# Watermarking Based on Independent Component Analysis In Spatial Domain

Abolfazl Hajisami
*Department of Electrical Engineering*
*Sharif University of Technology*
*Tehran, Iran*
*hajisami@ee.sharif.ir*

Alireza Rahmati
*Department of Electrical Engineering*
*Tarbiat Modarres University*
*Tehran, Iran*
*a.rahmati@modares.ac.ir*

Massoud Babaie-Zadeh
*Department of Electrical Engineering*
*Sharif University of Technology*
*Tehran, Iran*
*mbzadeh@yahoo.com*

***Abstract*—This paper proposes an image watermarking scheme for copyright protection based on Independent Component Analysis (ICA). In the suggested scheme, embedding is carried out in cumulative form in spatial domain and ICA is used for watermark extraction. For extraction there is no need to access the original image or the watermark, and extraction is carried out only with two watermarked images. Experimental results show that the new method has better quality than famous methods [1], [2], [3] in spatial or frequency domain and is robust against various attacks. Noise addition, resizing, low pass filtering, multiple marks, gray-scale reduction, rotation, JPEG compression, and cropping are some attacks which are considered in our extensive simulations to demonstrate the proposed algorithm performance.**

***Keywords*-watermarking; independent component analysis; blind source separation;**

## I. Introduction

Digital watermarking is used as an efficient technology for copyright protection of digital multimedia products, specifically those that are distributed over public networks [4]. Watermarked signals are subject to different intentional or unintentional manipulations; hence it is of crucial importance in most applications to design a watermarking strategy that is robust to both malicious and non-malicious attacks. An image watermarking method is typically evaluated based on three major criteria: the largest amount of the embedded data that is still visually imperceptible, robustness of watermark against certain attacks, and probability of the watermark extraction in adverse conditions.

Data embedding in an image may be carried out in different domains, including spatial and transform domains. Early image watermarking schemes operated directly in spatial domain, which were mostly associated with poor robustness properties. Accordingly, different transform domains have been studied in the last decade to improve the efficiency and the robustness of watermarking methods [1], [2], [3], [5], [6].

Watermarking methods can be categorized into three major groups: blind, semi-blind, and non-blind [7]. In blind methods, there is no need for the original signal or the watermark for watermark extraction. In semi-blind methods, some features of the original signal are to be known a priori, where the original signal should be available for extracting the watermark in non-blind methods. Our algorithm can be employed as a non-blind or blind method, as described later.

The ICA is typically known as a method for Blind Source Separation (BSS) and can be used in watermarking. Some ICA based approaches to the image watermarking have been reported in [5], [8], [9], [10], [11], [12], [6].

This paper proposes a watermarking scheme based on ICA in spatial domain which is also robust against a variety of attacks including noise addition, resizing, low pass filtering, multiple marks, gray-scale reduction, rotation, JPEG compression, and cropping parts of the image. Moreover, it is a blind method and does not need to have the original signal, watermark or any key in order to extract the watermark and also the embedding rate is equal to the size of original image.

This paper is organized as follows. An overview of BSS is discussed in Sect. II. The main idea and the proposed watermarking scheme is stated in Sect. III. The quality of the proposed method and its robustness against different attacks will then be experimentally studied in Sect. IV and the conclusion is drawn in Sect. V.

## II. Blind Source Separation

In BSS, a set of mixtures of different source signals is available and the goal is to separate the source signals, when we have no information about the mixing system or about the source signals expect their statistical independence (hence the name blind). The mixing and separating systems are shown in Fig. 1 and can be represented mathematically as:

$$\begin{aligned} \mathbf{x}(t) &= \mathbf{A}\mathbf{s}(t) \ , \\ \mathbf{y}(t) &= \mathbf{B}\mathbf{x}(t) \ , \end{aligned} \tag{1}$$

in which, $\mathbf{s}(t) = [s_1(t), \ldots, s_N(t)]^T$ is the vector of sources that are mixed by the mixing matrix $\mathbf{A}$ and creates the observations vector $\mathbf{x}(t) = [x_1(t), \ldots, x_N(t)]^T$. Let also $\mathbf{A}$ be a the square matrix $(N \times N)$ of full column rank that means number of sources are equal to the number of observations and observations are linear independent. The goal is to achieve the separating matrix $\mathbf{B}$ such that the $\mathbf{y}(t) = [y_1(t), \ldots, y_N(t)]^T$ is an estimation of the sources. The idea of ICA is to exploit the assumption of source independence and estimate $\mathbf{B}$ such that the outputs $y_i$'s are statistically independent. It has been shown [13] that this

978-0-7695-4376-5/11 $26.00 © 2011 IEEE
DOI 10.1109/UKSIM.2011.63

results in retrieving the source signals provided that there are at most one Gaussian source.

