Sumit Kumar Prajapati, AmitNaik, AnjulataYadav/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.991-997

Robust Digital Watermarking using DWT-DCT-SVD

Sumit Kumar Prajapati*, Amit Naik, Anjulata Yadav*****
* (Department of Electronics and Telecommunication, SGSITS, Indore (M.P.), India)
** (Department of Electronics and Telecommunication, SGSITS, Indore (M.P.), India)
*** (Department of Electronics and Telecommunication, SGSITS, Indore (M.P.), India)

Abstract: With the rapid growth of the Internet and the development of digital multimedia technologies, illegal copying, tampering, modifying and copyright protection have become very important issues. Hence, there is strong need of developing the techniques to face all these problems [1, 7]. Digital watermarking emerged as a solution for protecting the multimedia data.

In this paper, we propose a method of nonblind transform domain watermarking based on DWT-DCT-SVD. The DCT coefficients of the DWT coefficients are used to embed the watermarking information.The parameters used to test the robustness of the proposed algorithm are the Peak Signal to Noise Ratio (PSNR) and Weighted Peak Signal to Noise Ratio (WPSNR) and correlation coefficient (ρ).Also, Robustness of proposed algorithm is tested for various attacks including salt and pepper noise and Gaussian noise, salt & pepper, sharpened and contrast adjustment. The experimental results show that the proposed method is more robust against different kinds of attacks and the watermarked image has good transparency.

***Key Words*:**Watermark structure, SVD, DCT, DWT, Embedding and Extracting Algorithm.

I.INTRODUCTION

Digital Watermarking is the process of hiding or embedding an imperceptible signal (data) into the given signal (data). The imperceptible signal is called watermark and the given signal is called cover work. This cover work can be an image, audio or a video file.This embedded data can later be extracted from the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction or detection algorithm. Watermarks can be embedded in the pixel domain or a transform domain [3].Digital watermarking is a technique designed to secure a message by hiding that message within another object so that it can be kept secret from everyone except the intended recipient.

In visible digital watermarking, information is visible in picture or video. Typically, the is text or logo which identifies the owner of the media. In invisible digital watermarking, information is added as digital data to audio, picture or video but it can't be perceived as such. It may be a form of steganography where a party communicates a secret message embedded in the digital signal.

II. TECHNIQUES

According to the domain in which watermark is inserted, these techniques are divided into two broad categories-:

- Spatial Domain method
- Frequency Domain method

Embedding the watermark into spatial domain component of the original is straight forward method. LSB scheme is one of the example from spatial domain which modifies lower order bits of cover image to embed the watermark. It has the advantage of low complexity and easy implementation but problem with this scheme is low security, because it is possible to remove the watermarked image easily by setting all LSBs or pixels to zero.

Frequency domain schemes have become popular watermarking algorithms based on frequency domain. These are more persistent to general image processing than spatial domain algorithm. DFT, DCT and DWT are some algorithms from this category. In frequency domain, the watermark is embedded into transform coefficients of host image after applying DFT, DCT and DWT transform. As compared to spatial domain watermarking methods, frequency domain watermarking methods are more complex and have high robustness against various attacks.

In recent years, many watermarking schemes have been developed using these popular transforms. In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be less resilient to attacks. In image watermarking, two distinct approaches have been used to represent the watermark.

An important criterion for classifying is the type of information needed by the detector-:

- Non-blind schemes: Both original image and secret key for watermark embedding.
- Semi-blind schemes: The secret key and the watermark bit sequence.
- Blind schemes: Only the secret key.

The drawback with blind and semi-blind schemes is that when watermarked image is seriously destroyed, watermark detection will become very difficult. So, non-blind extracting watermark can only be detected by those who have a copy of original image.

