GRAYSCALE IMAGE WATERMARK DETECTION

Randeep Kaur
Assistant Professor
LCET, Katani kalan

Kamaljit Kaur Dhillon
Assistant Professor
GNDEC, Ludhiana

ABSTRACT

A Digital watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc; or it can be an image itself. Watermarking Based on DCT Coefficient Modulation technique embeds the watermark in the DCT domain to increase the robustness of the watermarking scheme.DCT based watermarking is an example of frequency domain watermarking. The objective of this research work is to implement DCT based watermarking technique on gray scale image. The study focuses on evaluating the robustness of watermarked image after having three different attacks on watermarked image and extraction of watermark from that particular image. To compare the DCT based watermarking with LSB based watermarking and to validate the proposed work & the comparative results of watermarking using DCT and LSB are also presented. This paper recommends DCT based technique for achieving robustness in digital image watermarking.

Keywords

DCT; LSB; Poisson; Speckle

1. INTRODUCTION

A large number of digital watermarking schemes have been studied to protect the intellectual property rights of the owner. All these schemes implement either visible or invisible watermarks. Digital watermarking is the process by which an image is coded with an owner's watermark using two general approaches: spatial domain and frequency domain. The spatial domain methods are to embed the watermark by directly modifying the pixel values of the original image. The second is to transform the host image in to its frequency domain representation and embed the watermark therein. Regardless of the embedding method, the embedding technique must satisfy several requirements such as the watermarked image should retain as closely as possible the quality of the original image. The watermark should be robust to various types of attacks.
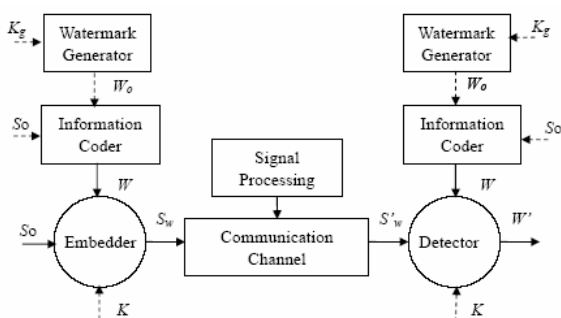
1.1 Applications of watermarking

1.1.1   Copyright protection
The objective is to embed information about the source/owner of the digital media in order to prevent other parties from claiming the ownership of the media.

1.1.2   Fingerprinting
The objective of fingerprinting is to convey information about the recipient of the digital media (rather than the owner) in order to identify every single distributed copy of the media. This concept is very similar to serial numbers of software products.

1.1.3   Copy protection
Watermarking can be used to control data copying devices and prevent them from copying the digital media in case the watermark embedded in the media indicates that media is copy-protected.

1.1.4   Image authentication
The objective is to check the authenticity of the digital media. This requires the detection of modifications to the data.

1.2   Classifications of watermarking

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content. In general, it is easy to create robust watermarks—or—imperceptible watermarks, but the creation of robust—and—imperceptible watermarks has proven to be quite challenging. There are four factors those are commonly used to determine quality of watermarking scheme. They are robustness, imperceptibility, capacity, and blindness.

1.2.1   Robustness
Watermark should be difficult to remove or destroy. Robust is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, collision attacks, noise etc.

1.2.2   Imperceptibility
Means quality of host image should not be destroyed by presence of watermark.

1.2.3   Capacity

It includes techniques that make it possible to embed majority of information.

1.2.4 Blind Watermarking

Extraction of watermark from watermarked image without original image is preferred because sometimes it's impossible to avail original image.

1.3 Discrete Cosine Transform

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio and images (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as explained below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the DFT, but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and *odd* functions, and the modified discrete transform (MDCT), which is based on a DCT of overlapping data.

1.4 Applications of DCT

The DCT, and in particular the DCT-II, is often used in signal and image processing, especially for lossy data compression, most of the signal information tends to be concentrated in a few low-frequency components of the DCT. A related transform, the modified discrete cosine transform, or MDCT is used in AAC, WMA, and MP3 audio compression. DCTs are also widely employed in solving partial differential equations by spectral methods, where the different variants of the DCT correspond to slightly different even/odd boundary conditions at the two ends of the array. The DCT is used in JPEG image compression, MJPEG, MPEG, DV, and Theora video compression. There, the two-dimensional DCT-II of NxN blocks are computed and the results are quantized and entropy coded. In this case, N is typically 8 and the DCT-II formula is applied to each row and column of the block. The result is an 8 × 8 transform coefficient array in which the (0,0) element (top-left) is the DC (zero-frequency) component and entries with increasing vertical and horizontal index values represent higher vertical and horizontal.

