Two Level DCT and Wavelet Packets Denoising Robust Image Watermarking

N.Koteswara Rao ¹, Y.Murali Krishna ²

¹, ² Department of Electronics and Communication Engineering, Narasaraopeta Engineering College, Narasaraopet, Andhra Pradesh, India.

¹ PG Student

² Asst Professor

E-mail: kotes408@gmail.com ¹, yadavalli437@gmail.com ²

Abstract — In this paper we present a low frequency watermarking scheme on gray level images, which is based on DCT transform and spread spectrum communications technique. The DCT of non overlapping 8x8 blocks of the host image is computed, then using each block DC coefficients we construct a low-resolution approximation image. We apply block based DCT on this approximation image, then a pseudo random noise sequence is added into its high frequencies. For detection, we extract the approximation image from the watermarked image, then the same pseudo random noise sequence is generated, and its correlation is computed with high frequencies of the watermarked approximation image. In our method, higher robustness is obtained because of embedding the watermark in low frequency. In addition, higher imperceptibility is gained by scattering the watermark’s bit in different blocks. We evaluated the robustness of the proposed technique against many common attacks such as JPEG compression, additive Gaussian noise and median filter. Compared with related works, our method proved to be highly resistant in cases of compression and additive noise, while preserving high PSNR for the watermarked images.

Key Words — Blind Digital Watermarking, DCT, JPEG compression, Spread Spectrum Watermarking

I. INTRODUCTION

In recent years, many digital watermarking techniques have been proposed to protect the copyright of digital multimedia data. Watermark embedding is performed in many domains such as spatial, Fourier transform, DCT1 and DWT2.

One of the commonly used domains for embedding a watermark in an image is the DCT. DCT splits up the image into the frequency bands, so upon the application, the watermark can be embedded in different frequencies. Furthermore, the sensitivity of human visual system to DCT frequencies has been extensively studied; which resulted in the recommended JPEG quantization table. These results can be used for predicting and minimizing the visual impact of distortion caused by embedding the watermark.

If we know the image compression domain, for example DCT, then it is better to embed watermark in those DCT coefficients which are unlikely to be discarded during the compression process. Since we are able to anticipate which DCT coefficients will be quantized by the compression scheme, we can choose not to embed the watermark in those coefficients. This approach can be extended to compression methods in other domains, as well. Furthermore, it is a common practice to apply additive noise for watermark embedding and use the correlation techniques for detection. In a watermarking technique is provided in which a watermark is embedded as pseudo-random noise sequences into middle-frequency range of the image.

The major objective of this paper is to develop a watermarking algorithm based on DCT and spread spectrum communications in such a way that it is highly robust with respect to JPEG compression and also other common attacks. Compared with similar works, our method provided the highest robustness for extracted watermark especially when JPEG compression was applied to the watermarked image. In addition, this high level of robustness did not decrease its PSNR3 (PSNR is defined in section 4).

The rest of paper is structured as follows. In Section 2, some related works are introduced, and then in section 3 a new watermarking method is proposed. In Section 4, the performance of the proposed watermarking method is evaluated by
Two Level DCT and Wavelet Packets Denoising Robust Image Watermarking

applying various attacks including JPEG compression and adding Gaussian noise to the watermarked images. In section 5, the comparison of proposed method with other methods is reported. Finally in Section 6 we conclude our method.

II. RELATED WORKS

Existing literature reveals two techniques for the watermarking of images: transform domain and spatial domain. Most of the recent watermarking schemes employ mainly the frequency domain approach because it is superior to the spatial domain approach in robustness and stability.

However, there is a crucial question that should be answered: which frequency band in frequency domain can be robust and imperceptible to various attacks? According to Weber’s rule, the low frequency area is more robust than high and middle frequency areas. There have been various methods to embed the watermark into the low frequency area. It is known that embedded watermark in the prior approaches are robust to various attacks to a certain extent but it is likely to be destroyed if the distortion exceeds a particular level. Despite their robustness, the key concern is that if the low frequency components are changed, the image quality is degraded and the watermark becomes meaningless. Thus, of importance is to make the modifications that made by watermark embedding in low frequency coefficients as low as possible. This problem can be solved by using spread spectrum communication techniques for embedding watermark in low frequencies.

