ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 3, March 2015

Robust DCT Watermarking for Digital Images

Sanjeevani subhash kagade[1], Prof.Dr. Kanade Sudhir Siddheshwar[2]

Department of E&TC Engineering, TPCT College of Engineering, Osmanabad, India[1,2]

Abstract: Owing to personal computers being applied in many fields and Internet becoming popular and easier to use, most information is transmitted with digital format. Therefore, data copying and back up are more and more easier in the world wide web and multimedia. The copyright and authentication gradually lose their security. How to protect intellectual property becomes important in technical study and research. Recently, the watermarking technique was proposed to solve the problem of protecting the intellectual property. In this paper, a watermark embedded in the host image by DCT transform has been proposed. There are several papers using the same manner to embed watermark into middle-band coefficients of DCT block. The Joint Photograph Expert Group
(JPEG) image compression usually discards the high-band frequency in DCT block including some middle-band data. In this paper the lower-band coefficient of DCT block was employed, since it is robust against the attack by the JPEG. In order to improve the imperceptions, only one bit was embedded in each coefficient of a DCT block. The experimental results show the proposed approach is correct.

Keywords: Discrete Cosine Transform (DCT), Frequency Domain, Joint Photographic Experts Group (JPEG), Robust, Transparency.

I. INTRODUCTION

The Computer and Internet make the world become digitization. Most of the information is easy to transmit and duplicate but unauthorized reproduction becomes a serious problem in this field. Unlike the traditional visible watermark found on paper, the dispute here is to introduce a digital watermark that does not vary the perceived quality of the image content. Watermarking is a potential method to discourage.

Digital image watermarking has received increasing attention in the last few years due to rapid growth in the internet traffic, as well as its significance in content authentication and copyright protection for digital multimedia data [1]. During images transfer, data integrity is not really secure. Watermarking can be an answer to such problems. For applications dealing with images, the watermarking objective is to embed an invisible message inside the image data [2]. Watermarking (data hiding) is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes [3]. In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity [4]. Watermarking applications include copyright protection, authentication, embedded and hidden information. Firstly, watermarking systems that are intended for copyright protection require a very high degree of robustness. Then, watermarking process for authentication belongs to the fragile class of schemes.

Slightest change in the image completely destroys the mark. Finally watermarking for embedding information requires resistance against moderate level of modification due to routine image processing such as compression or cropping [5]. Watermarking techniques developed for images are mainly classified into visible and invisible approaches. While the visible methods provide means for overt assertion of ownership with logos, the invisible methods provide covert protection of these rights [6]. In the classification of watermarking schemes, an important criterion is the type of information needed by the detector:

- Non-blind schemes require both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes require the secret key(s) and the watermark bit sequence.
- Blind schemes require only the secret key(s).

Currently the digital watermarking technologies can be divided into two categories by the embedding position—spatial domain and frequency domain watermark. Spatial domain techniques developed earlier and is easier to implement, but is limited in robustness, while frequency domain techniques is more robust and compatible to popular image compression standards. Thus frequency domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), (DCT) and others [7]. The DCT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain [8]. The DCT transformation is adopted in this paper.

Some perform content-based image watermarking scheme, e.g., the Harris-Laplace detector is adopted to extract feature points, which can survive a variety of attacks. The local characteristic regions (LCRs) are adaptively constructed based on scale-space theory. Then, the LCRs are mapped to geometrically invariant space by using image normalization technique. Finally, several copies of the digital watermark are embedded into the no overlapped LCRs by quantizing the magnitude vectors of (DFT) coefficients [9].

For authentication purposes, in addition to being imperceptible, the watermark has to be sensitive to the slightest modification. This is termed fragile watermarking and allows the detection of tampering attempts. In some cases, the watermark is required to be sensitive only to

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

IJIREEICE

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 3, March 2015

some attacks while not being affected by others, such as common processing techniques (semi-fragile watermarking)
[10]. In order for a watermark to be useful it must be robust to a variety of possible attacks by pirates. These include robustness against compression such as JPEG, scaling and aspect ratio changes, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks [11].