2. RELATED WORK

Several techniques for watermarking have been purposed in the literature some of them are discussed below:

In [1] An Improved and Robust DCT based Digital Image watermarking scheme" presents a new DCT based additive watermarking scheme which provides higher resistance to image processing attacks mainly JPEG compression. In our approach the watermark is embedded in the mid frequency band of the DCT blocks only in the sub band which is carrying low frequency components and the high frequency sub band components remain untouched.

In [2] A_New_DCT-Based Watermarking Method for Copyright Protection of Digital Audio paper proposes a new audio watermarking method based on Discrete Cosine Transformation (DCT) for copyright protection. In our proposed watermarking method, the original audio is transformed into DCT domain. The absolute values of DCT coefficients are divided into an arbitrary number of segments and the energy of each segment is calculated. Watermarks are then embedded into the selected peaks of the highest energy segment. Watermarks are extracted by performing the inverse operation of watermark embedding process.

In [3] A robust DCT-based watermarking for copyright protection presents A novel technique for embedding watermarks into a host image in the frequency domain is proposed. Unlike the traditional techniques, the method addresses that the watermark is embedded at low frequency. The weighted correction is also used to improve the imperceptibility of the watermark. Moreover the watermark is self-extractable and the algorithm is simple. Experimental results demonstrate that the watermark is robust to various attacks.

In [6] Novel DCT based watermarking scheme for digital images" presents There is an ever growing interest in copyright protection of multimedia content, thus digital watermarking techniques are widely practiced. Due to the internet connectivity and digital libraries the research interest of protecting digital content watermarking is extensively researched. In this paper we present a novel watermark generation scheme based on the histogram of the image and apply it to the original image in the transform (DCT) domain.

In [5] Multiple binary images watermarking in spatial and frequency domains proposes a scheme using which more data can be inserted in to an image in different domains using different techniques. This increases embedding capacity.

In [4] An overview of transform domain robust digital image watermarking algorithms is to provide complete overview of digital image watermarking, performance evaluation metrics and possible attacks. The generalized algorithms are presented for DWT, CDMA based, DCT-DWT combined approach.

3. PROPOSED WORK

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio and images (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient. whereas for differential equations the cosines express a particular choice of boundary conditions. The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the

image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain
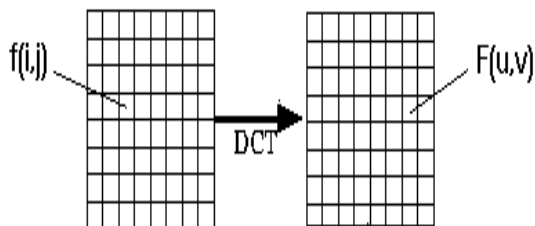
3.1 Discrete Cosine Transform

The discrete cosine transforms is a technique for converting a signal into elementary frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to Eq. 1 shown below. In the equation, x, is the input image having N x M pixels, x (m, n) is the intensity of the pixel in row m and column n of the image, and y (u, v) is the DCT coefficient in row u and column v of the DCT matrix.

$$y(u,v) = \sqrt{\frac{2}{m}} + \sqrt{\frac{2}{n}} \, \alpha_u \, \alpha_v \sum_{u=0}^{m-1} x(m,n) \cos\frac{(2m+1)4\Pi}{2m} \sum_{u=0}^{m-1} \cos\frac{(2n+1)4\Pi}{2n}$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0 \\ 1, & u = 1,2,3\ldots\ldots\ldots.n \end{cases}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}}, & v = 0 \\ 1, & v = 1,2,3\ldots\ldots\ldots.n \end{cases}$$

The image is reconstructed by applying inverse DCT operation according to Eq. 2:

$$x(m,n) = \sqrt{\frac{2}{m}} + \sqrt{\frac{2}{n}} \, \alpha_u \, \alpha_v \sum_{u=0}^{m-1} y(u,v) \cos\frac{(2m+1)4\Pi}{2m} \sum_{u=0}^{m-1} \cos\frac{(2n+1)4\Pi}{2n}$$

The popular block-based DCT transform segments an image non-overlapping block and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-ban and high frequency sub-band. DCT based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression. The basic operation of the DCT is as follows:

- The input image is N by M;

- f(i,j) is the intensity of the pixel in row i and column j;
- F(u,v) is the DCT coefficient in row k1 and column k2 of the DCT matrix.
- For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
- Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.
- The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level;
- 8 bit pixels have levels from 0 to 255.