In spread spectrum communications, a narrowband signal is transmitted over a much larger bandwidth such that, the signal energy present in any single frequency is imperceptible. Similarly, in spread spectrum watermarking schemes, the host image is viewed as a communication channel, while the watermark is viewed as a signal to be transmitted. So the watermark is spread over many samples of the host signal by adding a low energy pseudo-random noise sequence to them. The embedded watermark sequence is detected by correlating this specific pseudo random noise sequence with the watermarked signal itself.

Some techniques are proposed in which the watermark is embedded in the middle and high frequency components. The low frequency components are left unchanged in order to decrease the visibility of the watermark. Embedding the watermark in middle and high frequency components makes these techniques vulnerable to attacks such as compression and noise addition.

It is known that most of the energy of natural images is concentrated in the lower frequency range. Therefore, most lossy compression methods quantize and discard the information hidden in the higher frequency components. However, the human eye is more sensitive to noise in lower frequency components than in higher frequency ones. In order to invisibly embed the watermark that can survive lossy data compressions, a reasonable trade-off is to embed the watermark as low energy pseudo-random noise sequences into the low-frequency range of the image.

Also there are other arguments that, using the same transforms for both watermarking and compression will result in optimal performance or using complementary transform. For example, Fei et al. proposed using complementary transforms can potentially provide greater robustness.

But in this paper we show that using the same transforms for both watermarking and compression demonstrates the superiority of robustness and performance. That is, by anticipating which coefficients would be modified by the subsequent transform and quantization, we were able to produce a watermarking technique which has the highest resistance to JPEG compression compared with well known recent works. We could extract the watermark even if the watermarked image is compressed by JPEG with quality factor of 1%

Moreover, watermarking techniques can be divided into two distinct categories depending on the necessity of original images for the watermark extraction. Although existence of original image may facilitate watermark extraction to a certain extent, two problems can come out: (1) At the risk of insecurity the owners of original images may be compelled to share their work with anyone who wants to check the existence of the watermark and (2) it is time-consuming and cumbersome to search out the originals that correspond to a given watermark within the database. Thus, in order to overcome these problems we need a method for extracting the embedded watermark without requiring the original image.

This method is called a blind watermarking technique. Such techniques appear far more useful since the availability of an original image is usually unwarranted in real-world scenarios.

As described, for extraction of watermark from watermarked image we do not need to have the original host image.

Recently, research efforts have been devoted to security analysis in which successful attacks have been proposed to defeat previously proposed multimedia authentication systems. It is well known that many digital watermarking schemes, especially quantization based schemes, are weak against well-designed sophisticated attacks. Therefore, in the watermark-based authentication systems, security of the overall system including authenticator generation and embedding must be considered. In our development, we assume Kerckhoff’s principle which requires that the opponent knows the details of all
aspects of the authentication system except for the secret key shared between the transmitter and the receiver. We adopt the following stringent definition of security: given that an opponent has full knowledge of the watermarking system details except for the secret key, it must be computationally infeasible for the opponent to alter the watermarked data in an illegitimate manner such that the modified copy is wrongly accepted as legitimate.

III. PROPOSED METHOD

In this paper, we propose a novel watermarking scheme which is based on low frequencies of DCT transform and spread spectrum watermarking. In this method all the DC components of the block DCT transform of the original image are grouped together to form a pseudo image called DC image. Then each bit of the watermark is scattered through the high frequencies of DCT transform of this DC image. In other word, each bit is scattered in 64 blocks of the original image. Therefore, we obtain the robustness because of embedding the watermark in low frequency and gain the imperceptibility by scattering the watermark's bit in different block.

We then compute the NC4 and PSNR to judge the robustness and the invisibility of the watermarking algorithm (NC and PSNR are defined in section 4). The PSNR values for watermarked images are all greater than 38 dB, which is the empirical value for the image without any perceivable degradation.

A. Embedding Algorithm

Without loss of generality, we assume the host image is of size 512x512. BDCT5 is applied on 8x8 non-overlapping blocks. Then to embed the watermark, for each 8x8 transformed block of host image, only its DC coefficient is selected out of the 64 DCT coefficients. In each block, DC coefficient is the most important coefficient which has the largest value. Embedding watermark in DC coefficient makes the watermark robust against many attacks. Those selected coefficients are then mapped into a reduced image which is called low-resolution approximation image (LRAI). Therefore, the size of extracted LRAI is always 1/64 of the host image. For example for 512x512 host images, the size of extracted LRAI is always 64x64 pixels (Fig.1).

