Proposed Randomized Regular DCT Coefficients Algorithm for “Image Watermarking Against Blind Detection”

Jitendra Avasthi, Rahul Sharma, Vijay Kumar Sharma

Abstract—Shoppers printed with watermarked pictures will mix along to notice the watermark from the printed image. Detector will compare the photographs to urge the common watermarked pixels from the image. A replacement theme is planned that uses the options of separate circular function remodel Discrete Cosine Transform (DCT) for the entering of the watermark coefficients and uses a pseudo-random sequence for choice of the DCT coefficients to embed the watermark. These coefficients are dissimilar in numerous watermarked pictures thus there’s no probability of collusion of the watermarked pictures to notice the watermark illegitimately. The theme is healthier than the other watermarking algorithms like LSB based mostly watermarking; it's conjointly higher than the DCT mid-band theme wherever the coefficients to enter the watermark are perpetually fastened, and also the watermark is embedded by merely exchanging the coefficients in keeping with the watermark bits. Having all the properties of DCT watermarking this algorithmic rule enhances the strength of the watermark by involving the constant averaging construct. The prospect of a successful attack on the watermark by associate assaulter is extremely less attributable to use of this averaging technique. The main advantage of the theme is that the image is disorganized before embedding of the watermark and descrambled once embedding. This ends up in spreading of the watermarking data throughout the watermarked image and it's terribly tough to notice it. The correlation results show that the watermark is extremely strong. Since no presence of watermark are often detected.

Index Terms—Encoding, Decoding, Scrambling

I. INTRODUCTION

Watermarking is the process of inserting hidden information in an image by introducing modifications to its pixels with minimum perceptual disturbance. A recent survey of major techniques appears in [1][2]. A fixed number of highest magnitude DCT coefficients are randomly disturbed, so that the watermark is placed to the perceptually significant components of the image. Even though the method is quite robust against signal manipulations, the original image must be present for watermark recovery. Recently, the pursuit of a scheme that does not need the cover image during watermark recovery has become a topic of intense research. This is partly due to practical issues, like the fact that the recovery process can be simplified without comparison with the original image. Also, in many instances, release of original material for any purposes is not desired or prohibited[3][4][5].

An attack in watermarking technology is any processing that may impair detection of the watermark. Early attacks, such as random geometric distortions relied on the fact that most watermarking algorithms are based on some form of correlation, which itself requires good alignment properties. Breaking this alignment usually prevents reliable detection. Current techniques reported in the literature for watermarking benchmarks concentrate mainly on images and can be grouped into two main classes. The first group includes the attacks which attempt to remove the watermark and the other group those which just prevent the detector from detecting them. Random geometric distortions fall in the second category. Attacks in the first category usually try to estimate the original non-watermarked cover-signal, considering the watermark as noise with given statistic.

The concept of watermarking is very old and it is using more than thousand years back. Watermarking technique used by paper manufacturers to identify their products. Today, watermarks in paper can still be seen.Along with the years the concept of watermarking has penetrated into the field of security. Currency, such as rupees note, checks, postal stamps, and official documents can be seen to carry watermarks. Same degree of security in digital data can be achieved with the help of watermarking [6].

Manuscript received March 22, 2015
Jitendra Avasthi, Research Scholor, Rajasthan Institute of Engineering & Technology, Jaipur
Rahul Sharma, Assistant professor (CSE) Rajasthan Institute of Engineering & Technology, Jaipur
Vijay Kumar Sharma, Assistant professor (CSE) Rajasthan Institute of Engineering & Technology, Jaipur
In still image watermarking there exist two major types of watermarking: visible and invisible types. Visible watermarking marks a logo or text on the image of interest and resembles the traditional paper-based ones. The information or image is visible in the picture or video. The watermark is in form of text or a logo which is used to identify the owner of the original document. The image on the right in figure 2 shows the visible watermark in the form of image.

III. TYPES OF WATERMARKING

Different types of watermark currently available which are used for different – different applications. So watermarks are classified by their definitions, their features and possible applications, advantages and disadvantages (see Fig.3).

Watermarking in DCT Domain

The watermarking techniques in the DCT domain allow an image to break up into different frequency bands, making it much easier to include information about water marks on the appropriate frequency bands of an image. The low frequency band carries the most important parts of the visual image. Furthermore, the high frequency band is exposed to the attack phase through compression and noise. The middle frequency bands are employed to prevent the withdrawal, which means through compression, and contain no important visual information[8]. Therefore, the frequency bands mean suitable insertion region watermark. The
two-dimensional (2-D) DCT and its counterpart in 2-D inverse DCT, are the most complex systems in DCT-based watermarking [8].

