A Wavelet Based Watermarking Approach in Concatenated Square Block Image for High Security

Submitted: 26th August 2018; accepted: 15th November 2018

B. Sridhar

DOI: 10.14313/JAMRIS_3-2018/20

Abstract:
Watermarking in digital contents has gained the more attraction in research community. In this approach copyright information is concealed in to the concatenated square region of an image under wavelet domain, initially original image is undergoing an alternative pixel sharing approach and one of the shares undergo the circular column shift further, concatenates those shares. Next, square region is obtained by capturing the half of the row value in the last part of first share and the first part of second share which forms a square image. To enrich the robustness of the technique, watermarking is under consideration only in the folded square under wavelet. Further, the reverse process is carried out to generate the watermarked image. To show ownership, original and watermarked image have undergone the same operation and acquire the copyright information. Experimental results indicate that the proposed approach is robust against image processing attacks.

Keywords: *authentication, concatenation, copyright, watermarking, wavelet*

1. Introduction

In the fast growing of multimedia communications, the digital transmission of data is enormous. During the distribution unknown can easily acquired the data and claim ownership. Hence, the safeguard of the intellectual property is an important consideration for today's world [1–2]. Digital watermarking is a suitable approach for protecting the multimedia information [3–6]. Spatial and Transform domain are the two embedding approaches which are utilized in the watermarking techniques [7]. In spatial domain, ownership information into a host image is easily installed by altering the pixel values directly using bit substitution. But in transform based approaches copyright mark is embedded only in the transform coefficients. Hence transform based approach is robust and stable [8].

Discrete Wavelet Transform deserves an excellent property because to their spatial restriction, frequency distribution, multi-level of resolution characteristics and computationally more significant than other transform methods [9]. By using the sub component filters the DWT of the two dimensional images is obtained by sub sampled the low, middle, and high frequency sub components. At a low level resolution provides the image content where the high frequency part contains edge components. Any watermarking technique has to be evaluated based on the following features [10].

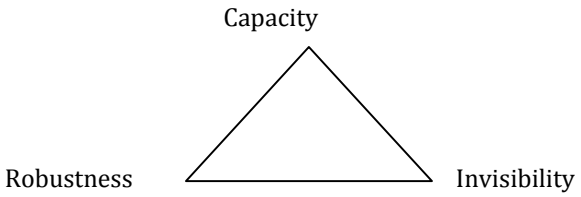

Fig. 1. Features of watermarking system

A copyright concealing scheme is said to be robust it can able to preserve the secret message under various attacks like filtering, compression or cropping. A watermarking technique has good invisibility property if human can unable to notice the changes in the cover medium after concealing the watermark. The above three requirements carry a trade-off triangle as shown in Fig. 1. If we achieve the two out of three properties, then the third one should be traded off.

The remaining sections are arranged as follows, related work involves in section 2. The proposed approach and the experimental results are discussed in section 2 and 4. Finally, conclusion is placed in section 5.

2. Related Works

The extensive literature gathered and related with the performance improvement of image watermarking techniques is critically inspected and exhibited in this section. Further, the summary of the review of literature is also furnished at the end of the review.

Delaigle *et al*. [11] addressed a watermarking technique on the account of the Human Perception System. Initially, m- number of binary sequences were created and combined on a random carrier signal. This copyright is treated as the ownership identity, and it is properly concealed in accordance with the contrast between the original image and the modulated image. The concealed copyright information is merged with the cover data to generate the watermarked image. These technique is robust to noise attacks, JPEG coding and rescanning.

Chen Yongquiang *et al.* in 2009 [12] demonstrated a transform domain based watermarking approaches on color image to fulfill the features of

watermarking like, security, intangibility and robustness. In this approach, a 2D chaotic stream encryption technique is adopted to scrambled a gray watermark. In order to enhance the imperceptibility properties of the watermarked image, Genetic algorithm is adopted to conceal the watermark data into the original color image.