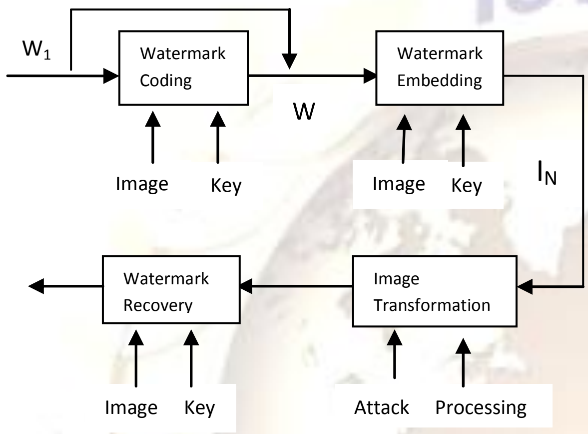

Fig.1 Digital image watermarking framework

III. REQUIREMENTS

There are three main requirements of Digital Watermarking. They are:

- *Transparency or Fidelity*:

The digital watermark should not affect the quality of the original image after it is watermarked. Transparency or Fidelity is defined as "Perceptual similarity between original and watermarked versions of the cover work".

- *Robustness :*

Robustness is the ability of a system to cope with errors during execution.

- *Capacity or Data Payload :*

This property describes how much data should be embedded as a watermark to successfully detect during execution.

IV. DIGITAL WATERMARKINGAPPLICATIONS

- *Copyright Protection*
- *Content Identification and Management :*

The speed with which digital content travels across the internet provides new opportunities for both the content creators and consumers if the contents can quickly and easily be identified and managed.

- *Communication of Ownership and Copyrights :*

Digital content continues to proliferate as today's consumers seek information and entertainment on their computers, mobile phones and some other digital devices. In our cyber culture, digital has become a primary means of communication and expression.

- *Document and Image Security :*

In today's corporate world, images and documents travel widely and rapidly in multiple manifestations, through email and across the Internet. Controlling and protecting sensitive or confidential documents and images has become impossible. Corporations have very little visibility into exactly where their documents are being accessed or by whom.

- *Authentication of Content and Objects (includes government IDs) :*

The impact of counterfeiting is significant, both in terms of lost revenue for businesses and fraud to the consumer, which can even endanger citizens in the case of counterfeit pharmaceuticals. It is clearly a global problem that affects numerous industries, and the problem is growing.

Digital watermarking, when used as part of a linked and layered security approach can provide a strong deterrence to counterfeiting and help to solve this costly and challenging problem. Implementation of the technology is relatively simple with minimal impact to most workflows.

V. SINGULAR VALUE DECOMPOSITION

In linear algebra, the singular value decomposition (SVD) is a factorization of a real or complex matrix, with several applications in signal processing [2]. The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square matrices. The basic idea behind SVD is taking high dimensional highly variable set of data points and reducing it to a lower dimensional space that exposes the substructure of the original data more clearly.

Suppose M is an m-by-n matrix. Then there exists a factorization for M of the form $M=U\Sigma V^T$ where, U is an m-by-m unitary matrix, a diagonal matrix Σ is m-by-n with non-negative numbers in descending order and V^T denotes the conjugate transpose of V, an n-by-n unitary matrix. Such a factorization is called a singular value decomposition of M.

A matrix is orthogonal if $U^T U = V^T V = I$

- The matrix V thus contains a set of orthonormal input vector directions for the matrix M.
- The matrix U thus contains a set of orthonormal output basis vector directions for the matrix M.
- The matrix Σ contains the singular values, which can be thought of as scalar gain controls by which each corresponding input is multiplied to give a corresponding output.

VI. DCT DOMAINWATERMARKING

Discrete Cosine Transform (DCT) method is used to convert time domain signal into frequency domain signal. Using DCT, an image is easily split into pseudo frequency bands and in this work watermark is inserted into middle band frequencies because as we discussed in all frequency domain watermarking schemes, there is a conflict between robustness and transparency.

A DCT is a Fourier related transform similar to Discrete Fourier Transform (DFT) but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry(since Fourier transform of real and even function is real and even).

