A Novel DCT-based Approach for Secure Color Image Watermarking

Narges Ahmidi
Amirkabir University of Technology
n_ahmidi@ce.aut.ac.ir

Reza Safabakhsh
Amirkabir University of Technology
safa@ce.aut.ac.ir

Abstract

In this paper, focusing on visually meaningful color image watermarks, we construct a new digital watermarking scheme based on the Discrete Cosine transformation. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in a color image.

In addition, to prevent tampering or unauthorized access, a new watermark permutation function is proposed, which causes a structural noise over the extracted watermark. Also, we have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark.

The experimental results show that embedding the color watermark adapted to the original image produces the most imperceptible and the most robust watermarked image under geometric and valumetric attacks.

1. Introduction

The rapid evolution of the Internet technology makes the transmission of digital multimedia content easier. So, digital watermarking techniques are proposed for copyright protection or ownership identification of digital media. A digital watermarking technique must meet the following three requirements:

Imperceptibility: According to the Human Visual System (HVS) parameters, the watermark embedded in the digital image should be perceptually invisible to human eyes.

Robustness: The embedded watermark must be difficult (hopefully impossible) to detect or delete, and any attack should result in severe degradation in fidelity.

Security: The security of the watermarking system relies on the use of secret keys known exclusively by the copyright owner. All the parameters using in embedding process can be a part of secret key. These keys are required in the extraction process.

In general, there is a tradeoff between the watermark embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images.

The proposed watermarking scheme adopts a color image as the watermark so human eyes can easily verify the extraction of this visually meaningful watermark. In general, a color image can provide more perceptual information [2] i.e. sufficient evidence against any illegal copyright invasion.

In sections 2 and 3, we will describe the proposed embedding and extraction processes. Section 5 gives the experimental results. We have evaluated robustness and invisibility of the proposed scheme and compared them to those of Tsai's [1], Cox's [2,5], Fridrich's [3, 6] and Koch's [4] methods under various attacks such as JPEG lossy compression, median filtering and cropping.

2. Embedding Process

As shown in Fig. 1, the proposed process embeds an M×M color watermark image W in an N×N original image X using secret keys K for better security. All the relations used in the embedding process are invertible. The following paragraphs describe the model briefly.

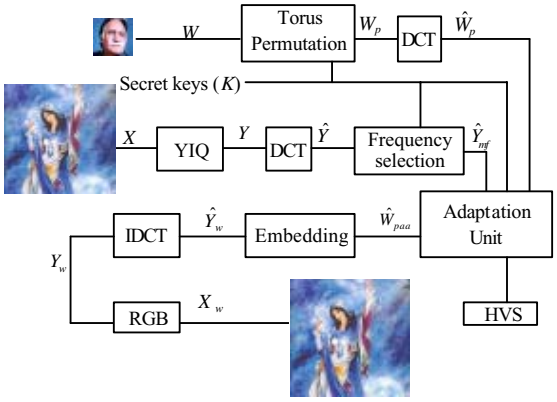


Figure 1. The proposed embedding process

Initially, the original image X is converted to the NTSC color space. One of the main advantages of the NTSC color space is that the grayscale information is separated from color data; as a result, the same signal can be used for both color and black-and-white images.

Then the original image luminance component Y is divided into non-overlapping 8×8-pixels blocks, and each block is independently transformed to frequency domain representation through 2D-DCT.

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)
0-7695-2108-8/04 $ 20.00 © 2004 IEEE

IEEE COMPUTER SOCIETY

A benefit of such a scheme is that if the images are stored as compressed JPEG bit streams, the watermark can be inserted directly into the partially decompressed bit stream.

2.1. Middle-frequency coefficients selection

DCT concentrates the signal energy in the low-frequency bands. So, embedding the watermark in lower frequencies produces more robust watermarked images with lower quality. Hence, to meet both the invisibility and robustness requirements, middle-frequency coefficients of the transformed blocks are selected in a zigzag order to embed the digital watermark in.

The total number of selected coefficients in each block, denoted as t, is determined by Eq. (1) [1].

$$t = \lceil (8M / N)^2 \rceil \tag{1}$$

The first coefficient is selected randomly using a secret key K_1 as the seed of a pseudo-random number generator (PRNG). All the selected coefficients compose a transformed M×M image $\hat{Y}_{mf}$. Furthermore, by using a seed value K_2, the position of each coefficient in the related block in $\hat{Y}_{mf}$ is selected.