Yingkun Hou and Chunxia Zhao in 2010 [13] addressed the semi sub sampled wavelet transform (SSWT) based watermarking techniques. It comprises two section non sub sampled tight frame transform and the difficulty sampled wavelet transform (WT). Concealing the ownership information into the approximation level of SSWT, the imperceptibility and robustness of watermarking technique can be worthfully enhanced by compare with previous watermarking schemes.

Sridhar and Arun (2012) [14] addressed a wavelet based multiple image watermarking techniques, in this approach the original gray image is sectioned into odd and even rows of images, further remove the zero rows in the respective shares. Watermark is implant in to deinterlace images under wavelet domain. After watermarking merge the two watermarked images in to single image by presenting some zero rows on the two watermarked images. Results achieved better PSNR value and it is robust against many geometrical attacks.

In order to enhance the security of the system, the proposed technique is address to implant the watermark information into the concatenated square region of an image. Hence the degree of authentication is high.

3. Proposed Approach

Our proposed scheme adds the watermark into the concatenated middle square region of two shares. Initially original gray image $[A]_{mxn}$ is subject to the alternative pixels sharing such as and $[A']_{mxn}$ and $[A'']_{mxn}$. Circular column shift is employed under this equation 1.

$$A^c(i,j)=\begin{cases} A''(i,j+1), & if \quad j=1 \quad to \quad n-1 \\ A''(i,1), & if \quad j=n \end{cases} \tag{1}$$

At the end horizontal concatenation is experienced to these shares $C=[A'_{mxn} \mid A^c_{mxn}]_{mx2n}$ as shown in equation 2.

$$C=\begin{pmatrix} a_{11} & 0 & \boldsymbol{a_{13}} & \boldsymbol{0} & \boldsymbol{a_{14}} & \boldsymbol{0} & a_{12} & 0 \\ 0 & a_{22} & \boldsymbol{0} & \boldsymbol{a_{24}} & \boldsymbol{0} & \boldsymbol{a_{21}} & 0 & a_{23} \\ a_{31} & 0 & \boldsymbol{a_{33}} & \boldsymbol{0} & \boldsymbol{a_{34}} & \boldsymbol{0} & a_{32} & 0 \\ 0 & a_{42} & \boldsymbol{0} & \boldsymbol{a_{44}} & \boldsymbol{0} & \boldsymbol{a_{41}} & 0 & a_{43} \end{pmatrix} \tag{2}$$

Further, square region is obtained by capturing the half of the row value in the last part of first share and half of the row value in the first part of second share which forms a square image. This marking region is obtained by using the equation 3. Folding process can be carried out before conceal the copyright information in equation 4 and 5.

$$D=C\left(1:m,\left(\frac{n}{2}\right)-\left(\frac{m}{2}\right)+1:\left(\frac{n}{2}\right)+\left(\frac{m}{2}\right)\right) \tag{3}$$

$$f(i,j)=D(i,j)+D(m+1-i,j) \tag{4}$$

$$f(i,j)=\begin{pmatrix} a_{13} & a_{44} & a_{14} & a_{41} \\ a_{33} & a_{24} & a_{34} & a_{21} \end{pmatrix} \tag{5}$$

$$X=f_2^{ll}+\alpha\times w \tag{6}$$

$$\begin{pmatrix} \boldsymbol{X} & f_2^{lh} & f_1^{lh} & f_1^{lh} \\ f_2^{hl} & f_2^{hh} & f_1^{lh} & f_1^{lh} \\ f_1^{hl} & f_1^{hl} & f_1^{hh} & f_1^{hh} \\ f_1^{hl} & f_1^{hl} & f_1^{hh} & f_1^{hh} \end{pmatrix} \xrightarrow{IDWT} f^W \tag{7}$$

Image Sharing

1. ***for*** *i from 1 to (Rows/2)* ***do***
2. ***for*** *j from 1to Columns* ***do***
3. ***if (i*** *mod 2)! = 0 && (j mod 2)==0;*

(or)

