Digital Watermarking Using 2-DCT

Trapti Singh, NamitaArya
University School of Information and Communication Technology,
Guru Gobind Singh Indraprastha University, Dwarka, New Delhi, India
traptisingh23@gmail.com, aryanamita12@gmail.com

Abstract: Digital Watermarking is the process of hiding a message into the digital file like image, audio, video, etc. for the protection and authentication of the content. Sometimes it is related with steganography, as both are used for hiding the message but difference is that in steganography there is no relation between digital file and message, it is only used to hide the message existence, on the other hand with watermarking one hides a message related to the digital content. Digital Watermarking consist of several characteristics like Invisibility, Robustness, Readability and Security from any unauthorized user.

Keywords: Digital Watermarking, PSNR,Watermarking Attacks

I. INTRODUCTION

In this paper discrete Cosine transform is used for insertion and extraction of watermark in original image. We will divide the image into blocks and watermark is added into the first bit of each block. This DCT technique is much simpler and robust than others. Just like Discrete Fourier transform, DCTalso transforms a signal or image from the spatial domain to the frequency domain. DCT helps in separating the image into spectral sub-bands having different visual quality.

Mohamed A. Suhail et al.[1] developed a watermarking algorithm based on discrete cosine transform and image segmentation. In this, a image is segmented into different portions based on the voronoi diagram and features extraction points. After, in the DCT domain of each image segment, a pseudorandom sequence of real numbers is added.

Soumitra Roy et al.[2] proposed a color multiple watermarking based on DCT and repetition code. In this, different watermark embedding is done over green and blue component, zigzag scanning of each DCT block is done to ensure watermarked host image imperceptibility.

Rajput, Tiwari [4] generated digital watermarking using 2-DWT and 2-DCT by extracting RGB elements and applying for more quality and security. In this research, they have used red component for embedding of secret image into the original image. In this, low frequency component is achieved by applying 2-level DWT over the frequency component of the original image. Then Inverse 2-level Inverse DCT is applied to form resultant secret image. Later the 2-level DCT is applied over the RGB elements. For calculating PSNR value, blurred attack is done over the image.

Priyanka, Maheshkar [3] noted that most of the visual part that is important reside in the low frequency sub band. Two images are taken i.e a cover image and a binary watermark, then cover is divided into non overlapping blocks and then block wise DCT is applied. Middle frequency sub-band of DCT block is used for watermark embedding for reducing loss during compression process and to reduce quality degradation.

Yu Yang et al [8] proposed technique based on DWT and DCT in which a Zero-Watermark is embedded by comparing adjacent frames mean absolute values coefficients and DWT-DCT applied on the host signal frames. The proposed algorithm is aslo robust to common signal processing operations.

S. Fazli, M. Moeini [10] proposed method that has a high capacity to embed large sequences and will be robust against various attacks. They suggested that the watermark can be embedded separately into the four different sub-images of the host image so that cropping attack can be resisted. The proposed scheme is based on DWT, DCT and SVD domains in which middle frequency components is used to balance between imperceptibility and robustness.

Shabir A. Parah et al[11] proposed technique based on block based DCT coefficient modification. In this paper, difference between two DCT coefficients of adjacent blocks is calculated, and then difference is brought between particular ranges by modifying one of the DCT coefficients.

Types of Digital Watermarking

Digital image watermarking is classified into two types:

1. Spatial-domain method
2. Frequency-domain method

1. Spatial Domain Method

Spatial Domain Method directly transforms the raw data into the original image. It can also implemented by using color separation so that watermark will appear in one of the color bands which will be difficult to detect by naked eye. But it can be made visible during printing by separating colors. This technique basically changes the image representation of object to enhance image for different kind of applications. This approach is mostly used by the journalists for inspecting the digital pictures. Spatial domain consists of following algorithms:

1.1 SSM Modulation Based Technique

Spectral Spectrum techniques generate energy over discrete frequencies which is distributed at time. This modulation technique helps in increasing robustness against natural interference, jamming and watermark detection, establish a secure communication. When SSM based watermarking is applied to the image, it embed the information by linearly combining the image with the embedded watermark modulated small noise signal.

1.2 Least Significant Bit(LSB)

In this technique, watermark is embedded in the LSB of the pixels. As we know pixel is represented by 8-bit sequence, we embed the watermark into the least significant bit in the selected pixels of the image. It is easier to implement and doesn't cause any major distortion in the image but it is not used commonly as it is not robust against different kind of attacks.

