# Hybrid Digital Image Watermarking using Contourlet Transform (CT), DCT and SVD

Venkateshwarlu Ananthaneni Research Scholar, Dept. of ECE Vignan University Guntur, AP-522 213, India wenkateswarlu@gmail.com

usharani.nsai@gmail.com

Usha Rani Nelakuditi Professor, Dept. of ECE Vignan University

Guntur, AP-522 213, India

#### Abstract

Role of watermarking is dramatically enhanced due to the emerging technologies like IoT, Data analysis, and automation in many sectors of identity. Due to these many devices are connected through internet and networking and large amounts of data is generated and transmitted. Here security of the data is very much needed. The algorithm used for the watermarking is to be robust against various processes (attacks) such as filtering, compression and cropping etc. To increase the robustness, in the paper a hybrid algorithm is proposed by combining three transforms such as Contourlet, Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD). Performance of Algorithm is evaluated by using similarity metrics such as NCC, MSE and PSNR

Keywords: Digital Image Processing, Discrete Wavelet Transform, Discrete Cosine Transform, Contourlet Transform, Hybrid Water Marking.

## 1. INTRODUCTION

Digital watermarking is an emerging area in computer science, digital signal processing and communications. It is intended by its developers as the solution to the problems of data copyright, content protection and ownership proof. Digital watermarking is the process of embedding a piece of information into the digital data (audio, image or video), which can be detected and extracted later to make an assertion about the data. Recently, several transforms are proposed to represent the image and watermark in a small number of coefficients. Hybrid watermarking is a method where more than one transform is used to generate image and watermark coefficients are more potential than a single transform method. Watermarking with single transform is robust or semi-fragile with limited and bounded. Hybrid watermarking with multiple transforms is a more robust and semi-fragile.

# 2. LITERATURE SURVEY

Watermarking can be implemented either in the time or frequency (transform) domain. Transform domain watermarking techniques apply some invertible transforms to the host image before embedding the watermark. Then the coefficients are modified to embed the watermark and finally the inverse transform is applied to obtain the watermarked image. The watermark embedded in the transform domain is irregularly distributed over the area and make more difficult for an attacker to extract or modify the watermark. The transforms commonly used for watermarking are hybrid Image Watermarking Methods are combining two or three transforms like DWT - DCT, DCT - SVD, DWT - SVD, DWT - DCT-SVD, Contourlet – DCT, and Contourlet – SVD ...etc. In this paper hybrid watermarking method combines three transforms such as Contourlet , DCT, and SVD are imperceptible and robust.

#### 2.1 Contourlet Transform (CT)

The Contourlet Transform is a geometrical transform, can efficiently detect image edges in all directions. It is widely used in various signal processing applications, including image watermarking. CT consists of two major parts, the Laplacian Pyramid (LP) and Directional Filter Bank (DFB) as shown in FIGURE1. The Laplacian Pyramid (LP) is constructed from a pair of filters known as Analysis and Synthesis filters as shown in FIGURE2(a) and (b) respectively. LP decomposition at

each level generates a low frequency subband image. The LP decomposes the image into octave radial-like frequency bands to detect the point discontinuities and differences between the original and the prediction, results in a band-pass image. These band pass images are fed into the DFB. CT used here is a combination of a Pyramidal and a Directional Filter Bank known as Pyramidal Directional Filter Bank (PDFB). The pyramidal filter and the directional filter both takes the ladder structure. Moreover the vector number of directional filter bank decomposition level at each pyramidal level i.e. from coarse to fine scale has been considered as four.



FIGURE 1: The Contourlet Transform.



(a) Decomposition



(b) Reconstruction

FIGURE 2: Single Level Pyramidal Decomposition and Reconstruction.

In Contourlet Transform, HF subband is created by subtracting the G-filtered LF subband from the original image. In this case the HF coefficients affect the LF coefficients, because of this characteristic

of LP, the Contourlet Transform is evidently different from the Wavelet Transform. In the Wavelet Transform, HF subband is created by filtering the original image with high-pass filter.

