Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Digital Color Image Watermarking using DWT-SVD Techniques in YUV and RGB Color Spaces

Jay Prakash Pandey
Information Technology RGPV
Bhopal, India

Gajendra Singh
HOD CSE SSSIT Shehore RGPV
Bhopal, India

Abstract ----Digital image watermarking is an emerging copyright protection technology. It aims at asserting intellectual property rights of digital images by inserting a copyright identifier in the contents of the image, without sacrificing its quality. It has been affirmed that the frequency domain techniques are more robust than spatial domain techniques. In this paper, we propose an imperceptible and a robust digital image watermarking algorithm. The algorithm is based on combining two powerful transform domain techniques; the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD) transform. . This paper proposes the design and hardware implementation of a fast RGB to YUV converter by standard NTSC conversion and reconstruction formulae using optimal 2-D systolic arrays for matrix multiplication. Performance evaluation results demonstrate the effectiveness of the proposed algorithm with respect to the requirements of image watermarking; imperceptibility and robustness.

Keyword— Digital Watermarking, Digital Wavelet Transform (DWT), Singular Value Decomposition (SVD), Peak Signal to Noise Ratio (PSNR), YUV, YIQ

I. INTRODUCTION

Today the increase in network and multimedia content has created an urgent need for copyright enforcement technologies that can protect copyright ownership of multimedia contents. Digital Image Watermarking is one such technology that has been developed to protect digital images from illegal manipulations. This technique is better than Digital Signatures and other methods because it does not increase overhead.

More than 700 years ago, paper watermarks were used in Fabriano, Italy to indicate the paper brand and the mill that produced it. After the paper watermarking invention, watermarks rapidly spread over Europe and then over Italy, and although originally used to indicate the paper make or paper mill, they later served as suggestion for quality ,paper format, and strength and were also used to date and authenticate paper. By the 18th century it began to be used as anti counterfeiting measures on money and other documents [1], [2]. Paper watermarking is still widely used as security features in currency today.

The term watermark was introduced near the end of the 18th century. It was given because the marks look like the effects of water on paper. The first example of a technology comparable to digital watermarking is a copyright filed in 1954 by Emil Hembrooke for identifying music works. In 1988, Komatsu and Tominaga emerge to be the first to use the term "digital watermarking" [3], [4].

In the late 1990s there was an explosion of interest in digital systems for the watermarking of various content. The main focus has been on photographs, audio, and video, but other content such as binary images, text, line drawings, three-dimensional models, animation parameters, executable code, and integrated circuits — has also been marked. The proposed applications of these methods are many and varied, and include identification of the copyright owner, indication to recording equipment that the marked content should not be recorded, verification that content has not been modified since the mark was embedded, and the monitoring of broadcast channels looking for marked content. Interest in steganology increased significantly after the terrorist attacks on September 11, 2001, when it became clear that means for concealing the communication itself are likely to be used for criminal activities [5]. The first steganalytic methods focused on the most common type of hiding called Least Significant Bit embedding in bitmap and GIF images. Later, substantial effort has been directed to the most common image format—JPEG and audio files. Accurate methods for detecting hidden messages prompted further research in Steganography for multimedia files.

In recent years, digital multimedia technology has shown a significant progress. This technology offers so many new advantages compared to the old analog counterpart. The advantages during the transmission of data, easy editing any part of the digital content, capability to copy a digital content without any loss in the quality of the content and many other advantages in DSP, VLSI and communication applications have made the digital technology superior to the analog system. Particularly, the growth of digital multimedia technology has shown itself on Internet and wireless applications [6], [7]. As audio ,vedio and images are available in digital form ,it may be that the ease with perfect copies can be made will lead to large scale illegal copying which will undermine music ,film ,book etc publishing industries Yet, the distribution and use of multimedia data is much easier and faster with the great success of Internet.

