A HYBRID DIGITAL WATERMARKING ALGORITHM FOR COLOUR IMAGES BASED ON DWT AND DCT

V.Madhu Viswanatham, Galma Santosh Reddy , Potluri Jagadeesh

VIT University, School of Computing Science and Engineering

ABSTRACT: Digital image watermarking is a copyright protection technology aimed at asserting intellectual property rights of digital images by inserting a copyright identifier in the contents of the image, without sacrificing its quality. In this paper, we propose an imperceptible and a robust digital image watermarking algorithm for the colour images. The proposed algorithm is a hybrid algorithm based on combining two powerful transform domain techniques; the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). The proposed algorithm deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained. Performance evaluation results demonstrate the effectiveness of the proposed algorithm with respect to the conflicting requirements of image watermarking; imperceptibility and robustness against common image processing operations.

KEYWORDS: Digital Watermarking, Discrete Wavelet Transform, Arnold Transform, Discrete Cosine Transform, Robustness, Imperceptibility

1. INTRODUCTION

A large amount of accessible information today is available in one or the other multimedia formats. The evolution of Internet led to faster and easier duplication and distribution of multimedia. The piracy of the multimedia data has become an important issue for the owners of the products, so the need to address these issues which are mainly related to protection of intellectual property rights has arrived. One solution to the problem is digital watermarking for copyright protection of multimedia data.

Digital watermarking is a technique by which the owners of the data, in any multimedia format, can embed watermark information in a way that can be later retrieved for verification purposes or to resolve ownership in case of conflicting claims on the ownership of data. In general, the watermark could be visible or invisible to the general user. A visible watermark typically contains a logo, trademark or proprietary information indicating the ownership of the image. On the other hand, invisibly watermarked content appears perceptually identical to the original data. The digital watermarking scheme is used in many applications like copyright protection, copy protection, image authentication etc. The watermark can be embedded into an image, video, audio or text form of multimedia. This paper deals with embedding watermark in digital images for copyright protection of digital images.

There are four essential factors that are commonly used to determine quality of watermarking scheme. They are robustness, imperceptibility, capacity, and security.

1. **Robustness:** Robustness is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, adding noise, image adjustment, resizing, cropping etc. The watermark should be reliably detected even after the image has been modified but not destroyed beyond recognition.
2. **Imperceptibility:** The presence of watermark should not destroy the quality of the host image.
3. **Capacity:** Majority of information should be embedded as a watermark in the host image.
4. **Security:** Attacker should be incapable of removing watermark in the watermarked image even though he/she knew the algorithm.

The major point of digital watermarking is to find the balance among the factors such as robustness to various attacks, embedding capacity and imperceptibility. The imperceptibility of watermarking technique is based on the intensity of embedding watermark. Better imperceptibility is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little trade off between the robustness and invisibility. Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images.

2. CLASSIFICATION OF WATERMARKING TECHNIQUES

For images, watermarking techniques are classified into two types based on perception:

1. Visible
2. Invisible

In the visible watermarking scheme, the watermark is embedded into the original (host) image such that

it is translucently visible to the observer. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Watermark embedded using invisible watermarking is imperceptible to the human eye.
Invisible watermarking is further categorized into two categories as follows:

1. Invisible-robust
2. Invisible-fragile

In case of invisible-robust watermarking, the watermark is embedded in such a way that it is very difficult to alter and can only be recovered by the proper extraction algorithm. Generally, a robust watermarking is generally used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations, which attempt to remove or destroy the mark. These algorithms ensure that the image processing operations do not erase the embedded watermark signal.
In case of invisible-fragile watermarking, the watermark can be altered or totally destroyed. These algorithms are mainly applied to content authentication and integrity verification because they are very sensitive to attacks, i.e., it can detect slight changes to the watermarked image with high probability. This paper deals with a robust watermarking.
Invisible-robust watermarking can be further categorized into two categories:

1. Blind
2. Non-blind

In case of blind invisible-robust watermarking, original image is not required during watermark extraction whereas original image is required during watermark extraction in case of non blind invisible-robust watermarking. In applications like copyright protection, there will not be access to the original image where the extraction or detection will be much difficult known as blind or private watermarking .In non-blind watermarking, the original image is required for detection of the watermark. Blind watermarking schemes are efficient for memory and processing time requirements. Since blind watermarking scheme does not need original image for extraction, it is better suitable for real-time applications.

