Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fusion of DWT and SVD digital watermarking Techniques for robustness

Jaishri Guru
M.E. Student,Dept. of CSE
S.R.I.T,R.G.P.V., Bhopal, India

Hemant Dhamecha
Asst.Professor,Dept. of CSE
S.R.I.T,R.G.P.V., Bhopal, India

Brajesh Patel
Asst.Professor & Head Dept.of CSE
S.R.I.T,R.G.P.V., Bhopal, India

Abstract - There are plenteous issues belongs to the impunity of the data and also related to copyright ignominy. So we are using digital watermarking techniques to plough these issues. By supervising a refrain examine on the Impalpability and robustness which yield to be its main objectives, these issues have to be reconciled. Now in this paper we adopted the usage of a mixed (hybrid) transformation to fulfil these objectives, The opinion behind applying a hybrid transform or mixed transformation is that the cover image is modified in its singular values rather than on the DWT sub-bands and also PSNR values of both cover image and watermark can be change, therefore the watermark makes it vulnerable to vivid attacks and maintains its original state by checking the robustness. To support the methods and relative study some simulation results are available.

Keywords - Authentication, Copyright protection, Robustness,Singular Value Decomposition (SVD) technique, Discrete Wavelet Transform (DWT) technique, Attacks.

I. INTRODUCTION

The large progress in the digital community is being by elongating use of digitization. Digital style of communication is composing its clutch strict on the expansion of digital information. In this way digital watermarking is best to impugn the copyright violation [1], [2]. Digital watermarking is a procedure in which we adjoin the watermark to image or other digital data and can extract the watermark [3].

The aspect of internet is growing day by day because nowadays all the communication and data distribution is commencing by internet. By development of aspect of internet magnitude of digital data is also vegetating. For duplication and modification various types of tools are available in the internet that's why for defend digital data from the unauthorized access we need to major security. Digital watermarking is a technique to provide security for protecting digital data. In this technique cover image is embedded in watermark and then extracted for authentication [4].

Digital watermarking techniques are classified which are based on different categories. Visible watermark, invisible watermark, spatial watermark, spectral watermark, fragile watermark, semi fragile watermark and robust watermark are the classification of digital watermarking techniques [5].

Digital watermark can be inserted in spatial domain or in transform domain. Both domains are different. In spatial domain watermark is embedded in veridical way. In this method elements of the real or original image are embedded along the digital watermark with respect to veridical in-charge behaviour. The plus point of this method is that it has facile implementation and less complexity. The drawback of spatial domain technique is that it is not undisguised to image-processing procedures and different type attacks.

On the other hand, The transform domain which is also known as frequency domain. It takes the embedding of the watermark by modulating the mass of the elements of the digital image in the desired frequency domain, an example: DCT (discrete cosine transform), DWT (discrete wavelet transform), and SVD (singular value decomposition) [6]. The plus point of frequency domain or transform domain is that after embedding the watermark, its capability to conduce maximal knowledge and latest robustness against different type of attacks. When we compare the transform domain with spatial domain the drawback of transform domain is that it has exceed computed cost then the spatial-domain [7].

On the ledger of discrete wavelet transform, The DWT has its estate of spatial frequency localization that clumps the whole digital image into discrete frequency elements and the eras in which the watermark can be embedded supersensibly are simply accessible. For rectifying the transparency and robustness, Singular value decomposition has a mathematical estate in which minute rectification in the singular values do not motivate much ravage on the sight perception of the cover image [8].

II. BACKGROUND REVIEW

A. DWT

Discrete wavelet transform skyline adhere the similar guidelines as discrete cosine transform. To transform digital image in wavelet transform, Wavelet rakes are used.Many rakes are available, the mostly usage rakes for watermarking are daubechies bi-orthogonal rake, haar wavelet rake and daubechies orthogonal rake. Every rake can dissolve the digital image into many frequencies. Now representation of four frequencies in digital image obtained by rot of single level [9].

