Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 49(63), Fascicola 2, 2004

Invisible watermarking for Copyright Protection

M. A. Matin[1]

Abstract – Due to the rapid expansion of the Internet and the overall development of digital technologies, millions of users, who are scattered all over the world, are able to use a vast number of multimedia products. Every participant in this process wants to assert their rights, which are given by their role in the business string. Naturally, solutions to digital copyright protection are required urgently to tackle the problem of unauthorized copying and distribution. The aim of this paper is concerned with inserting copyright information into host image. In this paper, discrete cosine transform (DCT) domain watermarking technique for copyright protection of still digital images is analyzed. The DCT is applied in blocks of 8 × 8 pixels as in the JPEG algorithm. The watermark can encode information to track illegal misuses concerned with the protection of copyright information contained in digital images.

I. INTRODUCTION

In general. digital images and digital video-streams can be easily copied one way or another. Even though such copying may violate copyright laws, it is widespread. The ease with which electronic images may be copied without significant loss of content contributes to illegal copying. One of the goals of digital watermarking is authentication for copyright protection. To prove the ownership of an image, a perceptually invisible pattern (a watermark) is embedded into the image and ideally stays in the image as long as the image is recognizable.

II REQUIREMENTS OF WATERMARKING

Digital watermarking, particularly digital image watermarking, has several conflicting requirements The three most important requirements are perceptibility robustness, and capacity[1]. For example: a very robust watermark can be obtained by highly modifying the host data for each bit of the watermark by increasing the watermark strength. However, this large modification will be perceptible. As a second example, increasing the number of embedded bits increases the capacity but decreases the robustness. Therefore, the maximum amount of modification that can be acceptable for the quality of the media and robustness are the two determining factors for the maximum amount of watermark bits that can be stored in a data object.

III. BUILDING WATERMARKING

It consists of two parts:- The first part is concerned with insertion strategy i.e. where in the host signal shall we place the information?. The second one is watermark structure -how shall we place the additional information into the signal?. It is often necessary to utilize Human Visual System (HVS) models for adaptively embedding the watermark. This can reduce the impacts of modifications on image quality or for the same visual quality a much stronger watermark can be embedded. The human eye is sensitive to the following characteristics of image-contrast, frequency, luminance sensitivity, edges and texture area[2]. One can combine the above four properties to construct a perceptual mask which determines the amount of modification permitted on each image cover data (pixels, transform coefficients) value. Using perceptual masks, energy can be added locally in places where the human eye can't notice it. This increases robustness and hence capacity

IV. WATERMARK EMBEDDING APPROACH

There are two general approaches to embedding a digital watermark. One approach is to transform the host image into its frequency domain representation and embed the watermark data therein. The second is to directly treat the spatial domain data of the host image to embed the watermark. Bruyndonckx *et al.* in [3] proposed a spatial domain scheme for copyright labeling of digital images based on pixel region classification.

The advantage of spatial techniques is that they can be easily applied to any image, regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark.

In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain.

[1] Department of Computer Science and Engineering, BRAC University, Bangladesh. e-mail: rumel120@yahoo.com

Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For example, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather then in smoother regions. The benefit is two-fold: degradation in smoother regions of an image is more noticeable to the HVS, and secondly becomes a prime target for lossy compression schemes.

Taking these aspects into consideration, working in a frequency domain of some sort becomes very attractive. Frequency domain watermarking was introduced by Cox *et al.*[4]. Cox's approach uses spread spectrum communication techniques to embed a bit in the image. However, it needs the original image to decode the watermark and Smith *et al.*[10] refer to these approaches (when the original image is needed in the decoding process) as "...of limited interest because of their narrow range of practical applications". The classic and still the most popular domain for image processing is that of Discrete-Cosine-Transform, or DCT. Koch *et al.*[5] reported an efficient DCT domain watermarking techniques resisting to JPEG compression. But our proposed approach is robust also against attacks such as filtering, cropping, Scaling and geometric rotation.

The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [6].

