Extraction. Figure 1, shows a general watermarking process involving various operations. Following is a brief description:

A. Embedding

In this stage the original watermark signal is embedded into the original host image. The watermark image is then transmitted or published.

B. Attack

While transmission or publishing, modification or alteration may be done by user other then the owner or unauthorized users to that watermarked data file, which is called an attack. It is also said to be as a malicious activity.

C. Extraction

The last activity is the use of detection algorithm to extract the watermark and check for its authenticity. *This paper has been divided into seven sections. Section 2 describes the classification of watermarking technique. Section 3 states the watermarking embedding and extraction algorithm. Section 4 deals with the attacks. Section 5 contains performance parameters used to analyse the watermarking techniques. Section 6 includes the result of each by conclusion in section technique followed 7*

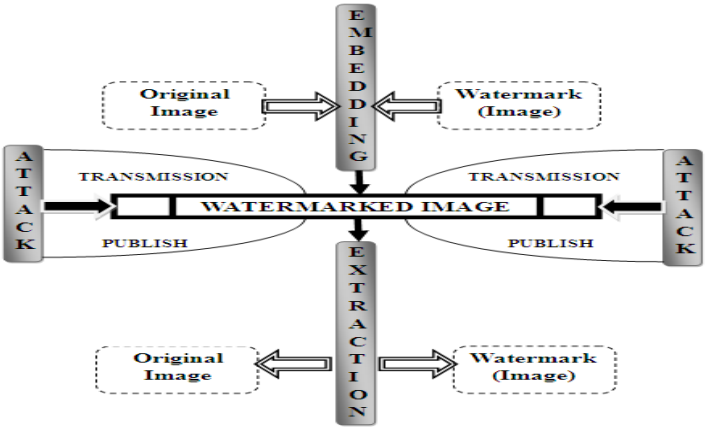

Fig. 1: General Watermarking Process

II. CLASSIFICATION OF WATERMARKING TECHNIQUE

Watermarking techniques are classified under various domains such as based on type of document used to embed watermark, based on working domain, based on human perception etc. Here we have chosen the broad category on how the watermark is embedded i.e. based on working domain. It is classified into two categories.

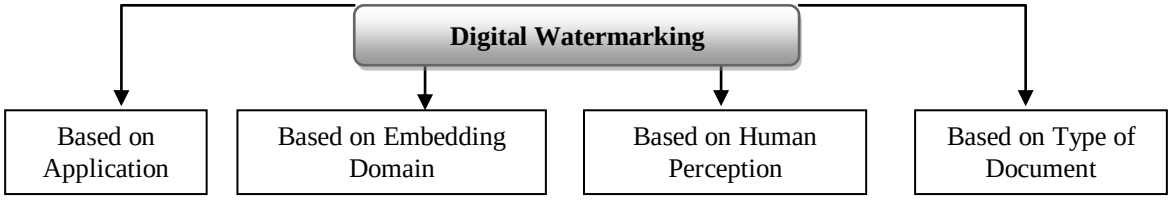

Fig 2: Classification of Watermarking under different domains

A. Spatial Domain

In this technique, the values of image pixels are directly modified. The technique we are comparing with is Least Significant Bit (LSB). It modifies the least significant bits of the image pixel data with the watermark pixels being embedded into it [7].

B. Transform Domain

In this technique transform coefficients are modified and not the pixels values. To extract the watermark inverse transform is performed. Some common transform falls in this category are Discrete Cosine Transform (DCT) [4], Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT)[5]. We have selected DCT and DWT from transform domain to compare.