3.2 Embedding Watermark

The information to be embedded in gray scale image is called a digital watermark. Watermark is embedded in the coefficients of DCT transformed image. The important consideration is, what locations are best for embedding watermarking in the frequency domain to avoid distortion. It is considered to be better to insert the data in the middle frequency coefficients of the host image.

3.2.1 Algorithm

Step1. Compute the 2-D DCT of the image to be watermarked.
Step2. Locate its K largest coefficients, c1, c2… ck, by magnitude.
Step3. Create a watermark by generating a K-element pseudo-random sequence of numbers, w1, w2… wk, taken from a Gaussian distribution with μ = 0 and variance is 1.
Step4. Embed the watermark step 3 in to the K largest DCT coefficients from step 2 using the following equation

$$c_i' = c_{i*}(1 + \alpha w_i) \quad 1 < I < K$$

for a specified constant α > 0. Replace the original c_i with the computed c_i 'from equation as above.
Step5. Compute the inverse DCT of the result from step 4.

3.3 Attack on watermarked image

PSNR, RMSE & MSE values are evaluated for different possible attacks: Following are different attacks applied on the watermarked image.

3.3.1 Salt & Pepper Noise

Salt and pepper noise is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels. An effective noise reduction method for this type of noise involves the usage of a median filter, morphological filter or a contra harmonic mean filter. Salt and pepper noise creeps into images in situations where quick transients, such as faulty switching, take place.

3.3.2 Speckle noise

Speckle noise is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images. Speckle noise in conventional radar results from random fluctuations in the return signal from an object that is no bigger than a single image-processing element. It increases the mean grey level of a local area.

3.3.3 Poisson noise

Poisson noise or shot noise is a type of electronic noise that occurs when the finite number of particles that carry energy, such as electrons in an electronic circuit or photons in an optical device, is small enough to give rise to detectable statistical fluctuations in a measurement. It is important in electronics, telecommunications, and fundamental physics. The parameter λ is not only the mean number of occurrences E [K], but also its variance $\sigma_k^2 = E[K^2]-E[k]^2$. Thus, the number of observed occurrences fluctuates about its mean λ with a standard deviation σ_k is root of mean. These fluctuations are denoted as poisson noise or (particularly in electronics) as shot noise.

3.4 Extraction of watermark

Step1. Compute the 2-D DCT of the attacked watermarked image.

Step2. Extract the K DCT coefficients and denote the coefficients $c_1^{\square}$, $c_2^{\square}$,……… c_k.

Step3. Compute the watermark using $w_{i'} = c_i^{\square} - c_i$ for $1 < i < K$.

Step4. Measure the similarity of $w_{i'}$ and w_i using a metric such as the correlation coefficient.

Step5. Compare the measured similarity, λ, to a predefined threshold, T, and make a binary detection decision D=1 indicates that watermark is present with respect to the specified threshold; D=0 indicates it was not present.

4. Experimental Results

To verify the effectiveness of the proposed method, a series of experiments were conducted. In these experiments, a set of original images of size 512 x 512 are used. It has been validated by applying algorithm on synthetic image. The following figures show the input image, DCT based watermarked image and watermarked images after applying Salt&pepper attack, Speckle attack and the poisson attack.

Fig 4.2: Above two images "flower.bmp" are input and watermarked images & below three images are images after three different attacks.

Fig 4.3: Above two images "Lady.bmp" are input and watermarked images & below three images are images after three different attacks.

Fig 4.1: Above two images "boat.bmp" are input and watermarked images & below three images are images after three different attacks.

Fig 4.4: Above two images "Lena.bmp" are input and watermarked images & below three images are images after three different attacks.
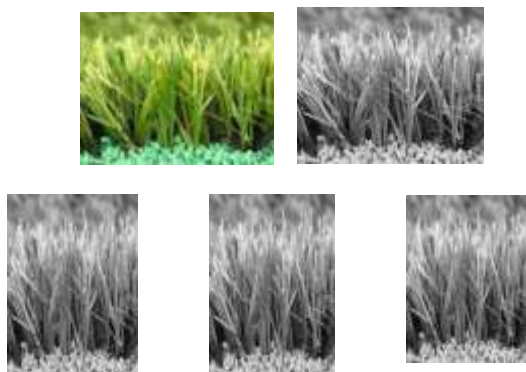
Fig 4.5: Above two images "Grass.bmp" are input and watermarked images & below three images are images after three different attacks.

