Hiding Information in Images by Digital Watermarking Technique

Rakesh Joon[1]
[1]Department of Electronics and Communication Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

Abstract : **Watermarking is a branch of information hiding which is used to secrete proprietary information in digital media like photographs, digital song, music or digital video. Watermarking can be used for proprietor identification to identify the content owner, finger printing, to identify the buyer of the content, for broadcast monitoring to determine royalty payments and authentication, to determine whether the data has been altered in any manner from its original form. This research proposes a technique that uses the DWT, DCT as well as the SVD. The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. The proposed technique uses the DWT, DCT as well as the SVD; this makes the proposed technique better as compared to the existing technique that uses only the DWT and the SVD in a different manner. The simulation of the proposed algorithm is done using the MATLAB. The simulation result shows that the proposed algorithm is better than the existing algorithm. The PSNR values analyzed over different image are better for the proposed algorithm as compared to the existing algorithm. The proposed algorithm is more imperceptible as compared to the existing algorithm.**

Keywords: Watermarking, DWT, SVD, DCT.

I. INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues [1]. Copyrighted material can be easily exchanged over peer-to-peer networks and this has caused key concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. Watermarking can be used for owner identification to identify the content owner, finger printing, to identify the buyer of the content, for broadcast monitoring to determine royalty payments and authentication, to determine whether the data has been altered in any manner from its original form. There are some properties of watermarks [2] that are Robustness, Tamper-resistance, Bit rate, Scalability etc. Digital watermarking [3] refers to specific information hiding techniques whose purpose is to embed secret information inside multimedia content like images, video, or audio data.

Many digital watermarking methods have been proposed over the last decade [4].Digital watermarking methods can also be roughly categorized into two types: non-blind and blind. Non-blind methods require the original image at the detection end, whereas blind methods do not. Blind methods are more useful than non-blind ones because the original image may not be available in actual scenarios [3].

Digital watermarking plays an increasingly vital role for proving authenticity and copyright protection. Unfortunately the currently available formats for image in digital form do not allow any type of copyright protection. A potential solution to this kind of trouble is an electronic stamp or digital watermarking which is intended to complement cryptographic process [5].

The process of embedding the watermark into a digital data is known as Digital Watermarking. It embeds some marking information directly into the digital carrier (including multimedia, documents or software), but it is not easily noticed by human perception. Digital watermarking is a way of hiding a secret or personal message to provide copyrights and the data integrity. The concept of digital watermarking is also associated with the steganography. It is defined as covered writing, which hides the vital message in a covered media while, digital watermarking is a way of hiding a secret or personal message to provide copyrights and the data integrity. It is a innovative approach, which is appropriate for medical, military, and archival based applications. The embedded watermarks are difficult to remove and typically imperceptible, could be in the form of text, image. [4].

II. DISCRETE WAVELET TRANSFORM

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an picture. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms [6].

For 2-D images, applying DWT corresponds to processing the image by 2 -D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1,LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 subbands consisting of the multi-resolution sub-bands LL_N and LHx, HLx and HHx where x ranges from 1 until N. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency subbandsHHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye [6].

III. PROPOSED TECHNIQUE

The proposed technique uses the DWT, DCT as well as the SVD (Singular Value Decomposition). The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. This process must provide better PSNR. The whole process can also be given in form of algorithm.

PROPOSED ALGORITHM

1. Input Host image say Ih
2. Take DCT of host image to get transformed image

   IHT=DCT2(Ih)

3. Take DWT of IHT . [LL LH HL HH]= DWT(IHT)
4. Take SVD of Each sub Frerency

   [u1 LLd v1]=svd(LL)

   [u2 LHd v2]=svd(LH)

   [u3 HLd v3]=svd(HL)

   [u4 HHd v4]=svd(HH)

5. Input Watermark Image say Iw
6. Take DWT of IW.

   [LLwLHwHLwHHw]= DWT(Iw)

7. Take SVD of Each sub Frerency

   [u1w LLdw v1w]=svd(LLw)

   [u2w LHdw v2w]=svd(LHw)

   [u3wHLdw v3w]=svd(HLw)

   [u4w HHdw v4w]=svd(HHw)

8. Add

   WLL=LLd +const * LLdw

   WLH=LHd +const * LHdw

   WHL=HLd +const * HLdw

   WHH=HHd +const * HHdw

9. Take inverse SVD

   WLL1= ISVD(WLL)

   WLH1= ISVD(WLH)

   WHL1= ISVD(WHL)

   WHH1= ISVD(WHH)

10. Take inverse DWT

    Res=Idwt2(WLL1 WLH1 WHL1 WHH1)

