International Journal of Research and Development in Applied Science and Engineering (IJRDASE)

Digital Image Watermarking With Composite Effects of SVD and Frequency Domain Data Processing

Azad Tripathi
M. Tech.-Software Engineering,
N.V.P.E.M.I., U.P.T.U., Lucknow, India
azadtripathi@gmail.com

Prateek Srivastava
Assistant Professor
Computer Science Department,
N.V.P.E.M.I., U.P.T.U., Lucknow, India
prateek.1809@gmail.com

***Abstract*- Image watermarking is a signal that is embedded in a image data permanently such that it can be extracted by dewater marking using some operations for checking the authenticity of data or user. The watermark is inseparable from the host image and it should be robust enough to resist any modifications along with preserving the image quality. In this way the watermarking helps in keeping intellectual properties accessible while being permanently water marked. In this paper we have focused on watermarking techniques and checked their robustness against environmental distortions during the storage and transmission of watermarked image. In this work we have applied a hybrid SVD-DCT-DWT watermarking approach in grey biomedical image watermarking to develop a robust algorithm against several image attack .We have also compared our algorithm with two different watermarking technique named as DCT-SVD, DWT-SVD.**

***Keywords*- De watermarking, DCT, DWT, SVD, Watermarking.**

1. Introduction

The Internet is an excellent sales and distribution channel for digital assets, but copyright compliance and content management can be a challenge. These days, digital images can be used everywhere – with or without consent. Images that are leaked or misused can hurt marketing efforts, brand image and, ultimately, sales. The possible implications of this situation include the unauthorized distribution of such material with the purpose of making illegal profit or otherwise damaging the legal owner. Inevitably the business world and the authorities have expressed great concern over this issue, and as a result, the scientific community has become extremely active trying to provide techniques for copyright protection of digital material.

One way to address this problem is Image Watermarking. It is the process of inserting hidden information in an image by introducing modifications of minimum perceptual disturbance. Robustness, perceptual transparency, capacity and blind watermarking are four essential factors to determine quality of watermarking scheme [1]. Image watermarking techniques can be divided into two groups in accordance with processing domain of host image. One is to modify the intensity value of the luminance in the spatial domain [2] and the other is to change the image coefficient in a frequency domain [3][4]. In recently, a transform called Singular Value Decomposition (SVD) was explored for watermarking [5][6]. Frequency domain techniques are used commonly because of their robustness to various types of attacks like JPEG compression, cropping, rotation, noise, blur etc. SVD-based watermarking algorithms are also very robust against these attacks. DWT has excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. DCT and SVD based watermarking techniques offer compression. Further Performance improvements in DWT-based digital image watermarking algorithms, DCT-based watermarking algorithms and SVD-based watermarking algorithms could be obtained by combining DWT, DCT and SVD. The idea of combining these transforms is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

In Singular Value Decomposition, singular values correspond to the luminance of the image (i.e. image brightness) and the corresponding singular vector specifies the intrinsic geometry properties of the image [2]. Many singular values have small values compared to the first singular value. If these small singular values are ignored in the reconstruction of the image, the quality of the reconstructed image will degrade only slightly. Slight variations of the singular values do not affect the visual perception of the image, i.e., singular values do have a good stability. Based on these properties of SVD, diagonal matrix containing singular values is mainly used to embed watermark. The DCT has special property that most of the visually significant information of the image is concentrated in low frequency coefficient of the DCT.

One of the main applications of watermarking is copyright protection. Information about the copyright owner is embedded into the data to prevent other people from claiming to be the legal owners of the data. The watermarks used for that purpose are supposed to be very robust against various attacks intended to eliminate the watermark.

Cryptographic attacks intend to break the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed deceptive watermarks. Brute-force search for the embedded secret information is one such technique. Another attack in this category is the so-called Oracle attack, which can be used to generate a non-watermarked signal when a watermark detector device is available. High computational complexity has restricted attackers from applying these attacks on watermarks.