These four frequencies representations are LL, LH, HL, HH sub-bands. The LH, HL, and HH sub-band shows the slender scale wavelet element in which the LL sub-band shows the poor level element that is less frequency element of the digital image [10]. To gain highest level of rot the LL sub-band can be dissolved again. Now for the application this rot can subsist until the desired level of rot is obtained. To maintain the features of digital image the watermark can also be embedded in the three sub-bands LH, HL, and HH. The LL sub-band is milder to human eyes [11].

Discrete wavelet transform is very suitable for dissolving the digital image. The wavelet transform for which waves are differently model, discrete wavelet transform can be defined. The profit of discrete wavelet transform compare to the Fourier transform is its capability of producing provisional conation and now it holds both location information and frequency data. Mother wavelet is responsible for causing the renditions and elucidation of the wavelets.

Discrete wavelet transform counts the both high and low frequency elements by dividing the digital image into its separate frequency elements. Now for the edge quest the high frequency elements bequeath. On the other hand the low frequency components are anew divided into both high and low frequency components. The watermarking aim is being by the high frequency elements like as the human eye is mild on the edge diversity [12].

B. SVD

SVD (Singular value decomposition) produces the purview of minimization of intricacy by segmenting the digital image matrix which is not negative into $U * S * V^T$, Here orthogonal matrices are U and V and original matrix has singular values which are orderly in reducing order [13]. S is the diagonal matrix of the image, for instance, when any disarrange is done on the digital image huge diversity in the singular values do not betide. Singular values also show actual algebraic features [14].

Singular value decomposition is a numerary method which is used in numerical assay for in diagonal matrix. For several of applications singular value decomposition is evolve as an algorithm. In image processing applications singular value decomposition has some features. SVs or singular values of digital image have wonderful indelible, for instance, when any disarrange is done on the digital image huge diversity in the singular values do not betide. Singular value decomposition (SVD) is used to un-ridden various numerical issues in linear algebra. The watermarking which is based on SVD method, many inlets are feasible. In original image's high frequency band SVD is imposed, which is mostly used inlet and embed the watermark information to modify the singular values. The notable feature of singular value decomposition is when huge of the tampered singular values change that is very small for many types of attacks [15].

III. NOISE AND ATTACKS IN DIGITAL WATERMARKING

Noise in watermarking: Noise and attacks both put different effect on watermarking. By noise procurement and transit, the images which are relates with medical field are reprobated. Noise in any image tries to harm its brilliance. Noise tends to evolve diversity in brilliance of the demonstrated image and the diversity is usually irrelevant. The irrelevant diversity in brilliance of image designated as noise. The noise can rely on image or it cannot depend on image [16].

1. Random Noise: When intensity of picture or an image increases then random noise spins around this. Random noise betide due to color diversity up and down where alter the intensity. It is severed to redeem the random noise because where random noise will betide; we cannot foretell [16].

2. Fixed pattern noise: Hot pixels are encircles by the fixed pattern noise. If fixed pattern noise does not lessen then it can be more ambiguous to human eye than random noise. It is easy to fix [16].

3. Banding noise: Banding noise relies on cameras but all digital cameras will not produce the banding noise. Digital cameras take the information which is creating in sensor during the digital procedure range and produce the noise. Banding noise produced due to large speed and picture or shadow brilliance [16].

4. Salt & Pepper Noise: Salt & pepper noise (Attack) is kind place in hardware [17]. In images mostly seen an attack which is known as salt & pepper noise. Black and white pixels of concussion attack which is evolved by camera sensor's pixels those are not in range, by noisy media, or by vicious anamnesis are inconsequently obtaining in salt & pepper noise [18].

5. Speckle Noise: Speckle attack is a pebbly attack that naturally preexist in radar and disrate the predicate [18].Speckle attack is the outcome of the ample scrambling. Speckles disrate the predicate of ultra sound image and synthetic aperture radar images [18, 16].

