 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

A Method for Tamper proofing Images Using DCT Watermarking

Jobin Abraham
BPC College, Piravom, Kerala, India

Abstract
This paper proposes a blind method for tamper proofing images using the watermarking techniques. The image is subdivided in to non-overlapping blocks. These are then sequentially indexed using watermarking. DCT transformation is applied on the image as well on the watermark information, yielding a set of coefficients. These transformed parameters are further processed to hide the index block number imperceptibly. Thus, every segment or region in the image carries a unique number. The proposed technique is also suitable with slight modifications for fingerprinting the images and also for covert communication by hiding the actual details.

Keywords
Image Watermarking, DCT Transform Domain, Embedding, Extraction, PSNR.

I. Introduction

Illegal copying, editing and redistribution of digital multimedia contents like image, audio, and video are posing a serious threat in the present digital era. Moreover, wide popularity of Internet as medium for publishing and data transfer, ownership protection and content verification of valuable contents has become a necessity.

Digital image watermarking techniques are originally developed as a tool for protecting the ownership rights of digital documents [1-2]. Any document comprising text, image or video can be watermarked prior to distribution. Usually, in such cases ownership details are integrated into the document imperceptibly for the purpose of owner identification.

Watermarking is also proposed as an effective mechanism for fingerprinting, tamper proofing, document labeling and broadcast monitoring. Tamper proofing mechanisms are used to detect unauthorized modifications done to the digital contents [3]. Digital fingerprinting, on the other hand is a method that detects the source of unauthorized copying and reselling of the digital contents. Whenever the original owner sells a copy of digital resource, some unique secret information such as customer ID or purchase number will be kept hidden in the document. This hidden information is the fingerprint that will help in locating the source of illegal copies.

The two common approaches in watermarking are spatial domain techniques [4] and transform domain techniques [5-7]. Spatial domain techniques operate directly on pixels modifying them to contain the watermark information. Whereas, in transform domain techniques, the image is transformed using FFT, DCT, DWT or any other suitable transform so as to modulate the pixel values for carrying the external watermark signal. In this paper, a transform domain method using DCT (Discrete Cosine Transform) is proposed.

II. The Method

The method discussed is for tamper proofing the images. The method is also adaptable to suit for more watermarking applications that are listed below.

Proposed uses:

- Tamper proofing – In this method, the blocks are imperceptibly numbered. Hence any editing or purposeful reordering in pixel positions can be detected.
- Fingerprinting – The hidden information can be the ID number or code of the buyer of the digital resource. Thus each copy will be carrying a unique code.
- Covert Communication - by shuffling the order, actual details or appearance in original image can be kept hidden during image transfer. At the receiving end, the decoding algorithm can reconstruct the actual version using the hidden block number.

In watermarking process there are two key stages: Watermark embedding and watermark extraction. In the embedding stage, the image is sub divided into non-overlapping blocks. The blocks are then watermarked sequentially using the number that corresponds to the block position in the image. For example if an image of size 512x512 is considered, there can be 1024 sub blocks of size 16x16. These blocks are numbered from the first to the last sequentially in order by the algorithm.

A. Embedding Algorithm

The algorithm accepts a base image of size N x N. For embedding the index number, construct non-overlapping blocks of size 8X8 or 16X16 and transform them into a set of coefficients by applying DCT. After hiding the watermark signal, apply inverse transform on coefficients and recombine the blocks in the similar way they where decomposed to give the watermarked image I'.

The watermark embedding algorithm has two stages. Stage 1 explains a novel encoding scheme, jos coding, for representing the number using gray scale values. And in stage 2 the image is sub-divided into blocks and is then processed to contain the index number. The embedding is done imperceptibly such that the visual appearances of the is not affected.

Stage 1: jos coding for number encoding

Preprocess the unique code number, n, for each block of the image I. Each digit in the number is encoded as below:

Assign grayscale values for all digits in decimal number system, d = {0, 1, 2, 3….9} from a predefined list of equivalent grayscale values, say, egv = {25, 50, 75, 100 …225}.