III. WATERMARKING ALGORITHM

Watermarking algorithms comprise of two main procedures embedding and extraction. This paper study and analyses three different digital image watermarking algorithms. First is LSB from spatial domain and other two are DCT and DWT from transform domain**.**

A. LSB Algorithm

1) Embedding Process

1. Get the Input Image called Img
2. Get the Watermark image called wimg
3. wimg to OneD bit format
4. Identify size of image called (w,h)
5. For I =1 to w
6. For j=1 to h
7. WatermarkImage(img,I,j,8)=wimg (k)
8. K=k+1;
9. If (k>length(wimg)
10. Exit
11. Return WatermarkImage
12. Exit

2) Extraction Process

1. Read the Watermark Image WatermarkImage
2. Read the size of message
3. Identify size of image called (w,h)
4. For I =1 to w
5. For j=1 to h
6. Message(k)=WatermarkImage(I,j,8)
7. K=k+1;
8. If (k>size)
9. Exit
10. Return Message
11. Exit

B. DCT Algorithm

1) Embedding Process

1. Get the Input Image called Img
2. Get the Watermark image called wimg
3. Define the blocksize called blk and the frequency threshold
4. Convert wimg to OneD bit format
5. For i=1length(wimage)
6. Perform the DCT for the specific block (img,x,y) and return the dCT block

7. If (wimage(i)=0)
8. Swap the DCT block in Ascending order
9. Else
10. Swap the DCT block values in Descending order
11. Perform the Frequency Analysis for the block and hide data at extract DCT Blcok
12. Perform Inverse DCT over the image and represent it as watermarked block
13. Return WatermarkImage
14. Exit

2) Extraction Process

1. Get the Watermark Image called dimage
2. Get the message size called size
3. Define dCT Block size called blk
4. For i=1 to size
5. Perform the DCT over the (x,y) Block DCT(img,x,y)
6. Move to next block
7. Compare the DCT Block frequency values set the higher value to 1 and lower to 0
8. Message= Message U Extract(DCTBlockValue,high,low)
9. Return Message
10. Exit

C. DWT Algorithm

1) Embedding Process

1. Get the Input Image called Img
2. Get the Watermark image called wimg
3. wimg to OneD bit format
4. Define Blocksize for DWT called bsize and the FrequencyThreshold called freq
5. For i=1 to length(wimage)
6. Extract the DWT coefficients from the Block at position (x,y) under 'Haar' Wavelet
7. Move to next block
8. If (wimage(i)=0)
9. Sort the Diagonal Coefficient Elements in Ascending order
10. Else
11. Sort the Diagonal Coefficient Elements in Descending order
12. Perform the Frequency Analysis for the block and hide data at extract coefficient position
13. Perform Inverse DWT over the image
14. Return the Watermarked Image
15. Exit

2) Extraction Process

1. Get the Watermark Image called dimage
2. Get the message size called size
3. Define dWT Block size called blk
4. For i=1 to size
5. Decompose the image using DWT for the specific block at position(x,y) and extract the DWT coefficients
6. Move to next block
7. Compare the DWT Diagonal Coefficient and and set the higher value to 1 and lower to 0
8. Message= Message U Extract(DWTCoefficientValue,high,low)
9. Return Message
10. Exit

IV. ATTACKS

An attack is an activity performed to destroy the embedded watermark or to detect the original watermark and replace or modify with another watermark[9]. To achieve robustness against attack is one of the major characteristics of watermarking. Some of the attacks are removal attacks, geometrical attacks, cryptographic attacks, protocol attacks etc. In this paper I have implemented following attacks on each watermarked image: Unsharp Attack, Gaussian Noise, Salt and Pepper, Contrast and Rotation.

V. PERFORMANCE PARAMETER

The performance analysis [7] deals with various parameters to be calculated to check the robustness of the technique. The main goal of watermarking is to resist both geometric distortion and signal processing attacks [8]. Since, no watermarking algorithm resists all the attacks. But, still one can find better technique which will give more robust watermark by performing various calculations. Attacks aim is to impair detection of watermark or destroy the embedded watermark. Attacks can be removal attacks, geometrical attacks, cryptographic attacks and protocol attacks. Robustness against attacks is an important aspect for watermarking schemes. Here parameters used by us are Embedding time, Extraction time, Peak Signal to Noise Ratio (PSNR), Mean square error (MSE), Similarity Ratio (SR), Correlation (CORR) and Bit Error Ratio (BER). Various other parameters like SNR (Signal to Noise Ratio), BCR (Bit Correct

Ratio), NAE (Normalized Absolute Error), MAE (Mean Average Error), UIQI (Universal Image Quality Index), MAE (Mutual Information) and SC(Structural Content)etc can also be used to check the robustness of the technique.

