IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Enactment and Performance Analysis of Discrete Transform based Watermarking Algorithms for Digitized Images

B.Gowri Sankaran[*1], Prof.B.Raghu[2], G.Meenakshi Sundari[3]

[*1,3] Associate Professor, Department of ECE, Sri Ramanujar Engineering College, Vandalur, Chennai – 127, TamilNadu, India

[2] Professor, Department of Computer Science, Sri Ramanujar Engineering College, Vandalur, Chennai – 127, TamilNadu, India

gowri_305@yahoo.com

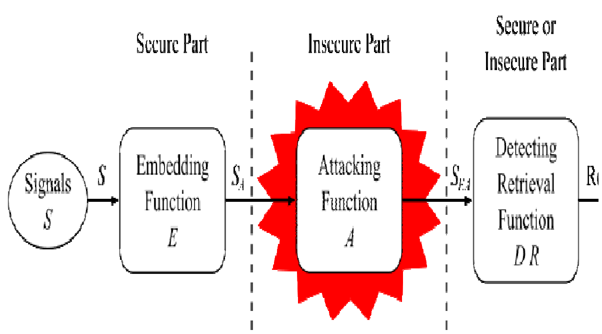
Abstract

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright Digital image watermarking technology protects digital content (text, images, audio, and video) from illegal manipulations. In this paper we proposed implementation and performance analysis of two different watermarking schemes based on DCT-DWT-SVD. Both are non-blind techniques. One is based on SVD of DC coefficients using second level DWT decomposition and other is SVD of all DCT values of second level DWT composition of cover image. PSNR and NCC parameters are used to check effectiveness of both techniques for Imperceptibility and robustness.

Keywords: Watermark; DWT; DCT; SVD; PSNR; NCC

Introduction

The fast growth of internet and applications using digital multimedia technologies has put the accent on the need to provide copyright protection to multimedia data. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data. So it can remain present within the cover media after any decoding process.



The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack*. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In *robust* digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In *fragile* digital watermarking, the extraction algorithm should fail if any change is made to the signal.

Watermarking scheme quality is determined using robustness, transparency and capacity. Transparency means after insertion of water mark the original image should not be distorted [13, 14]. Robustness is related to attacks. If watermark removal is difficult to various attacks like rotation, scaling, compression, noise then watermarking scheme is robust[15,16]. Capacity means amount which are inserted to cover i mage. More capacity means one can hide large amount of infor mation.

Robustness

A digital watermark is called *fragile* if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable commonly are not referred to as watermarks, but as generalized barcodes.

A digital watermark is called *semi-fragile* if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations.

A digital watermark is called *robust* if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

Perceptibility

A digital watermark is called *imperceptible* if the original cover signal and the marked signal are perceptually indistinguishable. A digital watermark is called *perceptible* if its presence in the marked signal is noticeable. A digital watermark that is perceptual, on the other hand, is imperceptible. It works context-sensitive/adaptive.

Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes: The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as *zero-bit* or *presence watermarking schemes*. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

Water mar king algorithms can be classified on several criteria are, according to domain of water mark insertion like Water marks can be embedded in the pixel/spatial domain or a transform domain [11]. Second is according to visibility of watermark visible and invisible) and according to watermark detection and extraction which contain blind and non blind techniques.

Then divide the selected band into 4X4 sub blocks and DCT is applied. First DCT value is selected from all sub blocks. Then SVD is perform on that. The method is tested against various attacks and result is good for LL band in compare to other band [2]. Robust water marking scheme is proposed by Navas. In that they combine advantage of three techniques (DCT-DWT-SVD).scheme is very robust for different kind of image processing attacks [3]. Middle band coefficient of DCT based watermarking scheme is given for image authentication. DWT is applied then after DCT of LL is computed. Then mid band coefficient is selected and SVD is applied on it. It is very robust against JPEG compression [4]. R. Mehul has suggested that to get robustness for vast range of attacks watermark insertion can be performed in both low and high value coefficients. Authors proposed color image water mar king using second level DWT decomposition and block base DCT.

First they divide color image into three channels Red, Green and Blue and then apply DWT to selected color and select HL or LH band for further decomposition. They selected low and high frequency band so robustness and imperceptibility result is very good[6]. A hybrid block based technique is proposed by V.Santhi.

