Discrete Cosine Transformation Based Image Watermarking for Authentication and Copyright Protection

Ritu Pareek, P.K. Ghosh

Abstract: In this paper, a digital image watermarking algorithm based on DCT transformation is proposed. The imperceptibility and robustness is provided against different attacks. A binary image is embedded in the host image by two different techniques based on DCT. One is middle band coefficient exchange technique, it utilizes comparison of two middle-band DCT coefficients to encode a single bit into a DCT block. Coefficient locations are selected based on the recommended JPEG quantization table. Second is based on PN sequence, PN sequences of the watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies. In extraction stages, the watermarked image, which may be attacked, is processed the same way as the embedding process. Finally, correlation and PSNR values are calculated to determine the level of accuracy and imperceptibility. Experimental results show that the proposed method improved the performance of watermarking algorithm.

Keywords: Discrete Cosine Transform, Digital watermarking, PN Sequence, Middle band frequency, Copyright protection, CDMA.

I. INTRODUCTION

In recent years, the study of watermarking scheme has attracted researchers in the emergent areas of watermarking security and image authentication [1-3]. It is indeed an important research field in Computer science, Cryptography, Signal Processing and Communication [4-8]. Digital Watermarking is an effective solution for protecting intellectual property of audio, image and video data.

Watermarking is broadly classified into two categories, namely Spatial Domain Watermarking and frequency domain watermarking. Frequency domain watermarking is found most robust. The watermarking schemes broadly consist of the three stages: Watermarking generation and Embedding, Distribution, Possible attacks and watermarking detection [9]. The embedded data should preserve the quality of the host signal after watermarking. Basic requirements for watermarking generation are:

(i) Robustness: This refers to the fact that for general signal processing operations [filtering, compression], geometric transformations, malicious attacks, the watermark has the ability of surviving.

(ii) Imperceptibility: The watermarked should not be visible, audible to the human eyes or ears. It means that the quality of the original image after special processing should not be altered.

(iii) Security: The watermark image should only be detected by authorized agent. Illegal detection, extraction of information or modification of the watermark shall not be done by unauthorized user.

(iv) Capacity: This refers to a number of bits that can be embedded in the host image in unit time. The cover image, therefore, needs to have sufficient redundant data. However, Watermarking system may often tradeoff the capacity, security for additional robustness [10].

II. SYSTEM MODEL FOR DIGITAL WATERMARKING

Digital Watermarking embeds data called the watermark or digital signature or some tag or level which stands for particular identity of the owner by some sort of algorithm into a multimedia object. The object may be an image, audio, video or even text. One can extract the watermark to verify the identity of copyright information and ensure legitimate ownership by using appropriate algorithms. In essence a complete digital watermark system comprises of three basic modules:

- The watermark
- Encoder algorithm
- Decoder algorithm

The general framework of watermarking is shown in fig.1

Fig.1 General framework of watermarking system

Revised Manuscript Received on February 05, 2012.

Ritu Pareek, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Mody Institute of Technology and Science (Deemed University), Lakshmangahr, Dist. Sikar, Rajasthan, PIN 332311, India
(e-mail: ritupareek135@gmail.com).

P. K. Ghosh, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Mody Institute of Technology and Science (Deemed University), Lakshmangahr, Dist. Sikar, Rajasthan, PIN 332311, India (e-mail: pkghosh_ece@yahoo.co.in).
The watermark procedure requires the information of original image, the watermark and the key. The role of the key is to determine certain parameters of the embedding function which should be kept secret to avoid eavesdropping by attacks. The secret key should be transmitted to the authenticated receiver for extraction of watermark. Without this key the attacker would not know in which domain the embedding took place. The encoding process begins with an original image, I, a watermark, W and a secret key, K. The watermarked image, I_w is generated by the encoding function as follows

\[ E(I,W,K) = I_w \]  

(1)

The watermarked image I_w may have suffered possible modifications due to channel distortion, noise addition etc. The decoder works with this modified watermarked image I_w, the key K, to extract the image W’ which we call the estimated image through the decoder function

\[ D(I_w,K) = W' \]  

(2)

The estimated watermark image W’ should be identical to the original watermark W. To verify this a comparator function may be used which operates with extracted watermark and the original watermark to generate the binary function x, as shown in fig.1. The comparator function is defined by

\[ C(W',W) = \begin{cases} 1 & \text{if } W' = W \\ 0 & \text{otherwise} \end{cases} \]  

(3)

The extraction of watermark is very useful for verifying ownership.

III. TRANSFORMED DOMAIN DIGITAL WATERMARKING TECHNIQUE

Digital watermarking in frequency domain has been proposed by I.Cox, et al [11] which is based on the idea of spread spectrum communication technology. The algorithm does a kind of orthogonal transformation of the image, embeds the watermark information in the transformed domain of the image and finally takes the inverse transformation for image recovery in spatial domain. This technique has the advantage in terms of transparency, robustness to signal processing and attempts to remove watermark. The robustness is realized by inserting the watermark in the perceptually significant portion of the image.