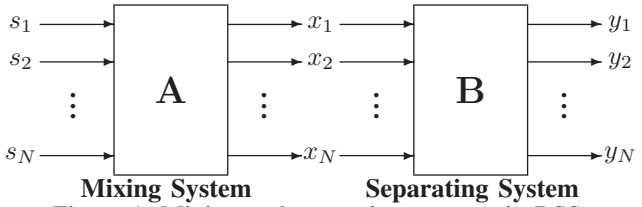


Figure 1: Mixing and separating systems in BSS.

## III. Our Proposed Watermarking Scheme

Consider a spatial domain watermarking scheme as:

$$C_W = C + \alpha W \quad , \tag{2}$$

where $C$ is the original image, $W$ is the binary watermark image, $C_W$ is the watermarked image and $\alpha$ is the embedding strength. As we noted in Sect. I, embedding in spatial domain is one of earliest methods for watermarking, but because of low performance, frequency domain methods become more interesting. In this paper, main idea is exploiting of ICA properties in order to improving the robustness, imperceptibility and embedding rate of spatial domain methods.

Before proposing the idea, we look at the watermarking problem as a BSS problem and realize the similarity between mixing of the sources and embedding the watermark in the original image, and also the similarity between the separation of the sources and the extraction of the watermark from the watermarked image, therefore in the extraction of the watermark we can apply the BSS methods. In this paper we use ICA for extraction and we know in ICA the number of sources must be equal to the number of observations, and the observations must be linear independent. In the watermarked images that are obtained by (2), we have two sources $C$ and $W$, therefore for extraction we need two observations or in other words two watermarked images.

We propose now that one who wants to distribute an image, embeds the watermark in each original image with different embedding strengths, using (2). In this case watermarked images can be treated as observations in a BSS problem, and hence without the need neither for the original image nor the watermark one can extract the watermark by applying ICA on any two of the watermarked images. Moreover, despite the simplicity of this idea, we will see in simulation that it is very practical in sense that it results in a high capacity for embedding information, while it is robust against a group of attacks.

Finally it must be added that because of quantization, for embedding we use $C_W = Q(C + \alpha W)$, that $Q$ denote quantization operator. The summary of above discussion can be presented as:

$$\begin{bmatrix} C_{W_1} \\ C_{W_2} \\ \vdots \\ C_{W_N} \end{bmatrix} = Q\left( \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \\ \vdots & \vdots \\ 1 & \alpha_N \end{bmatrix} \begin{bmatrix} C \\ W \end{bmatrix} \right) \text{and } \alpha_i \neq \alpha_j \text{ for } i \neq j \ , \tag{3}$$

where $C_{W_i}$'s are the watermarked images and $\alpha_i$'s are different embedding strength.

## IV. Simulation and Experimental Results

In this section, we experimentally study the robustness of the suggested method against adding noise, resizing, lowpass filtering, multiple marks, JPEG compression and cropping parts of the image. The results of these experiments show that although the idea of the method is simple and is done by just a simple BSS and although it is done in spatial domain, it is robust against the above attacks. Moreover by comparing this method to the famous methods of [1], [2], [3] that embed the watermark in different domains, we conclude that our method has better quality. In our simulations, for performing ICA, we have always used FastICA algorithm [14].

### A. Simulation Setup

In our simulation, we have used a database of 200 natural images as the original images and 100 various logos as the watermarks. Fig. 6 illustrates a sample of a binary watermark image (Sharif university logo) and original image (cameraman) of size $256 \times 256$, each of size $256 \times 256$. In Fig. 3, two watermarked images with different embedding strengths are shown, which are created by (2) for $\alpha = \frac{1}{255}$ and $\alpha = -\frac{1}{255}$, respectively. After embedding there is no quantization here because the values of $W$ are 0 or 255 and from (2) it is obvious that values of the original image have been altered by $-1$, 0, or 1. Figure 4 represents the extracted image and the watermark using ICA (in which for solving the scale ambiguity of ICA, we have used a threshold to decide which bit is 0 and which bit is 1). To measure the quality of the watermarked image, we use Peak Signal-to-Noise Ratio (PSNR). The PSNR between an image $X$ and its perturbed version $\hat{X}$ is defined as:

$$\text{PSNR} = 20 \log_{10} \left( \frac{255}{\sqrt{1/(MN) \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{(i,j)} - \hat{X}_{(i,j)})^2}} \right) , \tag{4}$$

where $M \times N$ is the size of the two images. In the watermarked images that are shown in Fig. 3, PSNR is equal to $49.88dB$ whereas the PSNR in the methods of [1], [2] and [3] methods are equal to $38.4dB$, $36.7dB$ and $34.2dB$, respectively. For study the extraction process we use Bite Error Rate (BER) that is defined as:

$$\text{BER} = \frac{\text{Number of error bits}}{\text{Number of total embedded bits}} \ . \qquad (5)$$

In our experiments over the given original and watermark databases, we had BER $= 0$, as the average error rate, that shows ICA has estimated all embedded bits correctly.