In that First singular value is selected for watermark embedding in all different band after first level decomposition[7]. A hybrid technique based on SVD and DCT is proposed. More transparency is obtained using only Singular values of a recognized pattern and LPSNR is adopted to achieve high robustness[8]. Author proposed watermarking scheme based on DCT- DWT-SVD. They apply second level decomposition of cover image. DCT is apply to second level HL coefficient and divide it into four quadrant using zigzag sequence. SVD is applied to each quadrant and modified with SVD of water mark. Algorithm gives good PSNR and also robust to various attacks. Quadrant B1 gives good results compare to other three[9]. Author proposed watermarking scheme based on DWT and SVD using all four frequency bands. Singular values of watermark is inserted into all four frequency bands singular values after first level DWT. Experimental results shows that LL gives highest magnitude of wavelet coefficient as well as of singular values[10].

Proposed Algorithm I

Proposed algorithm combines merits of three different techniques DCT, DWT and SVD. First one level DWT is applied to original cover image. To achieve imperceptibility LL band is select for second level decomposition and HH band is selected. It is divided into 4X4 sub blocks. DCT is applied to each sub blocks and first DC coefficient of each block is selected and for med it in matrix. SVD is applied to this matrix and singular values are modified with singular values of water mark. Inverse SVD, inverse DCT and inverse DWT is performed to get watermarked image.

The procedure for embedding and extracting the water mark is given below.

A. Watermark embedding process

The embedding process is divided into following steps and is briefly described as given below:

1. Let OI be the Original image of size N x N. Select color channel and apply DWT to decompose it into four N/2 x N/2 sub-bands LL , HL , LH and HH .
2. Select LL band and Apply DWT to decompose it into four N/4 x N/4 sub-bands LL_LL, LL_HL, LL_LH and LL_HH.
3. Select LL_HH band, divide it into 4X4 square blocks and apply DCT to it, select first DCT value of each block and get DCT coefficient matrix B.
4. Apply SVD to B, $B=U1*S1*V1^T$, and obtain U1, S1 and V1.
5. Let OW of size N/16 x N/16 to represent watermark. Apply SVD to it, OW= W_U*W_S*W_V’ and obtain W_U, W_S and W_V
6. Modify S1 with watermark such that S=S1 + Į* WS.
7. Obtain B* using $B^*= U^*S^*V^T$.
8. Apply inverse DCT to B* to produce LL_HH*.
9. Apply inverse DWT to LL_LL, LL_HL, LL_LH and LL_HH* to get matrix LL*.
10. Apply inverse DWT to LL*, HL, LH and HH, set it to selected color channel to get water mar ked image WI.

B. Watermark Extraction Process

The extraction process is divided into following steps and is briefly described as given below:

1. Select color channel and apply DWT to WI to get LL*, HL, LH and HH.
2. Apply DWT to WI to get LL_LL, LL_HL, LL_LH and LL_HH*
3. Select LL_HH* band and divide it into 4X4 square blocks.
4. Apply DCT to each block of sub band LL_HH*, select first DCT values and get matrix A.
5. Apply SVD to A, $A= WU^*WS^*WV^T$ and obtain WU,WS,WV
6. Obtain SW=(S-WS) /Į.
7. Obtain $EW= W\_U^*SW^*W\_V^T$

Proposed Algorithm Ii

In this algorithm first level decomposition of wavelet is applied to cover image then LL band is selected for second level decomposition and its HH band is selected. Now DCT is applied to this band and get DCT coefficient matrix. SVD is applied on this DCT coefficient matrix. Watermark image is decomposed at first level and HH band is selected. DCT is applied to this HH band and we get DCT coefficients of watermark then SVD is applied. Singular value of cover image DCT coefficients is modified with singular value of watermark. Perform inverse transform and we get watermark image.

A. Watermark embedding process

The embedding process is divided into following steps and is briefly described as given below:

1. Let OI be the Original color image of size N x N.
2. Select Color Component any one among R,G,B(1,2,3). Suppose for Red color select (:,:,1) from original image.
3. Apply DWT to decompose it into four N/2 x N/2 sub-bands LL , HL , LH and HH .
4. Select LL band and Apply DWT to decompose it into four N/4 x N/4 sub-bands LL_LL , LL_HL , LL_LH and LL_HH .
5. Select LL_HH band and apply DCT to it and get DCT coefficient matrix B.
6. Apply SVD to B, B=U*S*VT, and obtain U, S and V.
7. Let OW of size N/2 x N/2 to represent watermark. Apply DWT to decompose it into four N/4 x N/4 sub-bands WLL ,

ISSN: 2277-9655
Impact Factor: 1.852

WHL , WLH and WHH .

