

A Blind Digital Image Watermarking using Joint DCT-DWT and Twin Encoding Methodology

Poonam H. Mahajan, Pramod B. Bhalerao

Abstract: Digital Image Watermarking is that the method that embeds knowledge known as a watermark or digital signature or tag or label into a transmission object such watermark may be detected or extracted later to form associate assertion regarding the ob-ject. There square measure varied techniques with that the method of watermarking may be performed. we've summarized these techniques in brief. In this work, we tend to square measure presenting few recent watermarking algorithms. One ofthem may be a sturdy digital image watermarking algorithmic program supported Joint DWT-DCT Transformation. This methodology exploits strength of 2 common frequency domains method; DCT and DWT, to get more physical property and hardiness. the thought of inserting watermark within the combined rework is predicated on the very fact that joint rework may eliminate the downside of every alternative. then, associate elective watermarking methodology may be obtained. the opposite is powerful Blind Digital Image Watermarking mistreatment DWT and twin coding Technique. This algorithmic program exploits the sequence generated by Arnold and transformations. separate ripple transformation of third level decomposition is employed to convert the image into its frequency

Keywods: Digital Image Watermarking, Blind Digital Image Watermarking, twin coding, Arnold rework, Chaos rework, DWT, DCT

I. INTRODUCTION

The growth of high speed laptop networks which of net, particularly, has explored means that of recent business, scientifc, recreation, and social opportunities within the variety of electronic business and advertising, time period data delivery, product ordering, dealings process, digital repositories and libraries, net newspapers and magazines, network video and audio, personal com munication, lots more. The new opportunities may be broadly speaking classified below the label electronic commerce. the price e_ectiveness of commercialism code, prime quality art add the shape of digital pictures and video sequences by transmission over World Wide net (www) is greatly increased sequent to the advance of technology, causation arduous copies by post might presently be a factor of past. Though the business exploitation of the computer network is steady being additional appreciated, apprehension on the safety facet of the trade has solely funnelled the exploitation to be restricted to the transmission of demo and free versions of package and art. Ironically, the cause for the expansion is additionally of the apprehension use of digital formatted information.

Manuscript published on 30 November 2014.

*Correspondence Author(s)

Ms. Poonam H. Mahajan, PG Scholar, Department of Computer Science and Engineering, D.I.E.M.S., Aurangabad, Maharashtra, India.

Mr. Pramod B. Bhalerao, Asst. Prof., Department of Computer Science and Engineering, D.I.E.M.S., Aurangabad, Maharashtra, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

As we've witnessed within the past few years, the matter of protective transmission data becomes a lot of and a lot of necessary and lots of copyright homeowners ar involved concerning protective any embezzled duplication of their information or work. Some serious work has to be tired order to keep up the provision of transmission data however, within the in the meantime, the trade should return up with ways in which to guard property of creators, distributors or straightforward homeowners of such information. This can be a motivating challenge and this can be most likely why most attention has been drawn toward the event of digital data protection schemes. The watermark stems from the traditional art of a _gure or style incorporated into paper throughout its manufacture and showing lightweighter than the remainder of the sheet once viewed in transmitted light for an equivalent purpose. Ancient works formerly prompted for a technical answer for copyright protection of digital pictures as shortly as they were displayed in digital libraries on the market through the web.





Figure 1.1: Perceptible watermark embedded in a figure

II. LITERATURE SURVEY

Most of the analysis work is devoted to image watermarking as compared to audio and video. There is also three reasons for it. Firstly, due to prepared convenience of the take a look at pictures, second as a result of it carries enough redundant data to supply a chance to imbed water marks simply, and lastly, it's going to be assumed any prospering image watermarking algorithmic rule could {also be|is also} upgraded for the video also. Pictures area unit represented/stored in abstraction domain likewise as in remodel domain. The remodel domain image is pictured in terms of its frequencies; whereas, in abstraction domain it's pictured by pixels. In straightforward terms, remodel domain means that the image is divided into multiple frequency bands. To transfer a picture to its frequency illustration, we are able to use many reversible transforms like separate circular function remodel (DCT), separate rippling remodel (DWT), or separate Fourier remodel (DFT). every of those transforms has its own characteristics and represents the image in numerous ways in which.