V. FREQUENCY DOMAIN TECHNIQUE

One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a 8×8 DCT block. We first divide the NxN image into (N/8)*(N/8) = $N^2/64$ non overlapping 8x8 blocks; then take DCT on each block and embed the watermark middle-band DCT coefficients 8x8 Discrete Cosine Transform (DCT) is defined as:

I(u,v)=

$$\frac{m(u)}{2}\frac{n(v)}{2}\sum_{k=o}^{7}\sum_{l=0}^{7}X(k,l).\cos(\frac{(2k+1)u\pi}{16})\cos(\frac{(2l+1)v\pi}{16})$$

and 8x8 Inverse Discrete Cosine Transform (IDCT) is defined as:

X(k, l)=

$$\sum_{u=0}^{7}\sum_{v=0}^{7}\frac{m(u)}{2}.\frac{n(v)}{2}I(u,v)\cos(\frac{(2k+1)u\pi}{16})\cos(\frac{(2l+1)v\pi}{16})$$

where k,l,u,v $\in\{0,1,2,3,4,5,6,7\}$ and

m(u)= $\frac{1}{\sqrt{2}}$ for u=0 and m(u)=1 for u >0,m(v)= $\frac{1}{\sqrt{2}}$ for v=0 and m(v)=1 for v>0

DCT and IDCT are linear transformations and all DCT coefficients are real. Any image block can be represented as a superposition of scaled DCT transformed images scaled with DCT coefficients.

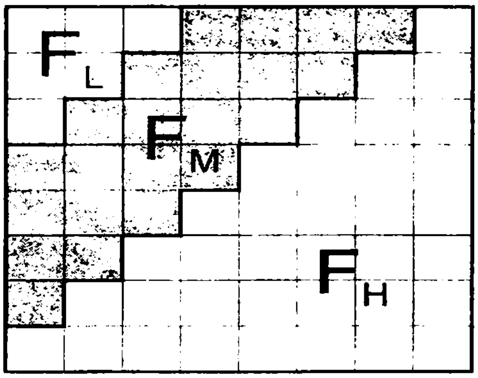
A. *Selection of DCT coefficient*

The low frequency components of an image are perceptually the more significant ones and any modification on them deteriorates the image fidelity. Therefore, watermarking shouldn't be applied on low frequency components. On the other hand, the high frequency components are the ones, which are usually less significant in terms of fidelity. As a consequence, compression techniques utilize this property and suppress the high frequency components first to reduce the size of images. Therefore, the watermarking techniques that modify high frequency coefficients cannot be robust carriers of watermark. This leaves us with the choice of mid frequency coefficients.

B. *DCT based techniques*

One such technique utilizes the comparison of middle-band (F_M) DCT coefficients to encode a single bit into a DCT block. Suppose two locations $B_i(u_1,v_1)$ and $B_i(u_2,v_2)$ are chosen from the F_M region for comparison. Rather then arbitrarily choosing these locations, extra robustness to compression can be achieved if we base the choice of coefficients on the recommended JPEG quantization shown below in table 2. If two locations are chosen such that they have identical quantization values, we can feel confident that any scaling of one coefficient will scale the other by the same factor preserving their relative size.

Table 1 – Definition of DCT regions



In table 1, F_L is used to denote the lowest frequency components of the block, while F_H is used to denote the higher frequency components. F_M is chosen as the embedding region.

Table 2 - **Quantization values used in JPEG compression scheme [7]**

0							7
16	11	10	***16***	***24***	***40***	***51***	61
12	12	***14***	***19***	***26***	***58***	60	55
14	***13***	***16***	***24***	***40***	57	69	56
14	***17***	***22***	***29***	51	87	80	62
18	***22***	***37***	56	68	109	103	77
24	***35***	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Based on the table, we can observe that coefficients (4.1) and (3.2), or (1,2) and (3,0) would make suitable candidates for comparison, as their quantization values are equal. Say B_i denotes the 8x8 DCT block and two locations $B_i(u_1,v_1)$ & $B_i(u_2,v_2)$ are chosen from F_M region. The DCT block will encode a "1" if $B_i(u_1,v_1) > B_i(u_2,v_2)$; otherwise it will encode a "0". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [7].