(a) (b)

Figure 2: Original image (a) and watermark (b).

(a) (b)

Figure 3: Watermarked images with different embedding strength.

(a) (b)

Figure 4: Extracted image (a) and watermark (b).

### *B. Robustness Against Different Attacks*

In this section, we study the performance of the suggested method against different types of attacks.

**Experiment** 1 **(Noise addition)**: In this experiment we added a Gaussian noise with zero mean and variance 0.25, and Salt & Pepper noise with a density of 3% to one of the watermarked images and FastICA could still extract the watermark as shown in Fig. 5. This is because, after adding the Gaussian noise, Equation (2) changes to $IC_W = IC_H + \alpha W + n$, where $n$ denotes the Gaussian noise. In this case, the two sources are $IC_H$ and $\alpha W + n$ and, following the extraction process, we retrieve $\alpha W + n$ as the watermark. In case of additive Salt & Pepper noise, instantaneous mixture model might be destroyed for a number of pixels, but the ICA could still retrieve the sources.

**Experiment** 2 **(Lowpass filtering)**: In another experiment we applied a lowpass filter to the one of the watermarked images by averaging each pixel with its neighbors. The result of this filtering process is illustrated in Fig. 6a. Our extraction algorithm was quite successful to detect the watermark, as shown in Fig. 6b.

**Experiment** 3 **(Resizing)**: We scaled down one of the watermarked images by factor 2 using the *bilinear* method. To examine the extraction performance in this case, we used the resized version of the another watermarked image due to the ICA requirement. However, because we might not be aware of the resizing procedure employed by the attacker, we used the *bicubic* method to resize the another watermarked image. Our mark extraction method was again found successful in all such resizing attacks applied to the images in our database. An example is shown in Fig. 7a.

**Experiment** 4 **(Gray-scale reduction)**: In this experiment the gray-scale of watermarked image is reduced from 256 down to 64. In this case, the pixel value of new image is almost $1/4$ times of the older one. Because the ICA is not sensitive to multiplying the observation by a constant, the watermark can still be retrieved, as illustrated in Fig. 7b.

**Experiment** 5 **(multiple marks)**: In order to study the performance of the suggested method when another watermark is embedded, we added another watermark shown in Fig. 8a to one of the watermarked image and noted that the watermark was retrieved as shown in Fig. 8b. Because after embedding a second watermark, watermarked image will be $C_W = C + \alpha W + \beta W^{'}$, and our new sources will be $C$, $W$ and $W^{'}$. In this case we can exploit three watermarked images as observations and extract both watermarks.

**Experiment** 6 **(Rotation)**: Here, we rotated one of the watermarked images by 10 degrees and using *bilinear* method. The result of this rotating process is illustrated in Fig. 9a. However, because we might not be aware of the rotating procedure employed by the attacker, we used the *bicubic* method to rotate the another watermarked image. By applying our method, watermark can be retrieved as shown in Fig. 9b.

**Experiment** 7 **(Cropping)**: Here, we cropped 25% of one of the watermarked images. As we can find the cropped parts of the image by correlation method, we are able to crop these parts from the another watermarked image. Now by applying the suggested method we can retrieve the watermark as shown in Fig. 10a. Obviously this is because after cropping, instantaneous mixture model still holds for remainder pixels.

**Experiment** 8 **(JPEG compression)**: In our last experi-

ment we JPEG compressed the watermarked images with different quality factors 70% and 90% and unexpectedly we retrieved the watermark as shown in Fig. 10b. Results of a brief comparison made with two other well-known watermarking methods [2], [3] are shown in Fig.11 against different JPEG quality factors.

## V. Conclusion

In this paper a blind watermarking idea for copyright protection was proposed in which embedding is implemented in a cumulative form with different embedding strengths, and watermark extraction uses two watermark images and applies ICA. It must be said that in this method for extracting the watermark, we do not need the original image, the watermark or the key and extraction is completely blind. Application of ICA in extraction results in robustness of this method against a variety of attacks including noise addition, resizing, lowpass filtering, multiple marks, gray-scale reduction, rotaion, JPEG compression, and cropping parts of the image.

## VI. Acknowledgment

This work is supported in part by the Education and Research Institute for ICT (ERICT) Tehran, Iran under grants 19167/500.

## References

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[2] G. C. Langelaar, J. C. A. van der Lubbe, and R. L. Lagendijk, "Robust labeling methods for copy protection of images," *Proceedings of SPIE*, vol. 3022, pp. 298–309, February 1997.