VI. RESULTS

This research included three different watermarking techniques LSB, DCT and DWT. We have used here four images: Image1, Image2, Image3 and Image4 of 256x256 pixels value in jpeg format for watermarking. The watermark embedded is of 20x50 pixels. Following are the images and watermark used in this research.

(a) (b) (c) (d) (e)

Fig. 2: Original Images (a) Image1 (b)Image2 (c) Image3 (d) Image4 (e) Watermark

We have performed simulation on these images using Matlab 7.8. Following are the result tables of each technique applied to embed watermark on all four host images. Several attacks like unsharp, Gaussian noise, salt & pepper, contrast and rotation are also applied on watermarked image. Later, the performance of each technique are analyzed on the basis of parameters like Embedding time, Extraction Time, PSNR, MSE, Similarity Ratio, Correlation and BER.

TABLE 1
EMBEDDING AND EXTRACTION TIME OF LSB, DCT, DWT ON ALL FOUR IMAGE

Performance Parameter	IMAGE	LSB	DCT	DWT
Embedding Time	1	0.664286	0.705693	2.904395
Extraction Time		0.354539	0.362168	1.301726
Embedding Time	2	0.300164	0.608242	2.822137
Extraction Time		0.257249	0.296002	1.319668
Embedding Time	3	0.253730	0.582917	3.943554
Extraction Time		0.300013	0.343660	1.361090
Embedding Time	4	0.303104	0.575552	2.818134
Extraction Time		0.265143	0.342136	1.300668

TABLE 2
RESULT OF VARIOUS ATTACKS ON LSB WATERMARKED IMAGES

ATTACK	P.P.	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4
1. Unsharp	PSNR	14.6335	16.7238	15.9914	11.8134
	MSE	0.0344	0.0213	0.0264	0.0659
	CORR	0.9811	0.9487	0.9776	0.9751
	SR	0.3222	0.2307	0.3243	0.3267
	BCR	-9.2678e+003	-1.5608e+003	-1.6544e+003	-1.8395e+003
2. Gaussian Noise	PSNR	20.6639	30.4931	24.9819	10.8510
	MSE	0.0086	8.9267e-004	0.0032	0.0822
	CORR	0.9574	0.9068	0.9411	0.9526
	SR	0.3185	0.2931	0.2963	0.2418
	BCR	-8.9237e+003	-1.3863e+003	-1.3402e+003	-1.3947e+003
3. Salt and Pepper	PSNR	35.1471	52.6326	40.1242	21.4504
	MSE	3.0570e-004	5.4543e-006	9.7180e-005	0.0072
	CORR	0.9911	0.9836	0.9889	0.9842
	SR	0.8458	0.8365	0.8247	0.8038
	BCR	-8.6276e+003	-1.1246e+003	-1.3581e+003	-1.3113e+003
4. Contrast	PSNR	28.4836	44.3774	32.1812	15.1413
	MSE	0.0014	3.6497e-005	6.0517e-004	0.0306
	CORR	1.0000	0.999	0.9998	0.9999
	SR	0.9972	0.9948	0.9800	0.9938
	BCR	-1.0914e+004	-3.2875e+003	-2.9766e+003	-2.1911e+003
5. Rotate	PSNR	11.2680	11.3347	11.2831	9.3562
	MSE	0.0747	0.0735	0.0744	0.1160
	CORR	0.5600	0.4963	0.6090	0.4407
	SR	0.0031	0.0025	0.0080	9.4795e-004
	BCR	-2.0479e+003	34077e+003	2.6134e+003	3.7835e+003