Published By: Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) © Copyright: All rights reserved. Watermarks are often embedded among pictures by modifying these values, i.e. the remodel domain coe_cients. just in case of abstraction domain [5], straightforward watermarks may well be embedded within the pictures by modifying the element values or the smallest amount Signi_cant Bit (LSB) values. However, a lot of strong watermarks may well be embedded within the remodel domain of pictures by modifying the remodel domain coe_cients. In 1997 Cox [3] given a paper Secure unfold Spectrum Water- marking for transmission, one in all the foremost cited paper (cited 2985 times until Apr 2008 as per Google Scholar search), and subsequently most of the analysis work is predicated on this work. even if abstraction domain based mostly techniques cannot sustain most of the common attacks like compression, high pass or low pass fltering etc., researchers gift abstraction domain based mostly schemes. Since LSB technique depends on modifications of the smallest amount significant bits, the watermark is definitely destroyed. Fur- ther, their technique is restricted to photographs, therein it seeks to insert the watermark into image regions that lie on the sting of contours. DFT may be a watermarking theme during which watermark is embedded by modifying the section data among the DFT. it's been shown that section based mostly watermarking is strong against image distinction operation. This theme is strong against geometrical attacks. The theme is, however, not strong against cropping and shows weak lustiness against JPEG compression. many DCT based mostly schemes area unit victimization the DCT to perform image watermarking [5], a picture will simply be break up in pseudo frequency bands so the watermark will handily be embedded within the most vital middle band frequencies. Embedding within the perceptually signi_cant portion of the image has its own blessings as a result of most compression schemes take away the perceptu- ally insigni_cant portion of the image. If watermarking techniques will exploit the characteristics of the Human sensory system (HVS), it's doable to cover watermarks with a lot of energy in a picture, that makes watermarks a lot of strong. From now of read, the DWT may be a terribly enticing remodel, as a result of it are often used as a computationally e_cient version of the frequency models for the HVS. Now- a-days, researchers area unit that specialize in mixture of abstraction and reworked domains (i.e. mixtures of DFT, DWT and DCT) ideas and additionally applying a lot of and a lot of mathematical and applied math model, and alternative knowledge base approaches in watermarking: for instance use of chaotic theory, pattern image secret writing etc. during this section we tend to area unit presenting the temporary of few recent watermarking algorithms.

III. PROPOSED METHOD

Following ar the 2 watermarking techniques which can be enforced in our project:

- 1. Watermarking by Joint DWT-DCT methodology
- 2. Blind Digital Image Watermarking by DWT and twin encoding methodology The terms introduced within the algorithms are:

Both these ways can facilitate US to require 2 di_erent approaches towards watermarking.

3.1 Joint DWT-DCT Formula

3.1.1 Watermark Embedding formula

- 1. Perform DWT on the host image to decompose it into four non-overlapping multi resolution coe_cient sets: LL1, HL1, LH1 and HH1.
- 2. Perform DWT once more on 2 HL1 and LH1 sub-bands to urge eight smaller sub-bands and select four coe_cient sets: HL12, LH12, HL22 and LH22
- 3. Perform DWT once more on four sub-bands:HL12, LH12, HL22 and LH22 to urge sixteen smaller sub bands and select four coe_cient sets: HL13, LH13, HL23 and LH23
- 4. Divide four coe_cient sets: HL13, LH13,HL23 and LH23 into four x four blocks.
- 5. Perform DCT to every block within the chosen coe_cient sets (HL13, LH13, HL23 and LH23).
- 6. Re-formulate the grey-scale watermark image into a vector of zeros and ones.
- 7. Generate 2 unrelated pseudorandom sequences by a key. One sequence is employed to introduce the watermark bit zero (PN0) and therefore the different sequence is employed to introduce the watermark bit one (PN1) . range of components in every of the 2 pseudorandom sequences should be adequate the amount of mid-band components of the DCT-transformed, DWT coe_cient sets.
- 8. introduce the 2 pseudorandom sequences, PN0 PN1, with a gain think about the DCT remodeled 4x4 blocks of the chosen DWT coe_cient sets of the host image. rather than embedding altogether coeffcients of the DCT block, it applied solely to the mid-band DCT coe_cients. If we have a tendency to gift X because the matrix of the mid-band coe_cients of the DCT remodeled block, then embedding is finished as equation three.1.
- 9. Perform inverse DCT (IDCT) on every block once its mid-band coe_cients are modi_ed to introduce the watermark bits as delineate within the previous step.
- 10. Perform the inverse DWT (IDWT) on the DWT remodeled image, includ- ing the modi_ed coe_cient sets, to supply the watermarked host image.

