A Novel Invisible Image Watermarking Insertion-Extraction Scheme using DWT Watermarking Technique

Basavaraj. S. Anami*, Rajesh. Yakkundimath
K.L.E.lnstitute of Technology,
Hubli ,India
anami.basu@hotmail.com
rajesh.yakkundimath@rediff.com

Prashant Bhandari
Alcatel-Lucent, Optics NM R&D, Manyata Embassy
Business Park, Nagawara,
Bangalore.India
prashantbhandarel@gmail.com

Abstract- In this paper, a robust algorithm of digital image watermarking based on discrete wavelet transform is introduced It adds binary image watermark into RGB or gray image using DWT Watermarking technique. In the proposed method, instead of directly applying DWT on a color image or a grayscale as in existing technique, RGB image is converted to a indexed image format of which 2-D DWT of a indexed image is been taken which computes four planes LL,LH,HL,HH. After adding a watermark to any of these planes take the IDWT convert the indexed format back to RGB format. Similar methodology is applied for Watermark extraction procedure. Experimental results show that the proposed algorithm improves quality of watermarked images in terms of MSE, PSNR, RMSE values when compared to conventional DWT watermarking technique.

Keywords- Index image, MSE, PSNR, RMSE, RGB image, Watermarking.

I. INTRODUCTION

Although digital data has many advantages over analog data, service providers are reluctant to offer services in digital form because they fear unrestricted duplication and dissemination of copyrighted material. Because of possible copyright issues, the intellectual property of digitally recorded material must be protected. To provide copy protection and copyright protection for digital audio and video data, two complementary techniques are being developed namely encryption and watermarking.

Until recently, encryption has been the primary tool available to help protect copy right of owners' contents such as movies, songs, photographs and the like [1]. Encryption protects the content during transmission from sender (host) to receiver. However, after receipt and subsequent decryption, the information remains no longer protected and is prone to danger of piracy. Watermarking techniques compliment encryption by embedding secret imperceptible information, a watermark, directly into the original data in such a way that it always remains present.. Such a watermark, for instance, is used for copyright protection, fingerprinting, indexing, broadcast monitoring, data authentication, and data hiding [2].

According to the human perception, the digital watermarks are divided into two different types namely Visible and Invisible [3]. In Visible watermarking technique, the watermark is visible to the casual viewers. Visible watermarks change the image altogether such that the watermarked image is totally different from actual image The image does not change in invisible watermarking.

Up to date, the proposed watermarking methods may be classified into three categories, i.e., methods in transform domain, spatial domain and mixed domain respectively. The earlier proposed scheme is based on LSB substitution. It gains great embedding capacity and computing efficiency, but the proposed method is fragile to general image processing [4]. Since the watermarking method in the transform domain is deemed as more suitable for invisible watermarking, in the last decades, more and more watermarking scheme are proposed in the transform domain such as DCT, DFT, DWT and so on [5-6].

Since the new generation of compression standard JPEG2000 is based on DWT, the research of image watermarking scheme in DWT domain is much more important than other transform domain. Many researchers have investigated the watermarking scheme in discrete wavelet transform (DWT) domain. The proposed methods have shown that it is more robust and transparency than others domain [7-8]

In this paper, we present a simple and effective method to embed a watermark into the discrete wavelet transform domain. Comparing the results based on proposed method and the original method it is found that the "mean square error" value for embedding the same amount of information is lower in the proposed method and PSNR is higher It is obvious that the watermarked image based on proposed method looks better exactly similar to original image and improves the quality with respect to conventional DWT method.

The paper is organized into five sections: Section II presents Existing DWT method. Section III presents proposed DWT technique. Section IV presents experimental results and discussion and Section V gives conclusions and future scope.

II. EXISTING DISCRETE WAVELET DOMAIN BASED WATERMARK

In the discrete wavelet domain, blind watermarking algorithm doesn't rely on the original image for recovering the watermark embedded in the DWT domain. The watermark is binary {+ 1, -I} in nature with pseudo random (PN) sequence added to the largest coefficients of the 3 detailed sub-bands [LH, HL, HH] of the DWT. The LL band is not modified. Detection of the watermark is done through correlation between original and the watermarked image. The watermarking process is shown in Fig. 1.
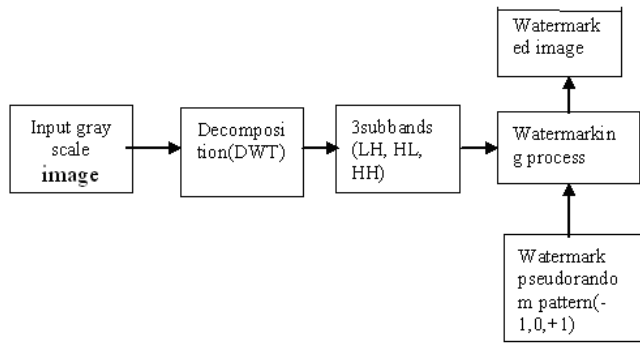
Figure.1.Proposed watermarking DWT embedding scheme