2.2. Permutation of the watermark

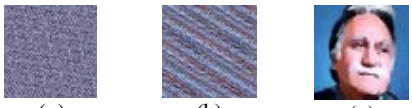
For getting more security and more robustness W must be shuffled before embedding into X [1]. Using a random permutation will add a noise to the extracted watermark (Fig. 6). Here, we propose a 2D permutation function that generates a structural noise over the extracted watermark that can be modeled (Fig. 8). Consequently, we propose a post-processing algorithm to eliminate this noise. This algorithm will be described in section 3.

The proposed Torus permutation function is inspired from Torus automorphism. A one-parameter Torus automorphism is as follows [8]:

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k_3 & k_3+1 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \bmod M \tag{2}$$

It means that each pixel at coordinates (i, j) of the watermark image is moved to (i', j') using Eq. (2). The number of transformations performed on the watermark image (K_4) and k_3 are kept as secret keys.

In the image permutation applications, this function is periodic with period R. The period depends only upon the parameters $k_3 \in [1, M-1]$ and M. Figure 2 shows the periodic property of the Torus permutation where parameters of Eq. (2) are $k_3=1$ and M=128. It shows that for these parameters the period is equal to 96.



(a) (b) (c)

Figure 2. Permuted watermark after p times with Eq. (2), where a) p=20, b) p=50, and c) p=96

2.3. Adapting watermark to the original image

For more security and imperceptibility, the watermark strength must depend on the intensity values of the DCT coefficients of the original image. In this way, the watermark signal will be strengthened in large DCT values, and attenuated in small ones. This adaptation procedure is fulfilled through the following steps:

1) Since the number of blocks in both the watermark image and the original images must be equal, the permuted watermark is divided into non-overlapping nxn blocks, where $n = 8M / N$. Then each block is DCT transformed individually to obtain $\hat{W}_p$.

2) A block-based mean is calculated over $\hat{W}_p$ using Eq. (3).

$$\overline{\hat{W}_p} = \frac{\sum_{i=1}^{(M/n)^2} f(i) \cdot \hat{W}_p(i)}{(M/n)^2} \tag{3}$$

where i represents the block number and $\hat{W}_p(i)$ is the i^{th} block in $\hat{W}_p$, and $f(i)$ is an nxn matrix used for the weighted averaging. The result ($\overline{\hat{W}_p}$) is an nxn matrix.

3) Using Eq. (5), Each block in $\hat{W}_p$ is normalized and then adapted to $\hat{Y}_{mf}$ by multiplying it by $\overline{\hat{Y}_{mf}}$ which is the mean of all coefficients in $\hat{Y}_{mf}$.

$$\hat{W}_{pa} = \frac{\hat{W}_p(i)}{\overline{\hat{W}_p}} \overline{\hat{Y}_{mf}} \tag{4}$$

2.4. Insertion process

A good visual model should provide the maximum watermark strength and size that can be inserted without visual distortions. We propose Eq. (5) for embedding the adapted watermark $\hat{W}_{pa}$ in $\hat{Y}_{mf}$.

$$\hat{W}_{paa}(i) = \hat{Y}_{mf}(i) + \alpha_i \cdot \hat{W}_{pa}(i) \qquad , \alpha_i \geq 0 \tag{5}$$

Here, i represents the current block number, and α_i is calculated via HVS parameters to meet invisibility and robustness requirements.

Consequently, a one-to-one replacement of each coefficient in $\hat{W}_{paa}$ with the corresponding one in $\hat{Y}$ is performed to obtain $\hat{Y}_w$. This procedure needs the secret

IEEE COMPUTER SOCIETY

keys K_1 and K_2, and the zigzag pattern to find the exact place of each coefficient.

If the amplitude of such watermarking scheme (α_i) is increased to thwart filtering attacks for a robustness, the watermark may become visible. The just noticeable difference threshold (JND) α_i can be used to determine the maximum amount of the watermark signal that can be tolerated at each region in the image without affecting its visual quality. In an image-dependent adaptation, α_i is calculated based on HVS properties: frequency sensitivity, luminance sensitivity and contrast masking. We will show that α_i is independent from the original image.

Finally, an 8×8 inverse-DCT is applied to $\hat{Y}_w$ to obtain NTSC format of the watermarked image (Y_w). Consequently, with a color space conversion the watermarked image (X_w will be obtained.

