Available online at www.sciencedirect.com

ScienceDirect

Digital Signal Processing 18 (2008) 762–776

Digital Signal Processing

www.elsevier.com/locate/dsp

A simple ICA-based digital image watermarking scheme

Thang Viet Nguyen, Jagdish Chandra Patra *

School of Computer Engineering, Nanyang Technological University, Singapore

Available online 16 October 2007

Abstract

In a digital watermarking scheme, it is not convenient to carry the original image all the time in order to detect the owner's signature from the watermarked image. Moreover, for those applications that require different watermark for different copies, it is preferred to utilize some kind of watermark-independent algorithm in extraction (does not need a priori knowledge of the watermark). In this paper we introduce a novel approach called WMicaT that employs an independent component analysis technique in watermark embedding and extraction. Using a single 'public image' that can be made publicly available, the new algorithm is able to extract the watermark without requiring the original image and any information about the watermark. In addition, the watermark is not limited to some specific binary sequences but can be any meaningful image. The WMicaT method, undergoing different experiments, has shown its robustness against many attacks.

Keywords: ICA; Digital image watermarking; WMicaT

1. Introduction

Digital watermarking, in which some information is embedded directly and imperceptibly into digital data to form the watermarked data, is one of the most effective techniques to protect digital works from piracy [1]. The watermark (the embedded data) could be any authentication information such as company's logo, a serial number for a certain copy of document or an author signature. Once embedded, the watermark is bound to the work and it should be extractable even if the watermarked work is modified either intentionally or unintentionally.

In order to estimate the watermark, some existing methods require the original image at the extraction site. Some others need a priori knowledge of the watermark for the extraction. It is not encouraged since original work should be restricted from public access, and watermark information are not always fixed in advance. For example, those applications that embed the copy's ID number to the copies of the work [2], hence, each copy will have a different watermark. Scanning through all the available watermarks is impractical in terms of time and computation. For such applications, one need an extraction method that is independent from the embedded watermark.

In this paper, we develop a simple method called WMicaT (watermarking by independent component analysis with image transpose) that can satisfy the above requirements. It uses a 'public image' (which is publicly available) instead of the original image for the extraction process. With the popularity of the Internet and the availability of large storage devices, storing and transferring a public image is simple and feasible.

* Corresponding author.
E-mail addresses: thangnguyen@pmail.ntu.edu.sg (T.V. Nguyen), aspatra@ntu.edu.sg (J.C. Patra).

1051-2004/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.dsp.2007.10.004

Independent component analysis (ICA) is an important technique in signal processing field for estimating unknown signals from their observed mixtures [3]. With its blind separation capability, several authors have tried to apply ICA to watermarking. When applied to watermarking, ICA presumes the watermarked work as a mixture of the original work and the watermarks, and therefore, it can do separation to estimate the watermark. Zhang and Rajan [4] and Gonzalez et al. [5] propose algorithms that extracts the independent components (ICs) from the original image and the watermark, and then combine these ICs to produce the watermarked image. These techniques, however, require a lot of computation and usually fails in brute-force attacks. Recently, in [6], the authors combine ICA with quantization index modulation (QIM) technique to develop a better algorithm which is robust for natural images. Results for other kind of images, however, have not been clearly stated.

Another approach considers the watermarked data as a mixture of the whole host data and the watermark, and manages to generate the other mixtures from the available data. This approach is simple to implement but usually need additional knowledge about the original data or the watermark. For example, in [7,8], the algorithm needs both secret key and the original image. Our WMicaT method follows the advantages of the second approach. Furthermore, we exploit the two-dimensional characteristic of an image to overcome the requirement of additional information while keeping the algorithm simple. The idea is, the image I and its transpose I^T can be considered as two independent sources for ICA. Comparing with other watermarking techniques, our proposed method has the following advantages:

(1) The original image is not needed for watermark extraction. Support information, i.e., the public image can be made publicly available.
(2) The extraction process is the same for images with different watermarks. No a priori watermark information is needed.
(3) The watermark is robust against many attacks.
(4) The watermark can be any meaningful image.

2. Watermarking using ICA

The ICA technique [9], which consists of recovering a set of unknown sources from their instantaneous mixtures, is an important technique in signal processing. Assuming that the sources are independent of one another, ICA algorithm tries to find a transform of the mixtures such that the recovered signals are as independent as possible [3]. An ICA model shown in Fig. 1 can be divided into two sub-models: mixing model and demixing model. The observations $x_1, \dots, x_N$ are assumed to be linear mixtures of N hidden statistically independent signals $s_1, \dots, s_N$. The mixing model can be expressed as

$$\mathbf{x} = \mathbf{A}\mathbf{s}, \tag{1}$$

where $\mathbf{x} = [x_1, \dots, x_N]^T$, $\mathbf{s} = [s_1, \dots, s_N]^T$ and $\mathbf{A}_{N \times N}$ is an unknown mixing matrix.