4. ***if (i*** *mod 2)= = 0 &&* ***(j*** *mod 2)!=0;****then***
5. *Move the row into (Rows+1-i)*
6. ***else***
7. ***endif***
8. ***endif***
9. ***end for***
10. ***end for***

$$[H]_{mx2n}=\left(C\left(1:m,1:\left(\frac{n}{2}\right)-\left(\frac{m}{2}\right)\right)\mid f^W \mid C\left(1:m,\left(\frac{n}{2}\right)+\left(\frac{m}{2}\right)+1:n\right)\right) \tag{8}$$

$$[F_{ws}]_{mxn}=H\left(1:m,1:\left(\frac{n}{2}\right)\right) \tag{9}$$

$$[S^c_{ws}]_{mxn}=H\left(1:m,\left(\frac{n}{2}\right):n\right) \tag{10}$$

$$S_{ws}(i,j)=\begin{cases} S^c_{ws}(i,n), & if \quad j=1 \\ S^c_{ws}(i,j-1), & if \quad j=2 \quad to \quad n \end{cases} \tag{11}$$

$$W(i,j)=F_{ws}(i,j)+S_{ws}(i,j) \tag{12}$$

Watermarking process is carried out only in the folded region in equation 6. Where α is the scaling factor, which reduces the weight of the watermark. Inverse transform is enabled by using equation 7. Unfold the folding image by using above algorithm. From equation 8 to 12 explains the steps to obtain the watermarked image. Figure 2 shows the procedure of proposed approach. In the extraction side again do the same operation of watermarked image and original image and make the difference to release the ownership.

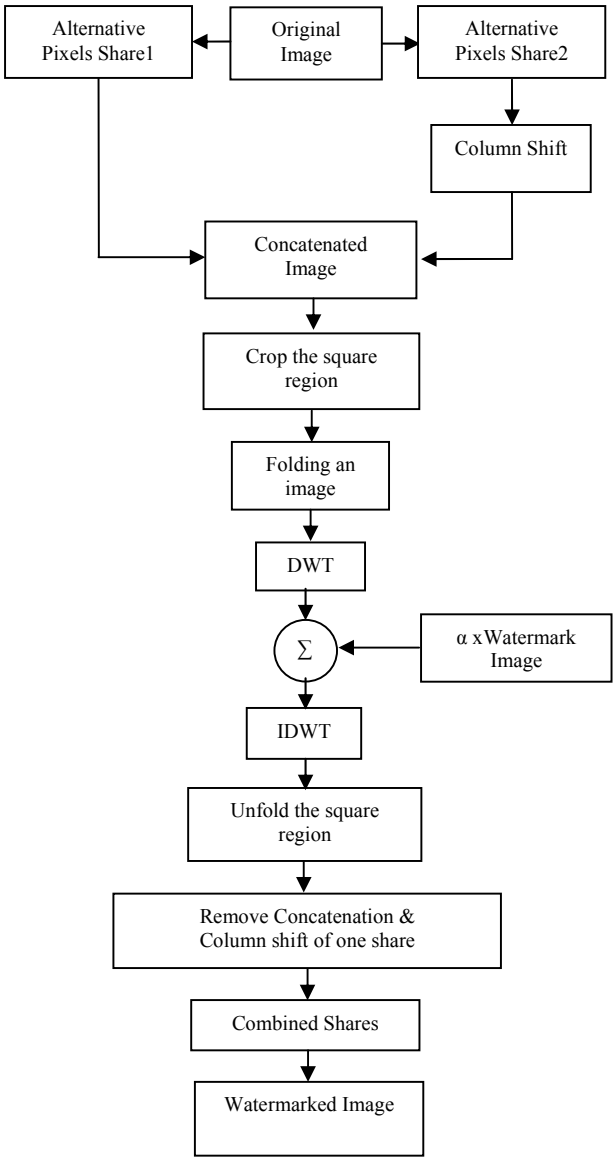

Fig. 2. Proposed image watermarking scheme

4. Experimental Results

In this experiment MATLAB software is utilized. A standard image like the cameraman image of size 512×512 is consider as a cover image and to fetch the watermark information like rice image of size 256×256 is utilized. Figure 3 displays the original cover image, concatenated image, square image, folded image, watermark image, and watermarked cover image.