[3] H.-J. M.Wang, P.-C. Su, and C.-C. J. Kuo, "Wavelet-based digital image watermarking," *Optics Express*, vol. 3, no. 12, pp. 491–496, 1998.

[4] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, 1999.

[5] S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images," *Journal of Machine Learning Research*, vol. 4, no. 7, pp. 1471–1498, 2003.

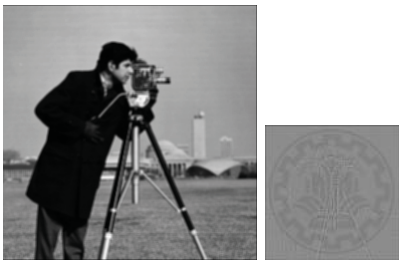
[6] A. Hajisami and S. Ghaemmaghami, "Robust Image Watermarking Using Independent Component Analysis," in *Third International Symposium on Information Processing*, Oct. 2010, pp. 363–367.

[7] C.-S. Lu, *Multimedia security : steganography and digital watermarking techniques for protection of intellectual property, Idea Group Publishing*. Idea Group Publishing.

[8] T. V. Nguyen, J. C. Patra, and P. K. Meher, "A new digital watermarking technique using independent component analysis," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, 2008.

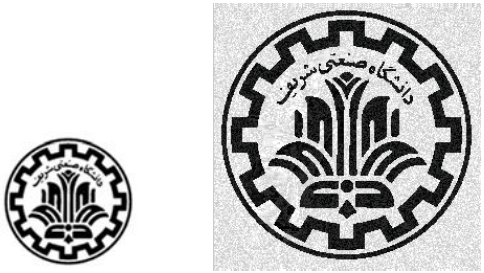
(a) (b)

Figure 5: Extracted watermark by applying (a) Gaussian noise, and (b) salt & pepper noise.



(a) (b)

Figure 6: Watermarked image by applying LPF filter (a) and extracted watermark (b).



(a) (b)

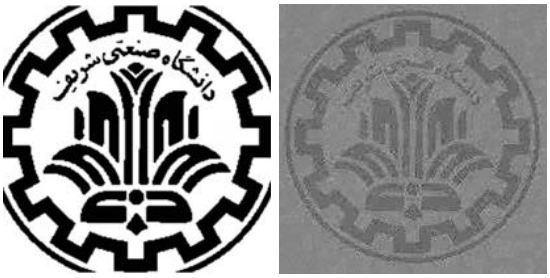
Figure 7: Extracted watermark after resizing the watermarked image (a) and gray-scale reduction (b).


(a) (b)

Figure 8: Another watermark added to watermarked image (a) and extracted watermark (b).

(a) (b)

Figure 9: Watermarked image after rotating process by 10 degrees (a) and extracted watermark (b).



(a) (b)

Figure 10: Extracted watermark after cropping (a) and after JPEG compression (b)

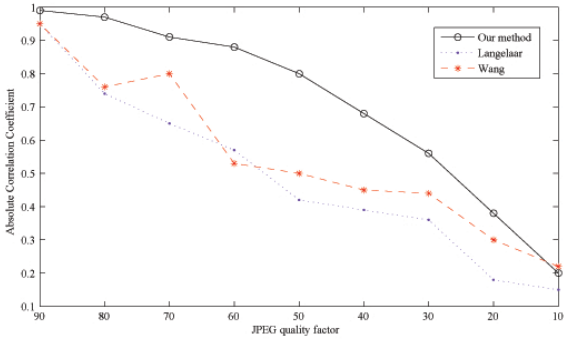



Figure 11: Performance of our method against JPEG compression


[9] L. Parameswaran and K. Anbumani, "Content-based watermarking for image authentication using independent component analysis," *Informatica*, vol. 32, pp. 299–306, 2008.

[10] M. Shen, X. Zhang, L. Sun, P. J. Beadle, , and F. H. Y. Chan, "A method for digital image watermarking using ICA," *Proceedings of the 4th International Symposium on Independent Component Analysis and Blind Signal Separation (ICA '03)*, pp. 209–214, April 2003.

[11] X. F. Ma and T. Jiang, "The research on wavelet audio watermark based on independent component analysis," *International Symposium on Instrumentation Science and Technology*, vol. 48, pp. 442–446, 2006.

[12] D. Yu. and F. Sattar, "A new blind watermarking technique based on independent component analysis," *Digital Watermarking: 1st International Workshop (IWDW '03)*, vol. 2613, pp. 37–73, 2003.

[13] P. Comon, "Independent component analysis, a new concept?" *Signal Processing*, vol. 36, no. 3, pp. 287–314, 1994.

[14] A. Hyvärinen, "Fast and robust fixed-point algorithms for independent component analysis," *IEEE Transactions on Neural Networks*, vol. 10, no. 3, pp. 626–634, 1999.