ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

Digital Image Watermarking Using DWT and SLR Technique Against Geometric Attacks

Sarvesh Kumar Yadav , Mrs. Shital Gupta, Prof. Vineet richariya

Abstract- Now days digital watermarking is very popular field for the researchers because it provide the better solutions for authentication and copyright protection problems of digital object. Digital watermarking is a highly evolving field, which involves the embedding of a certain kind of information under a digital object (image, video, audio) for the purpose of copyright protection. Both the image and the watermark are most frequently translated into a transform domain where the embedding takes place. The selection of both the transform domain and the particular algorithm that is used for the embedding of the watermark, depend heavily on the application. One of the most widely used transform domains for watermarking of still digital images is the Discrete Wavelet Transform (DWT) domain. In this paper we present a new algorithm which is more robust against different geometric attacks. Such as rotation and translation. Our algorithm has high embedding capacity, high imperceptibility and low calculating complexity.

Key words - digital watermarking, Attacks, DCT, DWT,

I. INTRODUCTION

The large-scale communication of multimedia data has created a pressing need to protect digital information against illegal duplication and manipulation. Digital watermarking addresses the growing concerns of theft and tampering through the use of advanced signal processing strategies to embed copyright and authentication information within media content**.** A watermark is a digital data embedded in multimedia objects such that the watermark can be detected or extracted at later times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc. Potential applications of digital watermarking include transaction tracking, copy control, authentication, legacy system enhancement and database linking etc. [2] [6]

Digital watermarking also known as watermark insertion or watermark embedding, represents the method of inserting information into multimedia data also called original media or cover media e.g. text, audio, image, video. The embedded information or watermark can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray

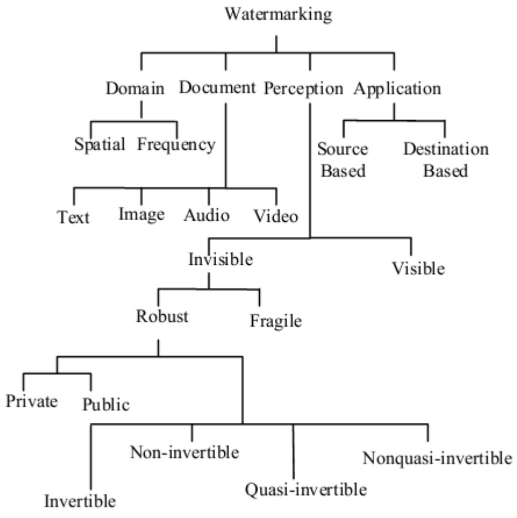


Fig.1: Types of Watermarking Techniques

Level images, text or other digital data formats. In the literature large number of text , image , audio and video watermarking algorithms can be found. These algorithms modify the original media to generate the watermarked media. There may be no or little perceptible differences between the original media and the watermarked media. Fig.1 [9] gives an overview of different types of watermarking methodologies depending on their working domains, cover media, perceptibility and application areas. [6]

II. DWT DOMAIN WATERMARKING TECHNIQUES

In the last few years wavelet transform has been widely studied in signal processing in general and image compression in particular. In some applications wavelet based watermarking schemes outperforms DCT [3][4] based approaches.

Characteristics of DWT

1) The wavelet transform decomposes the image into four bands.
2) Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution.
3) Magnitude of DWT [8] coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH,LH, HL) .
4) The larger the magnitude of the wavelet coefficient the more significant it is.
5) Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved.
6) High resolution sub bands helps to easily locate edge and textures patterns in an image.

III. PROPOSED METHOD

The watermarking models we have proposed provide greater security against sophisticated geometrical attacks in different domains while providing sufficient watermark-carrying capacity at the same time. The false-positives are extremely low in the models, thereby making accidental detection of watermark in a random object almost negligible.