4.1. Invisibility Test

The excellence of this approach is to genearate the invisibility of the watermark. To justify the imperceptibility, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are the two vital parameters. The MSE is the cumulative squared error between the original image *O(i,j)* and the watermarked image *W(i, j).* The average MSE of this proposed method is 0.0849. PSNR is employed to calculate the quality of the watermarked image. PSNR of our proposed approach is 46.5498 dB. Equation 13 and 14 shows the formula of MSE and PSNR.

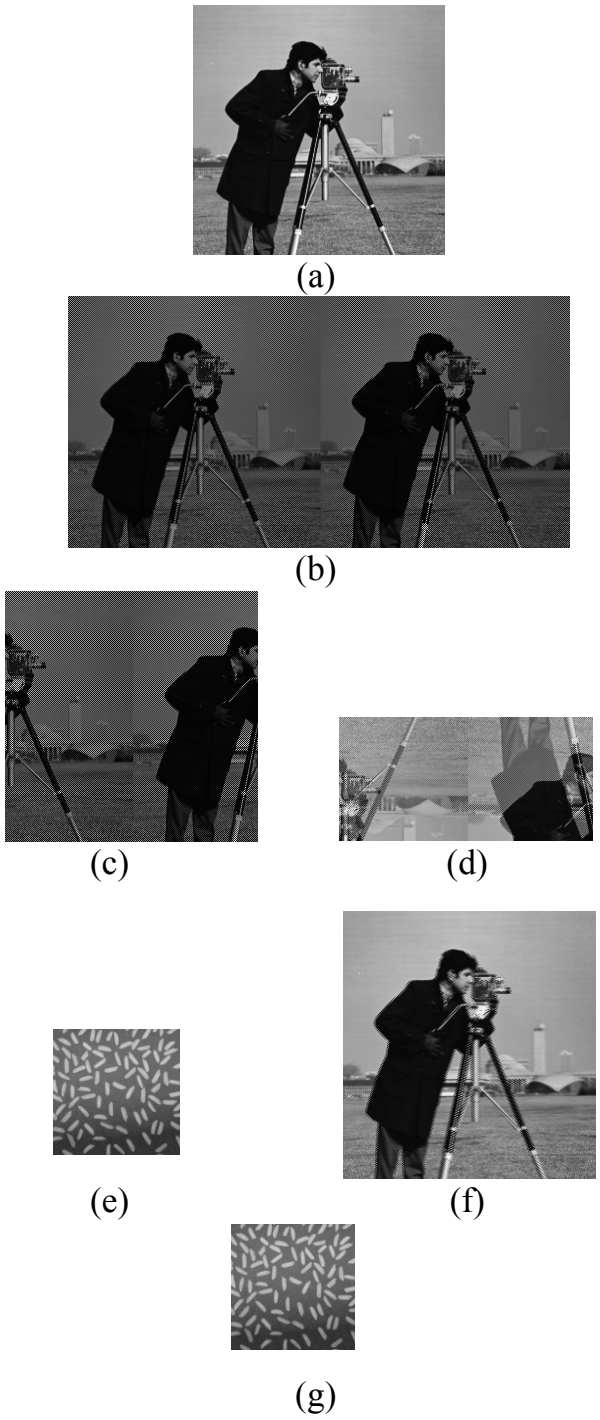

Fig. 3. (a) Original image; (b) Concatenated shares; (c) Square image; (d) Folded square image; (e) Watermark image, (f) Watermarked image, (g) Extracted Watermark

$$MSE = \left(1/xy\right)\sum_{i=0}^{x-1}\sum_{j=0}^{y-1}(O(i,j)-W(i,j))^2 \qquad (13)$$

$$PSNR \quad 10\log_{10}\left(\frac{255}{MSE}\right) \qquad (14)$$

The correlation co-efficient is another measure used to estimate the robustness of the watermarking algorithm against the possible attacks.