2. Related Work:

In 2000, Chiou-Ting Hsu et. Al. (IEEE), [7] proposed their work related to image watermarking by wavelet decomposition. In this work, they stated that, digital watermarking has been increasingly recognized as a highly effective means of protecting the intellectual property rights associated with multimedia data. Based on the multi-resolution structures of wavelet decomposition, both, on a real field and binary field, a multi-resolution watermarking technique was proposed. Since the Human Visual System (HVS) inherently performs a multi-resolution structure, each decomposed layer of a binary watermark is embedded into the corresponding decomposed layer of a host image. Therefore, in case of attacks or progressive transmission, the coarser approximation of a watermark is preserved in the coarser version of an image. In a progressive transmission, adding higher frequency components, allows us to obtain higher resolution image, and, correspondingly, extract a higher resolution watermark. There experimental results demonstrated the robustness and validity of the watermarking process.

In 2005,Maha Sharkas et. Al. [8] (IEEE) proposed their work related to dual digital-image watermarking technique. In their work, they presented that image watermarking has become an important tool for intellectual property protection and authentication. In this work a watermarking technique was suggested that incorporated two watermarks in a host image for improved protection and robustness. A watermark, in form of a PN sequence (will be called the secondary watermark), was embedded in the wavelet domain of a primary watermark before being embedded in the host image. The technique has been tested using Lena image as a host and the camera man as the primary watermark. The embedded PN sequence was detectable through correlation among other five sequences where a PSNR of 44.1065 db was measured. Furthermore, to test the robustness of the technique, the watermarked image was exposed to four types of attacks, namely compression, low pass filtering, salt and pepper noise and luminance change. In all cases, the secondary watermark was easy to detect even when the primary one was severely distorted.

In 2006 Chih-Yang Lin et. Al [9] proposed their work related to robust image hiding method using wavelet technique. There work stated that a robust wavelet-based image hiding methods, that hide still images, E, inside a covered image, C, to establish a composite image, P, are presented. We can hide up to three full-size embedded images inside a cover image while maintaining the quality of the composite image. The embedded images retain easily recognizable when extracted. The embedded images can be extracted fairly completely even when lossy compression or cropping is applied to the composite image. The proposed method does not require the original cover image to extract the embedded image.

In 2007 Ibrahim Nasir et. Al (IEEE) [10] proposed their work related to a new robust watermarking scheme for color image in spatial domain. This work presented a new robust watermarking scheme for color image based on a block probability in spatial domain. A binary watermark image was permutated using sequence numbers generated by a secret key and Gray code, and then embedded four times in different positions by a secret key. Each bit of the binary encoded watermark was embedded by modifying the intensities of a non-overlapping block of 8*8 of the blue component of the host image. The extraction of the watermark was by comparing the intensities of a block of 8*8 of the watermarked and the original images and calculating the probability of detecting '0' or '1'. Tested by benchmark Stirmark 4.0, the experimental results showed that the proposed scheme was robust and secure against a wide range of image processing operations.

In 2007, Chin-Chen Chang et. Al. [11] presented there work related to an SVD oriented watermark embedding scheme with high qualities for the restored images. In this work, they stated that SVD-based watermarking scheme, which successfully embeds watermarks into images, and its hidden watermarks can resist various attacks. In this work, we further extended their idea so that the hidden watermarks can be removed to provide authorized users better image quality for later usage after the ownership of purchased images has been verified. To achieve our objective, we modified their embedding strategy, and the extra information required for later restoration is embedded into the least important non-zero coefficients of the S matrices in the image. Experimental results confirmed that our scheme not only provided good image quality of watermarked images but also successfully restored images with high restoration quality.

3. Methodology:

Discrete Wavelet Transform (DWT) is a multi-resolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic thought is to decompose the image to sub images with different space and frequency, then, the coefficient is processed.

The DWT can be implemented as a multistage transformation. An image is decomposed into four sub bands denoted LL, LH, HL, and HH at level 1 in the DWT domain, where LH, HL, and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients.

DCT – SVD

STEP 1:- Define block size = 8/4 (for DCT) and define multiplying factor a=10

STEP 2:- Read host image and water mark image (H, W).