3.1 SLR Technique

SLR has been facilitated in the watermarking algorithms and is a solution to the secondary watermarking attacks. SLR is a digital image technique for the improvement of luminance component of image. SLR method has viewfinders that see the same luminance as the image, but in practice this isn't the only distinction. While the line between each continues to pixel, these two differences usually still apply.(1) Viewfinder Mechanism(2) Fixed vs. Interchangeable pixel. There's also a range of more minor differences, the above three are often what most impact one's technique. In the proposed technique we used YC_bC_r color model for distribution of color model. The given image in general in RGB format. Change these format into YC_bC_r. Y component is luminance component and C_b , C_r are chrominance components.

After conversion of color component we apply SLR technique for better compactness of color pixel position. In frequency component Hi (xi, yi) = Li (xi, yi) the SLR calculate the luminance of y component of the pixels in all frequency coefficient. If the luminance of y component of pixels of one frequency coefficient is more than other frequency coefficient then it interchanges the pixels position of the frequency coefficient. The SLR technique preserves the quality of image and increase the invisibility of watermark image. We apply DWT transform technique for watermarking these technique decompose image into horizontal ,vertical and diagonal formation of pixel ,so in this process pixel interchange and viewfinder is important aspect of digital image. That aspect is fulfill by the SLR technique. The watermark embedding in the DWT by using 2nd-level DWT to an input image f(x,y)(512*512*16 bits) generate 12 sub bands of high frequency (LHi,HLi,i=1-2) and one low frequency sub band(LL2).the SLR interchange the 16 bit pixel position for watermarking. And interchange the pixel correlation and improve the PSNR value of watermarked image.

3.2 Watermark Embedding Algorithm

The watermark embedding steps of this technique are as follows:

1. Read color host image f(x,y) and Convert RGB to YC_bC_r components.
2. Apply SLR techniques on Y component for better compactness of color pixel position getting the high luminance of Y component. The SLR interchanges the 16 bit pixel position for watermarking.
3. Apply 2nd level DWT on Y component for obtain the frequency subcomponents {HH1,HL1,LH1, {HH2, HL2 , LH2 }}.

4. Embed the watermark components into the frequency subcomponents, starting from HH1 for each row select the frequency coefficients in descending order with respect to their absolute values. Modify each frequency coefficient f\` to f +α Cij where α is Watermark gain factor, and Cij is watermark frequency coefficient
5. Save the location of the modified frequency components into a key array K of size 256x256. The key array K has value one if the coefficient is modified and zero if not
6. Apply IDWT
7. Convert YC_bC_r to RGB and Get watermarked image.

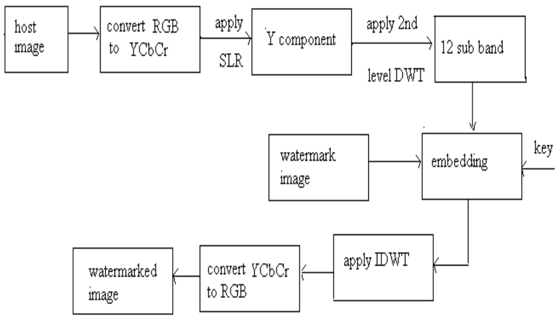


Fig 2: Flowchart of Watermark Embedding

3.3 Watermark Extraction Algorithm

The watermark extraction steps of this technique are as follows:

1. Read the watermarked image.
2. Convert image into YC_bC_r components.
3. Apply SLR techniques on Y component for better compactness of color pixel position getting the high luminance of Y component. The SLR interchanges the 16 bit pixel position for watermarking.
4. Apply 2^{nd} level DWT for obtain the frequency subcomponents {HH1,HL1,LH1, {HH2, HL2 , LH2 }}.
5. Extract the watermark bits from the frequency subcomponents, starting from HH1 and using key array K as W ij= (f `- f)/α . If Wij ‹ T, then Wij= 1 else Wij 0,Where f= frequency coefficient of YC_bC_r at the corresponding level and subcomponent, f``= frequency coefficient of $Y`C`_bC`_r$ at the corresponding level and sub component, T is between 0 and 1 and α is gain factor.
6. Calculate the quality of recovered image by using PSNR.
7. Calculate the similarity between original and extracted watermark using NC.

