Digital image watermarking based on angle quantization in discrete contourlet transform


Department of Computer & Communication Systems Engineering, Faculty of Engineering, University Putra Malaysia, UPM Serdang, 43400 Selangor Darul Ehsan, Malaysia

Received 1 December 2015; revised 10 January 2016; accepted 3 February 2016

KEYWORDS
Contourlet transform; Digital watermarking; Lagrange method; Quantization index modulation

Abstract A robust and transparent watermarking scheme based on contourlet transform and quantization index modulation is proposed in this paper. In proposal algorithm, after taking contourlet, the coefficients are divided into three quadrants by using the symmetric property of the contourlet coefficients, then the angle coefficients are modulated for each of three points. The experimental results revealed that if the information of the image is utilized to determine the watermark and by using quantization index modulation properties, a higher robustness and more effective imperceptibility in proposed algorithm are achieved.

© 2016 King Saud University. Production and hosting by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In recent years, computer networks and digital systems have been widely developed yielding to the rapid growth of internet users and a massive demand for sharing and distributing multimedia data, especially images, sounds and films. As a large number of these data are subject to copyright law, protection of digital documents against illegal distribution is one of the issues which have allocated many researches (Nematollahi et al., 2015a,b,c).

Some recent researches show that watermarking is one of the most effective methods for protecting of digital multimedia (Nematollahi et al., 2015; Malakooti and et al., 2012). Although watermarking faces some major issues, many companies still offer copyright protection and broadcast monitoring based on watermarking (Sharma and Jaiswal, 2015).

Firstly, the embedding of watermark information via watermarking algorithm is more complicated than setting this information in a header file. Secondly, addition of watermark may reduce the vocal or pictorial quality of the main signal.

In a watermarking system, some additional information known as watermark is added to the digital document in the form of noise signal, a different image or a binary sequence of data to be used for rightful ownership and protecting copyright (Nematollahi and Al-Haddad, 2013). The main assumption in watermarking is the additional information should not destroy the quality of the main signal or omit the simplicity from the main signal.

* Corresponding author.
E-mail address: nabdulmawla@yahoo.com (A. Najih).
Peer review under responsibility of King Saud University.

http://dz.doi.org/10.1016/j.jksuci.2016.02.005
1319-1578 © 2016 King Saud University. Production and hosting by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Please cite this article in press as: Najih, A. et al., Digital image watermarking based on angle quantization in discrete contourlet transform. Journal of King Saud University – Computer and Information Sciences (2016), http://dx.doi.org/10.1016/j.jksuci.2016.02.005.
Watermarking techniques are classified into two categories: embedding watermarks in the spatial domain or getting help from different transform domain techniques (Rani et al., 2015). On comparing with the transform domain, the spatial domain needs a shorter processing time and less hardware complexity. Least Significant Bit (LSB) is the simplest technique in the spatial domain which directly modifies the intensity of some selective pixels in an image (Bhatt and et al., 2015).

Transform domain methods are more robust than spatial domain algorithms because of providing the possibility to choose a transform with some desired properties and using it to optimize the embedding of the watermark (Chandran and Bhattacharyya, 2015). Furthermore, for an image, watermarking is atypical in the spatial domain due to its complexity for the resulted signal to be read and modified for aggressors (Chandran and Bhattacharyya, 2015).

In transform domain (or frequency) methods, the information is initially taken to transform domain. Then, the watermark information is embedded to the image via transform coefficients. Well-known transform domain methods are DFT (Cedillo-Hernandez et al., 2012), DCT (Gupta et al., 2015), DWT (Keshavarzian and Aghagolzadeh, 2015), CT (Mohan and Kumar, 2008; Akhaee et al., 2010), and SVD or a combination of them (Fan et al., 2014).