STEP 3:-Calculate rows & columns of H and W and calculate no. Of blocks,
Block count = (rows * columns)/ (block size) 2

STEP 4:- Take 2D DCT of host image blocks cb (cb= DCT blocks of H)

STEP 5:- Apply SVD on DCT block [U, S, V] = svd(cb)

STEP 6:- Takes the block of W and mix them with the S component of DCT of host image.
STEP 7:- Perform SVD of sm. [U1, S1, V1] = svd(sm)
STEP 8:- Reconstruct the image from UV of DCT(host image) and S1 of mixed watermarking image.
CM= U*S1*V
STEP 9:- Perform rearranging of the blocks of CM to get the watermarked image.
STEP 10:- Add Noise to the watermarked image [WM]. To get [WM] noisy.

DE- WATERMARKING
STEP 1:- Break the [WM] in predefined blocks and apply 2D DCT on these blocks.
STEP2:- Apply SVD on DCT blocks.
[U, S, V]=svd(cb)
STEP3:- Break the watermarked image into the blocks (cbm) and apply SVD on these blocks.
[Um,Sm,Vm] = svd (cbm)
STEP 4:- Now perform reconstruction of extracted watermarked image by following eq:-
Sl =[U1*Sm*V]
Wbm= extracted watermarked block = (Sl - S)/a.
STEP5:- Arrange the blocks of Wbm to reconstruct the extracted watermarked image.

DWT-SVD
STEP1:- Define block size = 8/4 (for DCT) and define multiplying factor a=10
STEP 2:- Read host image and water mark image (H, W).
STEP 3:- Calculate rows & columns of H and W and calculate no. Of blocks,
Block count = (rows * columns)/(block size)2
STEP 4:- Take the DWT of host image to get [CA1, CH1, CV1, CD1] image component, representing A as Approximation, H as Horizontal details, V is vertical details and D are Diagonal details.
STEP 5:- Apply DCT on the blocks of [CD1] to get dct_block matrix.
STEP 6:- ADD the pixel intensity of water marked image to the dct vale of each dct_block.
Dcvalue|DCT_blockij = dc value|DCT_blockij+ a*Wij
STEP 7:- Reconstruct the diagonal component by taking inverse dct of each dct blocks and save as CD1w.
STEP 8:- Apply inverse dwt on [CA1, CH1, CV1 and CD1w] to generate watermarked image [Wm]
Watermarke dimage = dwt[CA1,CH1,CV1,CD1w].

DE-WATERMARKING
STEP 1:- Apply DWT on Wm [CAM1, CHM1, CVM1 & CDM1] =dwt (Wm)
STEP 2:- We can recover water marked image by following eqn-
Dct(CDM1) -> dct_blockw
Watermark_extracted = dct_blockw – dct_block/a=WME
STEP 3:- By re-arranging the WME pixels after each dctblock processing we can recover water Marked image.

DWT-DCT-SVD
STEP 1 to 6 same as DCT-SVD
STEP 7:- Collect all the DC values of the DCT matrices to rm a new matrix named as [DC]
STEP 8:- Perform the SVD of DC matrix.
[U1, S1, V1]=svd[DC]
STEP 9:- Mix the value of watermarked pixel to the S1 component.
Sm=S1+a (*W)
STEP 10:- Again perform the svd[Sm] as given below:
[U2, S2, V2]=svd[Sm]
STEP 11:- Mixed the S2 with (U1,V1) to regenerate pdated DC matrix by following eqn:-
DCM=U1*S2*V1
STEP 12:- Now perform inverse dct for dct_block updated with DCm,to obtain [CD1w].
STEP 13:- Arrange the DCT blocks and apply IDWT on [CA1, CH1, and CV1 & CD1w] to generate water Marked image Wm.
WM= idwt(CA1,CH1,CV1,CD1)

DE-WATERMARKING
STEP 1:- Take DWT of Wm as given below:-
[Cam1, CHm1, CVm1, CDm1]=dwt[Wm]
STEP 2:- Apply dct on CDm1 block.
dct[CDm1] -> dct_blockw
STEP 3:- Generate the DC value matrix from dct block W named as [DCW] and apply svd on this Matrix sing following eqn:
[Um,Sw,Vm]=svd[DCW]
STEP 4:- Combine U2 and V2 svd component with Sw as given below:-
E=U2*Sw*V2
STEP 5:- Generate extracted water marked image by following eqn:-
WME=E-S1/a.