3. Extraction Process

The detection process proposed in this paper is depicted in Fig. 3. The recovered watermark $\tilde{W}$ is extracted from the possibly distorted image $\tilde{X}$ using the original image X and the secret keys.

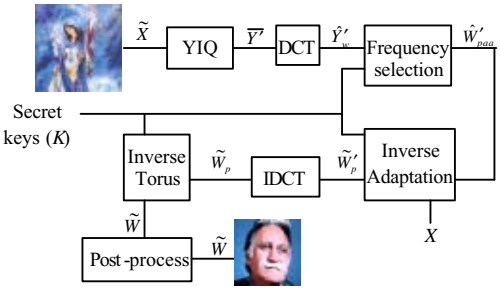


Figure 3. The proposed extraction process

Initially, the attacked watermarked image $\tilde{X}$ is converted to the NTSC color space and then divided into non-overlapping 8×8 blocks, and each block is DCT transformed independently to obtain $\hat{Y}'_w$.

After extracting t coefficients from each block in $\hat{Y}'_w$, reverse adaptation will be applied to obtain $\tilde{W}'_{paa}$ and $\tilde{W}'_p$, respectively.

Next, the inverse DCT can be applied to each $n \times n$ block in $\tilde{W}'_p$ to obtain the spatial-domain watermark image $\tilde{W}_p$. Finally, Torus function is performed (R-K_4) times over $\tilde{W}_p$ to obtain the embedded watermark ($\tilde{W}$).

A more reliable detection process has lower false positives and false negatives in the extracted watermark. So, we propose a post-processing procedure to obtain a higher quality watermark, especially for human eyes. The proposed extraction scheme decreases both false negatives and false positives.

4. Evaluation Process

By using $\tilde{W}$ and the registered watermark W, the arbitrator can verify the ownership of the original image. The evaluation of the watermarked image invisibility is calculated with Masked Peak Signal to Noise Ratio (MPSNR) that is a perceptual quality metric that exploits the contrast sensitivity and masking phenomena of the HVS and is based on a multi-channel model of the human spatial vision [7].

$$MPSNR\,(vdB) = 10\log_{10}\left(\frac{Mc^2}{MSE}\right) \qquad (6)$$

where MSE is the Mean Squared-Error between X and X_w. Values of X are between 0 and Mc.

The extracted watermark robustness is evaluated by Normalized Correlation (NC) ratio between W and $\tilde{W}$ [7].

In comparing two watermarking systems, the system with higher MPSNR value has better visual quality, and under an assumed attack, the system with higher NC value is more robust [7].

5. Experimental Results

In our experiments, a RGB-color Miniature (Morning Star miniature, painted by Mahmud Farshchian) with 512×512 pixels, and a 256-color watermark (Mahmud Farshchian's photo) with 128×128 pixels are used.

After performing the proposed scheme, the MPSNR value of the watermarked image (Fig. 4(a)) is equal to 57.9vdB, which indicates a higher quality watermarked image in terms of human visual system.

The NC value of the extracted watermark form an unattacked watermarked image is equal to 1; i.e. no degradation in the extracted watermark. In Tsai's method visual quality is 39.65dB and NC value is 0.99.

(a)

(b)

Figure 4. (a) Watermarked image, MPSNR=57.9 vdB (b) Extracted watermark, NC=1

As shown in Fig. 5, for $\alpha_i < 0.1$ the embedding strength parameter α_i increases, the invisibility decreases and the robustness increases. But for $\alpha_i > 0.1$, higher

IEEE COMPUTER SOCIETY

values for α_i results in less robust watermarked image. On the other hand, based on the HVS, an MPSNR value higher than 30 is suitable [7]. So, we selected $\alpha_i = 0.1$ which results in MPSNR=57.9vdB and NC=0.82 for an assumed attack such as 75% cropping over the watermarked image.

The proposed system was also tested with different original images and with this specific watermark. The results were the same as above; so the visual quality of the proposed scheme is independent of the original image.

5.1. The post processing unit advantages

The proposed scheme has been tested using a PRNG for watermark permutation, and an assumed attack such as image cropping to show the benefits of post-processing.