This paper demonstrates the watermarking scheme in the transform domain based on discrete contourlet transform (CT) and angle quantization index modulation (QIM). The main contribution of the paper is to develop a digital image watermarking system which not only provides enough robustness against geometrical and non-geometrical attacks, rather, it provides a good capacity and transparency. Capacity is referred to as carrying enough information to represent their unique identities and transparency is referred to as visual quality of the watermarked image which should not be disturbed by the embedded watermark.

The outline of this paper is as follows. Section 2 describes the background on discrete contourlet transform. In Section 3, the methodology of the proposed method is introduced. Experimental results and analysis are then given in Section 4.

2. Background

CT, as presented by Do and Vetterli (2005), captures the intrinsic geometrical structure that is the key in visual information. The nature of digital data is discrete and makes a challenge in exploring geometry in an image. Unlike the Curvelet method that initially develops a transform in the continuous domain and then discretizes it for sampled data (Channapragada et al., 2015), CT starts with a discrete domain construction and then seeks its convergence to an expansion in the continuous domain. CT generates a discrete domain with multi-resolution and multi-direction expansion by using some non-separable filter banks. It yields to flexible multi-resolution, localization, and directionality for image expansion using contour segments.

Wavelet transform is a multi-resolution transform and is applied in order to identify point discontinuity of an image derived from filter banks in the same way. If wavelet transform is combined to a directional filter bank, point discontinuities can be transformed to a linear structure. This combination is called Pyramidal Directional Filter Bank (PDFB) and its expansion is CT method (Akhaee et al., 2010; Fan et al., 2014; Po and Do, 2006).

Figure 1(a) illustrates a block diagram of CT as an iterated combination of the Laplacian pyramid and the directional filter bank. It has a valuable frequency decomposition and the spectrum is divided either radially and angularly. The obtained frequency division is shown in Fig. 1(b).

In CT, the number of directional bands can be determined by the user. As seen in Fig. 2, the main image is decomposed up to 5 levels, including 1, 2, 4, 8, and 16 under directional band, in which L is low frequency band of image and W, X, Y and Z are directional partial bands (Narasimhulu and Prasad, 2010).

3. Methodology

The combination of discrete CT and QIM in watermarking algorithms results in more robust algorithm against attacks
and adequate transparency of a watermarked image. By considering the features of image in determining the watermark and utilizing Lagrange optimization, a higher robustness can be achieved (Sathik et al., 2011). Similar to JPEG standard that uses discrete cosine transform (Sathik et al., 2011), proposed watermarking methods in this paper have high robustness against compression attacks.

3.1. Watermark generation algorithm

In this section, a watermarking technique for digital images is proposed based on angle quantization. It works based on the energy ratio between two angles which is not very sensitive against any manipulation. This digital image watermarking technique provides authentication over an unknown channel and imperceptibility. Although serious manipulation of the watermarked image can destroy the watermarked bits and replace them with random bit streams, small manipulation may not seriously change these angles. As a result, the quantization of the face’s angles can be a good candidate for our purpose in digital watermarking.

In order to apply angle quantization, each watermark bit is embedded in six sets of the original image. Sets’ sizes of the DCT of the original image, i.e., \((x_1, x_2, x_3, x_4, x_5, and x_6)\) are selected to present a space in the two dimensional coordinate system. Then, three coordinates of \(P(x_1, x_2)\), \(Q(x_3, x_4)\), and \(R(x_5, x_6)\) are considered. The slope and angles among the lines in Fig. 3 are calculated based on Eqs. (1)–(3).