Most common frequency domain digital image watermarking methods are:

a. Discrete Cosine Transform (DCT)

b. Discrete Fourier Transform (DFT)

c. Discrete Wavelet Transform (DWT)

The watermark algorithm in the frequency domain is summarized as follows:

- Calculation of DCT transform of original image.
- Selection of N random no’s with normal distribution.
- Transformation and superposition based on equation (4).

The random number is used in embedding as well as extraction process. The random number is treated as noise and used for testing robustness for the purpose of security. As a checking, noise is added to the watermarked image to vary the image pixel values by the use of the key. The extraction of original image from the watermarked image without this key will result in blurred image, different from watermark. However by using the secret key at the receiver end the authorized user can extract the watermark.

One another DCT technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (\(F_M\)) of an 8 x 8 DCT block as shown below in figure 2 [13].

![DCT Block Diagram](image)

The correlation factor \(\rho\) lies between 0 and 1.

Mention be made here that the DCT transform is based on the whole image rather than usual block-based approach, this transformation does not provide any local spatial control of the watermarks embedding process. This means that the addition of watermark to one of DCT coefficients affects the entire image. However there is another process that modulates some pre-selected DCT coefficients [12]. The main task of watermark embedding in DCT domain can be formulated as follows:

- Calculation of DCT transform of original image.
- Selection of N random no’s with normal distribution.
- Transformation and superposition based on equation (4).

The random number is used in embedding as well as extraction process. The random number is treated as noise and used for testing robustness for the purpose of security. As a checking, noise is added to the watermarked image to vary the image pixel values by the use of the key. The extraction of original image from the watermarked image without this key will result in blurred image, different from watermark. However by using the secret key at the receiver end the authorized user can extract the watermark.

One another DCT technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (\(F_M\)) of an 8 x 8 DCT block as shown below in figure 2 [13].
Fig. 2 Definition of DCT Region

The middle-band frequencies ($F_M$) of an 8x8 DCT block are shown in Fig.2. In this figure, $F_L$ is used to denote the lower frequency components of the block and $F_H$ is used to denote the higher frequency components. $F_M$ is chosen as an embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First, 8 x 8 DCT of an original image is taken. Then, two locations DCT $(u_1, v_1)$ and DCT $(u_2, v_2)$ are chosen from the FM region for comparison of each 8 x 8 block [14]. These locations are selected based on the recommended JPEG quantization table shown in Table I.

Table I. Quantization values used in JPEG compression scheme

<table>
<thead>
<tr>
<th>m</th>
<th>16</th>
<th>11</th>
<th>10</th>
<th>16</th>
<th>24</th>
<th>40</th>
<th>51</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>16</td>
<td>12</td>
<td>12</td>
<td>14</td>
<td>19</td>
<td>26</td>
<td>58</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>13</td>
<td>16</td>
<td>24</td>
<td>40</td>
<td>57</td>
<td>69</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>17</td>
<td>22</td>
<td>29</td>
<td>51</td>
<td>87</td>
<td>80</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>22</td>
<td>37</td>
<td>55</td>
<td>68</td>
<td>109</td>
<td>103</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>35</td>
<td>55</td>
<td>64</td>
<td>81</td>
<td>104</td>
<td>113</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>64</td>
<td>78</td>
<td>87</td>
<td>103</td>
<td>121</td>
<td>120</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>72</td>
<td>92</td>
<td>95</td>
<td>98</td>
<td>112</td>
<td>100</td>
<td>103</td>
<td>99</td>
</tr>
</tbody>
</table>

If two locations are chosen such that they have identical quantization values, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. Embedding in DCT domain is simply done by altering the DCT coefficients.

Another possible technique is to embed a PN sequence $W$ into the middle frequencies of the DCT block. We can modulate a given DCT block $(x, y)$ using the equation shown below for embedding of CDMA watermark into DCT middle frequencies:

$$I_{Wx,y}(u,v) = \begin{cases} I_{xy}(u,v) + k \times W_{xy}(u,v), & u,v \in F_M \\ I_{xy}(u,v), & u,v \in F_M \end{cases}$$

For each 8 x 8 block of the image, the DCT for the block is first calculated. In that block, the middle frequency components FM are added to the pseudo random noise sequence W, multiplied by a gain factor k. Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give us our final watermarked image $I_w$.

IV. MATHEMATICAL ANALYSIS

We can consider an image $x(m,n)$ as a matrix MxN in the spatial domain. The 2-D DCT can be obtained with the following expression:

$$X[k,l] = \frac{2}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} x(m,n) \cdot e^{j(2\pi k m/N)} e^{j(2\pi l n/M)}$$

$$K = 0,1,2, \ldots ,M-1; \quad l = 0,1,2, \ldots ,N-1$$

The inverse transform of DCT is:

$$x(m,n) = \frac{2}{\sqrt{MN}} \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} c(k) c(l) X(k,l). e^{j(2\pi km/M)} e^{j(2\pi ln/N)}$$

The effectiveness of digital watermarking technique for embedding and extraction of watermark image are evaluated by the metric called Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE).