3. RELATED WORK

Watermarking techniques for digital images can be broadly classified into two categories, namely, the spatial domain techniques and transform domain techniques depending on which domain the watermark is embedded. Typically, in spatial domain techniques the watermark is embedded in those parts of the data that do not distort the host image in any significant way. For instance, some of the well-known spatial domain techniques are least significant substitution [BIS10] and the correlation based approach [KBL07]. In least significant substitution technique, the watermark is embedded by replacing the least significant bits of the image data with the bits of the watermark data. There are many variants of this technique. In correlation based approach the watermark is converted to a pseudo-random noise (PN) sequence which is then weighted and added to the host image with a gain factor. For detection, the watermarked image is correlated with the watermark image. In the transform domain techniques, the watermark is embedded in those parts of the transformed host image which do not distort the image significantly. A survey of transform domain techniques is in [GM10].One of the earliest transform domain techniques is the one based on discrete cosine transform (DCT) [B+98]. In DCT, the image is decomposed in terms of various frequency bands and watermarks are embedded in the middle frequency bands which are not significant for the host image. Further, image transformations do not affect the watermark placed in those bands. DCT based methods are generally robust, particularly against JPEG and MPEG compression. The techniques based on wavelet decomposition are similar in spirit to DCT with the additional feature that the multi-resolution character of the wavelets allows graded information to be stored at various resolutions. For instance, in [KH97] wavelet coefficients of the image and the watermark at different levels of resolution are added together within the constraint of the so-called human-visual model. There is yet another method of digital watermarking based on singular value decomposition (SVD) techniques [LT02]. In contrast to DCT and wavelets based techniques, the advantage of singular value decomposition based methods is that they provide a transform space that is tailor made for the given image data matrix. Both in the DCT and wavelets, the basis for the transform space is a fixed set of functions. In the SVD, it must be calculated from the given data and the singular vectors so calculated form an optimal basis for the image matrix in the least square sense. It is worth mentioning that some authors [AlH08] have resorted to hybrid techniques i.e., algorithms based simultaneously on different domains to improve the watermarking results.

4. RELATED BACKGROUND

Watermarking technique generally consists of three logical steps:

1. Selection of watermarks
2. Insertion of watermarks

3. Extraction of watermarks

In this present work, watermark is generated based on the host image and this type of watermarking is called is called feature based watermarking. In this watermarking scheme, watermark is generated by applying some operations on the pixel value of host image rather than taking from external source. Recent researches on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme [SS10]. In the proposed watermarking scheme, watermark is created from the content of the host image and the generated watermark is scrambled using Arnold Transform to improve the security of the watermark. Embedding of watermark is done using frequency domain transforms – DWT and DCT. Also the watermark embedding is done in low and middle frequency coefficients of the transformed image based on the Human Visual System characteristics to maintain a balance between robustness and imperceptibility. Also blind scheme is proposed to suit the real time applications.

4.1 Switch of Color Space

RGB color space is a natural color space which is not in accordance with human visual system. So we change the color space to YCbCr color space. YCbCr color space represents each color with 3 numbers, similarly as the RGB space. The Y component represents the intensity of the light. The Cb and Cr components indicate the intensities of the blue and red components relative to the green component. YCbCr space has the character to separate brightness and chroma. Y is brightness component and Cb and Cr is chroma component.

YCbCr color space exploits the properties of the human eye. The eye is more sensitive to light intensity changes and less sensitive to hue changes. When the amount of information is to be minimized, the intensity component can be stored with higher accuracy than the Cb and Cr components. In the proposed algorithm, we embed the watermark in Y component for robustness against various attacks.

The formula for RGB to YCbCr conversion in matrix form is as follows:

$$\begin{bmatrix} Y \\ Cb \\ Cr \\ 1 \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.5870 & 0.1140 & 0 \\ -0.1687 & -0.3313 & 0.5000 & 0.5 \\ 0.5000 & -0.4187 & -0.0813 & 0.5 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \\ 1 \end{bmatrix}$$

4.2 Arnold Transform

A digital image can be considered as a two unit function f(x,y) in the plane Z. It can be represented as Z = f(x, y) where x, y ∈ {0,1,2,3....N −1} and N represents order of digital image. The image matrix can be changed into a new matrix by the Arnold transform which results in a scrambled version to offer security. It is a mapping function which changes a point (x, y) to another point (x^1, y^1) by the equation (1).

$$x^1 = x+y \bmod N \quad (1)$$
$$y^1 = x+2y \bmod N$$

Arnold mapping has a fixed area. At the same time it is all mapped. That is to say, every point in unit matrix uniquely transforms to another point. The character is very important. With it each watermarking pixel in different places can get a different place to embed. The number of times Arnold transform can be performed on an image can be taken as a secret key.