\[
m_1 = \frac{x_4 - x_5}{x_3 - x_1}, \quad m_2 = \frac{x_6 - x_4}{x_5 - x_3}, \quad m_3 = \frac{x_2 - x_4}{x_3 - x_5}
\]

\[
\theta_1 = \arctan \left( \frac{m_1 - m_2}{1 + m_1 \times m_2} \right)
\]

\[
\theta_2 = \arctan \left( \frac{m_2 - m_3}{1 + m_2 \times m_3} \right)
\]

\[\theta \] is quantized to embed the watermark bit in angle quantization. This method cannot tolerate attacks and watermark bits cannot be extracted which may result in serious errors. As a solution, quantization of the ratio between two angles’ points of the original image is embedded by using watermark bits, i.e., embedding one bit only into each of the three points. In order to reduce errors, each watermark bit is frequently embedded into a point. In other words for each of the six image values there are three points. The ratio of angles between these three points are calculated by Eq. (4) as follows.

\[
\text{Ratio} = \frac{\theta_1}{\theta_2}
\]

For the purpose of coefficients’ estimation after angle quantization, the variation for \(\theta_i\) should estimate the optimized values of the equation system as in Eq. (5):

\[
\begin{align*}
\text{Cost} : \quad J(Y) &= \sum ((\theta_i^0) - (\theta_i))^2 \\
\text{Condition} : \quad C(X) &= \sum (\theta_i^0 - \text{Ratio} \times \theta_2) = 0
\end{align*}
\]

For solving this optimization problem, Lagrange method should estimate the optimized values of the equation system as in Eq. (6):

\[
\nabla J(Y) = \lambda \nabla C(X)
\]

The optimized values are simply computed by solving Eqs. (7) and (8).

\[
\theta_i^{0, opt} = \frac{\theta_i}{1 - \lambda_{opt}}
\]

\[
\lambda_{opt} = 1 - \sqrt{\frac{\theta_1}{\text{Ratio} \times \theta_2}}
\]

Then, the amount of \(P^Q\) should be calculated. For this purpose, the value of \(m_i^{0}\) must be computed based on \(\theta_i^0\) as in Eq. (9).

\[
\theta_i^0 = \arctan \left( \frac{m_i^{0} - m_2}{1 + m_i^{0} \times m_2} \right) \Rightarrow m_i^{0} = \frac{\tan (\theta_i^0) + m_2}{1 - \tan (\theta_i^0) \times m_2}
\]

For computing the amount of \(P^Q\), Eq. (10) needs to be solved.

---

*Please cite this article in press as: Najib, A. et al., Digital image watermarking based on angle quantization in discrete contourlet transform. Journal of King Saud University – Computer and Information Sciences (2016), http://dx.doi.org/10.1016/j.jksuci.2016.02.005*
Finally, the amounts of $PQ_X$ and $PQ_Y$ are computed based on Eqs. (11) and (12).

$$PQ_X = \frac{X_4 - m_1^0 \times X_3 - m_3 \times X_5 - X_6}{m_5 - m_1^0}$$  \hspace{1cm} (11)

$$PQ_Y = m_3 \times PQ_X - m_3 \times X_5 + X_6$$  \hspace{1cm} (12)

3.2. Digital image watermarking algorithm

The proposed algorithm consists of two processes including embedding and extraction. Embedding process needs the following steps to be done.

(a) Select the original image for watermarking.
(b) Apply CT on image with $L$ levels to compute the different sub-bands.
(c) Select specific frequency sub-bands in the last level and arrange them into three data coordinate points.
(d) Compute the slopes among these points from Eq. (1).
(e) Compute the angles among these slopes from Eqs. (2) and (3).
(f) Compute the angle ratio for both sets of $m_1$ and $m_2$ as in Eq. (4).
(g) Embed the watermark bit repeatedly into all the ratios of different image partitions based on Eq. (13) as follows.

$$\theta^0 = \left[\frac{\theta + m_1 \times \Delta}{2\Delta + m_1 \times \Delta}\right] \times 2\Delta + m_1 \times \Delta$$  \hspace{1cm} (13)

where $\Delta$ corresponds to quantization steps, $m_1$ is the angle of the angle ratio, and $\theta^0$ is the modified angle of the angle ratio. Selecting small quantization steps gives more invisibility but less robustness.

