Journal of Advances in Computer Research
Quarterly ISSN: 2008-6148
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 3, No. 2, May 2012), Pages: 65-74
www.jacr.iausari.ac.ir

# A Modified Digital Image Watermarking Scheme Based on Nonnegative Matrix Factorization

**Mohammad Ali Shamszadeh[1]✉, Alimohammad Latif[2], Mohsen Rabbani[3]**

*(1) Department of Engineering, Sari Branch, Islamic Azad University, Sari, Iran*
*(2) Electrical and Computer Engineering Department, Yazd University, Yazd, Iran*
*(3) Department of Mathematics, Sari Branch, Islamic Azad University, Sari, Iran*

m.ali_shams@yahoo.com; alatif@yazduni.ac.ir; mrabbani@iust.ac.ir

**Received: 2012/04/05; Accepted: 2012/05/05**

**Abstract**

*This paper presents a modified digital image watermarking method based on nonnegative matrix factorization. Firstly, host image is factorized to the product of three nonnegative matrices. Then, the centric matrix is transferred to discrete cosine transform domain. Watermark is embedded in low frequency band of this matrix and next, the reverse of the transform is computed. Finally, watermarked image is obtained by multiplying nonnegative matrix components. The experimental results show that the proposed method is transparent and also is high robust against JPEG compression, scaling and median filter attacks.*

***Keywords:*** *Digital image watermarking, Nonnegative matrix factorization, Robustness, Transparency*

Archive of SID

## 1. Introduction

The use of the Internet as a digital media platform has grown rapidly in recent years. Although this has many advantages, it causes serious concerns over the unauthorized distribution and manipulation of the digital contents, including the copyright violation.

Security and legitimate use of digital products is a significant issue for most digital artificers. They are interested in protecting their work from unauthorized reproduction and also they want that the copyright of their work should belong to themselves. Therefore, cryptography and watermarking have proposed to solve these problems [1].

Cryptography is a general way of protecting data which is performed by reversible mathematical methods. In cryptography schemes, data is coded using encoding algorithm and some keys, and then the coded data is sent to the receiver. The received data is decoded using reverse algorithm and proper keys and finally, data is delivered to the user. One problem of cryptography is that there is no protection after decoding over the data anymore, and it is possible to copy an unauthorized decoded data.

Another problem to use cryptography in images is that in cryptography algorithm the decoded data may be forged based on changing the order of image pixels, which this cause the encoded data of the image does not appear as an image for the user. Due to these issues, it is less common to use cryptography systems for protecting data images.



www.SID.ir

Watermarking is a more powerful scheme, which can protect image data in more situations. By embedding a private sign related to the owner of data, it is possible to prevent visible or invisible change and forge [2].

A digital watermarking system includes two sections: Watermark embedding and watermark extracting. Watermark embedding receives watermark and host image. The watermark is inserted in the host image with a suitable algorithm in watermark embedding section and then the watermarked image is ready for storing or sending. (See Figure. 1).

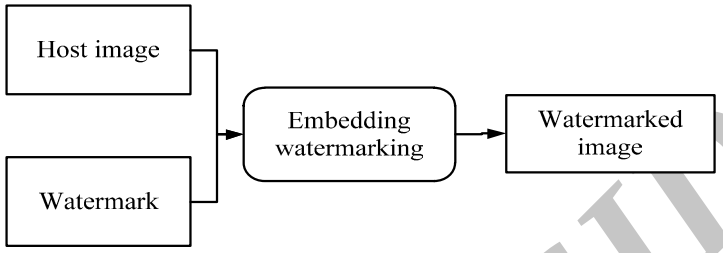



***Figure 1. Embedding section***

The watermarked image may be altered during transmission by attackers and make watermarked attacked image [3]. The received watermarked image can be examined in extracting section. In this part, the watermark is extracted using a proper algorithm, and then the originality of watermark is examined and it is recognized whether the extracted watermark is original or not? (See Figure. 2).