VII. DWTDOMAIN WATERMARKING

Wavelettransformhasbeenwidelystudiedinsignalprocessingingeneralandimagecompressioninparticular.Here DWT2 (Two dimensional Discrete Wavelet Transform) method is used to decompose the image into four sub bands namely LL, LH, HL & HH.

LL-Low frequency band

LH-Horizontal high frequency band

HL-Vertical high frequency band

HH-Diagonal high frequency band

Wavelet coding schemes are especially suitable for applications where scalability and tolerable degradation are important.

LL_1	HL_1
LH_1	HH_1

Fig.2 Single level Decomposition using DWT

- *CharacteristicsofDWT*

1) Thewavelettransformdecomposestheimageintothree spatialdirectionsi.e.horizontal,verticalanddiagonal.Hencewaveletsreflecttheanisotropicpropertiesof HVS moreprecisely.
2) Watermarkdetectionatlowerresolutionsiscomputationally effectivebecauseateverysuccessiveresolutionlevel therearefew frequencybandsinvolved.
3) As LL band contains largest wavelet coefficients, scale factor is chosen accordingly up to 0.05 for LL and 0.005 for other bands. For this pair of values, there is no degradation in watermarked image.
4) High resolution sub bands helpstoeasily locateedgeandtextures patternsinanimage [6].

VIII. DCT-SVD BASED WATERMARKING

Robustness, capacity and imperceptibility are the three important requirements of an efficient watermarking scheme. SVD based watermarking scheme has high imperceptibility. Although the SVD based scheme withstands certain attacks, it is not resistant to attacks like rotation, sharpening etc. Also SVD based technique has only limited capacity [4]. These limitations have led to the development of a new scheme that clubs the properties of DCT and SVD. This particular algorithm proves to be better than ordinary DCT based watermarking and ordinary SVD based watermarking scheme.

IX. DWT-SVD BASED WATERMARKING

The above mentioned SVD-DCT scheme has enormous capacity because data embedding is possible in all the sub-bands. Watermark was found to be resistant to all sorts of attacks except rotation and achieved good imperceptibility. Disadvantage is that the embedding and the recovery are time consuming process because the zigzag scanning to map the coefficients into four quadrants based on the frequency. Alternatively if we apply DWT we get the four frequency sub-bands directly namely; approximation, horizontal, vertical and diagonal bands. So the time consumption will be greatly reduced [15]. Also, SVD is a very convenient tool for watermarking in the DWT domain.

X.DWT-DCT-SVDBASED WATERMARKING

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the three high frequency sub bands of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity.

. The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility or fidelity, robustness and good capacity. Also, the method is robust against different kinds of mentioned attacks. This method can be used for authentication and data hiding purposes.

XI. WATERMARK EMBEDDING ALGORITHM

Let '*A*' be the cover image. Apply DWT to decompose the image into four sub-bands LL, HL, LH and HH. Take any of these four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as $B = U_B\Sigma\ B\ _BV\ B\ _B^T$ where U_B and V_B^T are the orthonormal unitary matrices of *B*. The term Σ_B constitutes the singular values of the matrix of *B*.

Let '*W*' represent the watermark. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*S*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*S*' can then bewritten as $S = U_S\Sigma_S V_S^T$ where U_S andV_S^T are the orthonormal unitary matrices of *S*. The term Σ_S constitute the singularvalues of the matrix *S*. Modify the singular values of *B* using singular values of *S*. Then perform IDCT followed by IDWT to obtain the watermarked image. The four sets of DWT coefficients can be used to embed four different visual watermarks or the same watermark.

XII. WATERMARK RECOVERY ALGORITHM

Let 'A' be the cover image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as $B = U_B\Sigma_B V_B^T$ where U_B and V_B^T are the orthonormal unitary matrices of *B*. Term Σ_B constitutes the singular values of the matrix of *B*.