Images shown in Figs. 6(a) and 6(b) are a watermarked image after 75% cropping and additive-noise attacks, respectively. Figs. 6(c) and 6(e) are the extracted watermarks, using pseudo-random watermark permutation without post-processing. Figs. 6(d) and 6(f) are the extracted watermarks using pseudo-random watermark permutation and post-processing. According to the calculated NC ratios for each extracted watermark, it is obvious that performing post-processing over an extracted watermark improves quality of the outputs, i.e. less false positives and false negatives in the extracted watermark.

As shown in Fig. 7, using the embedding process with pseudo-random permutation, the visual quality of a post-processed watermark (Rpost) is higher than that of the watermark without post-processing (Rand) in the extraction algorithm. It shows that even using pseudo-random watermark, the robustness of the proposed scheme is better than Tsai's method. So, using post-processing improves the visual quality of the extracted watermark.

5.2. Torus permutation advantages

In Fig. 7, the robustness of a pseudo-random permutation watermark (Rpost) and a 2D Torus permutation (Torus) are being compared under various image cropping ratios. This figure shows that using Torus permutation improves the watermark robustness and removing additive noise after watermark extraction improves the extracted watermark quality. Fig. 8(b) shows the extracted watermark from a 75% cropped watermarked image (Fig. 6(a)). Comparing Fig. 6(d) and Fig. 8(b), although the NC values are close to each other, the perceptual quality improvement is noticeable.

5.3. Robustness against attacks

Figure 9 illustrates that the NC value will only slightly decrease even for the highest JPEG lossy compression ratios.

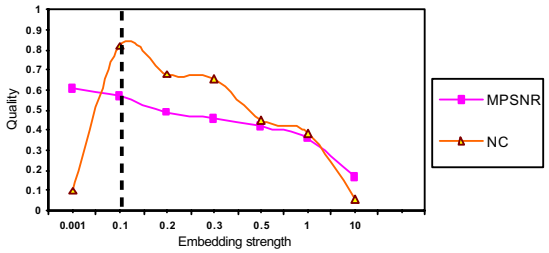


Figure 5. Embedding strength (α_i) versus visual quality (MPSNR*0.01) and robustness (NC) in the proposed embedding process

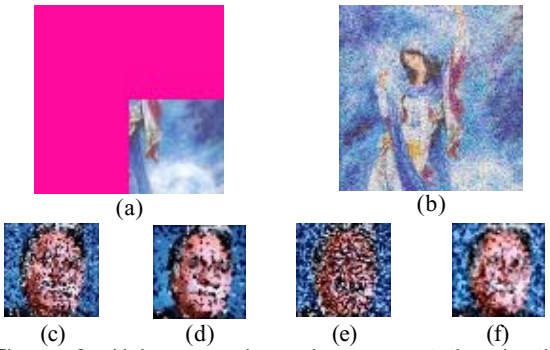


Figure 6. Using pseudo-random permutation in the embedding process, (a) 75% cropped watermarked image, (b) noisy watermarked image, (c) extracted watermark from a, NC=0.75, (d) c after post-processing, NC=0.79, (e) extracted watermark from b, NC=0.61, (f) e after post-processing, NC=0.68

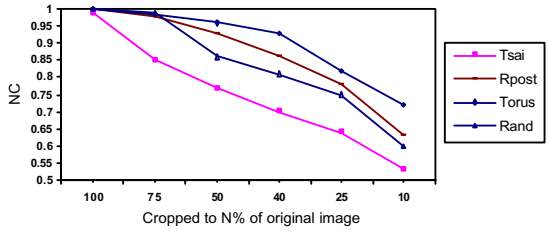


Figure 7. Comparison of robustness between the proposed scheme (Torus), Tsai's method, pseudo-random permutation without post-processing (Rand) and pseudo-random permutation with post-processing (Rpost) against an assumed attack (image cropping)

Figure 8. Extracted watermark using Torus permutation in the embedding process (a) without post-processing, NC=0.76, (b) with post-processing, NC=0.82

IEEE COMPUTER SOCIETY

Figure 10 shows the robustness of the proposed scheme under various median-filter sizes in comparison to that of other methods. Experiments show that the watermark is successfully extracted from the watermarked image even if the image undergoes more than once blurring attack. On the average, the proposed method is the most robust system under median filter attack. Furthermore, the NC values do not decrease when size of the filter increases.

As shown in Fig. 11, the proposed scheme is the most robust method against image cropping attack.

6. Conclusions

In this paper, we proposed a new block DCT-based digital watermarking scheme, which inserts an adapted color-watermark in the middle-frequency coefficients of the original color image transform.

