International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.4, pp : 12-15 01 Oct. 2012

# A Robust Secured Watermarking Approach using DCT-DWT & Chaotic Maps

**Charu Kavadia, Vishal Shrivastava**
Department of Computer Science & Engineering, Arya college of engineering & I.T. Jaipur
charukavadia@gmail.com,Vishal500371@yahoo.co.in

***Abstract: in this paper an efficient digital watermarking technique is proposed for copyright protection. The proposed watermarking algorithm a binary logo watermark security is also maintained by using chaotic map and then after it is embedded by modifying the appropriate subband in the wavelet domain. Level 2 and level 3 wavelet decompositions are utilized to embed the digital watermark. The approach can effectively hide a robust watermark due to the exploitation of the characteristics of the human visual system in wavelet domain. The watermark is detected by comparing the correlations between the wavelet coefficients and the watermarking code at level 2 and level 3 with the stored side information. The performance of the proposed watermarking is robust to a variety of image processing techniques, such as JPEG compression, sharpening, resizing, and geometric operations.***

***Keywords: Digital watermark, discrete wavelet transform, chaotic encryption.***

## 1. Introduction

As the Internet becomes the main mean of exchanging data and information, people concern more about the copyright protection of digital data such as images and audio files. For this aim, digital watermarking techniques are developing and their number is growing, searching all for the equilibrium between three criteria: data hiding capacity, imperceptibility, and robustness, depending on the image domain representation [1]. The choice of a domain lies mainly on robustness criteria required relating to specific data manipulations or malicious attacks. Between these domains the spatial presentation is robust against geometrical attacks [2]. In the other, hand its restrictions dissuades its use because of the poor capacity of data embedding with respect to the imperceptibility condition. In addition, the few bits embedded in the host image are effortlessly damaged by some specified attacks. Many researchers have been focusing on security and robustness [3], but rarely on the watermarking capacity [4]. Certainly, robustness and security are essential to obtain an irremovable and inappreciable watermark; nevertheless, if we can embed more data in the host image or a loss-less reduced data by compacting it through mathematical transformations, the application can concern many areas. In the present work, a new method for spatial domain watermarking is presented where the limitations of the conventional spatial methods as LSB or CDMA are defeated [5]. The technique uses an encrypted data to embed it through a logarithmic transformation. All the encoded eight bits of the watermark image is hidden through a gain factor chosen with respect to the perceptibility threshold.

## 2. Watermark Encryption

In the proposed algorithm watermark encryption is used for security of watermark. The encryption is performed such that the encrypted image should not increase in size hence the Arnold's Cat Map (chaotic map) is used.

For digital square image, discrete Arnold mapping can be achieve by using following equation.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \left[ \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right] mod\ N$$

The values of square matrix used in above equation can be used as key so that only same matrix can reverse the encryption.

Figure 1: original and shuffled watermark

## 3. Proposed Algorithm

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of spatial domain or to support additional features. Watermarking process is started by applying 3-leveles DWT on the host image. The agreement adopted by many DWT-based watermarking methods is to embed the watermark in the

middle frequency sub-bands HLx and LHx is better in perspective of imperceptibility and robustness. Consequently, HLx coefficient sets in level three is chosen to make to increase the robustness of our watermark against common watermarking attack, specially adding noise and blurring attacks, at little to no additional impact on image quality. Then, the block base DCT is performed on these selected DWT coefficient sets and embed pseudorandom sequences in middle frequencies. The watermark embedding procedure is represented in Figure 2 followed by a detailed explanation.

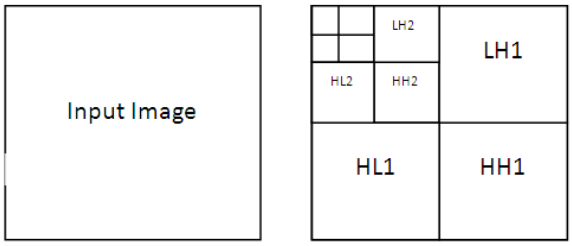


Figure 2: image with its wavelet decomposition Blocks.