These characteristics of CT help in identifying image areas where the watermark can easily embedded. The dual set of ladder based filter bank structures help in obtaining sparse expansion of typical images having smooth contours. The point discontinuities are taken care of by the Pyramidal filter bank based on Laplacian, while the linking of these to the liner structures is achieved via the Directional Filter Bank (DFB). By considering these advantages of CT is used as one of the transform out of three transforms.

#### 2.2 Discrete Cosine Transform (DCT)

A DCT represents the input data points in the form of a sum of cosine functions that are oscillating at different frequencies and magnitudes. There are mainly two types of DCT: one dimensional (1-D) DCT and two dimensional (2-D) DCT. Since an image is represented as a two dimensional matrix, for this research work, high compaction 2-D DCT is considered

#### 2.3 Singular Value Decomposition (SVD):

Every real matrix *A* can be decomposed into a product of 3 matrices  $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{V}^{T}$ , where *U* and *V* are orthogonal matrices. The diagonal entries of D are called the singular values of *A*, the columns of *U* are called the left singular vectors of *A*, and the columns of *V* are called the right singular vectors of *A*. This decomposition is known as the *Singular Value Decomposition* (*SVD*) of *A*, and can be written as  $A = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + ... + \lambda_r U_r V_r^T$ 

where *r* is the rank of matrix *A*.

It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image . In SVD-based watermarking, a common approach is to apply SVD to the whole cover image, and modify all the singular values to embed the watermark data. An important property of this technique is that the largest of the modified singular values change very little for most types of attacks. This property has been explored and extended in this paper as the singular values of watermark are embedded in those of cover object. DSR is applied on singular values as they can enhance the distribution of luminance in each layer. Singular Value Decomposition is a kind of orthogonal transforms used for matrix diagonalization. An image can be viewed as a non-negative real matrix. Let *A* be an image, and its size be  $M \times N$ . The SVD of A can be described as follows:  $A = U D V^{T}$ 

A = [ <i>u</i> 1	u2	 	uN]	Γλ1	N	N	λR	
				L			λR	$\left  \begin{bmatrix} \vdots \\ vN \end{bmatrix} \right $

where *U* and *V* are two  $N \times N$  unitary orthogonal matrices that specify the geometry details of the cover image, and *D* is a  $N \times N$  diagonal matrix. The elements of *D* are nonnegative values in a descending order.

we know that an image can be interpreted as a summation of N eigenimage. The singular value  $\lambda$ i indicates the energy intensity in its corresponding eigen image.

# 3. IMPLEMENTATION OF HYBRID DIGITAL IMAGE WATERMARKING

Digital watermark is an embedded (hidden) marker in digital multimedia data by watermarking method, the marker is generally unobservable, which can be extracted by special detector. The basic idea for digital watermark is to use human's insensitive perceptual organs and redundancy in digital signal and embed secret information in digital products, such as image, audio frequency and video frequency in order to easily protect its copyright, and in addition, the embedded information survives after attacks so as to perform copyright authentication and protection. Digital watermark doesn't change the basic characteristic and value of the products. Watermarking system is consists of two parts, 1) watermark creation and embedding 2) watermark extraction. The following steps are used to implement the watermarking:

- Watermark embedding process
- Watermark Extraction process
- Performance Evaluation

#### 3.1. Watermark Embedding Process

Before embedding the watermark in to the original image it will be transformed into coefficients by applying CT, DCT, and SVD. Original image also transformed into coefficients and then both are applied to the embedding algorithm which is known as watermarked image, now inverse transforms are applied to obtain the spatial domain watermarked image as shown in FIGURE 3. Selection of the coefficients to which a watermark is embedded is based on a predefined threshold and the watermark is cast into coefficients whose absolute values are larger than the threshold.



FIGURE 3: Watermark Embedding process.