8. Select WHH band and apply DCT to it and get DCT coefficient matrix D.
9. Apply SVD to D, D=U1*S1*V1T, and obtain U1, S1 and V1.
10. Modify S with watermark such that S2=S + Ị * S1
11. Obtain B* using B*= U*S2*VT.
12. Apply inverse DCT to B* to produce LL_HH*.
13. Apply inverse DWT to LL_LL, LL_HL, LL_LH and LL_HH* to get LL*.
14. Apply inverse DWT to LL*, HL, LH and HH to get watermarked image color name WI for selected color component.
15. Set value of that component to Original color image.
16. Get color watermarked image WI.

B. Watermark Extraction Process

The extraction process is divided into following steps and is briefly described as given below:

1. Selected watermarked image color component.
2. Apply DWT to WI to get LL*, HL, LH and HH.
3. Apply DWT to WI to get LL_LL, LL_HL, LL_LH and LL_HH *
4. Select LL_HH* band and Apply DCT to sub band HH* and get matrix A.
5. Apply SVD to A, A= WU*WS*WVT and obtain WU,WS,WV
6. Obtain Sr=(S-WS) /Ị.
7. Obtain Wr= U1*Sr*V1T
8. Apply inverse DCT to Wr and get W.
9. Apply inverse DWT to LL, HL, LH and W and get extracted watermark EW.

Evaluation Parameters

The PSNR and NCC are used as evaluation parameter.

Peak Signal to Noise Ratio (PSNR), is an engineering term for the ratio between the maxi mum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

To check the efficiency of proposed algorithm different size of images are considered for numerical simulation. It is tested using the tool MATLAB 7.8.0. Here results are given using 512 x 512 color image “LENA”, ”PEPPER”, ”MANDRIL”, ”KIDS” and HUNNAR” as cover image and 32 x 32 color football as watermark in algorithm one and 256x256 color Lena and Hunnar as watermark in second algorithm.

Fig. 1. Image Database

Fig. 2. Original color image, watermark, watermarked image and extracted watermark for algorithm I.

Fig. 3. Original color image, watermark, watermarked image and extracted watermark for algorithm II.

PSNR and NCC value and elapsed time for proposed algorithm I and II are shown in Table 1 and Table 2 respectively.

Table 3 and Table 4 shows results of proposed algorithm I and II respectively after various attacks on watermarked image.

ISSN: 2277-9655
Impact Factor: 1.852

TABLE 1:
Result of existing DWT+DCT+SVD based scheme

-	Results of some existing DWT+DCT+SVD based method		
	Ben Wang[1]	*S S Bedi[4*	*S. Murty[9]*
Without attack	0.9473		
Jpeg	0.9439	9887	0.9982
Cropping	0.8286	0.842	0.999
Rotation	0.8819	0.518	0.9597
Gaussian noise	0.9502		0.9628
Low pass filter	0.9335	0.8849	
Contrast adjustment	0.9666		0.9869
Gamma Correction (less than 1- for brighter)			0.9998
Salt n Pepper	0.9312		
Sharpened			0.8297

TABLE 2:
Result of proposed algorithm I with NCC values for different attacks, PSNR and elapsed time for watermark embedding.

Result of Algorithm I	Image database				
	lena	*Pepper*	*mandril*	*kids*	*hunnar*
Elapsed Time	1.5132	1.248	1.2636	1.2792	1.2948
PSNR	53.3126	53.1406	53.3126	53.3126	53.3126
NCC without attack	1	1	1	1	1
	NCC	NCC	NCC	NCC	NCC
JPEG 50%	0.2915	0.6272	0.2609	0.6748	0.391
Crop	0.9756	0.596	0.9101	0.8383	0.9682
Rotation 45	0.9168	0.58	0.0962	0.0395	0.2442
Gaussian noise	0.9481	0.987	0.9673	0.9546	0.9216
Low Pass filter 3x3	-3.621	-1.0942	-6.6589	-8.5204	0.0651
Contrast Adjust	1	1	1	1	1
Gamma Correction 0.8	0.9417	0.9932	0.9424	0.9934	0.9734
Gamma Correction 1.2	0.8836	0.9191	0.9569	0.9752	0.9538
Salt n Pepper	0.859	0.9467	0.8298	0.8328	0.8075
Sharpen	0.1701	0.1128	0.1861	0.192	0.2229