**Digital Watermarking Based on DCT in Invariant Wavelet Domain**

Xin-Yang Huang et al [9] Persisting geometric attacks in image watermarking is measured to be of great reputation. In the face of geometrical attacks, all failings of nearly all digital watermarking algorithms have been uncovered. This paper presents an enhanced invariant wavelet that is better than the bilinear exclamation and whose presentation is close to of bi cubic when scaling factor identical close to 1, and designs a original blind image watermarking algorithm created on DCT in the Rotation- then Scaling- then Translation- (RST) Xiong’s Invariant Wavelet, i.e. RSTXIW domain.[9].

Xin-Yang Huang et al [9] presents a better invariant wavelet, whose scaling error is fewer than of bilinear interpolation and is identical close to of bi cubic interpolation when scaling factor identical close to 1, and provides a novel watermarking outline based on DCT in RSTXIW field, which is robust to several attacks, such as geometrical attacks, many types of noise and compression attacks[10]. Our upcoming work will focus on watermarking outline against geometrical attacks with crop.

**CT Image Watermarking Technique Based on the Mix of Time-domain**

DongyangTeng et al [11] propose a new method of image digital watermarking the DCT image watermarking method based on the mix of time-domain. This method has pooled a pre-transformation in time-domain with DCT, and thus it can scatter the noise and make the recuperated watermarking image clearer. This paper deneronors several simulation experiments to treasure suitable orthogonal matrix by Matlab. This paper too carries out attack exams and simulation experiments for the diverse DCT digital watermarking, and compares the consequences with those of the predictable DCT digital watermarking. The consequences show that the DCT digital watermarking created on the mix of time-domain is extra robust and more invisible than the straight DCT digital watermarking. The scheme introduces a new method of watermark, uses Matlab to route simulation experiments and attack test for DCT image watermark method based on the mix of time-domain, and matches the result with those of traditional DCT. The consequences indicate that DCT image watermark method based on the mix of time-domain has improved performance on invisibility and stoutness. This paper only focuses on the method based on the combination of time-domain of DCT image watermarking, and does not assume relative research for additional image watermarking method; however, from what it has revealed from this paper, there should be added research in the field of image watermarking method based on the mix of time-domain [10][11].

**An Efficient DCT based Fingerprinting Scheme for Collusion Attacks**

Uwjala B. S et al [12] studied numerous watermarking schemes are developed to defend different types of media alike text, image, audio and video. Different types of attacks have been launched to yield illicit copies of media. Collusion attack is one of the most influential attacks against watermarking in general and fingerprinting in specific. This scheme [12] presents an well-organized scheme for hiding a logo based fingerprint in tranquil colored images. The scheme is essentially collusion attack resistant. It is based on averaging the mid band coefficients of block Discrete Cosine Transform (DCT) on an image. This technique is compared with the conventional mid band coefficient exchange algorithm. This paper displays the robustness of the scheme against dissimilar kinds of linear and non-linear collusion attacks. In all the techniques, fingerprint logo is removed. A higher efficacy in terms of robustness is attained in contrast with the middle band interchange scheme.

The simulation results for the suggested collusion attack resistant fingerprinting outline have shown the better robustness contrary to a class of linear and non-linear collusion attacks. A well PSNR has been exhibited by the suggested scheme. The performance of this outline against more sophisticated collusion attacks needs to be completed. The use of added transforms like DWT of DFT needs to be examined [12].

**Combined DWT-DCT Digital Image Watermarking**

Ali Al- Hai et al [13] suggested the proliferation of digital media, due to the fast growth of network multimedia systems has generated an critical need for technologies copyright application that can shield the copyright ownership of the media stuffs. Digital watermark is an image thus that technology has been developed to defend digital images of unlawful manipulation. In specific, the digital image watermarking algorithm built on discrete wavelet transform have been extensively recognized to be more common than others. This is because the place of the waves of an excellent space, spread, and frequency characteristics of multi-resolution, which are alike to theoretical copies of the human visual system. This paper defines an algorithm and a strong setim perceptible DWT-DCT digital image watermarking. The watermarking algorithm of a assumed digital image with a mixture of discrete wavelet transforms (DWT) plus Discrete Cosine Transform(DCT). Performance valuation consequences show that the grouping of the two transforms improved the enactment of watermarking algorithms that are based only on the DWT transform [13].

**IV.PROPOSED RANDOMIZED REGULAR DCT COEFFICIENTS ALGORITHM**

The proposed algorithm is a refined and efficient DCT watermarking scheme which enhances the most popular mid-band coefficients embedding schemes. Compare to classical algorithms scramble the original image not the watermark.