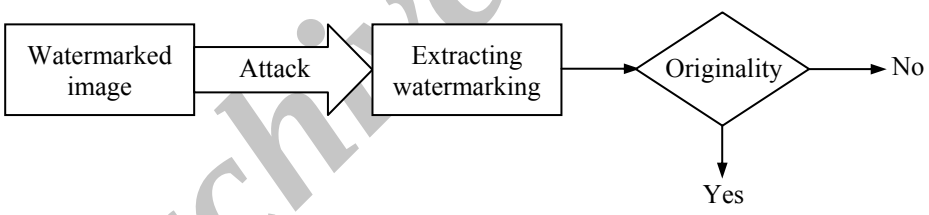



***Figure 2. Extracting section***

In some watermarking applications, it is possible to access the host image in extracting section so this method is known as non-blind scheme. However, if there is no access to the host image in extracting section, this method is known as blind scheme [4].

The watermarking algorithms are classified depending on how the watermark is embedded. In fact, depending on the domain in which the watermark is embedded, digital watermarking techniques can be classified as spatial and spectral domain techniques. In the spatial domain methods, a watermark is inserted into an image by modifying the images' pixel values directly [5]. However, spectral domain approaches transform the original image into the frequency domain and modulate the transfer's coefficients to embed the watermark. In general, spectral domain methods are more robust than spatial domain against many common attacks [6] (see Figure. 3).



Archive of SID

www.SID.ir

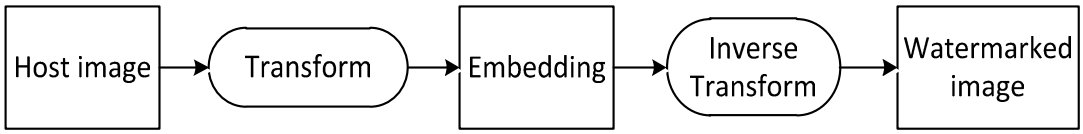



***Figure 3. Frequency domain embedding***

Some transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are used in image processing e.g. in image compression and watermarking. Note that, the JPEG and MPEG compression are based on the DCT decomposition, and embedding a watermark in the DCT domain makes it possible to integrate watermarking with image and video coding and produce real-time watermarking applications [7]. Thus, we use the DCT in this paper.

Watermark embedding in high frequency band decreases robustness property against compression attacks, since high frequency contents are eliminated in image compression. Therefore, our proposed algorithm inserts the watermark in low band frequency.

Watermarking algorithms have some requirements such as transparency and robustness. The transparency represents that the distortion between the host and watermarked image should remain imperceptible to a human observer. The robustness is that the ability of the detector to extract the hidden watermark from some altered watermarked image.

In addition, some unauthorized people tend to destroy hidden watermark in the image which perform some attacks such as compression, additive noise, and some filters over the watermarked image in order to eliminate or weaken the watermark [6].

This paper contains four sections. In the next section, the related work is explained and then in the third section, NMF is considered. Fourth section discussed the suggested scheme for embedding and extracting. The experimental results are presented in the final section.

## 2. Related Work

Maybe the earliest transforms which was utilized in watermarking schemes was DFT [8]. This transform scheme could utilize rotation, scale and translation invariant properties. Later, Pun embedded the watermark in the DFT coefficients with the highest magnitudes and used the similarity measure in detection procedure [9].

Next, DCT was extensively utilized in watermarking schemes. Using the DCT, an image was divided into frequency bands, and the watermark was embedded in low and middle frequency bands. Sensitivities of the Human Visual System (HVS) to changes in these bands were studied in the context of JPEG compression, and the results of these studies were exploited to minimize the visual impact of the watermark embedding distortion [10].

In addition, many multi-resolution watermarking techniques were proposed using DWT. In this group of watermarking schemes, the original image and watermark were decomposed into sub-bands and then, the watermark sequence was embedded into the corresponding level of the transformed image. The sub-band decomposition technique

Archive of SID



www.SID.ir

facilitated placement of the watermark which exploited HVS characteristics to obtain more fidelity of the watermarked images [11].