After extracting LRAI from host image, the extracted LRAI is divided into 8x8 non-overlapping blocks and BDCT of each block is calculated. Then according to the value of watermark bit which is going to be embedded in each block, a pseudo random noise sequence is added to the high frequencies of DCT transform of each 8x8 block of LRAI using equation (1). There are different definitions for high frequencies in a DCT block, but our experiments shows that the definition which is shown in Fig. 1 has low visual impact on watermarked image and also provides more accurate watermark detection.
Two Level DCT and Wavelet Packets Denoising Robust Image Watermarking

Coefficients in the low and middle frequencies that are copied over to the watermarked LRAI remain unaffected.

\[
L_{x,y}^w (u,v) = \begin{cases} 
    L_{x,y} (u,v) + k \times W_{x,y} (u,v), & u,v \in F_H \\
    L_{x,y} (u,v), & u,v \notin F_H
\end{cases}
\]

In (1), \(L\) denotes DCT transform of LRAI, \(F_H\) the high band frequencies, \(k\) the gain factor, \((x,y)\) the location of an 8x8 block of LRAI, \((u,v)\) the DCT coefficient in the corresponding 8x8 block of \(L\), and \(W_{x,y}\) the pseudo random noise sequence according to the value of \(i\).

We should note here that two separate pseudo random noise sequences are used to represent the bit values of 0 and 1. Furthermore, by choosing these two pseudo random noise sequences to be as un-correlated as possible, we can significantly reduce the rate of false detection.

Then each block is inverse-transformed to give us watermarked LRAI. The final step to construct the watermarked image is to replace the DC coefficients of LRAI with their corresponding watermarked ones, and then compute the IDCT transform of each 8x8 block of watermarked LRAI.

Since in each block of LRAI only one bit of watermark is embedded, so for a host image of size 512x512, watermark size is limited to 8x8 pixels. In other words, assume the size of host image is \(2^m \times 2^n\) so the size of extracted LRAI will be \(2^{m-1} \times 2^{n-2}\) and maximum size of watermark will be \(2^{m-2} \times 2^{n-4}\). Regarding to the watermark size we should note that practically a character string of length 10, or seventy bits, is enough for generation of an identification code and the authentication purpose.

The embedding algorithm is summarized as follows:

<table>
<thead>
<tr>
<th>Embedding algorithm:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Compute BDCT of host image.</td>
</tr>
<tr>
<td>2. Create LRAI.</td>
</tr>
<tr>
<td>3. Compute BDCT of LRAI.</td>
</tr>
<tr>
<td>4. Embed each bit of Watermark, as a pseudo-random noise sequence into (F_H) coefficients of each 8x8 block of transformed LRAI.</td>
</tr>
<tr>
<td>5. Compute IBDCT of watermarked LRAI</td>
</tr>
<tr>
<td>6. Replace the watermarked DC coefficients with the original ones in LRAI.</td>
</tr>
<tr>
<td>7. Compute IBDCT of LRAI.</td>
</tr>
</tbody>
</table>

B. Extraction Algorithm-

To detect the watermark, the same pseudo-random noise generator algorithm is seeded with the same key. It is known using a different key a seed of pseudo random noise generator will produce a different sequence of random numbers In this case the extraction algorithm will not detect the watermark pattern.

As it was explained in the embedding algorithm,for embedding the watermark we benefit from spread spectrum watermarking technique in a way that each bit of watermark is encoded as a pseudo random noise sequence and then it is added to the coefficients of the host image.By using this technique similar to the proposed method,we use wavelet packets denoising method to extract the noise distortion that was added to the host image in watermark embedding stage.In order to do this ,first the watermarked image must be denoised and then by subtracting the denoised image from watermarked im age, a new image will be created. This new image indicates the noise that was added to the host image by embedding the watermark.By performing the same actions as explained in embedding algorithm in previous section the transformed LRAI of difference image is constructed.Then the correlation between blocks of transformed LR A1 with both noise patterns related to bit values 0 and 1 are computed. If the higher correlation was obtained with noise pattern 0, then a watermark bit of 0 is detected. A watermark bit of 1 is detected in a similar way.