II. LITERATURE REVIEW

Kapre and Joshi [9] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT) and Singular Value Decomposition(SVD). The watermark, modeled as Gaussian noise, was added to the high frequency and middle bands of the image. The decoding procedure involved taking the DWT of a potentially marked image. Sections of the watermark were correlated and extracted with sections of the original watermark .If the cross-correlation was higher than a threshold, and then the watermark was detected. Otherwise, the image was decomposed into finer bands until the complete, extracted watermark was correlated with the entire, original watermark. This procedure proved to be more robust than the DCT method. Improvements on the above schemes were achievable by utilizing properties of the Human visual system.

Zhao et al. (2004) presents a dual domain watermarking technique for image authentication and image compression. They use the DCT domain for watermark generation and DWT domain for watermark insertion. A soft authentication watermark is used for tamper detection and authentication while a chrominance watermark is added to enhance compression. They use the orthogonality of DCT-DWT domain for watermarking [10].

Tao and Eskicioglu (2004) present an optimal wavelet based watermarking technique. They embed binary logo watermark in all the four bands. But they embed the watermarks with variable scaling factor in different bands. The scaling factor is high for the LL sub band but for the other three bands its lower [11].

In 2011 Baisa L. Gunjal and Suresh N. Mali introduced a strongly robust 'Digital Image Watermarking 'with increased security levels and producing exact recovery of original watermark for standard image database, giving correlation factor equals to 1 and PSNR up to 48.53 dBs. Experimental results have demonstrated that our technique is very effective supporting more security. As per ISO's norms, the still Image Compression standard JPEG2000 has replaced Discrete Cosine Transform by Discrete Wavelet Transform. This is the reason why more researchers are focusing on DWT, which we have used for implementation. The presented 'Digital Image Watermarking' methodology can be extended for 'color images and videos' for authentication and copyright protection [13][5].

III. PROBLEM STATEMENT

Imperceptibility and Robustness of watermark data are very important issues to be considered. A lot of research is going on to increase imperceptibility and robustness. In this thesis we are giving a new image watermarking method. This method increases the imperceptibility and robustness of watermark. To evaluate this concept of PSNR and Pearson's Correlation Coefficient is used. It is a semi-blind watermarking method. Means original image is not required at the time of watermark recovery.

IV. PROPOSED TECHNIQUES

In this thesis we are giving a new image watermarking method. This method increases the imperceptibility and robustness of watermark. To evaluate the performance of our watermark we use the concept of Peak-to-signal-noise-ratio (psnr) and Pearson's correlation coefficient. Means the difference between the original image and the attacked watermarked image is being calculated .It is a semi-blind watermarking method. Means original image is not required at the time of watermark recovery.

A. RGB Color Spaces

Some of researches have used RGB color space for watermark embedding. First R, G, B planes are separated using equations 1, 2, 3 and either one of these planes or combination of two can be used for embedding.

R = image (: ; : ; 1) (1)

G = image (: ; : ; 2) (2)

B = image (: ; : ; 3) (3)

But, RGB color space is complex in describing the color pattern and has redundant information between each component. Since Pixel values in RGB color space are highly correlated, RGB color space is converted into YUV or YIQ color spaces.

B. YUV Color Spaces

Here, RGB color space is converted into YUV Color space and then Watermark is embedded. Initially color image is read and R, G, B components of original Cover Image are separated. Then they are converted into YUV color Space using following equations.

Y = 0.299 * R + 0.587 * G + 0.114 * B (4)

U = -0.147 * R - 0.289 * G + 0.436 * B (5)

V = 0.615 * R - 0.515 * G - 0.100 * B (6)

After embedding the watermark using DWT, YUV color space is converted back into RGB color space using following equations.

R = Y + 1.140 * V (7)

G = Y - 0.395 * U - 0.581 * V (8)

B = Y + 0.2032 * U (9)

For embedding the watermark we use frequency domain techniques, because the major advantage of frequency domain methods is their superior robustness to common image distortions. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity [4]. Invisibility refers to the degree of distortion

introduced by the watermark and its affect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks, such as noise, filtering (blurring, sharpening, etc.), re-sampling, scaling, rotation, cropping, and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark.

Discrete cosine transform (DCT) and discrete wavelet transform (DWT), which are used in image compression standards JPEG and JPEG2000 respectively, are two main transform methods used in transform domain watermarking. As DWT decomposes images into four bands, DWT- based watermarking schemes can embed data in all frequencies. This result in robustness to a wide range of attacks for embedding in low and high frequency bands are complementary. Several watermarking methods resistant to geometric attacks have been presented in literature.