4.3 Discrete Wavelet Transform

The DWT decomposes input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns, which is shown in Figure 1. The LL component also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for *n* level wavelet transformation.

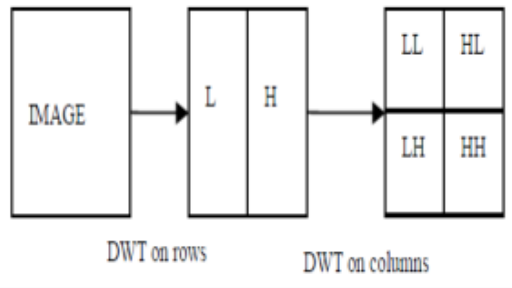

Fig. 1. DWT Decomposition

The DWT is very suitable to identify the areas in the original image where a watermark can be embedded effectively. This property allows the utilization of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. 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 humiliate the image appreciably. Embedding in the low frequency sub-bands, however, could increase robustness appreciably. On

the other hand, the high frequency sub-bands HHx 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 superficial by the human eye. The compromise accepted by many DWT-based watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LHy and HLy where good enough performance of imperceptibility and robustness could be achieved.

4.4 Discrete Cosine Transform

It's one of the most common linear transformations in digital signal process technology. Two dimensional discrete cosine transform (2D-DCT) is defined as

$$F(jk)=a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(mm)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

The corresponding inverse transformation (Whether 2D-IDCT) is defined as

$$f(mm)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

The 2D-DCT can not only concentrate the main information of original image into the smallest low-frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication. So it obtains the wide spreading application in the compression coding.

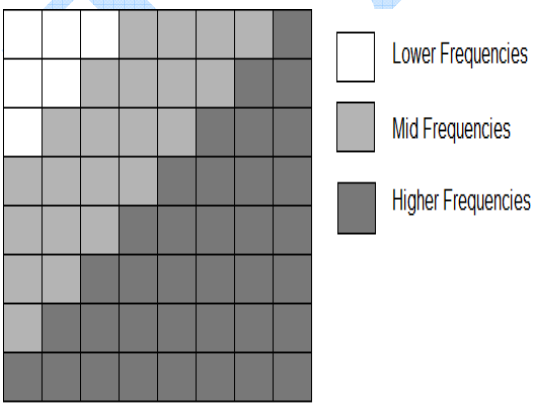

Fig. 2. 8×8 DCT block showing various frequencies in transformed domain

After applying DCT transform to the image the low, middle and high frequency component exists from top left in the DCT coefficient matrix to its bottom-right and their energy descended gradually .As mentioned above, the low frequency coefficient is lager, representing most of the energy in the image, while human eye is very sensitive to low frequency component, any modification in this region will be noticed easily. The high frequency coefficient is very small, although human eye is not so sensitive to it, large error will happen because critical visible error watermark in this region is relative low, furthermore, high frequency region will be destroyed easily by signal processing. The middle frequency coefficient is between the low and high ones, due to its relative large coefficient value, visual capacity and critical visual error of the embedded signal is high. It can still be reserved well after usual signal processing and noise interference. Embedding watermark in this region improves transparency and robustness effectively. Therefore the watermark is embedded in the low and middle frequency coefficient in DCT domain of the image.

5. PROPOSED METHOD

The central idea of the proposed algorithm is to embed the content based watermark information in host color image. The watermark is generated based on the feature of the image and hence the watermark is content based watermark. For watermark generation, a matrix is constructed by taking median of every pixel. DWT is applied to obtained matrix and LL sub band is divided into a non-overlapping blocks of size 2x2. A new matrix is constructed by obtaining minimum from every block. With the help of Arnold transform, the resultant matrix is scrambled for n times to improve security. Based on whether the elements of the matrix are even or odd, a binary watermark is constructed from the scrambled matrix, which is to be embedded within the host image. The operation of watermark embedding involves conversion of RGB color space to YCbCr color space. Discrete Wavelet Transform up to 2 levels is applied to the Y component and then Discrete Cosine Transform is applied to Y component. The generated watermark is embedded in low frequency and middle frequency coefficients of HL, LH sub bands of Y component. The operation of extraction of watermark involves reverse process of watermark embedding. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained.