(h) Apply Lagrange method on set to perform the required changes for minimizing the watermarked distortion as in Eqs. (7) and (8).
(i) Apply inverse CT to reconstruct the watermarked image.

Fig. 4 shows the block diagram of the embedding process in the proposed image watermarking technique.

The extraction process of watermarking is also reversed as described in the following.

(a) Select the original image for watermarking.
(b) Apply CT on image with $L$ levels to compute the different sub-bands.
(c) Select specific frequency sub-bands in the last level and arrange them into three data coordinate points.
(d) Computer slopes among these points.
(e) Computer the angles among these slopes as in Eq. (1).
(f) Compute the angle ratio for both sets of $m_1$ and $m_2$ as in Eqs. (2) and (3).
(g) Compute the angle ratio for both sets of $m_1$ and $m_2$ as in Eq. (4).
(h) Extract the binary watermark bit from angle $\theta$ which is the nearest quantization step to this angle based on Eq. (14):

$$b_k = \arg\min_{b_k \in \{0,1\}} |\theta_k - Q_{b_k}(r_k)|$$  \hspace{1cm} (14)

where is $r_k$ the angle of the angle ratio of the received image, $Q_{b_k}$ is the quantization function while the watermark bits $b_k \in \{0,1\}$.
(i) Perform Step (e) and Step (g) repeatedly for all the partitions of an image.
(j) By embedding the same watermark bit in each partition of an image, different bits extracted from the frame are converted to one bit. For this purpose, a threshold is assumed. When the total number of 1 in the extracted bits is higher than the threshold, the extracted watermark bit is considered as 1. If, the total number of 0 bits is higher than 1’s, the extracted watermark bit is 0.

Figure 4 Block diagram of embedding process in the proposed digital image watermarking technique in the transmitter side.
The developed digital image watermarking system is fragile when the threshold is considered near 1. On the other hand, the robustness of the developed digital image watermarking system is high when the threshold is close to 0.5.

Fig. 5 shows the block diagram of the extraction process in the proposed digital image watermarking technique.

4. Experimental results and analysis

The simulation parameters are assumed as follows.

(a) The size of an image is considered as the same size of a digital image watermarking that preserves the integrity for using watermarking techniques. Therefore, for an image with the size of 512×512 pixels, 262,144 samples are constructed.

(b) The level of the Contourlet transform is assumed as 3. The selected sub-bands for watermarking are explained in Fig. 4 and Daubechies’ Contourlet function has been used for CT.

(c) The size of partitions in the image are considered as 8×8 and the sizes of each set of X and Y in the partitions have been equally divided over 4.

(d) In order to preserve robustness and transparency, the quantization step is assumed as $\Delta = \pi/64$. Whenever the quantization step increases, the fragility of the watermark degrades. Moreover, a higher number of quantization steps results in lower transparency of an image in terms of Peak Signal to Noise Ratio (PSNR).

(e) The threshold for the extraction of the watermark bits is assumed as 0.9.

Fragility and robustness of developed digital image watermarking have a reverse relationship. When the threshold reaches 1, the fragility of the developed digital image watermarking system goes higher. On the contrary, if this threshold decreases to 0.5, the robustness of the developed digital image watermarking system increases. For serious noise (SNR = 0 dB), the threshold value does not affect the fragility of the watermark as the watermark bits have been extracted in a random sequence.

In order to measure the actual performance of the proposed scheme, 20 images with 256 gray levels and size 512×512 are captured from the internet including pictures of Baboon, Lena, Peppers. Collected images have been considered as the original images and the watermarked images have been built by using the original image pixels. MATLAB® version R2013a is utilized for performance evaluation of the algorithm in two aspects: imperceptibility and robustness.

4.1. Imperceptibility test

The imperceptibility level of watermark algorithm was investigated where the PSNR is defined by Eq. (15).