$$X' = \begin{cases} X + \alpha * PN0; & \text{if watermark bit} = 0\\ X + \alpha * PN1; & \text{if watermark bit} = 1 \end{cases}$$

3.1.2 Watermark Extraction Formula

- 1. Perform DWT on the watermarked image to decompose it into four non overlapping multi resolution coe_cient sets: LL1, HL1, LH1 and HH1.
- 2. Perform DWT once more on 2 sub-bands HL1 and LH1 to urge eight smaller sub-bands and select four coe_cient sets: HL12, LH12, HL22 and LH22.
- 3. Perform DWT once more on four sub-bands: HL12, LH12, HL22 and LH22 to urge sixteen smaller subbands and select four coe_cient sets: HL13, LH13, HL23 and LH23.
- 4. Divide four coe_cient sets: HL13, LH13, HL23 and LH23 into four x four blocks.
- 5. Perform DCT on every block within the chosen coe_cient sets (HL13, LH13, HL23 and LH23).
- 6. Regenerate the 2 pseudorandom sequences PN0 and PN1 victimization constant key that employed in the watermark embedding procedure.



- 7. for every block within the coe_cient sets: HL13, LH13, HL23 and LH23 calculate the correlation between the mid-band coe_cients and therefore the 2 generated pseudorandom sequences PN0 and PN1 If the correlation with the PN0 was on top of the correlation with PN1, then the extracted watermark bit is taken into account zero, otherwise the extracted watermark is taken into account as one.
- 8. The watermark is reconstructed victimization the extracted watermark bits, and calculate the similarity between the first and extracted watermarks.

3.2 Blind Digital Image Watermarking by DWT and Twin Encoding Methodology

3.2.1 Watermark Embedding formula

- 1. Take the first image and size it to 1024X1024 image. create three-level wave decomposition of the first image and therefore the waveband HL3 because the embedded domain, the wave coe_cient of HL3 extracted as CH3.
- 2. Take the watermark and size it to 32X32 bit binary image.
- 3. Then apply the Arnold transformation to the watermark.
- 4. once the Arnold transformation, apply the Chaoss transformation to the output of Arnold remodeled watermark.
- 5. Perform the embedding of the watermark within the original image as given in equation below: Where, Xw is that the watermarked image before inverse DWT. Wk is that the watermark bit at kth position and k=0,1,2,...1023. ninety two is that the variance of the first image and is that the depth of the watermark to be embedded.
- 6. Take the inverse DWT to urge the watermarked image and size it to 256 X256 image.

3.2.2 Watermark Extraction formula

- 1. Take the watermarked image and size it to 1024 X 1024 image.
- 2. Then take the DWT upto three level decomposition and mark the waveband HL3 as CH3 to extract the watermark.
- 3. Extract the watermark from CH3 as given in equation three.5 below: wherever, Xw is that the component wherever watermark was embedded. wk is that the extracted watermark bit.
- 4. Take the inverse Chaoss transformation of the extracted watermark.
- 5. Take the inverse Arnold transformation of the reverse Chaoss image to urge the required extracted

watermark.
$$W_k = \begin{cases} W_k = 1; & if \ X_w \ (i + 4, j + 4) = \frac{+\sigma^2}{\alpha} \\ W_k = 0; & if \ X_w \ (i + 4, j + 4) = \frac{-\sigma^2}{\alpha} \end{cases}$$

IV. EXPERIMENTAL RESULTS

Figure 4.1(b) (d) display three 512X512 examined images, Lena, Cameraman and Mandrill, respectively. A larger PSNR indicates that the watermarked image more closely resembles the original image O, meaning that the watermarking method makes the water- mark more imperceptible. Generally, if PSNR value is greater than 35dB-45db [2] the watermarked image is within acceptable degradation levels, i.e. the watermarked is almost invisible to human visual system. A lower MAE [2] reveals that the extracted watermark EW resembles the original watermark W more closely.