Let 'W*' be the watermarked image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*A**' denote the matrix obtained after applying DCT. Now *A** acts as the host image. Apply SVD so that '*B*' can then bewritten as $B = U_{A*}\Sigma_{A*}V_{A*}^T$ where U_{A*} and V_{A*}^T are the orthonormal unitary matrices of *A**. Term Σ_{A*} constitutes thesingular values of the matrix of *A**. Watermark is extracted by subtracting the singular values obtained above.

XIII. PARAMETERS TO EVALUATE

- *Peak Signal to Noise Ratio*

ThePSNRiscommonlyusedasameasureofquality ofreconstruction oflossycompression.Peaksignal-to-noiseratio(PSNR) isaqualitativemeasurebased onthemean-squareerrorof the reconstructedimage. Ifthereconstructedimageisclosetothe original image,thenMSEissmallandPSNRtakesalarge value.PSNRisdimensionless andisexpressedindB.

For N×M pixels image with pixel luminance value ranging from zero(black) to Lmax(white), PSNRis definedasfollow:

$$PSNR = 10\log\left(\frac{\mathrm{Lmax}^2}{\mathrm{MSE}}\right)$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}.\sum_{j=1}^{N}[\mathrm{y(i,j)} - \mathrm{x(i,j)}]^2$$

Where y and x are respective luminance values of original and watermarked image.Lmax is maximum possible pixel value of image. When pixels are represented using 8-bits per sample then Lmax is 255.

- *Weighted Peak Signal to Noise Ratio*

TheweightedPSNR(WPSNR) hasbeendefined asan extensionofthetraditional PSNR.Itweightseach of thetermof PSNRbylocalactivity factor(linkedtothelocal variance).The PSNR metric does not take into account image properties such as flat and textured regions. The watermark is embedding into textured regions and into edges, so the PSNR is inadequate to measure image quality in this case. The solution of this problem is using weighted PSNR.NVF characterizes the local image properties and identifies texture and edge regions. This allows us to determine the optimal watermark location and strength for watermark embedding stage.

$$WPSNR = 10log\frac{(\mathrm{Lmax}^2)}{(\mathrm{MSE} * \mathrm{NVF})2}$$

Where,$NVF = \frac{1}{(1+\theta\sigma_x^2(i,j)}$

$$\theta = \frac{D}{\sigma_{xmax}^2}$$

Where σ_{xmax}^2 is maximum local variance of a given image and D ∈ [50,150] is a determined parameter

- *Correlation Coefficient* (ρ)

Comparability of extracted watermark with the original watermark is quantitatively analyzed by using correlation coefficient. Value of ρ is between 0 and 1. The bigger the value of ρ, better is the robustness of watermark.

$$\rho(W,\bar{W}) = \frac{\sum_{i=1}^{r} W(i)\bar{W}(i)}{\sqrt{\sum_{i=1}^{r} \bar{W}^2(i)}\ \sqrt{\sum_{i=1}^{r} W^2(i)}}$$

whereW is the singular values of original watermark, $\bar{W}$ is the extracted singular values and r=max(M_1, N_1).

XIV. RESULTS

- *Figures:*

Fig.3Original Image

Fig.4Watermark

Fig.5Watermarked Image without attack

Fig.6Extracted Watermark

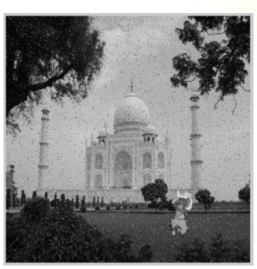

Fig.7Watermarked Image after Salt & Pepper Attack

Fig.8 Extracted Watermark

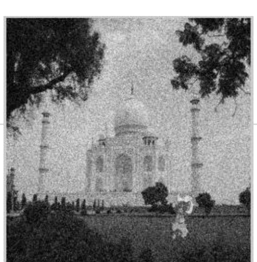

Fig.9 Watermarked Image afterGaussian attack

Fig.10 ExtractedWatermark

Fig.11 Watermarked Image after Sharpened attack

Fig.12 ExtractedWatermark

Fig.13 Watermarked Image afterContrast Adjustment

Fig.14Extracted Watermark

Figures show that the watermarked image and extracted watermark is robust against different kind of attacks. Also, the method offers better capacity and imperceptibility.