II. FREQUENCY DOMAIN TECHNIQUES

Frequency-domain methods are most widely used as compared to spatial-domain methods. This technique aims to embed the watermarks in the spectral coefficients of the image. Discrete Cosine Transform(DCT),Discrete Wavelet Transform(DWT),Discrete Fourier Transform(DFT) are most commonly used transforms under this technique.

Frequency Domain method use the property that Human Visual system (HVS) are better captured by the spectral coefficients. For example, HVS is less sensitive to the high frequency and more sensitive to low frequency coefficients. Hence, alterations to the low frequency components may cause distortion to the original image and high frequency coefficients are considered insignificant, hence processing techniques, such as image compression and watermarking tend to remove high frequency coefficients. Due to this reason, most of the algorithms embed watermarks in the midrange frequencies to maintain the balance between robustness and imperceptibility.

1.3 Discrete Cosine Transformation (DCT)

Just like Fourier transform, DCT represents data in terms of frequency space instead of amplitude space.This technique is more robust to image processing operations like blurring, brightness, low pass filtering,etc as compared to spatial domain techniques but it'sweak against geometric attacks like scaling, rotation, cropping etc. However, these are difficult to implement and computationally more expensive. It embeds the watermark into significant portion of the image as most of the compression schemes remove the insignificant portion of the image. It can be classified into two type's i.e Global DCT watermarking and Block based DCT watermarking.

2.2 Discrete Wavelet Transformation (DWT)

The Discrete Wavelet Transform decomposes the image into sub-image of different spatial domain and independent frequencies. It is used in different kind of signal processing applications, such as removing noise in audio, audio and video compression, etc. Wavelets consist of their energy concentrated in time and are very well suited for analysis of transient, time-varying signals. One of the major challenge watermarking faces is to balance between perceptivity and robustness. If we increase the strength of the embedded watermark, robustness increases but it may increase visible distortion. However, DWT is preferred as it provides both spatial localization and a frequency spread of the watermark within the given image [6].

III. METHOD:

Most of the lossy compression uses transform compression like JPEG (Joint Photographers Experts Group) for the image encoding. Lossy Compression involves sampling and/or quantization by reducing number of bits per sample or ignoring some of the samples as a result the size of data file may reduce.

The DCT uses cosine waves to present a signal unlike Fourier transform which uses both sine and cosine waves. DCT is taken in 8*8 group form which results in an 8*8 spectrum. As DCT is designed to work over the pixel values of range -128 to 127.After quantization, the low frequencies are present in the upper-left corner of the spectrum and high frequencies reside in the lower right. Later, the remaining coefficients will only be considered for reconstructed image.

Input Pixel Matrix

140	144	140	147	140	175	179	155
144	152	140	148	140	147	167	179
152	155	167	163	136	162	152	172
148	162	148	140	136	147	162	156
147	167	140	155	150	136	162	155
148	155	136	147	136	152	155	162
147	167	140	155	155	140	136	162
162	148	148	146	136	140	123	166

Output DCT Matrix

196	-18	15	-8	24	-9	-14	19
21	-34	26	-9	-11	11	14	8
-10	-24	-2	6	-18	3	-20	-1
-8	-5	14	-15	-3	-8	-3	8
-3	10	8	1	-11	18	18	15
4	-2	-18	8	8	-4	1	-7
9	1	-3	4	-1	-7	-1	-2
0	-9	-2	2	1	4	-6	0

Watermark Embedding using DCT:

Algorithm for watermark embedding:

Step 1. Read the input image and convert it into gray scale format.

Step 2. Read the watermark image and convert it into binary format.

Step 3. Compute the 2-D DCT coefficients of the input image.

Step 4. Divide the input image into 8*8 blocks and Insert the watermark into the first bit every block.

Step 5. Recombine the blocks into image and compute inverse DCT.

Step 6. Display the Watermarked image.

Watermark Extraction using DCT:

Algorithm for watermark extraction :

Step 1. Read the watermarked image.

Step 2. Compute the 2-D DCT Coefficients of the image.

Step 3. Divide the image into 8*8 blocks and extract the watermark from first bit of the block.

Step 4. Apply DCT and recombine the blocks into image.

Step 5. Display the extracted watermark.

Experiment Results

Fig. Input Image

Fig. Watermark Image

Fig. Watermarked image

Fig.Extracted Watermark

IV. CALCULATING PSNR:

The PSNR(Peak to noise ratio) ratio is used measure quality between compressed and original image, higher the ratio better the quality of reconstructed image.It is measured in decibels.