11. take inverse DCT

    res=iDCT2(res)

12. Res is the resultant Watermarked Image

Extraction Algorithm

1. Input Watermarked image say Ih
2. Take DCT of host image to get transformed image

   IHT=DCT2(Ih)

3. Take DWT of IHT . [LL LH HL HH]= DWT(IHT)
4. Take SVD of Each sub Frerency

   [u1 LLd v1]=svd(LL)

   [u2 LHd v2]=svd(LH)

   [u3 HLd v3]=svd(HL)

   [u4 HHd v4]=svd(HH)

5. Input HOST Image say Iw
6. Take DWT of IW.

   [LLwLHwHLwHHw]= DWT(Iw)

7. Take SVD of Each sub Frerency

   [u1w LLdw v1w]=svd(LLw)

   [u2w LHdw v2w]=svd(LHw)

   [u3wHLdw v3w]=svd(HLw)

   [u4w HHdw v4w]=svd(HHw)

8. Add

   WLL=LLd -const * LLdw

   WLH=LHd -const * LHdw

WHL=HLd -const * HLdw

WHH=HHd -const * HHdw

9. Take inverse SVD

WLL1= ISVD(WLL)

WLH1= ISVD(WLH)

WHL1= ISVD(WHL)

WHH1= ISVD(WHH)

10. Take inverse DWT

Res=Idwt2(WLL1 WLH1 WHL1 WHH1)

11. take inverse DCT

res=iDCT2(res)

12. Res is the resultant Watermark

The proposed algorithm can be implemented using the MATLAB and result can be compared with the existing Algorithm.

IV. RESULTS

- *Imperceptibility*

Embedding extra information in the original image will cause distortion in the image quality. The watermark is truly imperceptible if human cannot distinguish between the host image and the watermarked image. To evaluate imperceptible is to conduct subject tests where both original and watermarked image are presented to human subject. The most common evaluation method is to compute the peak signal to noise ratio (PSNR) between the host and watermarked image. PSNR is the measure of the image quality. Generally when PSNR is 40db or greater, then the original and the watermarked images are virtually indistinguishable by human observer. In our proposed watermarking scheme the value of PSNR ranges from 52 to 56 which mean that our algorithm is highly imperceptible. PSNR is defined as follows :

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}} \quad \text{and} \quad \text{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(I_m(i) - I_w(i)\right)$$

Where I_m and I_w are the original and watermarked image, respectively, n is the number of pixels. Higher the PSNR, the better the image quality.

The table 1 shows the comparison of the PSNR values of the existing and the proposed algorithm over various images. These images are shown in the appendix 2 with their names. The table shows only names of the images.

Table 1: Analysis Values of Existing and Proposed Algorithms

Host Image	Watermark image	PSNR(Existing technique)	PSNR(Proposed Technique)
Gitu.jpg	P2.jpg	44.9157	84.3259
P1.JPG	P2.JPG	44.7694	87.1814
P2.JPG	P1.JPG	44.7203	87.0347
P2.jpg	Gitu.jpg	45.9341	88.3960
P1.jpg	Gitu.jpg	45.9580	88.4787
Gitu.jpg	P1.jpg	44.8594	84.2619

The results shown in the above table can be plotted graphically. The comparison shows that the PSNR of the proposed algorithm is better than the existing algorithm. The increase in the PSNR value confirms the better performance of the proposed algorithm.

The figure 1 shows the original Host image. It is the Gitu.jpg and the watermark image will be hided in this image.

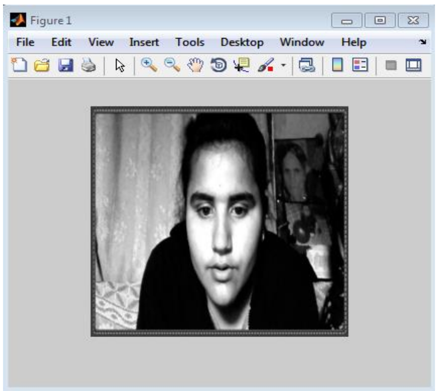

Figure 1: Original Image

The figure 2 shows the watermark image. It is the P1.jpg that will be watermarked in the host image shown in figure 1.