TABLE 3
RESULT OF VARIOUS ATTACKS ON DCT WATERMARKED IMAGES

ATTACK	P.P.	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4
1. Unsharp	PSNR	14.9195	17.1477	15.9914	10.7890
	MSE	0.0322	0.0193	0.0252	0.0834
	CORR	0.9734	0.9341	0.9669	0.9682
	SR	0.3036	0.2190	0.2949	0.2944
	BCR	-9.2265e+003	-1.5076e+003	-1.5703e+003	-1.8244e+003
2. Gaussian Noise	PSNR	20.6934	29.9048	25.2422	10.8990
	MSE	0.0085	0.0010	0.0030	0.0813
	CORR	0.9569	0.9055	0.9404	0.9517
	SR	0.3264	0.2896	0.2891	0.2425
	BCR	-8.9214e+003	-1.3561e+003	-1.2856e+003	-1.3604e+003
3. Salt and Pepper	PSNR	29.3156	44.1161	31.0932	15.5372
	MSE	3.0012	3.8760e-005	7.7746e-004	0.0279
	CORR	0.9910	0.9823	0.9874	0.9840
	SR	0.8174	0.8027	0.7826	0.7395
	BCR	-8.5957e+003	-1.1036e+003	-1.3286e+003	-1.3137e+003
4. Contrast	PSNR	28.4836	44.3774	32.1812	15.1413
	MSE	0.0014	3.6497e-005	6.0517-004	0.0306
	CORR	0.9990	0.9984	0.9988	0.9992
	SR	0.9183	0.9295	0.9062	0.9096
	BCR	-1.5331e+004	-3.2589e+003	-2.9563e+003	-2.1834e+003
5. Rotation	PSNR	11.2544	11.3322	11.2445	8.8837
	MSE	0.0749	0.0736	0.0751	0.1293
	CORR	0.5597	0.4958	0.6084	0.4398
	SR	0.0031	0.0025	0.0081	9.3999e-004
	BCR	-2.0302e+003	3.4300e+003	2.6286e+003	3.7828e+003

TABLE 4
RESULT OF VARIOUS ATTACKS ON DWT WATERMARKED IMAGES

ATTACK	P.P.	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4
1. Unsharp	PSNR	14.6299	16.7265	15.7004	11.7937
	MSE	0.0344	0.0212	0.0269	0.0662
	CORR	0.9785	0.9433	0.9739	0.9734
	SR	0.3103	0.2229	0.3108	0.3120
	BCR	-9.2471e+003	-1.5090e+003	-1.6163e+003	-1.8244e+003
2.Gaussian Noise	PSNR	20.6023	30.3462	24.9098	10.8675
	MSE	0.0087	9.2339e-004	0.0032	0.0819
	CORR	0.9573	0.9066	0.9410	0.9524
	SR	0.3214	0.2931	0.2962	0.2417
	BCR	-8.9093e+003	-1.3589e+003	-1.3225e+003	-1.3855e+003
3. Salt and Pepper	PSNR	36.1139	49.0537	38.6863	22.9970
	MSE	2.4469e-004	1.2435e-005	1.3532e-004	0.0050
	CORR	0.9913	0.9839	0.9879	0.9845
	SR	0.8480	0.8210	0.8060	0.8160
	BCR	-8.6172e+003	-1.0722e+003	-1.3418e+003	-1.3085e+003
4. Contrast	PSNR	28.4836	44.3774	32.1812	15.1413
	MSE	0.0014	3.6497e-005	6.0517e-004	0.0306
	CORR	0.9999	0.9998	0.9998	0.9999
	SR	0.9903	0.9901	0.9739	0.9849
	BCR	-1.0902e+004	-3.2405e+003	-2.9676e+003	-2.1870e+003
5. Rotation	PSNR	11.2466	11.3358	11.2643	8.9904
	MSE	0.0750	0.0735	0.0747	0.1262
	CORR	0.5599	0.4827	0.6088	0.4402
	SR	0.0031	0.0023	0.0080	9.4327e-004
	BCR	-2.0362e+003	1.4705e+003	2.6237e+003	3.7876e+003