Ganic and Zubair used Singular Value Decomposition (SVD) in image watermarking in 2003 [12]. First, they factorized the host image into $U$، $\sum$ and $V$ matrices, and then the watermark is embedded in $\sum$ component.

In 2009, Hamza et al. applied matrix factorization to watermarking algorithm [13]. He computed the DWT of the host image and decomposed the low and high frequency coefficients in two matrices based on NMF. Then, he embedded the watermark in the first matrix.

Since the DWT coefficients are positive and negative, the NMF factorization is not suitable for such watermarking algorithm. In addition, in Hamza's scheme few part of watermark was embedded and other parts of watermark have to be transformed to the receiver. Thus, in this paper we modify the Hamza's scheme and also use Tri-NMF (see Figure. 4) to decompose the host image and embed the whole watermark in the host image. As mentioned before, we use the DCT domain for extensively utilization in JPEG compression.

## 3. Nonnegative Matrix Factorization

To factorize a matrix into product of several matrices, various methods such as SVD have been suggested. In SVD factorization, the host image is factorized into three sub-matrices according to equation (1):

$$C = U \times \sum \times V' \tag{1}$$

where C is the host image with the size of $m \times m$, $U$ and $V$ are orthogonal matrices including positive and negative elements. Σ is a diagonal matrix which includes eigenvalues of the host image [14].

One of the main drawbacks of SVD is that the basic vectors of matrix include positive and negative components. The negative components, in majority of usage are not match with the brightness which is the physical reality of the image. To solve this problem, the NMF method has been suggested for image processing. It is should be noted that some of the main features of an image can be found in factorized matrices [13].

The NMF method was introduced by Tapper and Paatero and then, Lee and Seung used NMF in digital images [12]. It is worthy to mention that the NMF is not among accurate matrix factorization algorithm, but its error is few and can be ignored in digital images [15].

Figure 4 shows in Tri-NMF the host image, $C$, with the size of $m \times m$ can be factorized in to three nonnegative matrices $B$, $H$ and $K$ with the size of $m \times r$, $r \times p$ and $p \times m$ which $C = B \times H \times K$ and $r, n \leq m$ [13].

Archive of SID



www.SID.ir

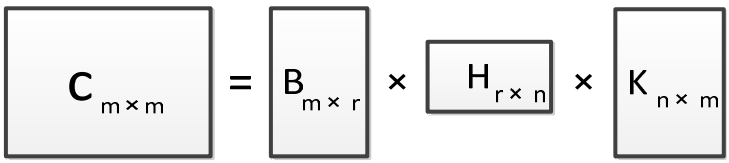



***Figure 4. Nonnegative matrix factorization***

Recursive algorithms are used to find factorization matrices, which by using initialization and some iterations, matrix factorization is performed [15].

## 4. Proposed watermarking scheme

In this section, our watermark embedding and extracting algorithms are separately indicated.

### *a. Watermark embedding algorithm*

For embedding watermark in an image, the host image is factorized to $B, H$ and $K$ matrices. The middle matrix is chosen as the position of watermark embedding; then, it is transferred to DCT domain. Finally, the watermark is embedded in the low frequency band according to the following equation:

$$H' = H + \alpha \times W \tag{2}$$

where $H'$ is the factorization matrix of watermarked image, $H$ is the host image factorization matrix and $\alpha$ is the watermark strength.

The factorization matrix is returned to the spatial domain after watermark embedding by multiplying three factorized matrices. The watermarked image, $C_W$, is obtained by equation. 3:

$$C_W \approx B \times H' \times K \tag{3}$$

The embedding of watermarking algorithm is pointed to Table 1.

***Table 1. Embedding algorithm***

| |
|---|
| 1. Apply Tri-NMF to the host image, C, of size $m \times m$ and decompose into three matrices; |
| 2. Divide the centric element into non-overlapped blocks; |
| 3. Compute the DCT of each block; |
| 4. Embed the watermark on the low frequency coefficients; |
| 5. Compute inverse DCT and multiply the elements of NMF; |

To summarize and clarity of the mentioned scheme, the procedure is indicated in the following flowchart.