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} (\text{dB})$$

(15)

Mean Square Error (MSE) of the watermarked image and the original image [40] is calculated by Eq. (16) where $F(i,j)$ and $F^\text{WI}(i,j)$ are the pixel values of the coordinate $ij$ in the original image and the watermarked image respectively and $M \times N$ is the size of both images.

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (F(i,j) - F^\text{WI}(i,j))^2$$

(16)

The obtained values of PSNR are greater than 55 dB for all images.

Fig. 6 shows the original image and the watermarked image for peppers. As seen, there is no significant difference between two images. Also, the PSNR for watermarked image is relatively high which can affect the transparency and imperceptibility of the watermark.

4.2. Robustness Test

After extracting the watermark, the normalized correlation coefficient is calculated. Based on Eq. (17) the similarity of extracted watermark with the original watermark is utilized to prove the presence of the watermark.

$$NCC = \frac{\sum_{i=1}^{N^2} H_s(i)H_i(i)}{\sqrt{\sum_{i=1}^{N^2} H_s^2(i)\sum_{i=1}^{N^2} H_i^2(i)}}$$

(17)
The robustness of the algorithm is evaluated for different attacks including:

- Adding salt & pepper noise, Gaussian noise, speckle noise, Poison noise, Gaussian filter, average filter, motion filter, median filter, Wiener filter, cropping, rotation, JPEG compression, JPEG2000 compression, resizing, Histogram equalization, negative image, Gamma correction, and Gaussian blur.

The result of normalized correlation demonstrated the robustness of watermarked image as seen in Table 1. The extraction of four embedded watermarks has been completed successfully in all cases and the correlation values of embedded watermarks and extracted watermarks have been very high. Therefore, the proposed image watermarking based on CT and QIM provides a good robustness. It can be proved by the high amount of correlation between embedded and extracted watermarks for various attacks.

The experimental results of the proposed algorithm is compared with DWT-DCT based (Feng et al., 2010) and DWT-SVD based methods (Malakooti et al., 2012) in Table 2. As delineated, the proposed image watermarking based on CT-QIM provides a higher robustness than DWT-SVD and

### Table 1: The correlation results of extracted watermark after different attacks.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>NCC B1</th>
<th>NCC B2</th>
<th>NCC B3</th>
<th>NCC B4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without attack</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Gaussian noise ($m = 0.6$, $v = 0.01$)</td>
<td>0.9622</td>
<td>0.9973</td>
<td>0.9945</td>
<td>0.9988</td>
</tr>
<tr>
<td>Salt &amp; pepper noise ($d = 0.3$)</td>
<td>0.9868</td>
<td>0.9887</td>
<td>0.9866</td>
<td>0.9942</td>
</tr>
<tr>
<td>Speckle noise ($v = 0.3$)</td>
<td>0.9942</td>
<td>0.9948</td>
<td>0.9963</td>
<td>0.9968</td>
</tr>
<tr>
<td>Poison noise</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Gaussian filter (10 × 10)1.3</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Average filter (10 × 10)</td>
<td>0.9902</td>
<td>0.9646</td>
<td>0.9569</td>
<td>0.9775</td>
</tr>
<tr>
<td>Motion filter (20°, 50)</td>
<td>0.9900</td>
<td>0.9522</td>
<td>0.9229</td>
<td>0.9747</td>
</tr>
<tr>
<td>Median filter (10 × 10)</td>
<td>0.9998</td>
<td>0.9993</td>
<td>0.9977</td>
<td>0.9985</td>
</tr>
<tr>
<td>Weiner filter (20 × 20)</td>
<td>0.9996</td>
<td>0.9992</td>
<td>0.9982</td>
<td>0.9994</td>
</tr>
<tr>
<td>Histogram equalization</td>
<td>0.9992</td>
<td>0.9989</td>
<td>0.9965</td>
<td>0.9979</td>
</tr>
<tr>
<td>Cropping size (384 × 384)</td>
<td>0.9532</td>
<td>0.9478</td>
<td>0.9627</td>
<td>0.9543</td>
</tr>
<tr>
<td>Rotation</td>
<td>0.9843</td>
<td>0.9957</td>
<td>0.9997</td>
<td>0.9887</td>
</tr>
<tr>
<td>Resizing (512–256–512)</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>JPEG2000 ($Q = 1$)</td>
<td>0.9891</td>
<td>0.9871</td>
<td>0.9962</td>
<td>0.9987</td>
</tr>
<tr>
<td>JPEG ($Q = 1$)</td>
<td>0.9994</td>
<td>0.9998</td>
<td>0.9999</td>
<td>0.9997</td>
</tr>
<tr>
<td>Gray scale inversion</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Gamma corrector 1.6</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Gaussian blur</td>
<td>0.9997</td>
<td>0.9930</td>
<td>0.9861</td>
<td>0.9976</td>
</tr>
</tbody>
</table>