The watermark is not embedded actually same as classical schemes but embed the watermark as replacing some randomly selected coefficients by the average of the mid-band coefficients. The average replaces more than one coefficient keeping multiple copies of the watermark in a single block. Due to scrambling of image the watermarking information is spread all over the watermarked image.
The overall process is divided into two processing stages, named Stage-A and Stage –B.

Stage A is use to operate on Original image

Stage-A

Step1 input original image
Step2 scrambling of image with the help of pseudorandom sequence.
Step 3 divide the image into 8x8 block size
Step4 divide the image in some mid band coefficients
Step5 select the some coefficients and take the average of these

Stage-B

Step1 Take the watermark
Step2 Find the linear vector of watermark
Step3 apply encoding process on watermark
At the last output of the both Stages are mixed with a threshold value and generate the watermarked image.

A. Scrambling/Descrambling Procedure

PN sequence is the pseudo random number which is generate in the matlab tool using the PN generator function. The scrambling of the original image is done before the embedding process. Scrambling process uses a PN sequence to randomize the spatial locations of the pixels. The watermark will be embedded into the scrambled image and the watermarked image is descrambled again to result into final watermarked image. The descrambling process brings all the pixels in their original positions as they were in the original image before scrambling. But the position of the watermark in the pixels can only be determined through the scrambling of the image using a PN sequence. After descrambling the pixels that were in a particular block have been now moved to some other blocks.

V.DESCRIPTION OF SIMULATOR

All the steps of proposed technique is implemented in the Mat Lab 2013a. The Matrix lab is very power full tool for implementing the different –different types of images. MATLAB is a high-performance language for technical computing. It integrates computation and programming in an easy way. Typical uses include:

1. Math and computation
2. Algorithm development
3. Modeling, simulation, and prototyping
4. Data analysis, exploration, and visualization
5. Scientific and engineering graphics

VI.RESULTS ANALYSIS

The scheme has been tested for various image sizes. We will see the results obtained for images of size 512x512. Block size for DCT is chosen 8x8. So the maximum number of blocks that can be formed in this image are 4096. One bit of watermark is required per block of the image. So the encoded watermark cannot be greater than 4096. Original watermark can be of maximum size 32x32. After encoding the size of watermark becomes double. The input images and watermark is shown below.

Fig: 4(a)Original Bamboo Image (b) Original Nature Image

Figure 5 : Original Watermark

Figure 6: Resize watermark according to available image size

Scrambling is done on the cover image. Scrambling of the image brings an advantage that the watermark data which will be embedded in next step is scattered all over the image. The watermark is embedded in the scrambled image. After embedding the image pixels are descrambled to their original spatial locations. Watermark bits are spread all over image. Scrambled images are shown below.
A. Piva, M. Barni, F. Bartolini, and V. Cappellini, “DCT Nature
Darshana Mistry, “Comparison of Digital Water Marking
An
ICIP, 1997.
Ujwala B. S, Chetan K.R, An Efficient DCT based Fingerprinting

The Mean square error will be increases, that decreases the PSNR value. Greater the mean square error between the images lesser the PSNR value in decibels leading to bad watermark image quality.

Table: PSNR for different watermarked images

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Image</th>
<th>PSNR (dB) (Proposed Algorithm)</th>
<th>PSNR (dB) (LSB Embedding)</th>
<th>PSNR (dB) (Mid Band Exchange)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baboon</td>
<td>29.72</td>
<td>28.32</td>
<td>28.71</td>
</tr>
<tr>
<td>2</td>
<td>Nature</td>
<td>24.82</td>
<td>23.99</td>
<td>23.01</td>
</tr>
<tr>
<td>3</td>
<td>Helipad</td>
<td>31.21</td>
<td>30.11</td>
<td>28.32</td>
</tr>
<tr>
<td>4</td>
<td>Girl</td>
<td>34.57</td>
<td>32.33</td>
<td>33.00</td>
</tr>
</tbody>
</table>

VII. CONCLUSION AND FUTURE WORK
In the proposed strategy, the watermark embedding is done using DCT frequency transform in different blocks of the image. The watermark is encoded through 4 to 8 bit encoding before watermarking. This strategy is completely new and effective for coding decoding process. The transformations are applied depending upon the high and low frequency regions of the image after performing statistical analysis. The strategy is effective against most image processing attacks. Experimental results demonstrate that the watermarks are difficult to detect blindly because of the noise like appearance of the encoded watermark. The main disadvantages of this scheme are high processing time since all the methods are block based and increased size of encoded watermark. The proposed future work is to reduce the complexity of the method, use of public and private key exchange method to exchange secret keys. Also this strategy can be mixed with linear transformation resistant methods of watermarking to increase the domain of resisting attacks.