Figure 4.1: (a) The Initial Watermark Image; (b) The Initial River Image; (c) The Initial Cinematographer Image; (d) The Initial Mandrillus Sphinx Image

The strength of a watermarking technique is assessed by comparison W with electronic warfare, wherever electronic warfare is extracted from the watermarked image that is more degraded by attacks. If a technique includes a lower MAE (W, EW), it's a lot of sturdy. The watermarking performance of each the strategies is compared. To research the strength of those strategies, many attacks area unit simulated to degrade the watermarked pictures. Besides the quantitative leads to terms of the PSNR and also the MAE, the experiment conjointly provides visual-comparison results.

4.1 Attack Free Case

Table 4.1 provides the quantitative leads to terms of the PSNR and also the MAE. to boot,4.2 displays the visual comparison results for the extracted watermarks. during this case Table four.1 and 4.2 show that the each the algorithms definitely makes the watermark undetectable and also the watermarks extracted area unit virtually like the original watermark victimization algorithmic program two. Therefore, the watermarks extraction results area unit better for algorithmic program two than algorithmic program one. Moreover, The quality of watermarks extracted with algorithmic program two is superior thereto extracted with algorithmic program one. In the following sections, results obtained when degrading the photographs with different attacks are conferred. These attacks are performed victimization inbuilt functions.



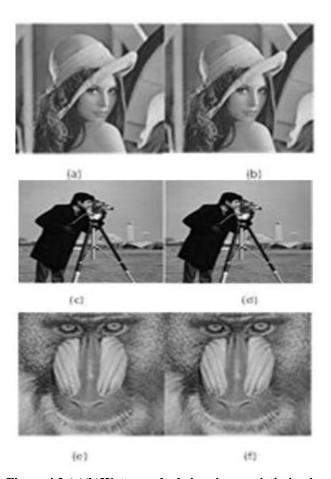


Figure 4.2:(a)(b)Watermarked river image victimization Algo1 & Algo2;(c)(d)Watermarked cinematographer image victimization Algo1 & Algo2;(e)(f)Watermarked Mandrillus sphinimage victimization Algo1 & Algo2

Image		al-to-Noise PSNR)	Mean Absolute Error(MAE)		
	Algorithm 1	Algorithm 2	Algorithml	Algorithm 2	
Lena	37.2013	42.7157	0.00613655	0.00195364	
Cameraman	37.5284	42.3476	0.00611125	0.00195164	
Mandrill 36.4686		43.5883	0.0061361	0.00195419	

Image	Algorithm1	Algorithm2	
Lena	Ĥï	Hi	
Cameraman	·Hi	Hi	
Mandrill	,Hj	Hi	

Table 4.1: Experimental Results for attack-free case and Table four.2: In attack-free case Extracted Watermarks

4.2 strength to Noising

The mathematician noise is intercalary at a variance of zero.02 and Salt pepper noise is intercalary at density of zero.02.

Attack	Image	Algorithm1	Algorithm2	Mean Absolute Error(MAE)	
	-			Algorithm1	Algorithm2
	Lena	Ĥï	.Hi	0.0742188	0.0761719
(At 20% depth)	Cameraman	.Hi	, Ĥi .	0.0742188	0.0810547
	Mandrill	Hj	Hi.	0.0859375	0.0742188
, ,	i i	3.77	T		
	Mandrill	His	Hi	0.134766	0.0722656

Attack	Image	Algorithm1	Algorithm2	Mean Absolute Error(MAE)	
				Algorithm1	Algorithm2
Gaussian Noise	Lena	kii -	Hị .	0.152344	0.0771484
	Cameraman	Hi	· Hì ·	0.140625	0.0761719
	Mandrill	ì fi	Hi	0.164063	0.078125

Table 4.3: Extracted Watermarks within the case of Salt and Pepper noise; and Table 4.4: Extracted Watermarks within the case of adding gaussion noise

4.3 lustiness to JPEG Compression

The watermark is embedded within the middle - frequency coe cients in each DWT and DCT in rule1 and therefore the watermark is encrypted usin 2 encoding techniques in Algorithm a pair of. Thus each the algorithms ar strong against JPEG compression. As seen from the results, the watermarks extracted victimization rule a pair of ar a lot of bet-ter than that obtained from rule one. Also, in case of rule one, the extracted watermarks ar higher just in case of Lena River image and therefore the quality is worst for baboon image.