### Table 2: Comparison of robustness and PSNR for DWT-DCT (Feng et al., 2010), DWT-SVD (Malakooti et al., 2012) and our algorithm.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>DWT-DCT (Feng et al., 2010)</th>
<th>DWT-SVD (Malakooti et al., 2012)</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>37.716</td>
<td>51.14</td>
<td>61.9914</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>0.9558</td>
<td>0.9567</td>
<td>0.9882</td>
</tr>
<tr>
<td>JPEG</td>
<td>0.9839</td>
<td>0.9658</td>
<td>0.9997</td>
</tr>
<tr>
<td>Average filter</td>
<td>N/A</td>
<td>0.9500</td>
<td>0.9723</td>
</tr>
<tr>
<td>Median filter</td>
<td>N/A</td>
<td>N/A</td>
<td>0.9988</td>
</tr>
<tr>
<td>Rotation</td>
<td>N/A</td>
<td>0.9772</td>
<td>0.9921</td>
</tr>
<tr>
<td>Resizing</td>
<td>N/A</td>
<td>N/A</td>
<td>1.0000</td>
</tr>
<tr>
<td>Histogram equalization</td>
<td>N/A</td>
<td>0.9862</td>
<td>0.9981</td>
</tr>
<tr>
<td>Gamma corrector 1.6</td>
<td>N/A</td>
<td>0.9957</td>
<td>1.0000</td>
</tr>
<tr>
<td>Time (s)</td>
<td>251</td>
<td>242</td>
<td>203</td>
</tr>
<tr>
<td>Memory (Kb)</td>
<td>711,546</td>
<td>734,232</td>
<td>710,984</td>
</tr>
</tbody>
</table>
Digital image watermarking based on angle quantization in discrete contourlet transform

DWT-DCT techniques for different attacks. This is due to embedding the watermark bits in angles of countered domain. Meanwhile the PSNR which demonstrate the quality of image is better.

Time and memory complexity of evaluated techniques were estimated by using profile (‘memory’, ‘on’) function in MATLAB®. In terms of complexity, the developed image watermarking based on CT-QIM required less processing time than DWT-SVD and DWT-DCT techniques and the same memory was required for all simulated techniques.

5. Conclusion

In this paper, a digital image watermarking algorithm was proposed that is a combination of discrete CT and quantization index modulation. Lagrange method was also applied for optimization. In this algorithm, the peak signal to noise ratio was high that demonstrated high imperceptibility of the watermarked image. Furthermore, for most cases the obtained normalized correlation values were almost one which showed a high robustness for the algorithm.

Finally, due to the combination of discrete CT, discrete cosine transform and singular value decomposition, and selection of adequate coefficients for embedding, this algorithm gained high transparency. It also archives a good robustness against attacks.

References


Gupta, G., Joshi, A.M., Sharma, K., 2015. AN efficient robust image watermarking based on AC prediction technique using DCT technique. ICTACT J. Image Video Process. 6 (1).