Step 1: Perform DWT on the host image to decompose it into four non-overlapping multi-resolution coefficient sets: $LL_1$ , $HL_1$ , $LH_1$ and $HH_1$ .

Step 2: Perform DWT again on two $HL_1$ and $LH_1$ coefficient sets to get eight smaller coefficient sets and choose four coefficient sets: $HL_{12}$, $LH_{12}$, $HL_{22}$ and $LH_{22}$.

Step 3: Perform DWT again on four coefficient sets: $HL_{12}$, $LH_{12}$, $HL_{22}$ and $LH_{22}$ to get sixteen smaller Coefficient sets and choose four coefficient sets: $HL_{13}$, $LH_{13}$, $HL_{23}$ and $LH_{23}$.

Step 4: Divide four coefficient sets: $HL_{13}$, $LH_{13}$, $HL_{23}$ and $LH_{23}$ into 4 x 4 blocks.

Step 5: Perform DCT to each block in the chosen coefficient sets ($HL_{13}$, $LH_{13}$, $HL_{23}$ and $LH_{23}$). These coefficients sets are chosen to inquire both of imperceptibility and robustness of algorithms equally.

Step 6: scramble the watermark signal with Arnold algorithm for key times and gain the scrambled watermark Ws (i, j), key times can be seen as secret key.

Step 7: Perform inverse DCT (IDCT) on each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 8: Perform the inverse DWT (IDWT) on the DWT transformed image, including the modified coefficient sets, to produce the watermarked host image.

**4. Experimental Results**

For the testing of the proposed algorithm following measures are used for assessment of quality of image and watermark.

**Mean absolute error (MAE)** is a quantity used to measure how close forecasts or predictions are to the eventual outcomes. The mean absolute error is given by

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|f_i - y_i| = \frac{1}{n}\sum_{i=1}^{n}|e_i|$$

As the name suggests, the mean absolute error $e_i = |f_i - y_i|$ is an average of the absolute errors, where $f_i$ is the prediction and the true value. Note that alternative formulations may include relative frequencies as weight factors.

The mean absolute error is a common measure of forecast error in time series analysis, where the terms "mean absolute deviation" is sometimes used in confusion with the more standard definition of mean absolute deviation. The same confusion exists more generally.

**Phrase peak signal-to-noise ratio (PSNR)**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

It is most easily defined via the mean squared error (MSE) which for two mXn monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

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

$$= 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20 \cdot log_{10}(MAX_I) - 10 \cdot log_{10}(MSE)$$

Here, $MAX_I$ is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

The proposed algorithm has been extensively tested on various standard images. Table I summarizes the watermarking results.

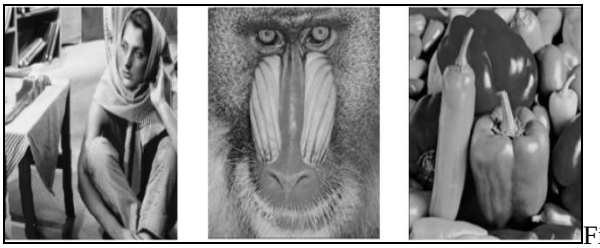

Figure 3: Test images Barbara, Baboon, and Peppers

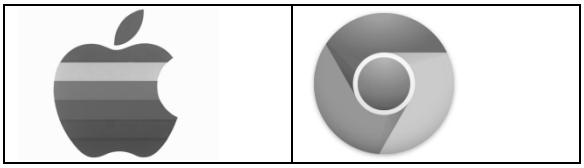

Figure 4: images used for watermarks

Table 1: Experimental results for non-attacked case

| Images | PSNR | MAE |
|---|---|---|
| Barbara | 37.88 | 0.026 |
| Baboon | 37.26 | 0.032 |
| Peppers | 37.45 | 0.014 |

**Blurring Attack**

In order to simulate blurring attack, Gaussian lowpass filter is used as a common blurring attack. It is implemented using Matlab function.