II. PROPOSED METHODS

A. Discrete Cosine Transform

The DCT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain. Many digital image and video compression schemes use a block-based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images [8]. In the standard JPEG encoding, the representation of the colors in the image is converted from RGB to YCbCr, then the image is decomposed in 8×8 blocks, these blocks are transformed from the spatial to the frequency domain by the DCT. Then, each DCT coefficient is divided by its corresponding constant in a

$$F(u,v)=\frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}f(j,k)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}],$$

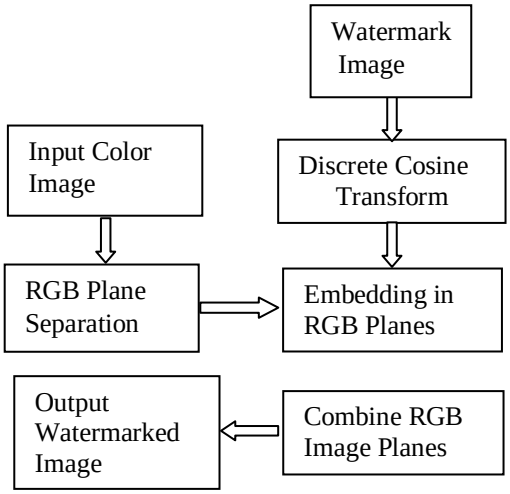
$$f(j,k)=\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}C(u)C(v)F(u,v)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}],$$

where

$C(w)=1/\sqrt{2}$ when $w=0$

$C(w)=1$ when $w=1,2,3,\ldots n-1$

standard quantization table and rounded down to the nearest integer. The DCT transform and its inverse manner can be expressed as follows: After this step, the DCT quantized coefficients are scanned in a predefined zigzag order to be used in the final step, the lossless compression. In each block the 64 DCT coefficients are set up from the lowest upper left corner) to the highest frequencies (lower right corner) [14].
The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing, and so on.
As an image transformed by the DCT, it is usually divided into non-overlapped m ´ m block. In general, a block always consists of 8´8 components. The block coefficients are shown in figure 1. The left-top coefficient is the DC valu e whil e the othe rs stan d for AC com pone nts. The



zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner. The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range. The watermark hidden in the higher frequency band might be discarded after a lossy compression. Therefore, the watermark is always embedded in the lower-band range of the host image that transformed by DCT is perfect selection.

III. PROPOSED ALGORITHM AND METHODS

Fig.1. Embedding watermark

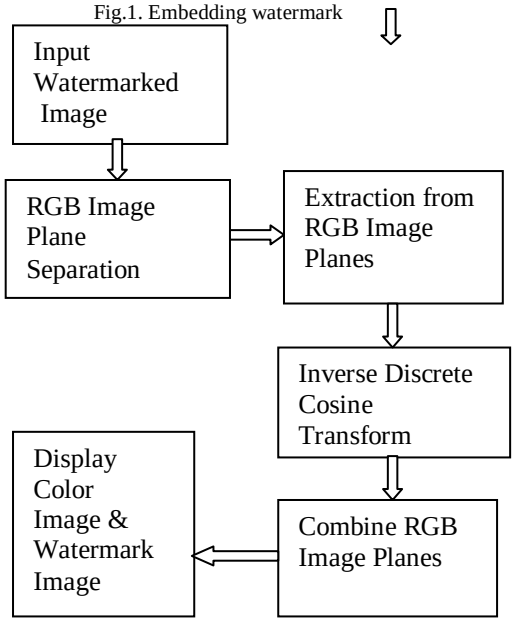


Fig.2. Extraction Watermark

This section describes the proposed watermarking scheme. DCT is applied to the sub-blocks of the watermark image to embed messages in center image. In the watermarking extraction process, embedded watermarks are extracted by the IDCT coefficient blocks.

A. *Watermark embedding*

Fig.1. shows a block diagram of the proposed watermark

DOI 10.17148/IJIREEICE.2015.3308

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 3, March 2015

embedding process. The whole process can be divided into four steps.

Step 1(Dividing into Sub-images): The host input image, is splits into R,G and B image planes.