$$r = \frac{\sum_x \sum_y (O_{xy} - \bar{O})(E_{xy} - \bar{E})}{\sqrt{\left(\sum_x \sum_y (O_{xy} - \bar{O})^2\right)\left(\sum_x \sum_y (E_{xy} - \bar{E})^2\right)}} \quad (15)$$

Correlation coefficient value may be one or zero based on the watermarked and original images is identical or not. Equation 15 shows the formula to generate the correlation coefficient between two images. Similarity value between the watermarked and original image is 0.9594.

4.2. Attacks in Image Watermarking

Most common attacks of image watermarking are noise attacks, geometrical attacks and filtering attacks. In our method, different noises like Salt & Pepper, Speckle, Gaussian and Poisson with default noise density are introduced in watermarked image with default noise density and measure the robustness of the system.

Table 1. PSNR values of the proposed approach with different bands

Scaling Factor	LL	LH	HL
	PSNR(dB)	PSNR(dB)	PSNR(dB)
0.01	**46.5498**	46.0187	46.0185
0.02	46.5198	45.9651	45.9651
0.03	46.4752	45.8608	45.8627
0.04	46.4467	45.7398	45.7492
0.05	46.3951	45.5642	45.5748
0.06	46.3608	45.3861	45.3983
0.07	46.3025	45.1488	45.1680
0.08	46.2641	44.9334	44.9585
0.09	46.1971	44.6603	44.6929
0.1	46.1369	44.4027	44.4363

Table 2. Performance values of the proposed approach

Attacks	Watermarked Image	Watermark Image
	PSNR (dB)	PSNR (dB)
No Attacks	46.5498	33.0321
Salt & Pepper	38.4125	26.2347
Speckle	43.9021	27.0934
Gaussian	35.0126	25.9093
Poisson	31.2262	26.4957
Median Filtering	35.0126	26.6457
Low Pass Filtering	40.3973	23.2759

Also some additional evaluation median filtering and low pass filtering also attack to the watermarked image and measure the performance of the algorithm. Table 1 and 2 shows the PSNR values and performance of an algorithm with different attacks.

Figure 4 displays the comparison sketch between the wavelet and Singular Value Decomposition (SVD). It is finding that wavelet based approach gained the benefits of high PSNR than SVD. Also proposed approach registered more PSNR value 46.5498 dB than Pinki Tanwar, *et al.* 37.676 dB.

5. Conclusion

In this paper, the optimal and robust region marking for high security is presented. Here, concealed the information only in the folded square region of concatenated shares under wavelet transform. Hence the robustness of this system deserves high. PSNR and Correlation coefficient of this method are 46.5498 dB and 0.9594. Also,this proposed approach is simple, efficient and with less complexity. In future the enhancement of this algorithm will be extended to the video.