4. Result and Discussion:
We have applied our DWT-DCT-SVD algorithm on host1 image (fig 1 (a)) to watermark the image wm1 (fig 1 (d)). host1 image obtained after applying DWT is shown in fig 1(b) . The image obtained after watermarking that is watermarked image is shown on fig 1 (c). Then no image attacks is apply on watermark image and it is directly Dewater marked and its extracted watermarked image is shown in fig 1(e)

Host Image

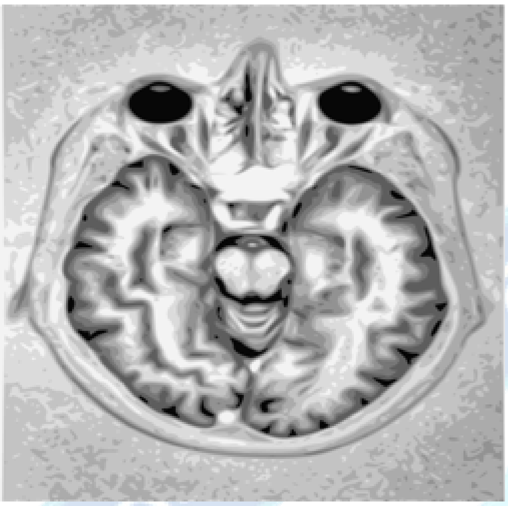

Fig. 1(a). Original Image.

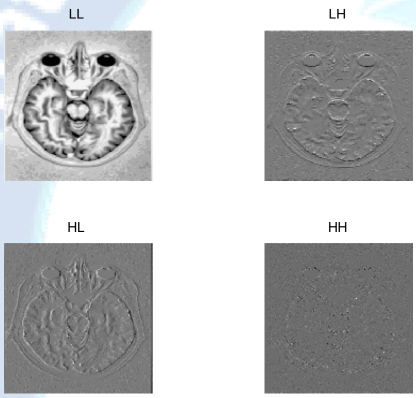

Fig. 1 (b) Host1 Image after Applying DWT

Watermarked Image

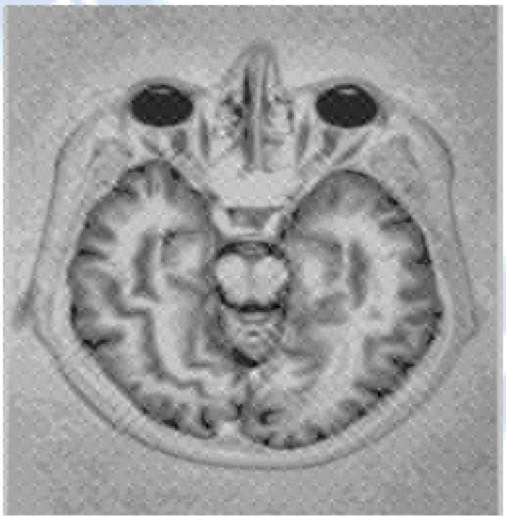

Fig. 1(C). Watermarked Image.

Watermark Image

Data:Brain MRI
Name :Rakesh
Age:34
Hospital:Apolo

Fig. 1(d). Watermark Image.

Extracted Watermark Image

Data:Brain MRI
Name :Rakesh
Age:34
Hospital:Apolo

Fig. 1(e). Extracted Watermarked Image.

We have applied our DWT-DCT-SVD algorithm on host2 image (fig 2 (a)) to watermark the image wm2 (fig 2 (d)). host2 image obtained after applying DWT is shown in fig 2 (b) . The image obtained after watermarking that is watermarked image is shown on fig 2 (c). Then no image attacks is apply on watermark image and it is directly Dewater marked and its extracted watermarked image is shown in fig 2(e)

Host Image

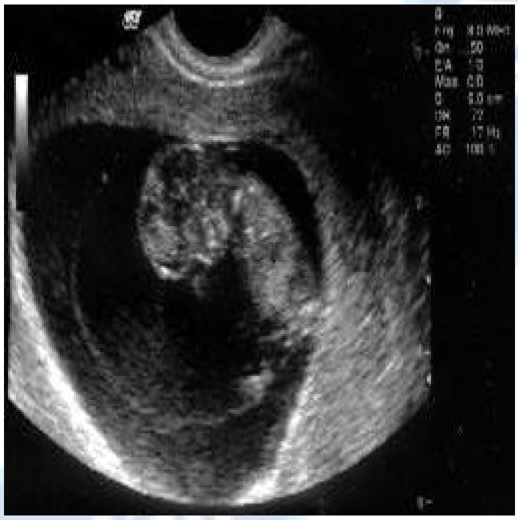

Fig. 2(a). Original Image.