Step 2(2-level DCT): The watermark / secrete image whose length is M x N. A two dimensional cosine transform is applied to watermark image and split the image into sub blocks.

Step 3 (Message encoding): the sub blocks of watermark / secrete image are embed into R,G and B image planes.

Step 4 (Images encoding): Combine the R,G and B image planes to get the watermarked image.

B. *Watermark Extraction*

Fig.2. shows a block diagram of the proposed watermark extraction process. The extraction is the inverse process of watermark embedding.

Steps 1(Dividing into sub-images): The host input watermarked image, is splits into R,G and B image planes.

Step 2: Extract the sub blocks from the R,G and B image planes by applying Inverse Discrete Cosine Transform (IDCT) to it.

Step 3: Combine the sub blocks elements to recover the watermark of each plane.

Step 4: Combine left R,G and B image planes to get the original image.

IV. EXPERIMENTAL RESULTS

The sizes of the input images are ranged from 720 x 576 to 1800 x 1500 pixels. To evaluate the algorithm we use two different block sizes 8 x 8 and 16x16 pixels. For simplicity and without loss of generality, a binary pattern is used to represent the embedding secret message, which is chosen on basis of his/her preference to fit the cover images with various resolutions.

To measure the perceptual quality, we calculate the peak of signal-to-noise ratio (PSNR) that is used to estimate the quality of the watermarked frames in comparison with the original ones. The PSNR is defined as follows:

$$PSNR = 20 \log_{10}\left(\frac{MAXi}{\sqrt{MSE}}\right) \qquad (4)$$

PSNR value is the lowest one among the test data. This experiment shows the high capacity by embedding the reference pattern into smaller block size (8 x 8), where the embedded message can also be a visually meaningful image.

Using the proposed techniques, the first step is to separate an input image into R, G and B image planes and then embed a watermark in each image.

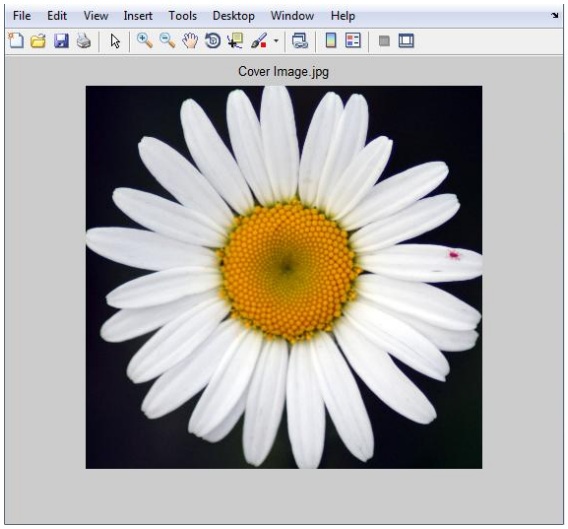


Fig.3. Original input image

Figure 3 shows the original input image.
Figure 4 shows the watermark image.
Figure 5 shows the watermarked image.
Figure 6 shows the extracted watermark image.