#### 3.2. Watermark Embedding Algorithm

- Step 1: Two level contourlet is applied to image and image is divided into nine sub-bands.
- Step 2: Sub-bands 2 and 3 of second level are selected for watermark insertion.
- Step 3: Apply DCT on each block.
- Step 4: Selected sub-bands are divided into  $N \times N$  blocks and the DCT of each block is computed. These blocks are denoted as  $block_i$ , i = 1, 2, ..., M and  $M \leq N_W$ , which  $N_W$  is the number of watermark bits. If dimensions of watermark logo are denoted as  $L_W$  and  $H_W$  then  $N_W = L_W \times H_W$ , is shown that the combination of CT and DCT can crease the quality of watermarked image, is shown that the combination of CT and DCT can increase the robustness of algorithm against both geometric and non-geometric attacks by comparing NC values.
- Step 5: If each element of watermark is denoted as  $W_j$ ,  $j = 1, 2, ..., N_w$ , Two uncorrelated pseudo-random sequences with zero mean are generated, one of them is used for embedding  $W_j = 0$  and the other one for  $W_j = 1$ , which denoted as  $PN_0$  and  $PN_1$  respectively.
- Step 6: Apply SVD on all blocks:  $O_i = U_{oi} \times S_{oi} \times V_{oi}^T$
- Step 7: Divide the watermark image into non-overlapping 16 × 16 blocks.
- Step 8: Apply SVD on all blocks say w, neural network having input  $O_i$  and output th, and normalization on each block of w using threshold th.
- Step 9: Modify the singular values of  $O_i: \overline{S} = S_{oi} + \alpha W$ , where  $\alpha$  is the watermark strength
- Step 10: To embed watermark into the produced blocks, the middle frequency coefficients of each block are selected. This selection is a tradeoff between robustness and imperceptibility of watermark.
- Step 11: Perform inverse SVD to get all the modified blocks
- Step 12: Perform inverse DCT on each modified block and then merge all the blocks to get the Watermarked image.
- Step 13: By Applying inverse DCT (IDCT) to each block after its mid-band coefficients have been modified, the CT of watermarked image is generated.
- Step 14: Finally the watermarked image can be produced by using inverse CT
- Step 15: Apply Inverse DCT and Inverse Contourlet Transform for reconstruction of watermarked image.

#### 3.3. Watermark Extraction Process

Watermark extraction process deals with the extraction of the watermark in the absence of the original image as shown in FIGURE 4. The aim of the watermark extraction algorithm is to obtain the reliable an estimate of the original watermark from the watermarked image. The extraction process is inverse of the watermark embedding process. One of the advantages of watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be extracted by certain mechanism even if the image has been further scaled or rotated.



FIGURE 4: Watermark Extraction process.

#### 3.4. Watermark Extraction Algorithm

The process of extracting the digital watermark is comparatively simpler and tedious process and which is explained as below:

- Step 1: Two level Contourlet is applied to the watermarked image and to the original image is divided into nine sub-bands.
- Step 2: Selected sub-bands are divided into  $N \times N$  blocks.
- Step 3: Take the watermarked image and partition the image into 16X16 blocks.
- Step 4: Apply DCT on each block. Two pseudo-random sequences PN0 and PN1 are regenerated by using same seeds as embedding stage. For each block in the selected sub-band, correlations between mid-band coefficients with PN0 and PN1 are calculated. If the correlation with the PN0 is higher than the correlation with PN1, the watermark bit will be considered as 0, otherwise it will be consideredas1.
- Step 5: Apply SVD on each block and Extract the singular values of the watermark
- Step 6: To extracting the watermark from the original image, the watermarked image is partitioned into non-overlapping 16 x 16 blocks. At first, SVD followed by DCT are applied on each block. Afterwards, the singular values of the watermark are extracted and inverse of SVD is performed to acquire the extracted watermark.
- Step 7: Perform inverse CT to get the extracted watermark and after watermark extraction, similarity between the original and extracted watermarks is computed.