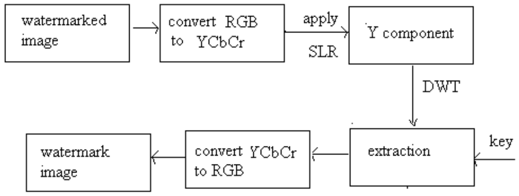


Fig 3: Flowchart of Watermark Extraction

IV. Performance Evaluation And Result

To evaluate the performance of the proposed method it has been extensively applied to various standard images and attempting different kind of attacks. We conducted experiment and evaluating the results with comparison to an existing watermarking scheme. This watermarking scheme is efficient due to its robustness against geometric attacks. The cover image used in this experiment is 'Lena' figure 4(a) of size 512 * 512 and the watermark image is 'house' figure 4(b) of size 256 * 256. In our Experiment we have set gain factor=0.5. This algorithm has been implemented using MATLAB 7.8.

Imperceptibility: Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used. PSNR in decibels (dB) is given below in eq.1

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (1)$$

Robustness: Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, internationally or unintentionally, by different types of digital signal processing attacks. In this chapter, we will report on robustness results which we obtained for two major attacks image rotation and image translation. We measured the similarity between the original watermark and the watermark extracted from the attacked image using the Normalized correlation factor given below in eq .2

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} W^2(i,j)} \qquad (2)$$

Where N×N is the size of watermark, W (i,j) and W'(i,j) represents the watermark and recovered watermark images respectively.

Fig 4(a) `Lena` host image

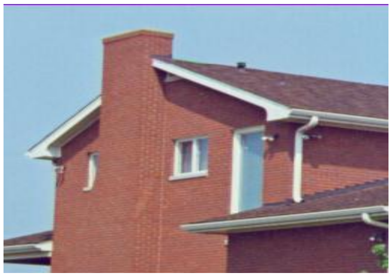
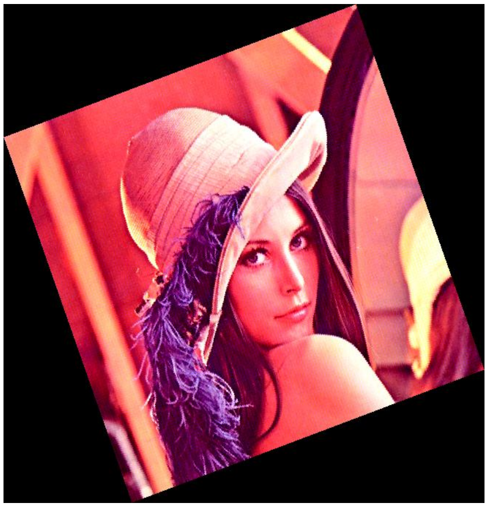


Fig 4(b) `House` watermark image



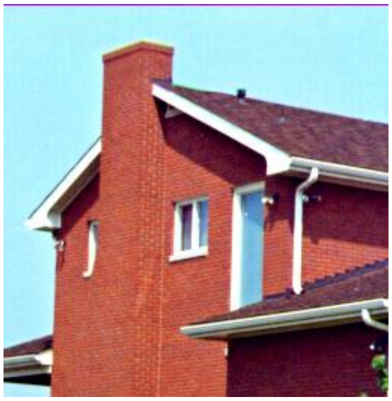
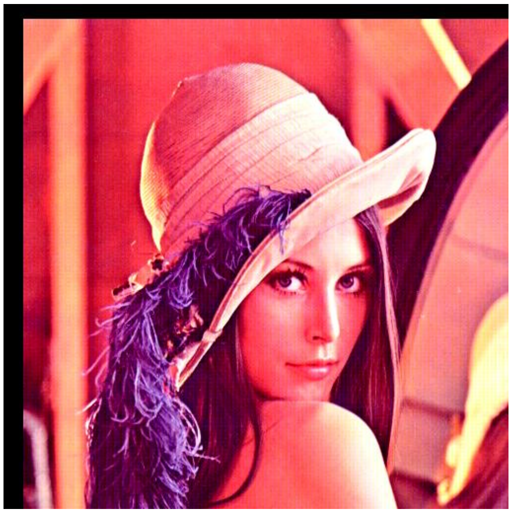