Fig.4. Watermark image

DOI 10.17148/IJIREEICE.2015.3308

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 3, March 2015

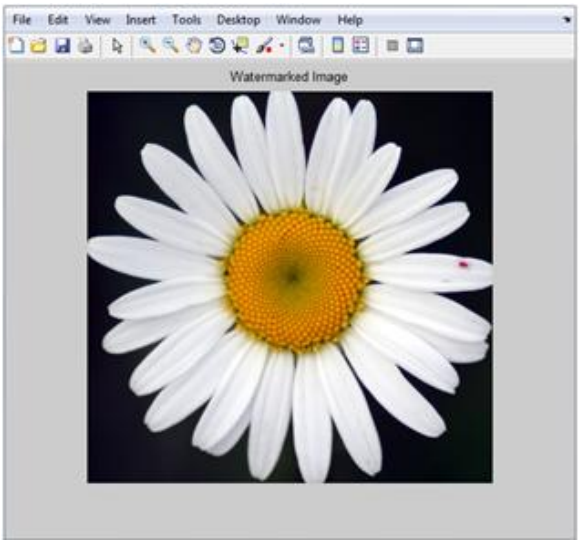


Fig.5. Watermarked image

Fig.6. Extracted watermark image

V. CONCLUSION

Many of watermarking techniques have presented in spatial domain and transform domain. The performance of watermarking is upgraded day by day. In this paper the watermarks were embedded the lower band of the DCT block in the host image. The pseudo random system are used to generate a scatter random number in order to enhance the security. The DCT have been applied successfully in digital image watermarking. In this paper we described a new approach based on DCT digital image water marking, which was done by embedding a watermark logo (image) in different color components as well as semi-random image blocks.

REFERENCES

[1] B. Mohan and S. Kumar, "A robust image watermarking scheme using singular value decomposition", J. Multimedia, vol. 3, no. 1, pp. 7-15, May 2008.
[2] G. Lo-varco, W. Puech, and M. Dumas, "DCT-Based watermarking method using color components", Second European Conference on Color in Graphics, Imaging and Vision, Germany 2004.
[3] A. Sverdlov, S. Dexter, and A. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies", International Multimedia Conference, Germany, pp. 166-174, 2004.
[4] E. Fu, "Literature survey on digital image watermarking", Technical Report, EE381K-Multidimensional Signal Processing, 1998.
[5] G. Lo-varco, W. Puech, and M. Dumas, "Content Based watermarking for securing color images", J. Imaging Science & Technology, vol. 49, no. 6, 2005.
[6] S. Mohanty, P. Guturu, E. Kougianos, and N. Pati, "A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction", 8th IEEE International Symposium on Multimedia, San Diego, USA, pp. 153-160, December 2006.
[7] L. Liu, A survey on digital watermarking technologies, Technical Report, Stony Brook Univ., New York, USA, 2005.
[8] C. Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations", Proceedings of the International Workshop Trends & Recent Achievements in Information Technology, Romania, pp. 116-121, May 2002.
[9] X.Y. Wang and J. Wu, "A Feature-based Robust Digital Image Watermarking against De-synchronization Attack", International Journal of Automation and Computing, 2007, Vol. 4, No. 4, pages 428-432.
[10] S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images", J. Machine Learning Research, Vol. 4, issue 7-8, pp. 1471-1498, November 2004.
[11] S. Pereira and T. Pun, "A framework for optimal adaptive DCT watermarks", European Signal Processing Conference, Finland, pp. 1669-1671, September 2006.
[12] A. Parthasarathy, Improved Content Based Watermarking for images, M.Sc. Thesis, Louisiana State University, August 2006.
[13] J. Seitz, Digital watermarking for digital media, Information Science Publishing, 2005.
[14] JPEG, jpeg.org.
[15] W. Puech and J. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT", 13th European Signal Processing Conference, Turkey, September 2005.
[16] Y. Z. Lu, A Novel Face Recognition Algorithm for Distinguishing Faces with Various Angles, International Journal of Automation and Computing, 2008, Vol. 5, No. 2, pages 193- 197.
[17] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[18] O. Bruyndonckx, J. J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in Proc. IEEE Nonlinear Signal and Image Processing, pp. 456-459, June., 1995 .
[19] W. N. Lie, and L. C. Chang, "Spatial-Domain Image Watermarking By Data Embedding At Adaptive Bit Position," IPPR Conference on Computer Vision, Graphics and Image processing, pp. 16-21, 1999.
[20] S. C. Pei, Y. H. Chen and R. F. Torng, "Digital Image and Video Watermarking Utilizing Just-Noticeable-Distortion Model," IPPR Conference on Computer Vision, Graphics and Image processing, pp. 174-182, 1999.
[21] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," IEEE Trans. On Image Processing, vol. 8, no. 1, pp. 58-68, Jan., 1999.
[22] C. T. Hsu and J. L. Wu, "DCT-Based Watermarking for Video," IEEE Trans. On Consumer Electronics, vol. 44, no. 1,pp. 206-216, Feb 1998.
[23] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT-Domain system for robust image watermarking," Signal Processing, vol. 66, pp. 357-372, 1998.