The presence of watermark is detected by comparing the average correlation coefficient of detected watermark with a pre-defined threshold. The watermark is considered to be present if the average correlation is greater than this threshold (fig. 4). The extraction algorithm is given as follows:
Extraction algorithm:
1. De noise watermarked image,
2. Calculate difference image by subtracting de noised image from watermarked image,
3. Do steps 1 through 3 from the Embedding algorithm for difference image,
4. Compute the correlation between each block of transformed LRAI, and both noise pat terns for one and zero bits,
5. Choose the noise pattern with higher correlation related to the extracted watermark bit,
6. Compute the average correlation coefficient over all extracted watermark bits, and then compare it with a pre-defined threshold. The Watermark is considered to be present if the average correlation coefficient is greater than the threshold.

In Fig. 2 the Goldhill image that is watermarked with gain factor $k=30$ is shown. As it is seen, watermarking this image with this gain factor has no visual impact on the host image and PSNR of watermarked image is around 43 dB. Although the extracted watermark using our previous method is detectable but it has 4 bits of error but we improved our previous work as follows. First the watermarked image is denoised by wavelet packets denoising with default parameters, available in Matlab R 2007b, (fig.3). Then the difference image is calculated (fig.5). Finally, the hidden watermark in difference image is extracted by the proposed method. In this method extracted watermark will be recovered with no error and $NC=1$.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS
Two Level DCT and Wavelet Packets Denoising Robust Image Watermarking

The proposed technique has been conducted on different standard test (host) images of size 512x512 with different level of details. Also robustness of the proposed technique against most common attacks is evaluated. For applying the attacks to the watermarked images, Stirmar and Checkmark benchmarks are used. An 8x8 watermark pattern as shown in fig. 5 is embedded in the host images. Some experimental results on Goldhill test image which is watermarked with gain factor k=30 are given in Figs. 6~7. In our experiments, we compute the PSNR to judge the difference between the original image and watermarked image or the attacked watermarked image. The PSNR similarity measure is defined as follows:

$$\text{PSNR} = 10 \log_{10} \frac{M_1 \times M_2 \times \max(f(i,j))^2}{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} [f(i,j) - f'(i,j)]^2} \quad (\text{dB})$$  \hspace{1cm} (2)

where $M_1$ and $M_2$ are the size of image, $f(i,j)$ the original image, $f'(i,j)$ is the watermarked image, or the attacked watermarked image. Also, we compute NC to quantitatively analyze the similarity of the extracted and the original watermark.

$$\text{NC} = \frac{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W(i,j) \times W'(i,j)}{\sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W(i,j)^2} \times \sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W'(i,j)^2}}$$  \hspace{1cm} (3)

where $M_1$ and $M_2$ are the size of watermark image, $W(i,j)$ and $W'(i,j)$ are the original and the extracted watermark, respectively. In the following to analyze the performance of our method, first as a sample, we show its robustness with respect to JPEG compression and Gaussian noise when an image is watermarked with one gain factor. Then to provide a more detailed analysis we watermark the Lena image with several gain factors and show its behavior when the watermarked image has gone through different attacks such as JPEG and JPEG2000 compression, different kinds of noise and etc. And finally we show the result of analysis when several images are watermarked using different gain factors.

A. A sample of performance analysis for gain factor $k=30$

In this section we present the robustness with respect to JPEG and Gaussian noise for only one gain factor ($k=30$).

JPEG compression

Digital images usually are stored and transmitted after image compression. JPEG is popular among image compression methods for still images. We examined the robustness of the proposed scheme by compressing the watermarked images with JPEG compression with quality factor 8 (Fig. 6). The extracted watermark from this picture is also shown. As it is seen in Fig. 6 even by setting the quality factor of JPEG compression to 8%, the watermark is extracted with NC=0.96 which is greater than the empirical threshold of NC=0.4. This is one of the most important advantages of our method.

Noise addition

We evaluate the robustness by adding Gaussian noise on the watermarked image. Fig. 7 shows the result of adding 20% Gaussian noise to the watermarked image. Although the attacked image is absolutely distorted by additive Gaussian noise which drops its PSNR to 9.07 dB, the watermark is extracted with NC=0.71 (Fig.14). It indicates that the proposed scheme is also robust to noise attack.