VII. CONCLUSION

This study analysed three digital watermarking techniques, concluding to there limitations and powers. Although only the very surface of the field was scratched, it was still enough to draw several conclusions about these techniques. By observing the result tables we conclude that LSB technique is not a very good technique due to its minimal level of robustness. Though its embedding and extraction time is less. But LSB embedded watermarks can easily be removed or get distorted by various attacks. Another observation is of transform domains DCT and DWT techniques. They are considered better techniques for watermarking then spatial domain. The wavelet domain as well proved to be highly resistant to noise, with minimal amounts of pixel degradation, this is shown in table 3. Here we have applied few attacks to distort the image. The wavelet domain may be one of the most promising domains for digital watermarking yet found. But on the contrary of the above techniques are completely robust to the all types of attacks.

REFERENCE

[1] C. S. Lu, Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property, Idea Group Publishing, 2005..

[2] Sin-Joo Lee and Sung-Hwan Jung, "A Survey of Watermarking Techniques Applied to Multimedia", ISIE 2001.

[3] Petitcolas Fabien A., Anderson Ross J., Kuhn Markus G., "Information Hiding – A Survey", Proceedings of IEEE, Special issue on protection of multimedia content, pp 1062-1078,July 1999.

[4] J.R. Hemandez, M. Amado, "DCT domain watermarking techniques for still images as detector performance analysis and a new structure," in IEEE Transactions on Image Processing, 2000, vol. 9, pp. 55-68.

[5] Tay P., Havlicek J.P., "Image Watermarking using Wavelets". IEEE, pp 258-261, 2002.

[6] H. Inoue, A. Miyazaki and T. Katsura, "An Image Watermarking Method Based on the Wavelet Transform", IEEE Conf. on Image Processing, Vol. 1, pp. 296-300, 1999.

[7] Taha El Areef, Hamdy S. Heniedy, S . Elmougy, and Osama M. Ouda, "Performance Evaluation of Image Watermarking Techniques", Third International Conference on Intelligent Computing and Information Systems, Faculty of Computer & Information Sciences, ICICIS 7002 ,March 15-18, 2007, Cairo.

[8] S. Voloshynovskiy, S. Pereira, T. Pun, University of GenevaJ.J. Eggers and J.K. Su, University of Erlangen-Nuremberg," Attacks on Digital Watermarks: Classification, E(1)stimation-based Attacks and Benchmarks ", 2001.

[9] Baisa L. Gunjal , R.R. Manthalkar "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences, 2010-11.

[10] Craver, S., N. Memon, B.L. Yeo and M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications". IEEE J. Selected Areas Commun, 1998.

[11] J. L., Dugelay, S. Roche, C. Rey, G. Doërr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. on Image Proc., vol. 15, no. 9, pp. 2831-2842, 2006

[12] S Jayaraman, S Esakkirajan, and T Veerakumar: Digital Image Processing. McGraw-Hill, 2009.

[13] Mustafa Osman Ali, and Rameshwar Rao., " Fundamentals of Digital Image Watermarking: an Overview". International Conference on Information and Communication Technology. pp. 64–67, Oct. 2011.

[14] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[15] Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), " A new LSB based Digital Watermarking Scheme with Random Mapping Function", in2008 IEEE DOI 10.1109/UMC.2008.33

[16] S. Z. Yu, "A color image-adptive watermark based on wavelet transform," in Computer Simulation, 2006, vol. 23, pp. 132-134.

[17] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal LSB substitution in image hiding by using dynamic programming strategy", Pattern Recognition, Vol. 36, No.7, 2003, pp.1583–1595.

[18] S. Shefali and S. M. Deshapande, "Mathematical Model for Improved Capacity Estimations for Data Hiding Techniques under Lossy Compression," in Proceedings of the 2nd IMT-GT Regional Conference in Mathematics, Statistics & Applications, Malaysia , 2006.

[19] AI-Gindy , H. AI-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-eCA 2008). , Amman, Jordan, 2008.