AUTHOR

B. Sridhar – Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, INDIA-500043,
email: sridharbece@gmail.com.

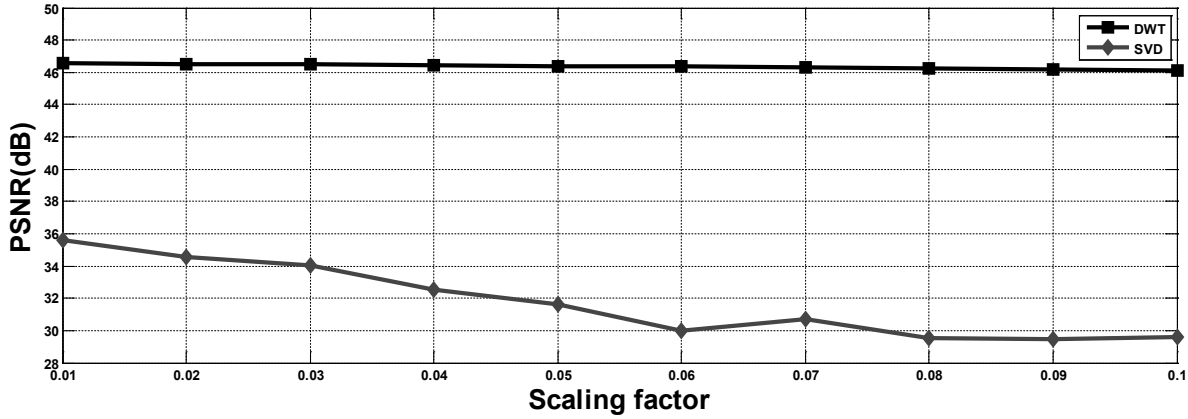

Fig. 4. Comparison sketch between DWT and SVD

REFERENCES

[1] Qiao Li, and I.J.Cox, "Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking", *IEEE Transaction on Information Forensics and Security*, vol. 2, no. 2, 2007, 127–139.

[2] Alessandro Piva, Tiziano Bianchi, Alessia De Rosa, "Secure Client-Side ST-DM Watermark Embedding", *IEEE Transactions on Information Forensics and Security,* vol. 5, no. 1, 2010, 13–26.

[3] A. Piva, F. Bartolini, M. Barni, "Managing copyright in open networks", *IEEE Transactions on Internet Computing*, vol. 6, no. 3, 2002, 18–26.

[4] B.Sridhar, C. Arun, "An Enhanced Approach in Video Watermarking with Multiple Watermarks Using Wavelet", *Journal of Communications Technology and Electronics*, Springer, vol. 61, no. 2, 2016, 165–175.

[5] M. Vidyasagar, M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 3rd International Conference on Industrial Informatics (INDIN), 2005, 709–713.

[6] Yiwei Wang, John F. Doherty, Robert E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image", *IEEE Transactions on Image Processing*, vol. 11, no. 2, 2002, 77–88.

[7] Frank Y. Shih, Scott Y.T. Wu, "Combinational image watermarking in the spatial and frequency domains", *Pattern Recognition*, vol. 36, 2003, 969–975.

[8] M.A. Suhail, M.S. Obaidat, "Digital watermarking-based DCT and JPEG model", *IEEE Transaction on Instrumentation and Measurement*, vol. 52, no. 5, 2003, 1640–1647.

[9] Mehdi Khalili, "A Novel Secure, Imperceptible and Robust CDMA Digital Image Watermarking in Jpeg-Ycbcr Channel Using DWT2", *International Journal of Enterprise Computing and Business Systems*, vol. 1, no. 2, 2011.

[10] C.H. Huang, J.L. Wu, "Attacking Visible Watermarking Schemes", *IEEE Transactions on Multimedia*, vol. 6, no. 1, 2004, 16–30.

[11] J. Delaigle, C. de Vleeschouwer, B. Macq, "Psycho visual Approach to Digital Picture Watermarking", *Journal of Electronic Imaging*, vol. 7, no. 3, 1998, 628–640.

[12] Chen Yongqiang, Zhang Yanqing, Peng Lisen, "A Novel Optimal Color Image Watermarking Scheme", *3rd International Conference on Genetic and Evolutionary Computing*, 2009, 121–124.

[13] Yingkun Hou, Mingxia Liu, Zhengli Zhu, Deyun Yang, "Semisubsampled Wavelet Transform Based Image Watermarking with Strong Robustness to Rotation Attacks", *Journal of Multimedia*, vol. 5, no. 4, 2010, 385–392.

[14] B. Sridhar, C. Arun, "On Secure Multiple Image Watermarking Techniques using DWT", 3rd International Conference on Computing Communication & Networking Technologies (ICCCNT), 2012, 1–4.

[15] Pinki Tanwar and Manisha Khurana, "Improved PSNR and NC in Digital Image Watermarking Using RDWT and SVD", *International Journal of Advanced Research in Computer Science and Software Engineering Research*, vol. 6, no. 5, 2016, 955–959.