5.1 Algorithm 1: Watermark Generation

1. Create a matrix from original image of size N*N by taking median value of (R,G,B) for each pixel.

2. Apply DWT to the generated matrix and select the LL sub band.
3. The LL sub band of size N/2*N/2 is partitioned into non overlapping blocks of size 2*2.
4. Compute minimum value from each block and construct a matrix M_b (p,q) where p in {1,2,....N/4} and q in {1,2,...N/4}
5. Perform Arnold Transform for n times based on the key value on M_b to scramble the elements and obtain matrix M_s.
6. Form the watermarked pattern to be embedded into the original image as
   W(p,q)=0 if M_s(p,q) is even
   =1 if M_s(p,q) is odd
7. For an N*N image, watermark pattern of size N/4*N/4 is generated.

5.2 Algorithm 2: Embedding Watermark

1. Switch the color space from RGB to YCbCr. It represents colours in terms of one luminance component/Yuma(Y) and two chrominance components/Chroma(Cb and Cr)

$$\begin{bmatrix} Y \\ Cb \\ Cr \\ 1 \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.5870 & 0.1140 & 0 \\ -0.1687 & -0.3313 & 0.5000 & 0.5 \\ 0.5000 & -0.4187 & -0.0813 & 0.5 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \\ 1 \end{bmatrix}$$

2. Take 2 levels DWT to Y component. Apply DCT to HL2 and LH2 sub image .
3. Select low and middle frequency coefficients from LH2 sub matrix.
4. Select low and middle frequency coefficients from HL2 sub matrix and make a matrix of size N/4*N/4 by combining with low and middle frequency coefficient of LH2 sub band.
5. Take a 16*16 bit watermark from the binary watermark generated during watermark generation phase.
6. Break the matrix obtained in step 4 into blocks of 8*8 size.
7. Embed a watermark bit in each block based on the following condition.
   If watermark bit=1
   Make block(4,3) >block(5,2)
   If watermark bit=0
   Make block(4,3) <block(5,2)
   Where block is 8*8 block for each block generated in step 6.
8. Restore the watermarked low and middle frequency coefficients in LH2 and HL2 sub bands.
9. Apply IDCT to Y component.
10. Apply IDWT up to 2 levels to the image.
11. Switch the color space from YCbCr to RGB.
12. The obtained image is the watermarked image.

5.3 Algorithm 3: Extraction of Watermark

1. Switch the color space of watermarked image from RGB to YCbCr. It represents colors in terms of one luminance component/Yuma(Y) and two chrominance components/Chroma(Cb and Cr)

$$\begin{bmatrix} Y \\ Cb \\ Cr \\ 1 \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.5870 & 0.1140 & 0 \\ -0.1687 & -0.3313 & 0.5000 & 0.5 \\ 0.5000 & -0.4187 & -0.0813 & 0.5 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \\ 1 \end{bmatrix}$$

2. Take 2 levels DWT to Y component. Apply DCT to HL2 and LH2 sub image .
3. Select low and middle frequency coefficients from LH2 sub matrix.
4. Select low and middle frequency coefficients from HL2 sub matrix and make a matrix of size N/4*N/4 by combining with low and middle frequency coefficient of LH2 sub band.
5. Break the matrix obtained in step 4 into blocks of 8*8 sizes.
6. Calculate the watermark bit in each block based on the following condition.
   If block(4,3) >block(5,2)
   watermark bit=1
   If block(4,3) <block(5,2)
   watermark bit=0
   where block is 8*8 block for each block generated in step 5.
7. The obtained pattern is the extracted watermark.

6. EXPERIMENTAL RESULTS

There was a need to analyze how attacks can modify the watermarked images and their corresponding detectors response. The primary purpose of the various attacks on the watermarked images is to know the survival, i.e., whether the watermark has survived or not. Survival of the watermark shows that it can be extracted as a replica of the original watermark. However, the extracted watermark was degraded due to channel noise while broadcasting and other intentional attacks. The watermarked image has been tampered with the built-in functions of Matlab software suite. The attacks we performed are as follows: joint photographic experts group (JPEG) compression, Image Adjustment, Histogram Equalization, Rotation, Salt and pepper noise attack, Gaussian noise attack, Median filtering.