4.4 lustiness to Blurring

In order to simulate blurring attack, mathematician lowpass lter is employed as a standard blurring attack. it's enforced victimization Matlab operate. The watermarked image Wisconsin is blurred. 3 watermark W on 3 pictures ar then extracted from the blurred and watermarked image O by victimization each the strategies.





Attack	Image	Algorithm1	Algorithm2	Mean Absolute Error(MAE)	
				Algorithm1	Algorithm2
Blurring (Gaussian Low Pass Filtering)	Lena	ĤΪ	Hi	0.0742188	0.0722656
	Cameraman	.Hi	Hi	0.0732422	0.0722656
	Mandrill	Hj	Hi	0.0908203	0.0722656

Table 4.5: Extracted Watermarks within the case of JPEG Compression; Table 4.6: Extracted Watermarks within the case of Blurring the image

4.5 lustiness to Sharpening

For playacting sharpening unsharp distinction improvement lter was used and was applied to the watermarked pictures at a depth of zero.2, which is that the default price [6]

Attack	Image	Algorithm1	Algorithm2	Mean Absolute Error(MAE)	
				Algorithm1	Algorithm2
	Lena	ĤΪ	Hi	0.0742188	0.0722656
Sharpening	Cameraman	Hi	Hi	0.0722656	0.0722656
	Mandrill	Hį	Hi	0.0751953	0.0722656

Table 4.7: Extracted Watermarks within the case of Image Sharpening

V.CONCLUSION AND FUTURE SCOPE

In this paper, two rules for Digital Image watermarking were performed the rst algorithm being 'Digital Image Watermarking supported Joint DWT DCT 'and therefore the different 'Robust Digital Image Watermarking supported DWT and twin encoding Techniques'. 3 customary pictures were embedded victimization each the al-gorithms and their watermarks were extracted before playacting attacks and once playacting attacks. The results show that the performance of the second rule was higher than that of rst in terms of recoverability and lustiness. The second rule provided higher lustiness against noising and JPEG compression than the rst rule. Digital watermarking may be a speedily evolving space of analysis and development. One key analysis downside that we have a tendency to still face nowadays is that the development of really strong, clear and secure watermarking technique for di erent digital media together with pictures, video and audio. The lustiness of the algorithms is that the main question to be answered to the standard of embedding info (message) furthermore as sheer volume of the transferred message. additional enhancements is created to the rule by victimization higher encoding technique like FAN remodel ,etc. The project will more be extended to colored pictures. additional researches and experiments got to be done to succeed in a stronger technique taking less process power thus on use the technique within the home basis. Since its application is nearer to security problems, the study might be done at tier of cryptography.

REFERENCES

- Gursharanjeet Singh Kalra, Dr. Rajneesh Talwar, Robust Blind Digi-tal Image Watermarking Using DWT and Dual Encryption Technique, Third International Conference on Computational Intelligence, 2011,
- Saeed K. Amirgholipour , Ahmad R. Naghsh-Nilchi, Robust Digital Im-age Watermarking Based on Joint DWT-DCT, Computer Engineering Dept, Isfahan University, IRAN, 2009,
- I. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, Vol. 6, Pages: 1673-1687, December, 1997,
- Chunlin Song, Sud Sudirman, Madjid Merabti and David Llewellyn-Jones, IEEE Communications ociety, School of Computing and Mathe-matical Science, 2010.
- Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le, "Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools", Second IEEE International Conferences on Advances in Multimedia, 2010, pp.67-73
- Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique, 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks.

AUTHOR PROFILE



Ms. Poonam H. Mahajan, received the BE degree in Computer Engineering, From Govt. college of engg., jalgaon, North Maharashtra University, Maharastra, India And ME Applied CSE from Deogiri Institute Of Engineering & Management Studies, Aurangabad, Maharastra, India in 2012 and 2014.

Mr. Pramod B. Bhalerao, received the ME Degree in Computer Science And Engineering, Aurangabad. Presently he is working As Assistant Professor in Computer Science and Engineering at DIEMS, Aurangabad, Dr BAMU University, Maharastra, India.