Recently, a transform called singular value decomposition was explored. In this paper, we present a hybrid SVD-DWT semi blind approach to embed the visual watermark in high frequency band of the image. This is unlike traditional viewpoint that assumes watermarking should be embedded in low or middle frequency to have good robustness.

In a DWT- based watermarking scheme, the host image is decomposed into four frequency bands. Then apply SVD on high band and also compute the SVD of watermark. Modify the singular values of host image in high sub-band according to those of watermark image, and lastly apply the inverse DWT and find the watermarked image. Modification in all frequencies enables watermarking schemes using DWT robust to a wide range of attacks but embedding data in high frequency band is more robust to geometric attack. So for making more robust SVD-DWT scheme. We proposed a new watermarking scheme; in this we embed the watermark in only high frequency band.

V. PROPOSED ALGORITHM

WATERMARK EMBEDDING ALGORITHM

1. Take the color image and separate the R, G and B color
2. Convert into Y, U and V color model
3. Decompose the Y channel using DWT in 4 sub bands: A, H, V, and D.
4. Apply IDWT to D and get high frequency image I^h.
5. Apply SVD to high frequency image $I^h = U^h S^h V^h$
6. Apply SVD to watermark to embed $W = U^w S^w V^w$
7. Modify $S = S^h + \alpha S^w$ where α is scaling factor.
8. Obtain the modified high frequency image $I^h = U^h S^h V^h$
9. Apply DWT to I^h and get modified D: D = DWT (I^h)
10. Using A, H, V, and D apply IDWT to obtain the watermarked image I^*.

Separate the watermarked image and the cover image into individual color channels red, green and blue. Convert to the embedding YUV Color Space and select a channel depending on the key. then decompose the Y channel using discrete wavelet transform in 4 sub bands: A,h,V and D. Then decompose the selected channel of the watermarked image and the cover image using IDWT. Perform SVD transformation to the high frequency image on selected sub band of the watermarked image and the cover image and then embed. Apply scaling factor and finally get watermarked image

WATERMARK EXTRACTING ALGORITHM

1. Take watermarked image I^* and separate the R, G and B color
2. Convert into Y, U and V color model
3. Decompose the watermarked image I^* into 4 sub bands: A H V and D Using DWT.
4. Apply IDWT to D^* and get modified high frequency image I^{*h}
5. Apply S VD to $I^{*h} = U^{*h} S^{*h} H^{*h}$
6. Apply S VD to watermark W: $U^w S^w V^w$
7. Extract the singular values of watermark: $S^{*h} = (S^{*h} - S^{w})/\alpha$ where S^{*h} are the singulars of origin image.
8. Original the watermark from D band: W: $U^w S^{*w} V^{w'}$

Read in the watermarked image and apply DWT to this watermarked image into 4 sub bands. Apply SVD to each subbands of image then obtain four image component and extract singular value from each subbabnds.Then decompose into inverse SVD (ISVD) to Perform inverse DWT (IDWT) method. Then finally original watermark image recovered.

5.1PERFORMANCE EVALUATION

PSNR (The Peak Signal-to-Noise Ratio)

The performance of the watermarking methods can be measured by imperceptibility and robust capabilities. Imperceptibility means that the superficial quality of the original image should not be distorted by the presence of watermark. On the other hand, the robustness is the measure of the intentional and unintentional attacks. It was found that image is evaluated using peak-to-signal-ratio (psnr) and mean square error (mse) which is defined as in Equation (1) and (2).

The PSNR computes the peak signal-to-noise ratio between two images in decibels. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between

the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE is, the lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (1)$$

In the previous equation (1), *M* and *N* are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \quad (2)$$

In the equation (2), *R* is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.