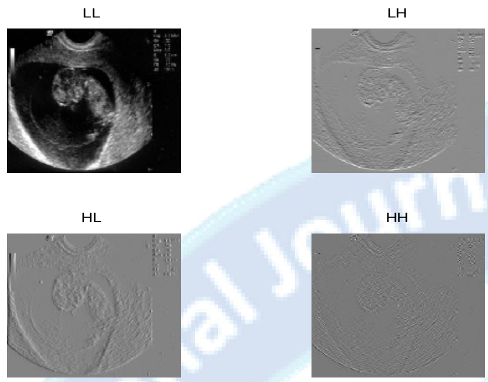

Fig 2 (b) Host2 Image After Applying DWT

Fig. 2(c). Watermarked Image.

Fig. 2(d). Watermark Image.

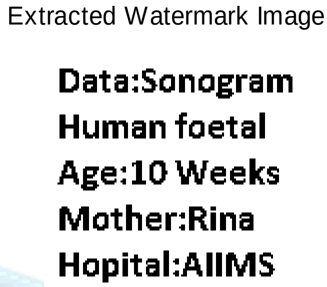

Fig. 2(e). Extracted Watermarked Image.

5. Conclusion:

The results suggests that DWT-DCT-SVD based watermarking scheme is giving best performance in the presence of recovery of watermark image used to indicates the text based data of biomedical images. The results are verified analytically in terms of PSNR and normalization coefficients and both are found high for novel DWT-DCT-SVD watermarking scheme.

In future the work can be extended for considering other image attacks effect and code parameter optimization in terms of additional image attacks. Presently we have considered the algorithm robustness for salt and pepper noise and Gaussian noise. In future effects of compression, transformation and cropping can also be considered for demonstrating the performance of developed watermarking scheme.

6. References:

[1] M. S. Hsieh, "Perceptual Copyright Protection using Multiresolution Wavelet Based Watermarking and Fuzzy Logic," International Journal of Artificial Intelligence & Applications, Vol.1, No.3, July 2010.

[2] N.Nikolaidis and I.Pitas, "Robust image watermarking in the spatial domain," Signal Processing, Vol.1, No.66, pp.385-403, 1998.

[3] C. T. Hsu and J. L. Wu, "Multiresolution Watermarking for Digital Images," IEEE Transaction on Circuits and System II, Vol. 45, No. 8, pp. 1097-1101, August 1998.

[4] W. C. Chu, "DCT-Based Image Watermarking Using Sub sampling," IEEE Transaction on Multimedia, Vol. 5, No. 1, March 2003.

[5] R. Sun, H. Sun, "A SVD and quantization based semi-fragile watermarking technique for image authentication," International Conference on Signal Processing, Vol.2, pp 1952–1955, 2002.

[6] R. Liu and T. Tan, "A SVD-Based watermarking scheme for protecting rightful ownership," IEEE Transaction on Multimedia, Vol. 4,No.1, pp 121-128, March 2002.

[7] Chiou-Ting Hsu1 and Ja-Ling Wu2, "Image Watermarking By Wavelet Decomposition" Academy of Information and Management Sciences Journal, Vol. 3, No. 1, pp. 70-86, 2000

[8] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy "A Dual Digital-Image Watermarking Technique" World Academy of Science, Engineering and Technology 5 2005

[9] Chih-Yang Lin And Yu-Tai Ching "A Robust Image Hiding Method Using Wavelet Technique" Journal Of Information Science And Engineering 22, 163-174 (2006)

[10] Ibrahim Nasir, Ying Weng, Jianmin Jiang "A New Robust Watermarking Scheme for Color Image in Spatial Domain" Signal-Image Technologies and Internet-Based System, 2007. SITIS '07.

[11] Chin-Chen Chang "An Svd Oriented Watermark Embedding Scheme With High Qualities For The Restored Images" International Journal of Innovative Computing, Information and Control ICIC International °c 2007 ISSN 1349-4198 Volume 3, Number 3, June 2007