- *Tables:*

PSNR(dB)	MSE	ϱ	WPSNR(dB)
30.1776	62.4189	0.99987	33.0624

Table.1 Values of parameters between original and extracted watermark without attack using DWT-SVD method.

	PSNR	MSE	ϱ	WPSNR

	(dB)			(dB)
Salt and Pepper	7.8592	10645479.5	0.0092791	22.0788
Gaussian Noise	7.8561	10652923.9	0.0092719	22.0757
Sharpened	10.2126	6191824	0.57909	32.1305
Contrast Adjustme-nt	7.8472	10674908.9	0.010936	22.0767

Table.2 Values of parameters between original and extracted watermark with different attacks using DWT-SVD method.

PSNR(dB)	MSE	ϱ	WPSNR(dB)
52.3295	0.38031	0.99996	80.2034

Table.3 Values of parameters between original and extracted watermark without attack using DWT-DCT-SVD method.

	PSNR(dB)	MSE	ϱ	WPSNR(dB)
Salt and Pepper	47.3899	1.186	0.99987	75.3853
Gaussian Noise	43.1322	3.1613	0.99966	71.1477
Sharpened	41.3842	4.7279	0.99949	70.5133
Contrast Adjustment	46.3421	1.5096	0.99984	74.8932

Table.4 Values of parameters between original and extracted watermark with different attacks using DWT-DCT-SVD method.

Tables show the comparison between earlier DWT-SVD method and our DWT-DCT-SVD.Higher the value of PSNR, it is hard to be aware of the differences with the cover image by human eye system. When watermark is embedded in textured region and into edges, WPSNR is adequate to calculate. Value of WPSNR will be slightly higher than PSNR to reflect the fact that human eye will have less sensitivity to modifications in textured areas than in smooth areas. Also, value of correlation coefficient is close to 1 which is required. The bigger the value of correlation coefficient, better is the robustness of watermark.

XV. CONCLUSION AND FUTURE WORK

A cascading approach of watermarking based on DWT-DCT-SVD is suggested. The DCT-SVD based method is very time consuming because it offers better capacity and imperceptibility. DWT-SVD method is found to be similar to the DCT-SVD scheme except that the process was fast. The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility or fidelity, robustness and good capacity.Also, the method is robust against different kinds of mentioned attacks. This method can be used for authentication and data hiding purposes.

The future work includes the extension ofthis technique to other category and formats of images, for example, color images and DICOM images.

REFERENCES

[1] W.H.Lin,Y.R.Wang,S.J.Horng,T.W.Kao ,andY.Pan,"Ablind watermarkingmethodusing maximumwaveletcoefficient quantization,"Journal ofExpert SystemswithApplications,vol. 36,pp.11509-11516,2009.

[2] V. Gorodetski, L. J. Ipopyack,and V.Samoilov, "SVD-based approachtotransparentembeddingdataintodigitalimages," inProc. Int.Workshop,MMM-ACNS,St.Petersburg,Russia,2001,pp.263–274.

[3] Cox, IJ,Miller,ML &Bloom,JA2002,Digital Watermarking, MorganKaufmannPublisher,San Francisco,CA,USA.

[4] I.JCox,J.Kalian,F.T.Leighton,andT.Shamoon,“Securespread spectrumwatermarkingformultimedia”inIEEE Transactionson ImageProcessing,vol.6,no.12,Dec.1997,pp:1673-1687.