Attacks in watermarking: The digital watermarking attacks may be accidental or intentional. The attacks which are intentional use all the present appliances to corrode or alter the watermark and for extraction it is impossible.On the other way, each image transmission error may cause mitigation. These types of attacks which are inescapable are called as accidental attacks. There are also other types of attacks which are based on estimation. In these types of attacks, watermark information and original image estimates can be gained by using stochastic techniques. Some attacks are listed here [19]:

1. Removal and Interference attacks: Removal attacks intend to transplant the watermark information from the watermarked image. The watermark is mostly an agglomerative noise allusion appear in the host allusion, this is exploit by the removal and interference attacks. And also interference attacks in which add adscititious noise to the watermarked image [19].

2. Cryptographic attacks: Above attack do not break the rules of impunity of the digital watermark algorithm. But cryptographic attacks negotiate with breaching of the impunity. One instance is, cryptographic attack in which exploring the esoteric watermarking key using tedious Brute Force technique. Oracle attack is second instance of cryptographic attack [19].

3. Protocol attacks: The Protocol or bunch of rule attacks exploit the slots in digital watermarking. IBM attack is an instance of Protocol or bunch of rule attacks. The IBM attack is also known as the setback or deadlock attack, dummy original attack or inversion attack. Protocol attacks embed one or many more watermarks in such a way that it is implicit which the actual owner's watermark was [19].

4. Active attacks: In active attacks hacker attempts deliberately to transplant the watermark or easily make the watermark which is not detectable. In copyright sheathed fingerprinting applications active attacks are very big teaser [20].

5. Passive attacks: In passive attacks, Invasive is not attempting to transplant the watermark but easily trying to prescribe if a evolved mark is appear or not. As the lector should prudent, impunity adverse passive attacks is of the categorical heft in secret communications in which easy information of the appearance of watermark is almost more to concession [20].

IV. PROPOSED DWT-SVD SCHEME

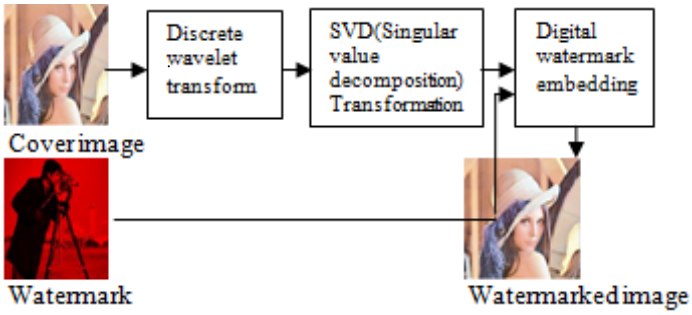


Figure.1. Procedure of embedding watermark in an Image

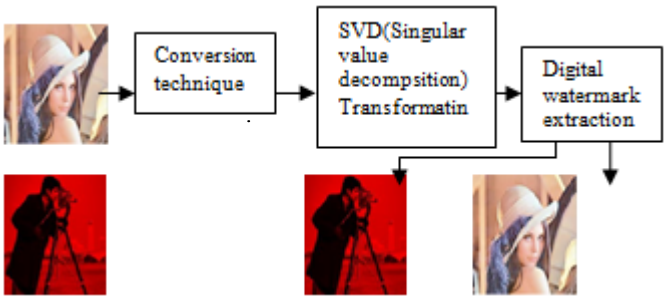


Figure.2. Procedure of extracting watermark from an Image

V. PROPOSED APPROACH AND ALGORITHMS

The proposed DWT-SVD scheme is formulated as given under:

1) Extract the red component of the image with (:, :, 1)
2) One level 'Haar' Discrete Wavelet Transform to decompose cover image into four subbands.

$$[ca1, ch1, cv1, cd1]=dwt2\ (image,'haar')$$

3) Apply Singular Value Decomposition to the vertical (cv1) and horizontal (ch1) coefficients.

$$[U1, S1, V1]=svd(ch1)$$
$$[U2, S2, V2]=svd(cv1)$$

4) Divide the watermark into two parts.