B. Performance analysis in presence of different attacks for different gain factors

In this section we discuss the robustness of our proposed method against most common attacks on the standard image of Lena that is watermarked with different gain factors.
Gaussian noise

In Fig. 8 robustness is tested against adding Gaussian noise of different variances. Based on the results of Fig. 8, we can conclude that increasing gain factor in embedding procedure, increases the robustness of watermark against Gaussian noise.

JPEG and JPEG2000 Compressions

Fig. 9 and Fig. 10 show the results of applying JPEG and JPEG2000 compressions with different compression ratios to test image Lena which is watermarked with different gain factors. As it is clear from these figures, by increasing gain factor, Robustness of watermark is improved. For example for Lena which is watermarked with gain factor of 25, and compressed using JPEG with QF=1% the correlation of extracted watermark and original watermarks about 0.73. This shows the great robustness of our method against JPEG compression. Note that according to Fig. 11, PSNR of the watermarked image with gain factor 25 is about 44 db.

C. Performance analysis with several gain factors on different images

In Fig 11 and Fig 12 we show the results obtained by applying the proposed method on 8 different standard gray scale images (Lena, Boat, Mandrill, Barbara, Goldhill, Pepper and Zelda). All of them were sized 512x512. From Fig. 11 it is understood that higher gain factors make lower PSNR for watermarked images, but as shown in Fig. 12 the correlation of original watermark and the extracted watermark gets better for higher gain factors. The trade-off between visual quality and watermark robustness is about gain factors 25 to 30.
In this section, we compare the average robustness of the proposed method with 3 other recently published methods which will be described later in this section. Also we compare the results with our previous method which did not have the denoising scheme.

The proposed scheme is based on embedding a pseudorandom sequence of real numbers in DCT coefficients of each segment of the host image. It relies on some of the ideas proposed by Cox et al. and outperforms the Cox algorithm but still it is not robust against most of attacks. In their scheme, rather than embedding the watermark globally in the host image as the Cox algorithm suggests, the host image is first segmented in different segments based on Voronoi diagram and the feature extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment. This method is referred as Seg-DCT.

In an approach is proposed which is based on the method given by Dugad et al. In the watermark is embedded in the discrete multi-wavelet transform (DMT) coefficients that are larger than some threshold values. They use the GA6 techniques to search for optimal values for these parameters in order to achieve optimum performance. They compared the experimental results before and after optimization using GA and also compared them with the results of previous works. We choose GA-Dugad method which has the best performance from to compare with our results.

In two novel transforms are defined, which are respectively called DWT-IDCT transform and DCT-IDWT transform. Then two novel watermarking schemes based on these two transforms are proposed. The authors claim that the scheme based on DCT-IDWT has better robustness against the attacks than the other, so we choose it to compare with our method.

In Fig. 13 the average robustness of our proposed method and other mentioned methods against JPEG compression with different quality factors are shown. As described before, and it is clear from this figure, our proposed method has the highest robustness against JPEG compression.

In Fig. 14, robustness of the mentioned methods against median filtering of different size is reported. This figure shows that even against median filtering of size 9x9 our proposed method has higher robustness compared with other methods.
VI. CONCLUSION

In this paper, we proposed a DCT-based blind watermarking scheme based on spread spectrum communications. The low frequency nature of the proposed algorithm makes the embedded watermark very robust to common image manipulations such as filtering, scaling, compression and malicious attacking. By anticipating which coefficients would be modified by the subsequent transform and quantization, we were able to produce a watermarking technique which to the best of our knowledge has the highest resistance to JPEG compression compared with well known similar works. We could extract the watermark even if the watermarked image is compressed with JPEG with quality factor of 1%. In addition, our method is also robust with respect to additive Gaussian noise, median filtering and other attacks that were mentioned in this paper.

In our future works, we will try to generalize the proposed method for color images. Also we will consider other compression techniques like EPIC, SPIHT, EZW and JPEG2000 for watermarking. Since for each compression technique, it is better to embed watermark in those coefficients which are unlikely to be discarded during the compression process. For a known compression technique we are able to anticipate which coefficients will be quantized by the compression scheme; thus we can choose not to embed the watermark in those coefficients. So the watermark will be robust against that compression technique.

REFERENCES


Two Level DCT and Wavelet Packets Denoising Robust Image Watermarking