Table 2: Experimental results for blurred image

| Attack | Image | MAE |
|---|---|---|
| Gaussian LPF (hsize = 3,Sigma = 10) | Barbara | 0.039 |
| | Baboon | 0.089 |
| | Peppers | 0.014 |
| Gaussian LPF (hsize = 7,Sigma = 10) | Barbara | 0.012 |
| | Baboon | 0.140 |
| | Peppers | 0.020 |

**Noise Attack**

Table 3: Experimental results for Noisy image

| Attack | Image | MAE |
|---|---|---|
| Salt & Pepper Noise addition (5%) | Barbara | 0.039 |
| | Baboon | 0.058 |
| | Peppers | 0.014 |
| Salt & Pepper Noise addition (10%) | Barbara | 0.061 |
| | Baboon | 0.075 |
| | Peppers | 0.026 |

**Cropping Attack**

Table 4: Experimental results for Cropping Attack

| Attack | Image | MAE |
|---|---|---|
| Cropping (9%) | Barbara | 0.026 |
| | Baboon | 0.032 |
| | Peppers | 0.014 |
| Cropping(18%) | Barbara | 0.051 |
| | Baboon | 0.053 |
| | Peppers | 0.037 |

**Scaling Attack**

Table 5: Experimental results for Scaling Attack

| Attack | Image | MAE |
|---|---|---|
| Scaling(50%) | Barbara | 0.240 |
| | Baboon | 0.284 |
| | Peppers | 0.170 |
| Scaling(75%) | Barbara | 0.086 |
| | Baboon | 0.138 |
| | Peppers | 0.070 |

**JPEG Compression Attack**

Table 6: Experimental results for JPEG Compression Attack

| Attack | Image | MAE |
|---|---|---|
| CPR = 4 | Barbara | 0.034 |
| | Baboon | 0.031 |
| | Peppers | 0.004 |
| CPR = 40 | Barbara | 0.181 |
| | Baboon | 0.161 |
| | Peppers | 0.173 |

**5. Conclusion**

Our study focused on presenting a joint DWT-DCT digital image watermarking algorithm. Proposed method exploits strength of two common frequency domains method; DCT and DWT, to obtain further imperceptibility and robustness. The idea of inserting watermark in the combined transform is based on the fact that jointed transform could eliminate the drawback of each other. Implementation results show that the imperceptibility of the watermarked image is acceptable. Presented method is tested by most of the common

image processing attack such as: different size of Gaussian filtering as an enhancement attack, adding salt and paper noise, scaling with two common factors: 50% and 75%, cropping, and compression attack. this shows that proposed method is more robust compare to previous method, in spite of having the same imperceptibility and complexity.

**References**

[1] Santi Prasad Maity, Malay Kumar Kundu "Robust and Blind Spatial Watermarking in Digital"Image"http://www.isical.ac.in/~malay/Papers/ Conf/ICVGIP_02_WM.pdf.

[2] 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. Third International IEEE Conference on 16-18 Dec. 2007.

[3] Hassen Seddik, Mounir Sayadi, Farhat Fnaiech, and Mohamed Cheriet "A New Spatial Watermarking Method, based on a Logarithmic transformation of An Encrypted embeded Mark" Seventh IMACS Seminar on Monte Carlo Methods (MCM2009) Université Libre de Bruxelles, Brussels, September, 6-11, 2009.

[4] Saeed K. Amirgholipour , Ahmad R. Naghsh-Nilchi, "Robust Digital Image Watermarking Based on Joint DWT-DCT"

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

[6] Jiang-Lung Liu, Der-Chyuan Lou *, Ming-Chang Chang, Hao-Kuan Tso "A robust watermarking scheme using self-reference image" Computer Standards & Interfaces 28 (2006) 356–367.

[7] John N. Ellinas "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection" World Academy of Science, Engineering and Technology 34 2007.

[8] Xiaojun Qi "An Efficient Wavelet-Based Watermarking Algorithm"