#### 3.5. Performance Evaluation

An important way of evaluating watermarking algorithms is to compare the amount of distortion introduced into a host image by watermarking algorithm. In order to measure the quality of the image at the output of the decoder, Mean Square Error (MSE) and Peak to Signal to Noise Ratio (PSNR) are used .

## 3.5.1 Mean Square Error (MSE)

MSE is an estimator to gives a value which measures the how much it differs from the true value of the quantity being estimated. As a loss function, MSE is called squared error loss. MSE measures the average of the square of the 'error'. The error is the amount by which the estimator differs from the quantity to be estimated. A lower value for MSE means lesser error.

Mean Square Error (MSE) = 
$$\frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} [I(x, y) - I'(x, y)]^2$$
 (1)

M and N are the dimensions of the images.

#### 3.5.2 Peak Signal to Noise Ratio (PSNR)

The PSNR represents the distortion caused by the watermarking depends on the MSE. This factor evaluates the imperceptibility of the digital watermarking. In fact, a great distortion of the media indicates the presence of a watermarking. Because many signals have a very wide dynamic range, SNR or PSNR is usually expressed in terms of the logarithmic decibel scale as given in the Equation 2 and 3. The SNR or PSNR is most commonly used as a measure of quality of reconstructed image. There is an inverse relation between the MSE and SNR or PSNR values. Logically, a higher value of SNR or PSNR is a good because it means that the ratio of signal to noise is higher. Here, the signal is the original image and the noise is the error in reconstruction. So, find a compression scheme having a lower MSE and a high SNR or PSNR.

$$SNR = 10 \log_{10} \left\{ \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} I(x,y)^{2}}{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I'(x,y)]^{2}} \right\}$$
(2)

$$PSNR = 20 \log_{10} \left(\frac{255}{\sqrt{MSE}}\right) \tag{3}$$

I(x,y) is the Original image

l'(x,y) Approximation version (Decompressed image)

#### 3.5.3 Normalized Cross Correlation (NCC)

Normalized Cross Correlation is used to measure the correlation between the watermarked image and the original image. It is defined by the equation 4.

$$NCC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - \overline{I'(x,y)}] [I(x,y) - \overline{I'(x,y)}]}{\sqrt{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - \overline{I'(x,y)}]^2 \sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - \overline{I'(x,y)}]^2}}$$
(4)

I(x,y) is the Original image;  $\overline{I(x,y)}$  is the mean of the original image; I'(x,y) represent the watermarked image,  $\overline{I'(x,y)}$  is the mean of the original image having the range of 0 to 1.

#### 3.5.4 Similarity

Similarity is used to find at what range both the original watermark and Extracted watermark are similar to each other defined by equation 5.

$$Similarity = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} w(x,y) \times w'(x,y)}{\sum_{x=1}^{M} \sum_{y=1}^{N} [w'(x,y)]^2}$$
(5)

Where W(x, y) represent the original logo image, W'(x, y) represent the extracted logo image Similarity is having the value in between the 0 to 1.

#### 3.6. Details of data used for Watermarking

Watermark extraction algorithm for the simulation of proposed watermark embedding and extraction is appied on the images of size 512x512, A Lena image of size  $512 \times 512$  is used. The image is transformed through various transforms via wrapping and randomly generate M=262144 length watermark. As noted, the each parameter is set scale= [4,5], strength parameter  $\alpha = 0.7$ . A 512 × 512 logo image with the written letters of JNTU and each letter of size  $170 \times 170$  as a watermark image is used for embed in to the edge of original image. Edges have high frequency components compared with other locations. Common signal processing procedures such as noise addition, Lowpass filtering, Median filtering and Highpass filtering as well as geometrical attacks such as cropping is used to analyze the watermarked image. In addition, further experiments are performed to evaluate the robustness against more commonly used image processing attacks such as cropping, adding noise, low-pass filter, high-pass filter, DCT compression and JPEG2000 compression. In this paper a novel algorithm is proposed which combines three transforms in watermarking digital images. Normalized cross correlation and similarity based method is used to evaluate the effectiveness of the proposed method. Our preliminary results show that the method is robust against some important image processing attacks.