The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be improved by introducing a watermark "strength" constant *k*, such that $B_i(u_1,v_1) - B_i(u_2,v_2) > k$. Coefficients that do not meet this criteria are modified using random noise to satisfy the relation. Increasing *k* thus reduces the chance of detection errors at the expense of additional image degradation [7].

Another possible technique is to embed a PN(Pseudo random noise) sequence W into the middle frequencies of the DCT block. We can modulate a given DCT block x,y using the equation (1) shown below.

$$I_{W_{x,y}} = \begin{cases} I_{x,y} + k * W_{x,y} & \text{In } F_M \text{ region} \\ Ix, y & \text{In } F_L \text{ and } F_H \text{ region} \end{cases} \quad \text{------(1)}$$

Where $I_{x,y}$ is the original image and *k* is the watermark "strength".

For each 8x8 block x,y of the image, the DCT for the block is first calculated. In that block, the middle frequency components F_M are added to the PN sequence W, multiplied by a gain factor k. Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give us our final watermarked image I_W [8].

The watermarking procedure can be made somewhat more adaptive by slightly altering the embedding process to the method shown in equation 2.

$$I_{W_{x,y}} = \begin{cases} I_{x,y} * (1 + k * W_{x,y}) & \text{In } F_M \text{ region} \\ Ix, y & \text{In } F_L \text{ and } F_H \text{ region} \end{cases}$$

(2)

This slight modification scales the strength of the watermarking based on the size of the particular coefficients being used. Larger *k*'s can thus be used for coefficients of higher magnitude...in effect strengthening the watermark in regions that can afford it and weakening it in those that cannot [8].

For detection, the image is broken up into those same 8x8 blocks, and a DCT performed. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold T, a "1" is detected for that block; otherwise a "0" is detected. Again k denotes the strength of the watermarking, where increasing k raises the robustness of the watermark at the expense of quality [8].

C. *Proposed approach*

Researchers can compare different algorithms and see how a method can be improved or whether a newly added feature actually improves the reliability of the whole method [9].

In section 4 "Building watermarking" we discussed about the watermark structure. The most straight-forward approach would be to embed watermark (text strings) into an image by allowing an image to directly carry information such as author, title, date...and so forth. The drawback however to this approach is that ASCII text in a way can be considered to be a form of LZW (Lempel–Ziv-Welch) compression, where each letter being represented with a certain pattern of bits. By compressing the watermark-object before insertion, robustness suffers.

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be quite easy for even a simple task such as JPEG compression to reduce a copyright string to a random collection of characters. The properties of the HVS (Human visual system) can easily be exploited in recognition of a degraded watermark.

In this work the host image is divided into 4096 blocks of size 8x8. The binary watermark with a size of 20×50 pixel is embedded into the image. The algorithm works on selected 1000 of 8x8 DCT Coefficient blocks and the coefficients of the same quantization value is taken for comparison and are encoded such that (4,1) > (3,2) when watermark bit is 0 and that (4,1) < (3,2) when watermark bit is 1, and the two values are adjusted such that their difference >= k. Finally the block is transformed back into spatial domain.

For detection, the watermarked image is broken up into those same 8x8 blocks, and a DCT is performed The same PN sequence is then compared to the middle frequency values of the transformed block.

VI. RESULTS AND DISCUSSION

The experiment involved evaluating the reliability of extracted watermark and demonstrating the copyright effectiveness of the proposed approach. In this work, five kinds of manipulations are considered- filtering, lossy JPEG compression, cropping, scaling and rotation. The experiments were performed on monochrome images with a size of 512×512 pixels. Figure 2(a) shows three images that were used:- airplane, Lena, bird and were selected to represent three kinds of images - those containing large smooth areas, containing both smooth and detailed areas, and with large amount of details.

PSNR (Peak signal to noise ratio) is calculated using the equation 3 to give us a rough approximation of the quality of the embedded image in the experiments.

$$PSNR = 10\log_{10}\frac{\max(x)^2}{\| x' - x \|^2} \text{-------------}(3)$$

Where x' is the image under test and x is the original imag .