Fig 4.6: Original Watermark Image

Fig 4.7: DCT based Extracted watermarks after applying Salt & pepper, Speckle & poisson attack respectively.

Extracted watermarks shown above represents that Salt & pepper and poisson noise does not affect the watermark applied on the image .So, the DCT based watermarking scheme is robust and even after applying three different attacks best quality watermarks extracted in DCT based watermarking technology. These results have been analyzed based on PSNR, RMSE & MSE metric.

Table 4.1 Computational Result and Analysis of results based on PSNR metric.

Type of Images	No attack	Salt & pepper	Speckle	Poisson
Boat	36.9	1.04	1.05	1.058
Flower	37.6	1.05	1.05	1.06
Lady	37.5	1.05	1.06	1.07
Lena	37.3	1.1	1.06	1.05
Grass	36.3	1.05	1.05	1.07

Table 4.2 Computational Result and Analysis of results based on RMSE metric.

Type of Images	No attack	Salt & pepper	Speckle	Poisson
Boat	3.9	225.8	225.8	225.8
Flower	3.3	225.8	225.7	225.7
Lady	3.4	225.9	225.8	225.8
Lena	3.4	225.7	225.7	225.9
Grass	3.9	225.8	225.9	225.7

Table 4.3 Computational Result and Analysis of results based on MSE metric.

Type of Images	No attack	Salt & pepper	Speckle	Poisson
Boat	13.4	50981.9	50995.1	50968.7
Flower	10.9	51002.3	50972.7	50967.6
Lady	11.5	50986	50967.6	50967.6
Lena	12.1	50977.8	50981.4	50968.2
Grass	15.3	50985.5	50991.1	50968.7

Table 4.4 Comparative values of three metrics based on DCT & LSB for Synthetic Image "Grass.png".

Type of attack	Algorithm used	PSNR	RMSE	MSE
NO Attack	DCT	36.3	3.9	15.3
	LSB	57.9	0.3	0.10
Salt & pepper	DCT	1.05	225.8	50985.5
	LSB	5.9	129.2	16711.4
Speckle	DCT	1.05	225.9	50991.1
	LSB	2.8	184.02	33866.5
Poisson	DCT	1.07	225.7	50968.7
	LSB	2.9	182.2	33218.3

The performance of proposed algorithm is evaluated based on three different metrics. In this work results which have been achieved using DCT based watermarking are compared with the LSB based watermarking technique. The following   figure shows the watermarks extracted from the LSB based watermarking after passing through salt & pepper, speckle & poisson attack.

Fig 4.8: LSB based Extracted watermarks after applying Salt & pepper, Speckle & poisson attack respectively.

From the results shown above, the performance of DCT based watermarking can be compared with the LSB based watermarking technique. Watermarks extracted from the proposed algorithm are comparatively better than the watermarks extracted from the LSB based watermarking technique.

5. CONCLUSIONS AND FUTURE WORK

In this paper we have presented DCT based watermarking technique for authentication of grayscale image. Watermarks are also extracted after passing through salt & pepper, speckle & poisson attack. Based on the results in the previous chapter, I conclude that DCT based watermarking give best quality extracted watermarks after passing through salt & pepper, speckle & poisson attack. It shows that DCT based watermarking is robust technique. Proposed algorithm is also compared with the existing watermarking technique. Proposed algorithm can be applied on color images & the watermarking image can also color image.

7 REFERENCES

[1] Tribhuwan Kumar tiwari and vikas saxena (2010) in "An Improved and Robust DCT based Digital Image watermarking scheme" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.1, June 2010

[2] Pranab Kumar Dhar, Mohammad Ibrahim Khan and Saif Ahmad (2010) in "A_New_DCT-Based Watermarking Method for Copyright Protection of Digital Audio" International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010

 [3] Lin, S.D.;   Chin-Feng Chen; in "A robust DCT-based watermarking for copyright protection"

[4] Baisa L.Gunjal, R.R. Manthalkar (2011) in "An overview of transform domain robust digital image watermarking algorithms".

[5] K.Ganesan, Tarun Kumar Gupta (2010) in "Multiple binary images watermarking in spatial and frequency domains.

[6] Neminath Hubballi, Kanyakumari D P, "Novel DCT based watermarking scheme for digital Images" International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009

[7] R. Liu and T. Tan, " A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Transactions on Multimedia, 4(1), March 2002, pp.121-128.