The equation of PSNR can be described as:

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

where, M is taken to be 256.

The expression for MSE of the image with MxN pixels is defined as:

$$\text{MSE} = \frac{1}{MN} \sum (f(m,n) - \overline{f(m,n)})^2$$

where, $f(m,n)$ is the original pixel value and $\overline{f(m,n)}$ is the processed pixel value.

V. EXPERIMENTAL RESULTS

We select a 512 x 512 pixels, grayscale Lena as the original image and 20 x 50 pixel grayscale image as the watermark image as shown in figure 3. There are 256 different grayscale level in the original image (8-bit resolution).
Table III demonstrate the results of proposed method precision versus common image processing attacks. The success rates of watermark extraction are listed. There is a trade-off between imperceptibility and robustness. Mid-Band coefficient exchange is quite efficient against JPEG compression, cropping, noising and other common image manipulation operations. The use of two PN sequences watermarking is based on the idea of spread spectrum communications. Table IV shows the quality rates under various executions and Table V shows PSNR and NC values for different values of k (gain factor).

Table IV. Quality rates under various executions

<table>
<thead>
<tr>
<th>k</th>
<th>JPEG Q60</th>
<th>JPEG Q20</th>
<th>Salt &amp; Pepper Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.8755</td>
<td>0.8958</td>
<td>0.8606</td>
</tr>
<tr>
<td>15</td>
<td>0.9729</td>
<td>0.8972</td>
<td>0.8892</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>0.8978</td>
<td>0.899</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>0.9109</td>
<td>0.9396</td>
</tr>
<tr>
<td>50</td>
<td>1</td>
<td>0.9723</td>
<td>0.982</td>
</tr>
<tr>
<td>70</td>
<td>1</td>
<td>1</td>
<td>0.9938</td>
</tr>
</tbody>
</table>

The technique is motivated by perceptual transparency and watermark robustness. Results of the correlation-based DCT techniques were fairly similar. Correlation-based DCT appeared to be slightly weaker for lower levels of distortion, yet stronger for the higher levels. The use of two PN sequences is better in almost all aspects.

The elapsed time of embedding and extraction process for different values of k is more or less the same. PSNR above 20dB shows perceptually good watermarked image. In Table V as the JPEG Quality (Q) increases the PSNR increases and for particular JPEG quality decreases as k increases.

REFERENCES


Table V. The Quality rates under various executions

<table>
<thead>
<tr>
<th>k</th>
<th>JPEG Q20</th>
<th>JPEG Q60</th>
<th>JPEG Q100</th>
<th>Salt &amp; Pepper Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR</td>
<td>NC</td>
<td>PSNR</td>
<td>NC</td>
</tr>
<tr>
<td>5</td>
<td>33.5196</td>
<td>.8065</td>
<td>36.5456</td>
<td>.8286</td>
</tr>
<tr>
<td>10</td>
<td>33.1722</td>
<td>.8454</td>
<td>32.8056</td>
<td>.9842</td>
</tr>
<tr>
<td>20</td>
<td>28.7331</td>
<td>.9397</td>
<td>27.7682</td>
<td>.9911</td>
</tr>
<tr>
<td>30</td>
<td>23.1015</td>
<td>.9905</td>
<td>23.9516</td>
<td>.9989</td>
</tr>
<tr>
<td>50</td>
<td>21.8071</td>
<td>.9922</td>
<td>20.7600</td>
<td>.9990</td>
</tr>
<tr>
<td>70</td>
<td>17.1751</td>
<td>1</td>
<td>19.2363</td>
<td>.9994</td>
</tr>
</tbody>
</table>

AUTHORS PROFILE

Ritu Pareek was born in Jaipur, India in 1989. She received her B.Tech degree in 2010 from Rajasthan Technical University, Kota. She is pursuing her M.tech in Signal Processing from Mody Institute of Technology and Science (MITS), Lakshmangarh.

Dr. P.K. Ghosh was born in Kolkata, India in 1964. He received his B.Sc (Hons in Physics), B.Tech and M.Tech degrees in 1986, 1989, and 1991, respectively from Calcutta University. He earned Ph.D.(Tech) degree in Radio Physics and Electronics in 1997 from the same University. He served various institutions, namely, National Institute of Science and Technology (Orissa), St. Xavier’s College (Kolkata), Murshidabad College of Engineering and Technology (West Bengal), R. D. Engineering College (Uttar Pradesh) and Kalyani Government Engineering College (West Bengal) before he joins Mody Institute of Technology and Science (Rajasthan). To his credit, he has more than 30 research papers in Journals of repute and conference proceedings. He is life member of Indian Society for Technical Education (ISTE), New Delhi. His research interests are in the areas of reduced order modeling, VLSI circuits & devices, wireless communications and signal processing.