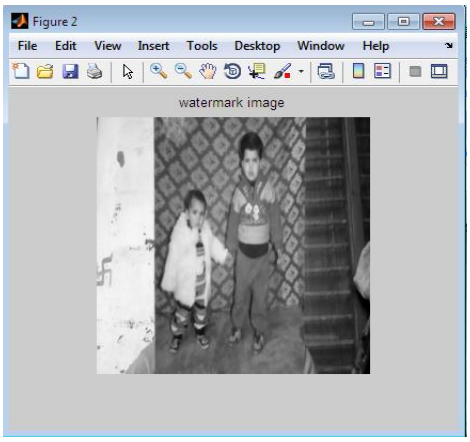

Figure 2: Watermark Image

The figure 3 shows the water marked image. This is the resultant image after inserting the watermark image into the host image. There is no visual difference in this and the host image. This means the proposed technique is effective.

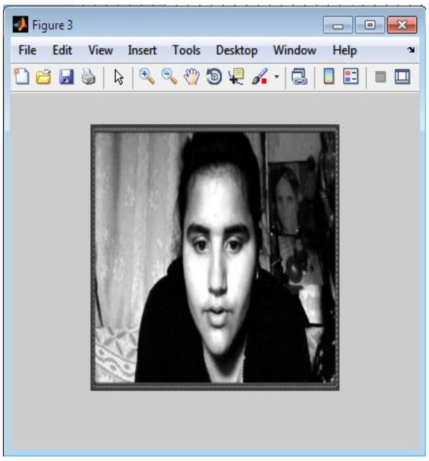

Figure 3: Watermark Extracted From Watermarked Image

The graphical comparison of the PSNR values of the existing and proposed algorithm is shown in the figure 4.

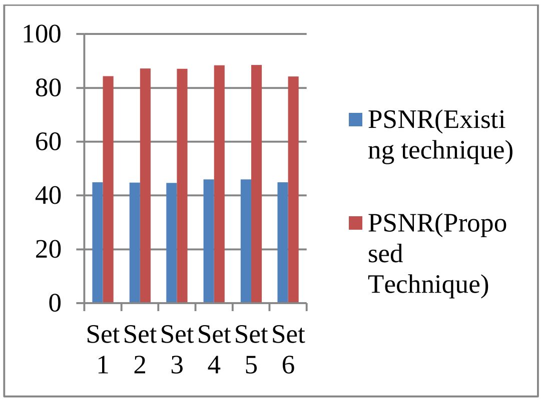

Figure4: PSNR of Existing And Proposed Technique

The results confirm the better performance of the proposed algorithm as compared to the existing algorithm. The proposed algorithm has better PSNR value as compared to the existing algorithm and there is no visual difference between the HOST image and the watermarked image.

V. DIGITAL WTERMARKING : APPLICATIONS

The applications of watermarking are following:

1. Digital copyright protection
2. Transaction tracing and fingerprinting
3. Digital content management
4. Copy control
5. Digital content authentication and verification
6. Broadcasting Synchronization System
7. Forgery Prevention
8. Lyric syn services

VI. CONCLUSION

This research proposes a technique that uses the DWT, DCT as well as the SVD. The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. The proposed technique uses the DWT, DCT as well as the SVD; this makes the proposed technique better as compared to the existing technique that uses only the DWT and the SVD in a different manner. The simulation of the proposed algorithm is done using the MATLAB. The simulation result shows that the proposed algorithm is better than the existing algorithm. The PSNR values analyzed over different image are better for the proposed algorithm as compared to the existing algorithm. The proposed algorithm is more imperceptible as compared to the existing algorithm.

REFERENCES

[1] Potdar, V. M., Han, S., & Chang, E. (2005, August). A Survey Of Digital Image Watermarking Techniques. In *Industrial Informatics, 2005.INDIN'05. 2005 3rd IEEE International Conference on* (pp. 709-716). IEEE.

[2] Cox, I. J., & Miller, M. L. (1997, June). Review of Watermarking And The Importance Of Perceptual Modeling. In *Electronic Imaging'97* (pp. 92-99). International Society for Optics and Photonics.

[3] Minamoto, T., & Aoki, K. (2010). A Blind Digital Image Watermarking Method Using Interval Wavelet Decomposition. *International Journal of Signal Processing, Image Processing & Pattern Recognition*, *3*(2)..

[4] Cox, I. J., Miller, M. L., Bloom, J. A., &Honsinger, C. (2002). *Digital watermarking* (Vol. 53). San Francisco: Morgan Kaufmann.

[5] Verma, Vishal. Digital Image Watermarking Techniques: A Comparative Study.*International Journal of Advances in Electrical and Electronics Engineering*,IJAEEE ,Volume2, Number 1.

[6]Chaturvedi, Navnidhi. "Various Digital Image Watermarking Techniques And Wavelet Transforms." *International Journal of Emerging Technology and Advanced Engineering* 2.5 (2012): 363-366