$$W=W1+W2$$

5) Extract the red component of the watermark as well like for the image, with (:, :, 1).
6) Modify the singular values of vertical and horizontal plane in 2. Along with the inputted scale factor (α).

$$S1 + \alpha W1 = Uw * Sw * Vw^{T}$$
$$S2 + \alpha W2 = Uw * Sw * Vw^{T}$$

7) Two sets of modified DWT coefficients are made available by 4.

$$Mod\_c\_h = U1 * Sw * V1'$$
$$Mod\_c\_v = U2 * Sw * V2'$$

8) Apply the inverse Discrete Wavelet Transform, i.e. i-dwt on the two sets of modified coefficients in 5 (cv1 and ch1) and non-modified coefficients in 1 (ca1 and cd1).

$$WI=idwt2\ (ca1,Mod\_c\_h,Mod\_c\_v,cd1,'haar')$$

9) Replace the first component of the image that is processed with the original image's first component.
10) Extraction of the watermark:

For the Extraction of the watermark: (in the red component). Apply one level Haar DWT to the watermarked image obtained in 6.

$$[ca2, ch2, cv2, cd2] = dwt2\ (WI,"haar')$$

11) Apply SVD to the vertical and horizontal coefficients, where U and V are of original image and S is of the watermarked image from 2 and 4 respectively.

$$[U1, Sw, V1] = svd (ch2)$$
$$[U2, Sw, V2] = svd (cv2)$$

12) Compute the replaced coefficients by placing the U and V of the original watermark along with the singular value S used in 8.

$$M\_c\_h = Uw * Sw * Vw'$$
$$M\_c\_v = Uw * Sw * Vw'$$

13) Extract half of the watermark by

$$W1^* = (M\_c\_h - S1) / \alpha$$
$$W2^* = (M\_c\_h - S2) / \alpha$$

14) Combine the results of 4 to obtain the original watermark.

$$W^* = W^*1 + W^*2$$

VI. EXPERIMENT AND RESULTS

Experiments are conducted to demonstrate the proposed approach. The coloured image "Lena" of size 512 × 512 is used as the cover image and "cameraman" of size 256 × 256 is used as the watermark image. These images are shown in Fig.3(a) and 3(b) which are of the cover and watermark respectively. Fig.3(c) illustrates the watermarked image and Fig.3(d) is the extracted watermark image. The observation of the proposed approach yields the preserved high perpetual quality of the watermarked image.

As a parameter of quality, peak signal-to-noise ratio (PSNR) has been used. The PSNR illustrates the maximum fluctuation of pixels with the mean square error of the images and helps in easy analysis of the variations and degradations being caused on the image by comparing the peaking pixel values.

$$PSNR = 10 \log_{10} (R^2 / MSE)$$
$$MSE = \text{sum} [(I1 (m, n) - I2 (m, n))^2] / m*n$$

Where, R is the maximum fluctuation of pixels and m, n are the row and column matrix of the images.

(a) (b)

Figure. 3. (a) Cover Image (b) Watermark

(c) (d)

Figure. 3. (c) Watermarked Image (d) Extracted Watermark (PSNR = 52.92)

In the experiment the values of the scale factor has been carried out from 0.01 to 0.09 with a constant interval of 0.02. The graph presented in the Fig.4 illustrates the PSNR of the extracted image, and of the watermarked image. It is clear from the presented graph that the robustness of the watermark is maintained at a perpetually high level.