# 4. ATTACKS ON WATERMARKED IMAGE

Common signal processing procedures such as noise addition, Lowpass filtering, Median filtering and Highpass filtering as well as geometrical attacks such as cropping is used for the analysis of the watermarked image. In addition, we perform further experiments to evaluate for the robustness against more commonly used image processing attacks such as cropping, adding noise, lowpass filter, highpass filter DCT compression and JPEG2000 compression. In this paper we proposed a novel use of the combining of transforms in watermarking digital images. Normalized cross correlation and similarity based method are used to evaluate the effectiveness of the proposed method. Our preliminary results show that the method is robust against some important image processing attacks as shown in Figure 6.



DCT Compression	J T	<u>N</u> 	DCT Extracted Watermark
Block - Truncation Compression	J T		Block - Truncation Extracted Watermark

FIGURE 6: Simulation Results of watermarked image, attacked images with extracted watermarks

TABLE 3.1: Performance evaluation of Simulation Results of Hybrid Digital Image Wa	atermarking
using DWT-DCT-SVD Vs CT-DCT- SVD.	

Type of Method		Existing Methods				Proposed Method			
Types of Hybrid Transforms		DWT-DCT-SVD				CT-DCT-SVD			
Image	Dependable	Similarity	NCC	MSE	PSNR	Similarity	NCC	MSE	PSNR
after/before	Parameters				[dB]				[dB]
attacks									
Watermarked	Strength	0.99513	0.9991	6.8247	39.79	0.99804	0.9999	0.11146	57.6596
Image	Parameter () =		0				8		
	0.1								
Low-Pass	3 x 3 mask filter	0.81384	0.7496	27.634	33.7164	0.81549	0.9756	25.4035	34.0819
Filtering							4		
Median Filtering	3 x 3 mask filter	0.98557	0.9986	4.3349	41.761	0.98815	0.9994	1.2135	47.2905
			4				8		
High-Pass	3 x 3 mask filter	0.030443	0.2178	254.589	624.0724	0.029986	0.2190	254.598	24.0722
Filtering			3				8	5	
Pyramid	64 x 64 size	0.83958	0.9735	26.8899	33.8349	0.84008	0.9721	26.4633	33.9044
Compression			9				7		
DCT	64 x 64 size	0.78182	0.9664	37.2406	32.4206	0.78293	0.9649	36.6369	32.4916
Compression			5				1		
Block	64 x 64 size	1	1	0		1	1	0	
Truncation									
Compression									
JPEG2000	64 x 64 size	0.86523	0.9882	20.6965	34.9718	0.86466	0.9875	20.4444	35.025
Compression			4				7	8	
Cropping	64 x 64 size	0.539	0.3543	100.190	28.1225	0.55819	0.4236	96.874	28.2687
			9	7			1		
Gaussian Noise	Variance = 0.01	0.71412	0.9618	95.155	41.0085	0.71705	0.9604	2.02	45.0773
							6		

# 5. CONCLUSION

From the simulation results it is observed that high quality image i.e. Watermarked image with high PSNR is obtained by embedding the watermark high level decomposition. With the increase in the density of variance of Gaussian noise the amount of noise induced in to the image is increased and these affected the quality of image and modify the watermark embedded coefficient of the image. With the increase in density/variance of the noise the PSNR values decreases and the robustness of the watermark is affected, in spite of huge noise addition the recovered watermark is still highly recognizable. The watermarking algorithm sustains the cropping attack the watermark is highly recoverable even for the cropping block size of 256 x 256. We can say that even the image pass through different attacks such as Geometric, Adding noise, Filtering , the logo is get extracted perfectly. We can say that the embedding algorithm is robust. More over the logo is extracted if the location of embedded is known, so the embedding algorithm is secure. The image after watermarking is subjected to the low pass filtering and high pass filtering to remove the detailed coefficients. High pass filter removes the low frequency coefficients. Low pass filter is used to reduce the high frequency components. The watermarking algorithm sustains the compression attack; the watermark is highly recoverable even for the compression block size of M x N. We can say that even the image pass through different attacks such as Geometric, Adding noise, Filtering, the logo get extracted perfectly. We perform further experiments to evaluate the robustness against more commonly used image processing attacks such as JPEG2000 compression, and DCT Compression.