In the above equation the PSNR penalizes the visibility of noise (watermark) in all regions of the image in the same way. However, due to phenomena of contrast masking the visibility of noise in flat regions is higher than that in textures and edges.

Therefore, a simple approach to adapt the classical PSNR for watermarking applications consists in the introduction of different weights to the perceptually different regions oppositely to the PSNR where all regions are treated with the same weight. Originally this idea was presented by Netravali and Haskell [11] with application to image compression. Application to watermarking quality evaluation was reported in [12] using the NVF (noise visibility function) as a weighting matrix:

$$wPSNR = 10\log_{10}\frac{\max(x)^2}{\| x' - x \|^2_{NVF}}$$

$$= 10\log_{10}\frac{\max(x)^2}{\| NVF(x' - x) \|^2} \text{------------}(4)$$

Figure 1(a) Original images

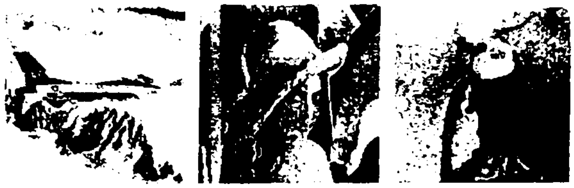


Figure 1 (b) watermarked images

PSNR=38.3 dB *PSNR=34.1dB* *PSNR=34.7dB*
wPSNR=40.2dB *wPSNR=35.6dB*
wPSNR=35.4dB

The ever- popular miss November (Lena) image is used as a reference image. From the difference between original and watermarked image of Lena, the error is visible. The error is most significant at black hair. At the receiver site, the watermark is extracted from the transmitted image and compared with the original watermark ('Copyright') to perform the copyright protection.

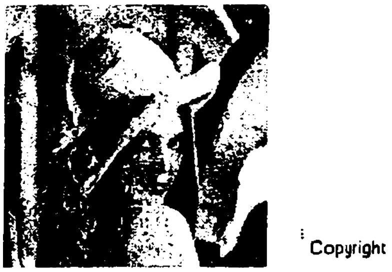


Figure 2 (a) Low pass filter (b) Recovered watermark

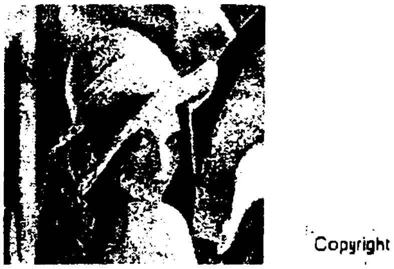


Figure 2: (a) Median filter (b) Recovered watermark

Figure 2(a) and 4(a) shows a low pass and median filtered watermarked image using a 3x3 filter mask consisting of 0.9 intensity values. The median filtered image is more blurred than the low pass filtered image (which is blurred also compared to the original host image). The reconstructed watermark is also still better in median filter.

Fi-ur- 4:(a) I-d-x-100jp-   (b) I-d-x-25 jpe-

The above figure shows watermarked image compressed using lossy index-100 JPEG and index-25 JPEG compression. The index ranges from 0 to 100, where 0 is the best compression and 100 is the best quality. The reconstructed watermark is a good reproduction in our experiment.

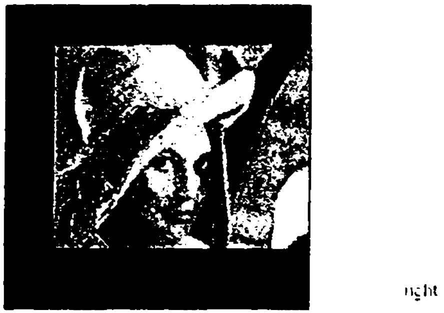


Figure 5 (a) Cropping (b) Recovered watermark

Figure 5(a) shows a cropped watermarked image cropped with a mask of size 340x425 pixels. The reconstructed watermark is still recognizable.