The image to be watermarked is first decomposed into 4 levels through DWT.The watermark pseudo random sequence is inserted by modifying the 3 detailed bands at level 0,i.e. $I_0^{LH}, I_0^{HL}, I_0^{HH}$ This offers the best compromise between robustness and invisibility. But makes the watermark more sensitive to attacks.[9].

Consider an image to be watermarked of size(2mx2n).Insert the PN sequence into the image to be watermarked. The levels are represented from I=0,…….3MN-1 (image size=2Mx2N).The watermarked bands are given by

$$\tilde{I}_O^{LH}(i,j)=\tilde{I}_O^{LH}(i,j)+\alpha X_{iN+j} \qquad \text{---------------------} \qquad (1)$$

$$\tilde{I}_O^{HL}(i,j)=\tilde{I}_O^{HL}(i,j)+ \alpha X_{MN+iN+j} \qquad \text{---------------------} \qquad (2)$$

$$\tilde{I}_O^{HH}(i,j)=\tilde{I}_O^{HH}(i,j)+ \alpha X_{2MN+iN+j} \qquad \text{---------------------} \qquad (3)$$

Here α is the gain factor and represents strength of the watermark. The gain factor is set constant (α =4) for embedding the watermark. The size of the message and the cover object is determined. The message to be embedded is reshaped into vector. After obtaining the vertical, horizontal, diagonal coefficients, PN sequences are added to the coefficients, when message is zero. The message in the form of PN sequence is added to the cover object (also called original image) to get the watermarked image.

Watermark Extraction: Watermarking detection is done independent of the original image.

III. PROPOSED BLINDWATERMARKING TECHNIQUE

In the proposed method ,instead of directly applying DWT on a color image or a grayscale as in existing technique, we convert RGB image to a indexed image format and now 2-D DWT of a indexed image is been taken which computes four planes LL,LH,HL,HH.Now we may add the watermark to any of the planes. After adding a watermark next step is to take the IDWT of a resulting plane..IDWT gives out the new indexed format. Now convert the indexed format back to RGB format. The proposed watermarking method of embedding and extraction is given in algorithm 1 and algorithm 2.
Algorithm1:To insert watermark.
Input: RGB Image and Watermark.
Output: Watermarked Image.
Step l: Read the image
Step 2: Convert the image from rgb 2 index (gives Cdata and map)

Step 3: Take the transform of the OrgCdata its dwt2 (SAVE THIS)
Step 5: Add the watermark (B=Cdata+wmark)
Step 6: Take the inverse of Result (inverse transform of B) (Save this)
Step 7: Reconstruct the original image from inverse transform.
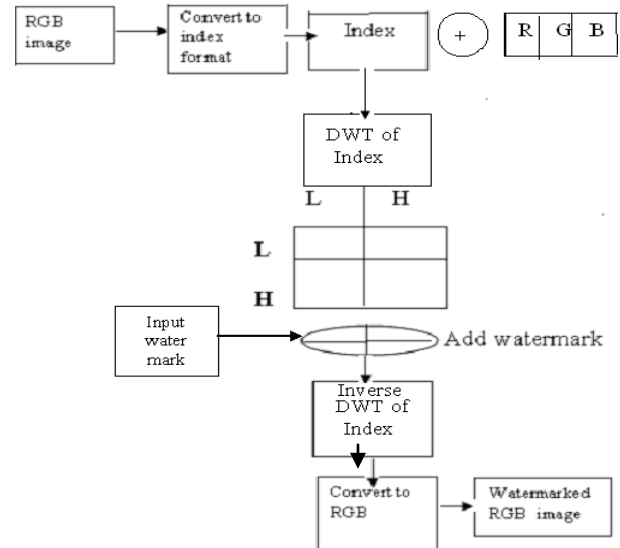The watermark embedding procedure is shown in Fig.2