Archive of SID

www.SID.ir

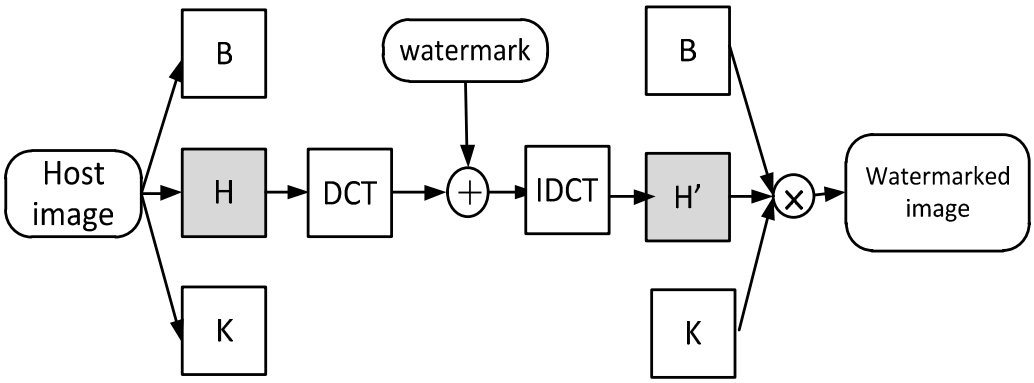



***Figure 5. Embedding proposed scheme***

***b. Watermark extracting algorithm***

To extract a watermark, the watermarked image, $C_W$, and the host image, $C$, Singular Value Decomposition (SVD) are factorized to three matrices as $C_W \approx B_W \times H_W \times K_W$ and $C \approx B \times H \times K$ using Tri-NMF then, the watermark , $W$, is extracted by using the following equation:

$$w = (H_W - H)/\alpha \qquad (4)$$

The extracting of watermarking algorithm is pointed to Table 2.

***Table 2. Extracting algorithm***

| |
|---|
| 1. Apply Tri-NMF to the host and watermarked image; |
| 2. Divide the centric element into non-overlapped blocks; |
| 3. Compute the DCT of each block; |
| 4. Extract the bits of watermark from the low frequency coefficients; |
| 5. Attach the extracted bits of watermark in order to retrieve the complete watermark; |

To summarize and clarity of the mentioned scheme, the procedure is indicated in the following flowchart.

Archive of SID



www.SID.ir

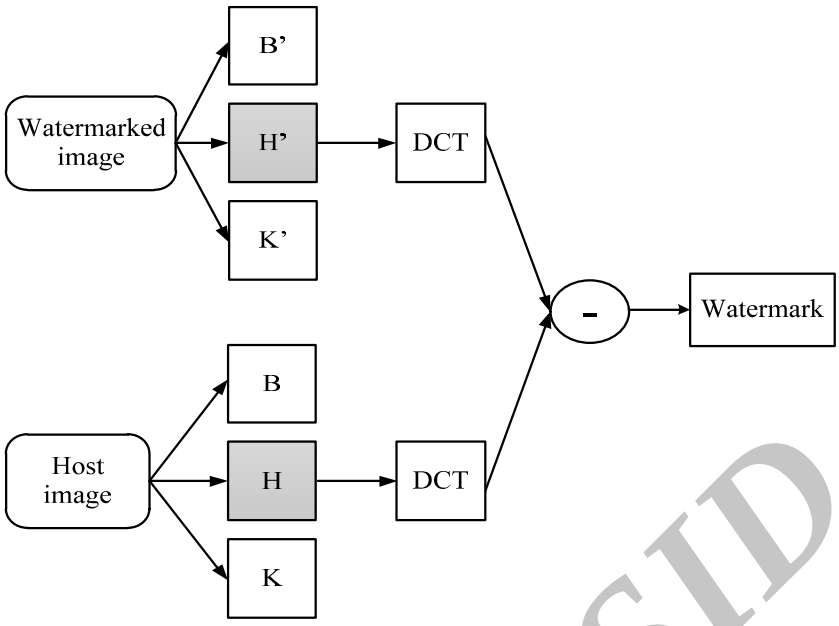



*Figure 6. Extracting proposed scheme*

## 5. Experimental results

Our scheme is implemented on Matlab 2011 platform. Gray images of Cameraman, Lena, Boat and Baboon in figure (7) with size 256×256 are used as host images and university logo in figure (8) is employed as watermark with size of 32×32.