5.2 EXPERIMENTAL RESULT

We test the proposed scheme on gray scale image with the size 256 x 256, watermark with the same size. We used the scaling factor α as 0.02.The proposed watermarking scheme was tested using ordinarily image processing: Gaussian noise, rotation and salt & pepper. The correlated coefficient of the original watermark, psnr and extracted watermark is shown in the Table 1 and 2. In this we observe that this scheme is robust against various attacks. The computational analysis of the complete system with respect to PSNR and %CR is given in Table 1 and Table 2 correspondingly. The image quality analysis of the proposed design is illustrated in Fig. 3 and extraction of watermark image for different quadrants with varying scaling factor is depicted in Fig. 4

Table 1: Computational Analysis of Proposed Algorithm with measurement of PSNR by varying Scaling Factor (α)

Type of Image		Filename, Ext with dimension	Rank of Matrix (k)	Scaling factor α=0.01				Scaling factor α=0.04				Scaling factor α=0.08			
				I	II	III	IV	I	II	III	IV	I	II	III	IV
Gray Scale	Cover image Watermark image	Lena.bmp 512 X 512 Cameraman.tif 256 X 256	150	42.9767	42.8399	42.2979	42.7522	46.0961	45.9081	46.1801	45.1178	42.3165	33.2493	36.1123	36.5965
			175	43.9022	43.9061	43.6058	42.6445	50.0005	49.5370	50.0409	48.3403	43.4436	33.3402	36.4078	36.8240
			200	43.2954	43.0542	43.8806	43.7568	52.3392	51.7231	52.8287	49.5780	43.8446	33.3431	36.5640	36.9496
Colour	Cover image Watermark image	Lenna.bmp 512 X 512 Baboon.png 256 X 256	150	37.3936	36.2460	37.1536	37.2539	36.5766	29.2951	31.2981	35.1107	34.6077	23.4504	24.9738	28.6455
			175	40.0213	38.3225	39.9860	40.2224	38.9951	29.5897	31.8630	36.7193	35.9631	23.5296	25.0970	28.9337
			200	41.7036	39.5773	41.6845	42.3925	40.4812	29.7526	32.0934	37.4588	36.6595	23.5650	25.1531	29.0663

Table 2: Measurement of %CR for watermark image by varying Scaling Factor (α)

Type of Image		Filename, Ext with dimension	Rank of Matrix (k)	Scaling factor α=0.01	Scaling factor α=0.04	Scaling factor α=0.08
Grey Scale	Cover image Watermark image	Lenna.bmp 512 X 512 Cameraman.tif 256 X 256	150	17.11	45.68	50.86
			175	17.26	44.11	50.39
			200	17.26	43.32	50.70
Colour	Cover image Watermark image	Lenna.bmp 512 X 512 Baboon.png 256 X 256	150	12.39	27.03	35.88
			175	12.44	27.08	35.88
			200	12.44	27.03	35.88