Table 3

Result of Algorithm II	Image Database				
	lena	pepper	mandril	kids	hunnar
Elapsed Time	0.7176	0.9048	0.7644	0.702	0.9984
PSNR	50.8039	50.4547	50.2827	50.4547	50.4547
NCC without attack	0.9994	0.9991	0.9991	0.9991	0.9991
	NCC	NCC	NCC	NCC	NCC
JPEG 20%	0.9995	0.9995	0.9997	0.9994	0.9992
Crop	0.9994	0.9992	0.9995	0.9991	0.9991
Rotation 45	0.9991	0.9988	0.9995	0.9988	0.9983
Gaussian noise	0.9895	0.985	0.9878	0.9847	0.9849
Low Pass filter 3x3	0.9999	1	0.9981	1	0.9998
Contrast Adjust	0.9994	0.9991	0.9991	0.9991	0.9991
Gamma Correction	0.9994	0.999	0.9993	0.9991	0.9994
Gamma Correction	0.9993	0.9991	0.999	0.9991	0.999
Salt n Pepper	0.9961	0.994	0.9961	0.9939	0.9818
Sharpen	0.9963	0.9952	0.9879	0.9956	0.9963

Conclusions

As per experimental results, proposed algorithm I gives NCC value 1 for no attack. PSNR values for all five i mages are higher in algorithm I than algorithm II. So imperceptibility in algorithm I is better than algorithm II. Various attacks are performed and experiment result shows that robustness of algorithm II is higher than algorithm I. Algorithm II gives best results in comparison with existing techniques results. Algorithm I is not robust again jpeg as we embed watermark in DC values of HH band of LL band after second level decomposition. Also for low pass filter this method does not give good results. Algorithm II gives quiet better results in all listed attacks. It gives good NCC value for jpeg up to 20% quality factor. In both algorithm extraction of watermark is done using original cover image so both are nonblind scheme. In future will try to develop algorithm which do not depends on original cover i mage at the time of extraction using Discrete transforms.

References

[1] Ben Wang , Jinkou Ding , Qiaoyan Wen , Xin Liao , Cuixiang Liu "An Image Watermarking Algorithm Based On DWT DC T And SVD", Proceedings of IC-NIDC2009, 978-1-4244-4900-2/09/$25.00©2009 IEEE.pp.1034-1038.

[2] V.Santhi and Dr. Arunkumar Thangavelu "DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition", International Journal of Computer and Electrical Engineering, Vol.3, No.1, February, 2011. 1793-8163.

[3] K A Navas, Mathews Cheriyan Ajay, M Lekshmi, Tampy S Archana, M Sasikumar "DWT-DC T-SVD Based Watermarking", 3rd International Conference on Communication Systems Software and Middleware and Workshops COMSWARE 08 (2008).

[4] S S Bedi, Ashwani Kumar, and P iyush Kapoor "Robust Secure SVD Based DC T – DWT Oriented Watermarking Technique for Image Authentication", International Conference on IT to Celebrate S. Charmonman' s 72nd Birthday, March 2009, Thailand,pp 46.1-46.7.

[5] R. Mehul and R. Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proceedings of IEEE Region10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 2003

[6] R. Eswaraiah, Sai Alekhya Edara, E. Sreenivasa Reddy "Color Image Watermarking Scheme using DWT and DC T Coefficients of R, G and B Color Components", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.8, July 2012.

[7] V.Santhi, N. Rekha , S.Tharini "A Hybrid Block Based Watermarking Algorithm using DWT-DCT-SVD Techniques for Color Images", proceed ings of International Conference on Computing, Communication and Networking, 2008. ICCCn 2008.

[8] Fangjun Huang, Zhi-Hong Guan "A hybrid SVD-DCT watermarking method based on LPSNR", Pattern Recognition Letters 25 (2004) 1769–1775,© 2004 Elsevier

[9] Satyanarayana Murty. P, Dr. P. Rajesh Kumar "A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DC T-SVD Technique", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.10, October 2010

[10] Emir Ganic, Ahmet M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All F requencies", MM&SEC'04, Magdeburg, Germany, Copyright 2004 ACM

[11] F.Hartung and M. K utter, "Multimedia Watermarking Techniques," in proc. of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[12] Ali Al-Haj "Combined DWT-DCT Digital Image Watermarking," Journal of computer science 3 (9),740-746, ISSN, 2007.

[13] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding,", IBM S ystems Journal, vol.35, no. 3&4, pp.313-336, 1996

[14] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon,"Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12,pp. 1673-1687, December 1997.

[15] J. J. K. 0 Ruanaidh, W. J. Dowling and F. M. Boland, "Watermarking digital images for copyright protection," IEEE Proceed ings - Vision, Image and S ignal Processing, vol. 143, no. 4, pp. 250-256, August 1996.