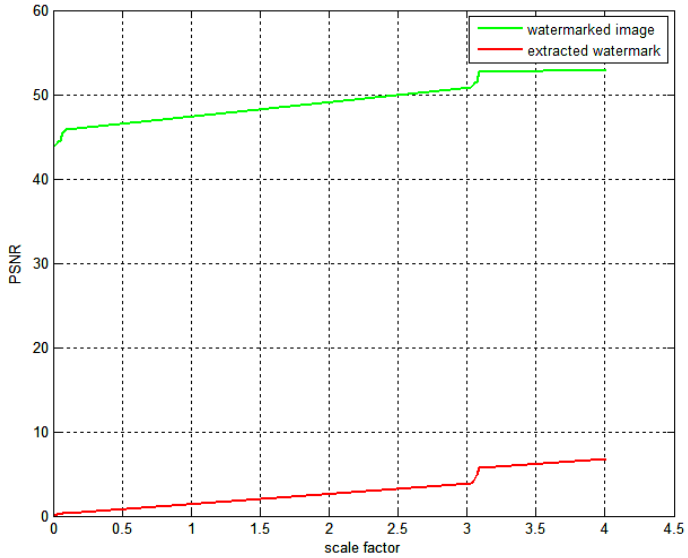


Figure. 4 PSNR of the Watermarked Image and Extracted Watermark

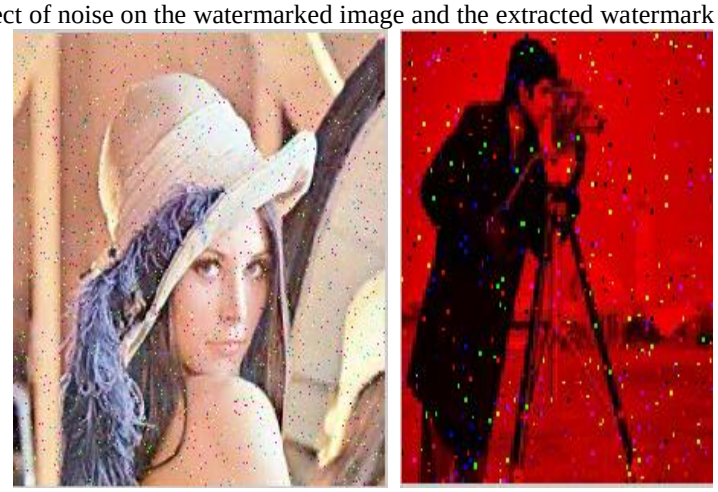
The varying range of the PSNR of the images used in order to draw the comparison has been presented in the Table 1 below:

Table I. Comparative analysis of PSNR at different scale factor values for resultant images

Scale Factor	0.01	0.03	0.05	0.07	0.09
Watermarked Image	52.92	50.65	48.56	43.20	39.80
Extracted Watermark	6.80	5.70	4.90	4.20	3.90

On changing the value of the scale factor the PSNR fluctuates indicating the status of the robustness of the watermark in the image and after extraction.

To contemplate the robustness of the presented approach the watermarked image is tested against various attacks Fig.5 demonstrates the effect of noise on the watermarked image and the extracted watermark with high robustness.



(a) (b)

Figure .5 (a) Salt & Pepper Noise on Watermarked Image (b) Extracted Watermark

The Table 2 below reads the PSNR of the watermarked image after introducing noise in it and of the extracted watermark with the same noise.

Table II. Comparison between PSNR with varying scale factor and noise

Scale Factor	0.01	0.03	0.05	0.07	0.09
Watermarked Image	21.80	21.65	20.40	19.88	19.20
Extracted Watermark	26.49	26.40	25.96	25.32	24.99

(c) (d)

Figure. 5 (c) Speckle Noise on Watermarked Image (d) Extracted Watermark

The presented results in Table 3 are after introducing speckle noise in the watermarked image and then successfully extracting the watermark and thereby preserving the copyrights.

Table III. Comparison of PSNR based on introducing speckle noise.

Scale Factor	0.01	0.03	0.05	0.07	0.09
Watermarked Image	20.98	20.32	19.93	18.67	17.60
Extracted Image	32.06	31.89	30.88	29.78	28.55

The robustness of the image is of great authentication and proves to enhance the copyrights and amenable to various attacks being forecast on the image.