Figure.2. Proposed watermarking embedding scheme

Watermark Extraction: Similarly Fig.3 provides a schematic overview of extracting the embedded watermark. The first 2 steps remain same which convert the watermarked RGB image to index format and apply 2-D DWT on it which gives four planes. Choose the plane in which watermark was added and take difference of this plane with that of the same plane in the original image. The difference is the extracted watermark.
Algorithm 2: To Extract Water mark.
Input: Watermarked RGB Image, DWT plane of Original Image.
Output: Extracted Watermarked Image.
Step l: Take the transform of the newly constructed image (To which watermark is added) save it as CdataNew.
Step 2: Take the difference of the OrgCdata and CdataNew, gives out the watermark and the results are given as mentioned above.
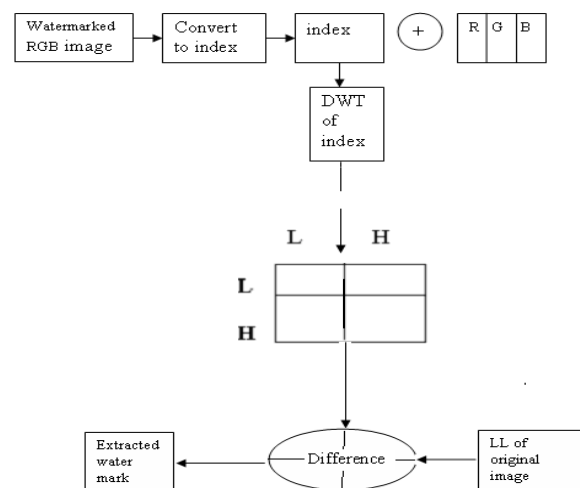

Figure.3.Watermarking extraction scheme

In the modified method of DWT watermarking we have considered standard images available on MATLAB 7.1. We have compared conventional methods with modified methods in terms of, MSE, PSNR, and RMSE values.

Table.1.shows values for MSE, RMSE and PSNR tested for standard images. The results shows quality of Watermarked images is better when compared to conventional DWT watermarking techniques [9].

Table.1.DWT Based Image Water Marking on color images

Image	MSE	RMSE	PSNR
Lena	1.0403e-015	3.2254e-008	198.2275
Pepper	3.3990e-016	1.8436e-008	200.6636
Football	3.7801e-016	1.9442e-008	200.5444
Mandrilla	6.0604e-022	2.4618e-011	260.0289

IV.   CONCLUSION AND FUTURE SCOPE

A new approach for DWT Watermarking technique is presented in this paper. The comparative study reveals that the modified method have decreased the mean square error rate and increased PSNR values which improves the quality of watermarked image.

The work has a scope for containing the concept of Cryptography and Digital Watermarking can be combined to implement more secured Digital Watermarking system.

V.   REFERENCES

[1].   B. Forth and D. Kiosk "Multimedia Security Handbook," February 3, 2004.

[2].   R. B. Wolfgang, EJ. Delp. "Overview of image security techniques with applications in multimedia systems", Proc. of SPIE97 Conference on Multimedia Networks: Security, Displays,Terminals, and Gatweys. Vol. 3228, 1997, pp. 297-308.

[3].   P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol.10, Oct,2001

[4].   Chan, C.-K. and L. M. Cheng. "Hiding data in images by simple LSB substitution."Pattern Recognition 37:   469-474.2004.

[5].   Cox I.J., Leighton FT., and Shamoon T., Secure Spread spectrum watermarking for multimedia, IEEE Trans. on Image processing, vol.6 (12), 1997, pp.   1673- 1687

[6].   Niu X.M., Lu Z.M. and Sun S.H., digital image watermarking based on multiresolution decomposition, Electronic letters, vol.36 (13), 2000, pp.1108-111O. Kaewkamnenl N.and Rao K.R., wavelet bilaed image lIflIptive watermarkingsdteme, Electroflic letters, vol.36 (4), 2000, and pp.312-314.

[7].   Lee W.B., Chen T.H., A public verifiable copy protection technique for Still images, The journal of systems and software, vol.62 (3), 2002, pp.195-204.

[8].   M. Bami et aI, "A DWT based technique for spatio frequency masking of digital signatures," Proc. IS&T/SPIE Conf. Security and watermarking of multimedia contents, vol. 3657, pp. 31-39, Ian.1999.

[9].   Na Lil , Xiaoshi Zhengl ., Yanling Zhao I, Huimin Wul ,2, Shifeng Li "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform" International Symposium on Electronic Commerce and Security.

CONFERENCE PAPER
International Conference on Issues & Challenges in Networking,
Intelligence & Computing Technologies
Organized by Krishna Institute of Engineering and Technology
(KIET) Ghaziabad. India