*(a). Cameraman* *(b). Lena* *(c). Boat* *(d). Baboon*

*Figure 7. Host images*

*Figure 8. Watermark*

### *a. Performance evaluation of transparency*

Figure (9) shows the results of watermarked images. They indicate that our suggested algorithm have a good visual quality.



Archive of SID

www.SID.ir

***(a)*** ***(b)*** ***(c)*** ***(d)***

***Figure 9. Watermarked image***

The Peak Signal to Ratio (PSNR) value, which is the ratio of signal to noise, is used to check transparency of watermarked image and host image [16]. The mentioned metric is obtained by equation (5):

$$PSNR = 20\log\left(\frac{MAX_i}{\sqrt{MSE}}\right) \quad (5)$$

where $MAX_i$ is the largest pixel intensity in the image and $MSE$ [1] indicates the mean square error between the host image and watermarked image.

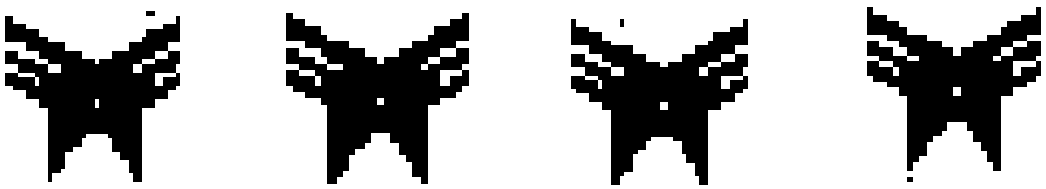
The PSNR of our proposed scheme and Hamza scheme are demonstrated in Table (1). According to the acceptable value of PSNR, the results show that the transparency of suggested method is high as Hamza's method [17].

***Table 1. The PSNR value of proposed and Hamza's scheme***

| | Baboon | Cameraman | Boat | Lena |
|---|---|---|---|---|
| Hamza Scheme | 44 | 40 | 41 | 42 |
| Proposed Scheme | 42 | 43 | 40 | 45 |

***b. Performance evaluation of transparency***

Robustness against attacks is another basic and main standard metric to evaluate the performance of watermarking scheme. In this study, JPEG, scaling and median filter attacks have been used to evaluate the robustness of suggested method. The extracted watermarks are shown in figure (10).



***(a) BCR=99.9*** ***(b) BCR=100*** ***(c) BCR=99.9*** ***(d) BCR=99.9***

***Figure 10. Extracted watermark image from (a) Cameraman (b) Lena (c) Boat (d) Baboon***

1. Mean Square Error (MSE)



Archive of SID

www.SID.ir

The Bit Correct Ratio (BCR) metric is applied for objective evaluation based on equation (6):

$$BCR_{(W,W')} = \frac{\sum_{i=1}^{MN} (\overline{W_i \oplus W'_i})}{M \times N} \times 100\% \quad (6)$$

where $W$ is the original watermark, $W'$ is the extracted watermark, $M$ and $N$ are the size of watermark [18]. This value shows the similarity between the original and extracted watermark. The higher value of BCR means the more similarity between the original watermark and extracted watermark.

The BCR values of our proposed and Hamza's method against some attacks are indicated in Table (2).

In these simulation numerical results, the robustness of proposed algorithm against JPEG and median filter are higher than Hamza's scheme.