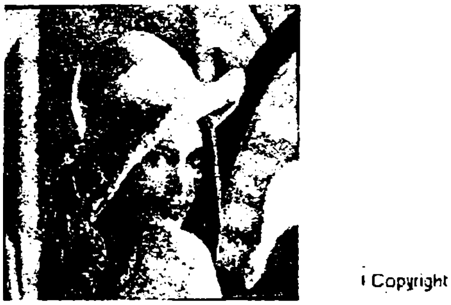


Figure 6.(a) Rotation 2 degree (b) Recovered watermarked

Geometric transforms are one of the most difficult conditions for a watermarking technique to deal with embedding domain. This can be chosen both by shifting or rotating invariance such as Cartesian or Polar DCT; however these domains are typically resistant to only a specific geometric distortion.

The only difference between the rotated image and the cropped image is the bilinear interpolation used to realign the pixels after it is rotated back to its original alignment. The bilinear interpolation can be approximated as an averaging filter.

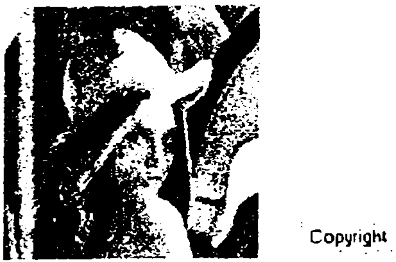


Figure 7 (a) Scaling   (b) Recovered watermarked

The scaling experiment was done by scaling the watermarked image down to one quarter of its original size (256x256) and rescaled back to 512x512 using bilinear interpolation The algorithm requires the pixels in the watermarked image to be in the corresponding location as the original host image in order to extract the watermark correctly.

VII. CONCLUSION

In this Paper the message is invisibly embedded into the source image. A verification key, which is stored and known only to the author, is produced in the embedding step and used in the verification process to extract the embedded message inserted in the host. Here some attacks -- such as low pass filtering, median filtering, lossy JPEG compression, cropping, rotation and Scaling 'a been 'one on wa'ermarke' image 'o 'es'roy 'he copyright information but it is still recoverable and recognizable of the owner.

REFERENCES

[1].Cox, J., M. L. Muller and J. A. Bloom, *Digital Watermarking*, Morgan Kauffman Publishers, ISBN 1-55860-714-5, 2002

[2] Swanson, M. D., B. Zhu and A. H. Tewfik, "Robust data hiding for images", *7th IEEE Digital Signal Processing Workshop*, pages 37-40, 1996

[3] O. Bruyndonckx, J.J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images", in *Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Halkidiki, Greece, June 1995.

[4] I J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", Tec nical Report 95-10, NEC Research Institut .

[5] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling", in *Proc Workshop Nonlinear Signal and Image Processing*, Marmaros, Greece, June 1995.

[6] Podilchuk, C. I. and W. Zeng," Perceptual watermarking of still images", *ElectronicProceedings of the IEEE Signal Processing Society 1997 Workshop on Multimedia Signal Processing*, Princeton, New Jersey, June 1997

[7] N F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in *Information Techniques for Steganography and Digital Watermarking*, S C. Katzenbeisser et al., Eds Northwood, MA Artec House, Dec. 1999, pp 43-75

[8] G. Langelaar, I. Setyawan, R.L. Lagendijk, "*Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine*, Vol 17, pp 20-43, September 2000

[9] F A P. Petitcolas, "Watermarking Schemes Evaluation" ", in IEEE Signal Processing Magazine, Vol 17, pp 58-64, September 2000

[10] J. Smith and B. Comiskey, "Modulation and information hiding in images", ", in *Proc. First International Workshop on Information Hiding*, Lecture Notes on Computer Science, Cambridge, UK, pp. 207-226, June 1996.

[11] A. Netravali, B. Haskell, Digital Pictures Representation and Compression, Plenum Press, New York, 1988.[12] S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgartner, T. Pun, A generalized watermark attack based on stochastic watermark estimation and perceptual remodulation, in: P.W. Wong, E.J. Delp (Eds.), IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, SPIE Proceedings, Vol. 3971, San Jose, CA, USA, 23} 28, January 2000.