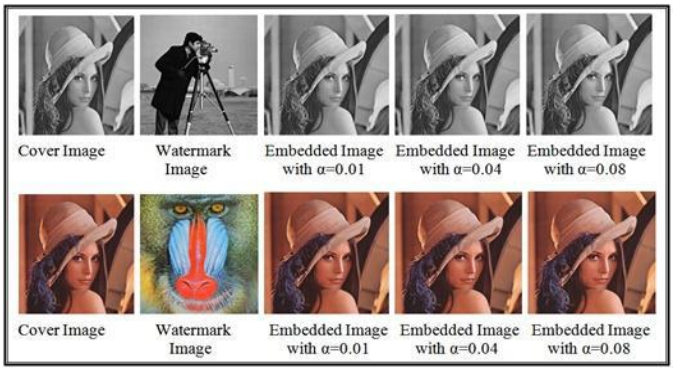

Fig. 3. Image Quality Analysis of Complete Proposed System Design

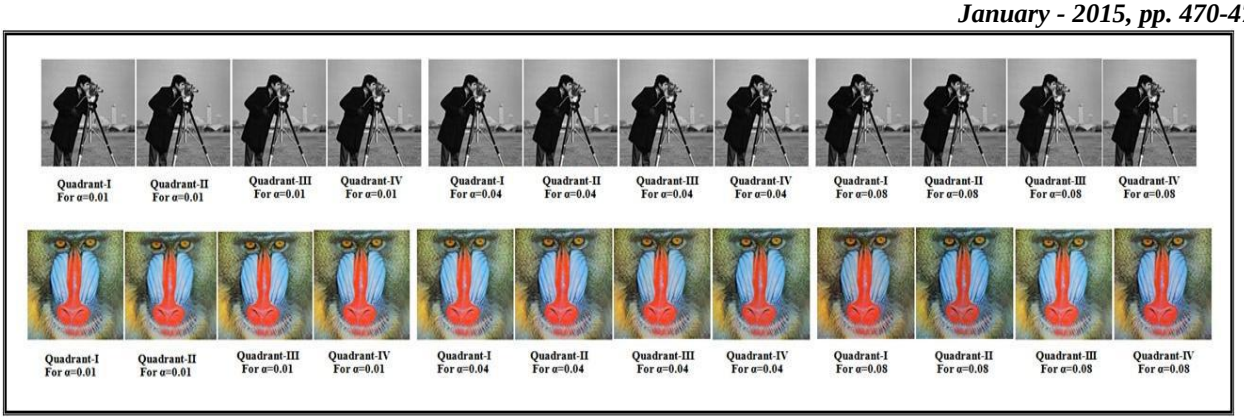

Fig. 4. Image Results for four quadrants by varying Scaling Factor (α)

VI. CONCLUSION

This thesis presents a semi-blind watermarking technique that uses DWT at level 2 and then embed watermark in high frequency band of the image. In our scheme, the most difference from traditional scheme is that the watermarking is embedded in high frequency. It has good performance in a variety of image processing.SVD decomposition belongs to spatial domain transform and has robustness to geometrical attack. For considering this, we use DWT and IDWT transformation to obtain the high frequency image. Accordingly the scheme has robustness to geometrical attack. We notice there are three frequency image (low frequency image, middle-low frequency image, middle-high frequency image) are not used. Different watermarks can be embedded in them. As it's a semi-blind scheme so when extraction is done there is no need for original cover image, only original watermark and the algorithm is required for detection of content ownership. The PSNR value is between 20db-50db which shows that the extracted watermark from the attacked image is closer to the original watermark.

REFRENCES

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," in Proc. of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999

[2] Saraju Prasad Mohanty, "Watermarking of Digital Images", Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999.

[3] CHAN Pik-Wah, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery", submitted at The Chinese University of Hong Kong, pp. 7 – 15, July 2004

[4] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.

[5] Cox, I., Millar, M., and Bloom, J. 2002. "Digital watermarking", Morgan-Kaufmann, San Francisco, CA, ISBN: 1-55860-714-5.

[6] Dazhi Zhang, Wu,Sun and Huang , " A New Robust Watermarking Algorithm Based on DWT" Image and Signal processing 2009 ,CISP'09

[7] Rowayda A Sadek , "Blind Synthesis Attack on SVD Based watermarking Technique" , Computational Intelligence for modeling Control :2008 pp 140-145.

[8] Zheng, D., Liu, Y., Zhao, J., and El Saddik, A. "A survey of RST invariant image watermarking algorithms", ACM Computing Surveys, Volume 39, No. 2, Article 5, June 2007.

[9] Kapre and Joshi .,"Robust Image Watermarking based on Singular Value Decomposition and Discrete Wavelet Transform", Nanded ©2010 IEEE

[10] Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", in IEEE Transactions on linage Processing, vol. 13, no. 3, pp. 430-448, March 2004.

[11] Tao, P & Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", in Symposium on Internet Multimedia Management Systems V, Philadelphia, PA, 2004.

[12] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A survey on watermarking application scenarios and related attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993, Oct. 2001

[13] Baisa L. Gunjal and Suresh N. Mali "Comparative Performance Analysis of DWT-SVD Based Color Image Watermarking Technique in YUV, RGB and YIQ Color Spaces" International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011

[14] A White paper on "Digital Watermarking: A Technology Overview", Wipro Technologies, pp. 2 – 8. Aug. 2003.

[15] Zude Zhou, Bing Tang and Xinhua Liu, "A Block-SVD Based Image Watermarking Method", Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China