Fig 5 the watermarked retrieved from the watermarked image after rotation. 20 degree anticlockwise with NC=0.4827and PSNR= 24.647



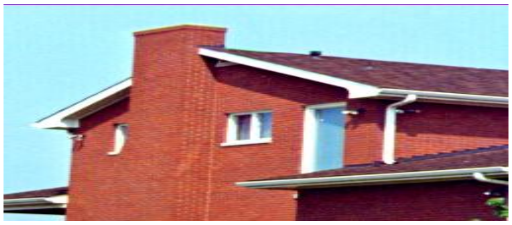


Fig 6 the watermarked retrieved from the watermarked image after translation (15, 20) with NC=0.7354and PSNR= 23.236

Attack	PSNR	NC
No attack	22.996	.793
Rotation(20)	24.647	.482
Rotation(30)	24.881	.424
Translation(5,10)	23.105	.768
Translation(15,20)	23.236	.735

Table1.Results of the experiments using PSNR and NC

V. CONCLUSION

There are several types of algorithms for watermarking. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the watermarking algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. In this paper we presented a new method of embedding watermark into color image.

The RGB image is converted to YC_bC_r and watermarked by using discrete wavelet transform. The luminance component Y of image is considered for embedding watermark and we apply SLR technique for preserve the quality of image and increase the invisibility of the watermark image. The performance of the proposed method can be evaluated in terms of normalized correlation coefficient and PSNR. Experimental results have demonstrated that technique presented in this paper is very effective supporting more security and exact correlation between original watermark and extracted watermark. However the proposed technique not examined other geometrical attacks such as scaling, and cropping. Thus further work is directed towards the testing of others geometric attacks on digital watermarked image in wavelet domain and this methodology can be extended for digital video watermarking.

REFERENCES

[1] Dr. Sandeep Kumar Sood , A.P Meenakshi, Sharma Manjit Thapa “Digital Image Watermarking Technique Based on Different Attacks” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011

[2] Dhruv Arya “A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques” International Journal of Scientific & Engineering Research, Volume 1, Issue 2, November-2010.

[3] Tibhuwan Kumar Tewari , Vikas Saxena “An Improved and Robust DCT based Digital ImageWatermarking Scheme” International Journal of Computer Applications (0975 8887) Volume 3 No.1, June 2010

[4] Hang SU, Chuqing LV, Yanbing JI, Yulin WANG “A Watermarking E-note Technique against Geometric Attacks” in 2nd International Conference on Mechanical and Electronics Engineering (ICMEE)IEEE 2010.

[5] Jiang Xuehua “Digital Watermarking and Its Application in Image Copyright Protection” International Conference on Intelligent Computation Technology and Automation 1EEE 2010.

[6] L. Robert, T.Shanmugapriya, “A Study on DigitalWatermarking Techniques” International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[7] Harsh K Verma , Abhishek Narain Singh , Raman Kumar “Robustness of the Digital Image Watermarking Techniques against Brightness and Rotation Attack” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

[8] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University “Watermarking with Wavelets: Simplicity Leads to Robustness”, Southeastcon, IEEE, pages 587 – 592, 3-6 April 2008.

[9] Verma, B., Jain, S., Agarwal, D.P. and Phadikar, A. “A New color image watermarking scheme”, Infocomp, Journal of computer science, vol. 5,N.2, Pp. 37-42 2006.

[10] Sourav Bhattacharya, T.. Chattopadhyay and Arpan Pal “A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC” 1-4244-0216-6/06 IEEE 2006.