VII. CONCLUSION

In this paper a hybrid watermarking scheme using SVD and DWT has been introduced, where the watermark is embedded in the singular values of the red component of the cover image's DWT subbands and then combined with the other two i.e. green and blue components to yield the watermarked image. The method is also focus on rgb colour image component and this experimental result is used with red layer components. Same algorithms will we used for green and blue components. The methods adopted fully exploit the features of the SVD and DWT transform. The intrinsic algebraic properties of the image represented by SVD and the spatio-frequency localization of DWT are well utilized. Experimental results are made available which depict the improved imperceptibility and robustness under attacks and preserve copyrights by using this technique. Further work of integrating human visual system characteristics into our approach is in progress.

REFERENCES

[1] J. Sang and M. S. Alam,"Fragility and robustness of binary-phase only filter- based fragile/semi-fragile digital image watermarking," IEEE Trans. Instrum. Meas., vol. 57, no. 3, pp. 595–606, Mar. 2008.

[2] H.-T. Wu and Y.-M. Cheung,"Reversible watermarking by modulation and security enhancement," IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 221–228, Jan. 2010.

[3] Jaishri Guru, Hemant Damecha, "Digital Watermarking Classification : A Survey", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014, pp.8-13.

[4] V.Santhi and Dr. Arunkumar Thangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space", International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009.

[5] Jaishri Guru, Hemant Damecha, " A Review of Watermarking algorithms for digital image", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 9, September 2014, pp.5701-5708.

[6] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[7] A. Nikolaidis and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," IEEE Trans. Image Process., vol. 12, no. 5, pp. 563–571, May 2003.

[8] V. Aslantas, L. A. Dog˘an, and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer," in Proc. IEEE Int. Conf. Multimedia Expo, Hannover, Germany, 2008, pp. 241–244.

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

[10] E. Ganic and A. M. Eskicioglu,"Robust DWT-SVD domain image watermarking: Embedding data in all frequencies," in Proc. Workshop Multimedia Security, Magdeburg, Germany, pp. 166–174, 2004.

[11] Seema, Sheetal Sharma, "DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[12] G. Bhatnagar and B. Raman,"A new robust reference watermarking scheme based on DWT-SVD," Comput. Standards Interfaces, vol. 31, no. 5, pp. 1002–1013, Sep. 2009.

[13] Q. Li, C. Yuan, and Y.-Z. Zhong,"Adaptive DWT-SVD domain image watermarking using human visual model," in Proc. 9thInt. Conf. Adv. Commun. Technol., Gangwon-Do, South Korea, pp. 1947–1951, 2007.

[14] S. Mallat, "The theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, pp. 654–693, Jul. 1989.

[15] Sangeeta Madhesiya, Shakil Ahmed, "Advanced Technique of Digital Watermarking based on SVD-DWT-DCT and Arnold Transform", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May 2013.

[16] Ms. Alka Vishwa Ms. Shilpa Sharma, " Speckle Noise Reduction in Ultrasound Images by Wavelet Thresholding", Volume 2, Issue 2, February 2012 ISSN: 2277 128X.

[17] Rupinder Kaur ,Prof. Yogeshwar Singh Randhawa , "Comparative Analysis of Mean and Median Filter for High Density Salt and Pepper Noise Removal", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014 ISSN: 2277 128X, pp. 1394-1401.

[18] P. Shanthi, R. S. Bhuvaneswaran, **"**Robust Chaos Based Image Watermarking Scheme for Fractal-Wavelet", Applied Mathematical Sciences, Vol. 8, 2014, no. 32, 1593 – 1604.

[19] Kirti, Vikram Nandal, "A Review on Digital Watermarking and Its Techniques", Kirti et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 686-690.

[20] Vallabha VH, "Multiresolution Watermark Based on Wavelet Transform for Digital images",Multiresolution Watermarking for Digital Images.

AUTHOR PROFILE

Miss jaishri guru received her B.E. in CSE from Takshshila institute of engineering and technology (R.G.P.V.Bhopal),Madhya Pradesh, India in 2011.Currently she is pursuing M.E. in Software systems from S.R.I.T (Affiliated to R.G.P.V,Bhopal). She is working on project related to "DIGITAL WATERMARKING". Her interest areas are Digital Image Processing, Network security and Network Management.