The proposed adaptive embedding procedure improved robustness and invisibility of the watermarked image. Image-dependent adaptations not only take the advantage of HVS frequency sensitivity, but also rely on adapting the watermark to local image properties in order to provide maximum performance in terms of robustness, while satisfying the invisibility constraint.

For getting higher security and higher robustness, a 2D periodic Torus permutation function has been described which improved robustness and perceptual quality of the extracted watermark. Consequently, to decrease both false positives and false negatives in the extracted watermark, a post-processing algorithm was proposed which improved the visual quality of the extracted watermark. The visual quality of the proposed scheme was independent of the original image.

The experimental results showed that the proposed scheme was the most robust method, especially for higher lossy compression ratios. Also, on the average, it was the most robust system under blurring attacks. Indeed, the watermarked image robustness did not decrease when blurring increased due to larger filter size. In addition, the proposed scheme was the most robust method under image cropping attacks.

7. References

[1] C-S Tsai, C-C Chang, T-S Chen, and M-H Chen, Distributed multimedia databases: Techniques and Applications, National Chung Chang University, and National Taichung Institute of Technology, Taiwan, 2001.

[2] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, 1997, pp. 1673-1687.

[3] J. Fridrich, "Combing low-frequency and spread spectrum watermarking," *SPIE Symposium on Optical Science Engineering and Instrumentation*, San Diego, USA, July 1998.

[4] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," *IEEE International Workshop on Non-Linear Signal and Image Processing*, Neos Marmaras, Greece, June 1995, pp. 452-455.

[5] I.J. Cox and M.L. Miller, "Robust digital watermarking," *United States Patent*, patent number 6278792, August 21, 2001.

[6] J. Fridrich, "Image watermarking for tamper detection," *IEEE International Conf. On Image Processing (ICIP'98)*, Vol. 2, 1998, pp. 404-408.

[7] M. Kutter and F.A.P. Petitcolas, "Fair evaluation methods for image watermarking systems," *Journal of Electronic Imaging*, Vol. 9, No. 4, October 2000, pp. 445-455.

[8] G. Voyatzis and I. Pitas, "Chaotic mixing of digital images and applications to watermarking," *European Conf. on Multimedia Applications, Services and Techniques (ECMAST'96)*, Vol. 2, 1996, pp. 687–695.

[9] R.B. Wolfgang, CI. Podilchuk, and E.J. Delp, "Perceptual watermarks for digital images and video," *IEEE proc.*, Vol. 87, No. 7, July 1999, pp. 1108-1126.

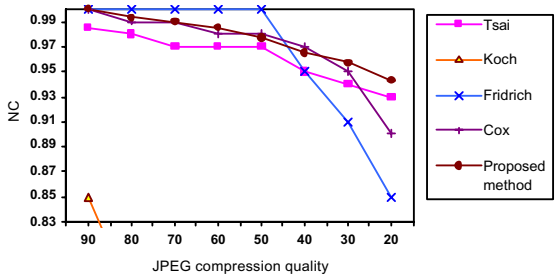


Figure 9. Comparison of robustness between the proposed scheme and other methods against JPEG lossy compression attack

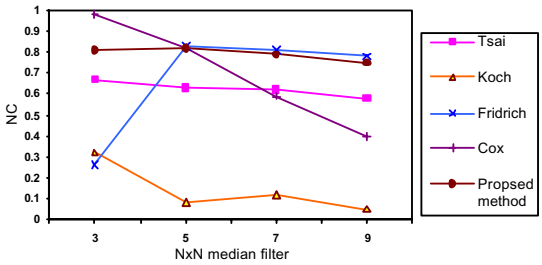


Figure 10. Comparison of robustness between proposed scheme and other methods against blurring attack.

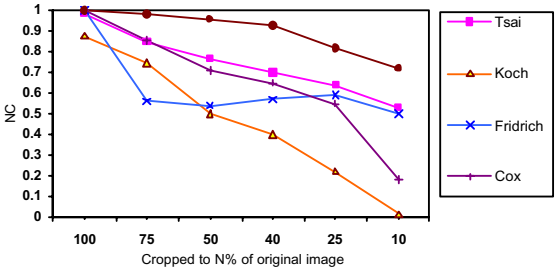


Figure 11. Comparison of robustness between proposed scheme and other methods against image cropping attack

IEEE COMPUTER SOCIETY