***Table 2. The BCR value of proposed and Hamza's scheme against some attacks***

| | Our proposed Scheme (Tri-NMF) | | | | Hamza's Scheme (NMF) | | | |
|---|---|---|---|---|---|---|---|---|
| | Lena | Cameraman | Baboon | boat | Lena | Cameraman | Baboon | boat |
| Jpeg (Q = 50) | 99.6 | 99.3 | 99.7 | 99.6 | 99.3 | 99.1 | 99.4 | 99.3 |
| Jpeg (Q = 20) | 99.1 | 98.9 | 99.3 | 99.2 | 98.8 | 98.5 | 98.7 | 98.8 |
| Median (3×3) | 99.6 | 99.5 | 99.6 | 99.8 | 99.4 | 99.2 | 99.3 | 99.4 |
| Median (5×5) | 99.3 | 99.1 | 99.4 | 99.2 | 98.8 | 98.8 | 99 | 98.9 |
| Scaling (2) | 99.6 | 99.5 | 99.8 | 99.6 | 99.3 | 99.2 | 99.5 | 99.3 |

## 6. Conclusions

In this paper a new method of digital image watermarking using DCT and NMF has been presented. The superior of our algorithm is that we use Tri-NMF in digital images. The suggested method was conducted on some images and its robustness has been checked against different various attacks. The simulation results reveal that the suggested method has higher performance than Hamza's method which he used NMF to factorize the image.

## 7. References


[1] Cox, I.J., M.L. Miller, and J.A. Bloom. Watermarking applications and their properties. 2000: IEEE.

[2] Tewfik, A. and M. Swanson, Data hiding for multimedia personalization, interaction, and protection. Signal Processing Magazine, IEEE, 1997. 14(4): pp. 41-44.

[3] Bounkong, S., et al., ICA for watermarking digital images. The Journal of Machine Learning Research, 2003. 4: pp. 1471-1498.

[4] Soheili, M.R., A Robust Digital Image Watermarking Scheme Based on DWT. Journal of Computer Engineering, 2009. 1: p. 3-11.

[5] C.C. Chang, C.C. Lin and Y.S. Hu, An SVD oriented watermark embedding scheme with high qualities for the restored images, International Journal of Innovative Computing, Information and Control, vol.3, no.2, pp. 609{620, 2007.

[6] Zheng, D., et al., A survey of RST invariant image watermarking algorithms. ACM Computing Surveys (CSUR), 2007. 39(2): pp. 5.

[7] De Vleeschouwer, C., J.F. Delaigle, and B. Macq, Invisibility and application functionalities in perceptual watermarking an overview. Proceedings of the IEEE, 2002. 90(1): pp. 64-77.




Archive of SID

www.SID.ir

[8] D. Zheng and J. Zhao, Apply phase information in RST image watermarking, IEEE Int. Conf. on Consumer Electronics, pp. 218-219, 2003.
[9] C. Pun, A novel DFT-based digital watermarking system for images, Int. Conf. on Signal Processing,vol.2, 2006.
[10] S. Lin and C. Chen, A robust DCT-based watermarking for copyright protection, IEEE Trans. On Consumer Electronics, vol.46, no.3, pp. 415-421, 2000.
[11] A. A. Reddy and B. Chatterji, A new wavelet based logo-watermarking scheme, Pattern Recognition Letters, vol.26, no.7, pp. 1019-1027, 2005.
[12] Ganic, E., N. Zubair, and A.M. Eskicioglu. An optimal watermarking scheme based on singular value decomposition. 2003: Citeseer.
[13] Cichocki, A., et al., Nonnegative matrix and tensor factorizations: applications to exploratory multi-way data analysis and blind source separation. 2009: Wiley.
[14] Chandra, D.V.S. Digital image watermarking using singular value decomposition. 2002: IEEE.
[15] Ghaderpanah, M. and A.B. Hamza. A nonnegative matrix factorization scheme for digital image watermarking. 2006: IEEE.
[16] Lee, C., et al., Non-negative Matrix Factorisation for Network Reordering. Monografias de la Real Academia de Ciencias de Zaragoza, 2010. 33: pp. 39-53.
[17] Ouhsain, M. and A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform. Expert Systems with Applications, 2009. 36(2): pp. 2123-2129.
[18] Khan, A. and A.M. Mirza, Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. Information Fusion, 2007. 8(4): pp. 354-365.

Archive of SID



www.SID.ir