1. Let n be a number and d a digit from n.
2. Substitute, $d_i = egv_i$, where i=0,1…9.
3. Represent every digit di using a 2x2 block, by repeating the grayscale value for that digit selected from the list egv.
4. Repeat the steps above (2-4) for converting all the digits in n.
5. Assuming there are four digits in n; construct a 4x4 block for the number using 2x2 segments now representing a digit.
6. Repeat the steps (1-5) for generating the grayscale equivalent for the next number.

The fig.1 below shows how the number 1024 is encoded. Thus all the required sequence numbers are encoded. To encode a single number 16x16 values are used, hence for generating 1 to 1024 numbers the effective watermark size will be 128x128.

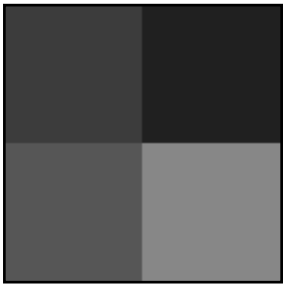

Fig. 1: Pattern for 1024 Using Jos Coding

Stage 2: Watermark Embedding

1. Input an image I of size N x N and the coded watermark numbers computed in stage 1.
2. Compute DCT of each 4x4 watermark code block and generate a 1D array of 16 coefficients.
3. Next step is to divide the image I into non-overlapping sub-blocks fi(x, y) of any suitable size k x k, say, k = 8 or 16.
4. Consider the first block, f1(x, y), from image I for integrating the watermark and then apply DCT.
5. Enforce a watermark image coefficients in the image block $f_i(x, y)$ as:
   $f_i'(x, y) = sf * W_k$

Here, x is a row from mid coefficient region, y=1,2….m. sf is the strength factor and W_k is the watermark coefficient, k= 1,2….16. If m<16, increment x and repeat for varying y till all watermark coefficients are embedded.

6. Repeat the above step, considering the subsequent block from the image I and corresponding equivalent pattern for the block number.
7. Take inverse DCT and recombine the blocks to produce the watermarked copy, I'.

B. Extraction Algorithm

The extraction algorithm retrieves the watermark, which is the block numbers. The retrieved code can be verified to figure out if the image is intact or not. The watermark extraction algorithm is discussed below:

1. First step in watermark extraction is to decompose the image I' into blocks of size, k x k, as in embedding process.
2. Compute DCT of block, $f'_o(x, y)$, where the block numbers are, o = 1, 2….N/k * N/k.
3. Extract embedded values as:
   $wmk(j) = f'_o(x, y)/sf$, where x and y are the row and column positions used during the process of embedding.
4. Extract all watermark bits by considering the next subsequent block from the watermarked images.

Once all the embedded values are retrieved from watermarked image, decode the 1D array for finding the hidden block number. The steps are as follows:

- Use the first set of 4 coefficients from the extracted array, wmk, to form a 2x2 block corresponding to the digits.
- Use four such set from above to form 4 x 4 equivalent of the number.
- Compute inverse DCT to get the equivalent grayscale value.
- Using the scale adopted in stage 1 in embedding process, decode the numbers.
- Repeat the above steps for the next set of 16 coefficients in extracted watermark array for finding the next hidden number.
- Once all the number are decoded, verify the numbers generated are in order and represent the block numbers.

As we are using transform techniques, truncation of few coefficients will take place during DCT conversion and inverse transformations. Hence a threshold of ± 5 is used while verifying an extracted grayscale value against the scale.

If all the numbers regenerated after extraction similar to the blocks numbers assigned during the embedding stage, it follows that the image is not tampered. And in cases where the sequence code numbers generated are incorrect, it can be assumed that in those block areas the image is been illegally edited and altered.

III. Experimental Analysis

The algorithm presented above is tested on number of images. Fig.1(a) shows gray scale base images of size 512 x 512. The algorithm first constructs 16X16 non-overlapping blocks. As a result there are 1024 blocks, which will be then sequentially numbered by the embedding algorithm.