# 6. REFERENCES

- [1] S. Azizi, M. Mohrekesh and S. Samavi. "Hybrid image watermarking using local complexity variations." In *Electrical Engineering (ICEE), 2013 21st Iranian Conference on*, pp. 1-6. IEEE, 2013.
- [2] B. Fadaeenia and N. Zarei. "Hybrid DCT-CT Digital Image Adaptive Watermarking." In *DBKDA* 2011: The Third International Conference on Advances in Database, Knowledge, and Data Applications.pp. 47-53. IARIA, 2011.
- [3] A. Akter and M. A. Ullah. "Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm." In *Informatics, Electronics & Vision (ICIEV), 2014 International Conference on*, pp. 1-6. IEEE, 2014.
- [4] S. A. Kasmani and A. Naghsh-Nilchi. "A new robust digital image watermarking technique based on joint DWT-DCT transformation." In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2, pp. 539-544. IEEE, 2008.
- [5] A. Al-Haj. "A hybrid digital image watermarking algorithm." In *Innovations in Information Technology, 2007. IIT'07. 4th International Conference on*, pp. 690-694. IEEE, 2007.
- [6] F. Golshan and K. Mohammadi. "A hybrid intelligent SVD-based digital image watermarking." In Systems Engineering (ICSEng), 2011 21st International Conference on, pp. 137-141. IEEE, 2011.
- [7] Y. Chen, W. Yu and J. Feng. "A digital watermarking based on discrete fractional fourier transformation DWT and SVD." In *Control and Decision Conference (CCDC), 2012 24th Chinese*, pp. 1383-1386. IEEE, 2012.
- [8] C. C. Lai, C. F. Chan, C. S. Ouyang and H. F. Chiang. "A robust feature-based image watermarking scheme." In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS International Conference on, pp. 581-585. IEEE, 2013.
- [9] R. Chouhan, R. K. Jha, A. Chaturvedi, T. Yamasaki and K. Aizawa. "Robust watermark extraction using SVD-based dynamic stochastic resonance." In *Image Processing (ICIP), 2011* 18th IEEE International Conference on, pp. 2745-2748. IEEE, 2011.
- [10] A. Kaushik and K. Yadav. "An Enhanced and Hybrid Approach on Digital Watermarking." In Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on, pp. 463-466. IEEE, 2013.
- [11] A. Wang, J. Ding, Q. Wen, X. Liao and C. Liu. "An image watermarking algorithm based on DWT DCT and SVD." In *Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on*, pp. 1034-1038. IEEE, 2009.
- [12] Z. Li, K. H. Yap and B. Y. Lei. "A new blind robust image watermarking scheme in SVD-DCT composite domain." In *Image Processing (ICIP), 2011 18th IEEE International Conference on*, pp. 2757-2760. IEEE, 2011.
- [13] D. Singh, N. Choudhary and M. Agrawal. "Scrambled hybrid wavelet-singular domain digital image watermarking." In Software Engineering (CONSEG), 2012 CSI Sixth International Conference on, pp. 1-6. IEEE, 2012.
- [14] M. M. Dixit, P. K. Kulkarni, P. S. Somasagar and V. C. Angadi. "Variable scaling factor based invisible image watermarking using hybrid DWT—SVD compression—Decompression technique." In *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, pp. 1-4. IEEE, 2012.
- [15] B. Jagadeesh, S. S. Kumar and K. R. Rajeswari. "A genetic algorithm based oblivious image watermarking scheme using singular value decomposition (SVD)." In *Networks and Communications, 2009. NETCOM'09. First International Conference on*, pp. 224-229. IEEE, 2009.