The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. Lower the value of MSE, then loweris the error.

The MSE(Mean Square Error) and PSNR both are used to calculate image compression quality.The MSE consists the cumulative square error of both original and compressed image,low error for the lower value of the MSE and PSNR denotes the peak error measure.

To Calculate the PSNR,firstly we find the mean-squared error using the following equation:

$$\text{MSE} = \frac{\sum_{M,N}\left[I_{1(m,n)} - I_2(m,n)\right]^2}{M*N}$$

Here, M and N represents the number of rows and columns of the given input image.After we can calculate PSNR by using following:

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

Resultant PSNR: 41.7412534

V. WATERMARKING ATTACKS

Nowadays there are several harmful attacks that may intentional or unintentional that can be done over a watermarked object. There are various kind software that are available to perform attacks over the watermarking methods to check its robustness. It is basically done to protect the watermark from any future malicious attacks.

i) **Interference attacks**:

Interference attacks are those attacks in which we add some additional noise to the object that is watermarked. Few examples of Interference attacks are quantization, Lossy compression, collusion, remodulation, denoising, averaging, and noise storm.

ii) **Removal Attacks:**

In Removal attacks, we try to remove the watermark data from the object that is watermarked. These kinds of attacks intend to exploit the fact that the watermark can be easily harmed by additive noise signal present in the host signal.

iii)**Geometric attacks**:

Geometric attacks are intend to affect the image geometry,for example rotation, flipping, cropping ,etc and these should be detectable.Example of geometric attack is cropping attack from left-hand side and top of the image.

VI. CONCLUSION

In this paper we watermarked the images by our choice using 2 dimensional discrete cosine transform. We calculated MSE and PSNR to compare original input image and reconstructed image.

This watermarking algorithm provides a better quality picture as we are reduce the coefficient of watermark. The above algorithm can be used to watermark the image that is used in the web applications and where we need different copyright over an image as it need less processing time. Furthermore in future we can analyze different image transform algorithms for improvement of different parameters.

VII. REFERENCE:

[1] Mohamed A. Suhail, Mohammad S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model" IEEE Transactions on Instrumentation and Measurement, Vol. 52, No. 5, Oct 2003.
[2] SoumitraRoy ,Arup Kumar Pal " A blind DCT based color watermarking algorithm for embedding multiple watermarks" Int. J. Electron. Commun. (AEÜ) 72 (2017) 149–161
[3] Priyanka,SushilaMaheshkar, "An Efficient DCT based Image Watermarking Using RGB Color Space",2015 IEEE 2nd International Conference on Recent Trends in Information Systems.
[4] Uma Rajput,NirpumaTiwari , "A Novel techniques for RGB Invisible Watermarking Based on 2-DWT-DCT Algorithm"
[5] Pillai Praveen Thulasidharan ,Madhu S. Nair, "QR code based blind digital image watermarking with attack detection code", Int. J. Electron. Commun. (AEÜ) 69 (2015) 1074–1084
[6] G. Bouridane. A, M. K. Ibrahim, "Digital Image Watermarking Using Balanced Multi wavelets", IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.
[7] Pillai Praveen Thulasidharan, Madhu S. Nair, "QR code based blind digital image watermarking with attack detection code", Int. J. Electron. Commun. (AEÜ) 69 (2015) 1074–1084
[8] Yu Yang ,Min Lei ,Xiaoming Liu , ZhiguoQu , Cheng Wang, "Novel Zero-Watermarking Scheme Based on DWT-DCT",China Communications July 2016
[9] Gonzalez RC, Woods RE. Digital image processing. 3rd ed. India: Pearson Education.
[10] SaeidFazli, MasoumehMoeini, "A robust image watermarking method based on DWT,DCT, and SVD using a new technique for correction of main geometric attacks" Optik 127(2016) 964–972
[11] Shabir A. Parah, Javaid A. Sheikh, Nazir A. Loan, Ghulam M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing" Digital Signal Processing 53 (2016) 11–24
[12] W.N Cheung, "Digital Image Watermarking in Spatial and Transform Domains", 2000 TENCON Proceedings. Intelligent Systems and Technologies for the New Millennium (Cat. No.00CH37119)
[13] Barni M, Bartolini F, Cappellini V, Piva A. "A DCT-domain system for robust image watermarking" Signal Process 1998;66(3):357–72.
[14] Khalili M. DCT-Arnold chaotic based watermarking using JPEG-YCbCr. Optik-Int J Light Electron Opt 2015;126(23):4367–71.