The watermark is a 4x4 grayscale 2D array, where each 2x2 block in turn represents a digit from the number. Thus four 2x2 block will represent a 4 digit number can be used for numbering the blocks in the base image. DCT is also applied on the 4x4 block number, thus giving sixteen coefficients. These sixteen coefficients watermark coefficients are now substituted for the sixteen mid-frequency DCT coefficients in the base image. After inserting the watermark, inverse DCT is taken to convert the coefficients back to the image pixels in spatial domain. This process is repeated for all non-overlapping blocks in the image for integrating watermark index in all regions in the base image.

During the extraction stage, the algorithm successfully retrieved the hidden numbers from the watermarked image. Since the hidden watermark employed is redundant in nature, the extracted values matched the original integrated figures very closely.

At the time extraction, if the retrieved pattern do not match the original or is not in sequential order it can be interpreted that the image is been tampered. As the image is sub-divided into 8x8 blocks at the time of watermarking, the block from which incorrect patterns are extracted corresponds to tampered regions. Thus the proposed algorithm identifies portions in the original base image that were illegally edited.

(a) Base Image_1

(b) Watermarked Image_1

(c) Base Image_2

(d) Watermarked Image_2


(e) Base Image_3 (f) Watermarked Image_3

Fig. 2: Watermarking on Test Images and Corresponding Results

Table 1: PSNR Measurement

Image	Image Size	No. of blocks Watermarked	PSNR (dB)
Lena	512 x 512	1024	36.60
Deer	512 x 512	1024	36.53
Boat	512 x 512	1024	36.44

Peak Signal to Noise Ratio (PSNR) is used to evaluate the distortion introduced by the proposed watermarking scheme. Table1 shows the PSNR values measured for various test images in fig. 2.

IV. Conclusion

A watermarking scheme for tamper proofing images is discussed. The method is also equally suitable for fingerprinting the images. In this method, DCT transform is employed on non-overlapping blocks from the image for converting into a set of coefficients. As the DCT transform on image segments coefficients into three different frequency regions namely, low frequency, mid frequency and high frequency; the region that is most suitable can be selected for hiding the watermark information. The proposed scheme selects mid frequency region to ensure that the visual characteristic of the output watermarked image is reasonably unaffected. During the experimental phase the hidden code is successfully extracted in correct order. Thus the retrieved values will testify whenever the contents are untampered.

References

[1] Vidyasagar M Potdar, S.Han, E Chang,“ A survey of Digital Image Watermarking technique”, IEEE International Conference on Industrial Informatics, 2005.

[2] I.J Cox, Matt L Miller, J A Bloom,“Watermarking Applications and their Properties”, International Conference on Information technology: Coding and Computing, 2000.

[3] P. Meenakshi Devi, M Vekatesan, K Duraiswamy,“A fragile watermarking Scheme for Image Authentication with Tamper Localization using Integer Wavelet Transform”, Journal of Computer Science 5(11), 2009.

[4] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, "Reverse Data Hiding”, IEEE Transactions on Circuits and Systems for Video Technology, March 2006.

[5] Neminath Hubbali, Kanyakmari D. P,“ Novel DCT based watermarking scheme for Digital Image”, International Journal of Recent Trends in Engineering, May 2009.

[6] Tribhuvan Kumar Tewari, Vikas Saxena,“An Improved and Robust DCT based Digital Image Watermarking Scheme”, International Journal of Computer Applications, June 2010.

[7] P. Ramana Reddy, Munka V N K Prasad, D. Sreenivasa Rao,“Robust Digital Watermarking of Color Images under Noise Attacks”, International Journal of Recent Trends in Engineering, May 2009.

Jobin Abraham received B.E in Electronics and Communication from Bharathiyar University, M.Tech in Computer Science and Engineering from Manipal University in 2001 and MBA in Human Resource Management from IGNOU. He has 14 years of experience in the line of Teaching and Projects. His area of interests covers Image Processing, Microcontrollers and Embedded Systems.