[5] Kundur D. Hatzinakos,“DigitalWatermarking using MultiresolutionWavelet Decomposition”, Proc.IEEEInt. Conf.On Acoustics,SpeechandSignalProcessing,Seattle, Washington,vol.5, pp.2969-2972,May1998.

[6] V.M. Potdar, S. Han and E. Chang, A survey of digital image watermarking techniques, in: Proceedings of the IEEE 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August 2005, pp. 709-716.

[7]Lu,C.S., Huang,S.-K.,Sze,C.-J., Liao, H.-Y.,"Anewwatermarkingtechnique formultimediaprotection,"inMultimediaImage

andVideoProcessing,L.Guan,S.-Y. Kung,and J.Larsen,Eds.Boca Raton,FL: CRC,2001,pp.507--530.

[8] Ganic,E.,Dexter,S.D.,Eskicioglu,A.M., “Embedding Multiple WatermarksintheDFTDomainUsingLow andHighFrequency Bands”IS&T/SPIE’s 17thAnnualSymposium on ElectronicImaging, Security, Steganography,andWatermarkingof MultimediaContents VIIConference,SanJose,CA,January17–20,2005.

[9] Fotopoulos, V.,Skodras, A.N.,"ASub bandDCT Approachto Image Watermarking,"inProceedingsofX EuropeanSignalProcessing Conference, Tampere,Finland,September 4-8,2000.

[10] Choi,Y.,Aizawa,K.,“DigitalWatermark ingTechnique usingBlock CorrelationofDCT Coefficients”inElectronicsandCommunica-tions, Japan,Part 2,vol.85,no.9,2002

[11] Suhail,M.,A.,Obaidat,M.,s.,“DigitalWa termarkingBasedDCT andJPEGModel”,inIEEE TransactionsonInstrumentationand Measurement,Vol.52,No.5,Oct.2003.

[12] Tao,B.,Dickinson,B.,“AdaptiveWaterma rkinginDCTDomain”,in Proc.IEEE International ConferenceonAcoustics,Speech, and SignalProcessing,ICASSP'97,1997,Vol.4,pp.198 5-2988.

[13] Kundur.D., Hatzinakos,D.,“Digital Watermarkinguses MultiresolutionWavelet Decomposition”,inProc.IEEEInt.Conf.On Acoustics,SpeechandSignal Processing,Seattle,Washington, vol.5, pp.2969-2972,May1998.

[14] Tao,P&Eskicioglu,AM2004,'ARobustM ultipleWatermarking SchemeintheDiscreteWaveletTransformDomain', inSymposium onInternetMultimediaManagement Systems V,Philadelphia,PA.

[15] Ganic,E.,Eskicioglu,A.M.,“Robustdigita lwatermarking:Robust DWT-SVDdomainimagewatermarking:embedding datain all frequencies”,Proceedingsofthe 2004multimediaand security workshoponMultimediaandSecurity,September2 004,pp.166–174.

Author’s Profile

SUMIT KUMAR PRAJAPATI

He received his Bachelor of Technology degree in Electronics and Communication Engineering from Malwa Institue of Technology. Indore(M.P.)-India in 2009 with Honors .He is currently pursuing Masters of Engineering degree in Electronics and Telecommunication from S.G.S.I.T.S. Indore(M.P.)-India.

AMIT NAIK

He is working as ASSISTANT PROFESSOR in SGSITS, Indore. He received Bachelor of Engineering in 2003 in Electronics and Telecoms from GEC, Ujjain (M.P.), INDIA and masters of technology in 2009 in Microelectronics & VLSI design from IIT, BOMBAY, India.

ANJULATA YADAV

She is working as ASSOCIATE PROFESSOR in SGSITS, Indore. She received Bachelor of Engineering in 1996 in Electronics from GEC, Ujjain (M.P.), INDIA, and masters of engineering in 2002 in Digital Techniques & Instruments from S.G.S.I.T.S., Indore (M.P.), India.