The primary goal of this experiment was to determine whether the proposed watermarking scheme improved the robustness without any loss in the quality of the image. In order to measure the invisibility of the watermark we used two performance measures, PSNR (peak signal-to-noise ratio) and MSE (mean squared error) and correlation

coefficient to measure robustness. MSE of the distorted image DI compared to that of the stored original image OI of size M x N, is given by equation

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{[OI(i,j) - DI(i,j)]^2}{MxN}$$

and PSNR is given by the equation

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

The metric PSNR give the measure for invisibility. We observed that at greater PSNR the visual quality of watermarked images is very good and that it is almost indistinguishable for the human eyes from the original image.

The test image is Lena color image of size 512×512. We implemented the algorithm in joint photographic experts group (JPEG) compressed images (.jpg files) and bitmap (.bmp) files. The watermark is in bitmap (.bmp) format. The experiments on the image reveal the efficiency of the proposed algorithm in producing watermarked images with good visual quality and robustness.

The below table displays the different attacks performed on the watermarked image and the PSNR value obtained for each attack.

Table 1. Assessment of PSNR under attacks

Attack	Values		Proposed System PSNR (dB)
No attack(color image)			46.0138
No attack(Y component)			48.57
Median Filter(Y component)			33.4739
Histogram Equalization(Y component)			18.2751
Image Adjustment(Y component)			20.9008
Rotation	5 degrees		13.7795
	10 degrees		11.6437
Salt and Pepper Noise	0.002 noise density		32.1925
Gaussian Noise	Mean	Variance	
	0.01	0	38.5947
	0	0.001	30.0178
JPEG	Quality Factor		
	90		35.1497
	70		34.5031
	50		31.6191
	30		31.1718
	10		27.2001

The correlation value between original and extracted watermark is 0.9797 which shows the robustness of the blind algorithm.

The below figures display the Original Lena color image and the watermarked Lena color image:

Fig. 3. Lena original color image of size 512×512

Fig. 4. Lena watermarked color image of size 512×512

The below figures display the Original Lena Y component image and the watermarked Lena Y component image.

Fig. 5. Lena original Y component image of size 512×512

Fig. 6. Lena watermarked Y component image of size 512×512

7. CONCLUSIONS

The imperceptibility of watermark in the proposed method has been evaluated against incidental attacks by using the metric PSNR and is compared against [XXM11]. The PSNR value for Y component under no attack (48.57dB) is greater when compared to [XXM11] (38.1678dB). The PSNR value for color image under no attack is 46.0138dB.
The robustness of watermark in the proposed method has been evaluated against incidental attacks by using the metric correlation .The correlation value between original and extracted watermark is 0.9797 which shows the robustness of the blind algorithm.
From the results we concluded that the proposed watermarking algorithm is robust to the attacks and also maintained good visual quality for the watermarked images.

REFERENCES

[AlH08] **Ali Al-Haj** – *A Hybrid Digital Image Watermarking Algorithm,* IEEE 978-1-4244-1841-1, 2008.

[BIS10] **Abdullah Bamatraf, Rosziati Ibrahim, Mohd. Najib B. Mohd Salleh -** *Digital Watermarking Algorithm using LSB*, International Conference on Computer Applications and Industrial Electronics, Kuala Lampur, Malaysia, 2010.

[B+98] **M. Barni, F. Bartolini, V. Cappellini, A. Piya** – *A DCT domain system for robust image watermarking,* IEEE Transactions on Signal Processing, 66(3), 1998.

[GM10] **Baisa L. Gunjal, R. R. Manthalkar** - *An overview of Transform Domain Robust Digital Image Watermarking Algorithms*, Journal of Emerging Trends in Computing and Information Sciences, Volume 2 No. 1, 2010.

[KH97] **D. Kundur, D. Hatzinakos** - *A Robust Digital Image Watermarking Scheme using Wavelet-Based fusion,* IEEE-ICIP.1, 1997.

[KBL07] **M. Kallel, M. S. Bouhlel, J. C. Lapayre** - *A new Multiple Watermarking Scheme for medical images in Spatial Field*, GVIP Journal 7(1), 2007.

[LT02] **R. Liu, T. Tan** – *An SVD based watermarking scheme for protecting rightful ownership,* IEEE Trans. Multimedia 4(1), 2002.

[SS10] **M. Mohammed Sathik, S. S. Sujatha** – *An Improved Invisible Watermarking Technique for Image Authentication,* International Journal of Advanced Science and Technology Vol.24, 2010.

[XXM11] **Zheng Xiong-Bo, Zhang Xiao-wei, Sun Ming-jian** – *A Blind Digital Watermarking Algorithm based on Wavelet Transform,* IEEE, 2011.