To estimate the unknown signals, s_i, we have to build a demixing model, i.e., to compute a demixing matrix $\mathbf{B}$. ICA carries out this task by maximizing the statistical independence criteria among the outputs $y_1, \dots, y_N$. When converged, the outputs, $y_1, \dots, y_N$ will be a permutation of the unknown sources $s_1, \dots, s_N$. The demixing model, therefore, can be formulated as

$$\mathbf{y} = \mathbf{B}\mathbf{x}, \tag{2}$$

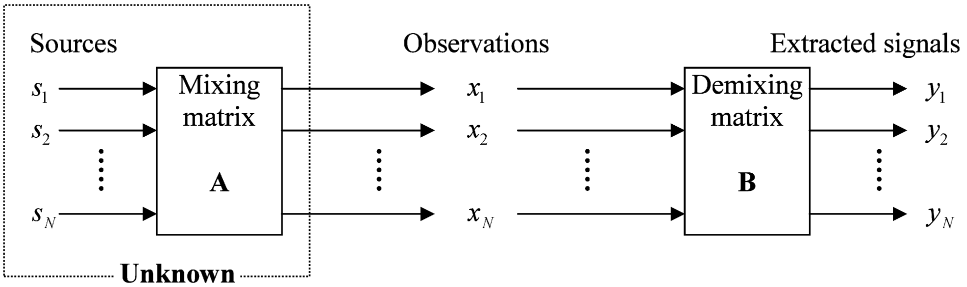


Fig. 1. The ICA mixing and demixing model.

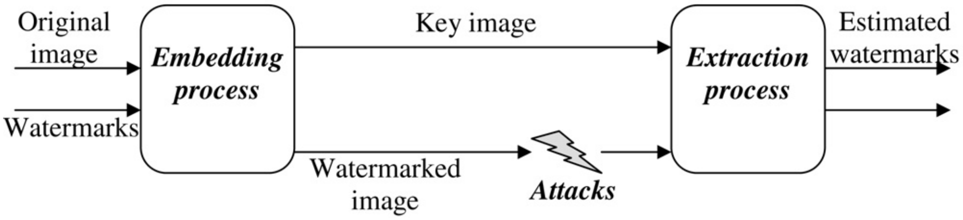


Fig. 2. A scheme of the watermarking problem.

where $\mathbf{y} = [y_1, \ldots, y_N]^T$. The objective is to make $\mathbf{B}$ be an inverse of $\mathbf{A}$, i.e., $\mathbf{B} \approx \mathbf{A}^{-1}$. Many algorithms have been developed for ICA, for example, Infomax [10], FastICA [11] and ThinICA [12]. More details on ICA techniques can be found in [3].

The similarity between an ICA model and a watermarking model can be seen by comparing Fig. 1 with Fig. 2. The embedding stage in Fig. 2 can be viewed as a mixing process that mixes original image and the watermarks to produce the watermarked image. Likewise, the extraction stage can be viewed as a demixing process that estimate the watermarks from one of the mixture, the watermarked image. That is, we can apply ICA to the watermarking problem. Several studies on ICA-based watermarking can be found in [4,5,7,8,13].

3. WMicaT embedding scheme

A complete embedding scheme of WMicaT is shown in Fig. 3. A small-sized image representing the owner's signature S is tiled to generate an initial watermark W_0. Next, a visual mask V is applied on W_0 to generate the watermark W. The purpose of a visual mask is to identify the significant areas of the host image, i.e., the texture and edge regions, in which the watermark can be more strongly embedded. With the help of a visual mask, one can increase the watermark strength considerably while maintaining the original image quality as well as the watermark invisibility [14,15]. Finally, the watermark W and its transpose W^T are inserted into the original image to form the watermarked image I^+ given by

$$I^+ = I + \alpha W + \beta W^T, \tag{3}$$

where α and β are called 'embedding strengths.' The values of these two parameters will determine how strongly the watermarks are embedded.

A public image K_P, the additional data needed for extraction, is also generated during the embedding process. It is a mixture of the original image, the original image transpose and a key image. The key image K is obtained by

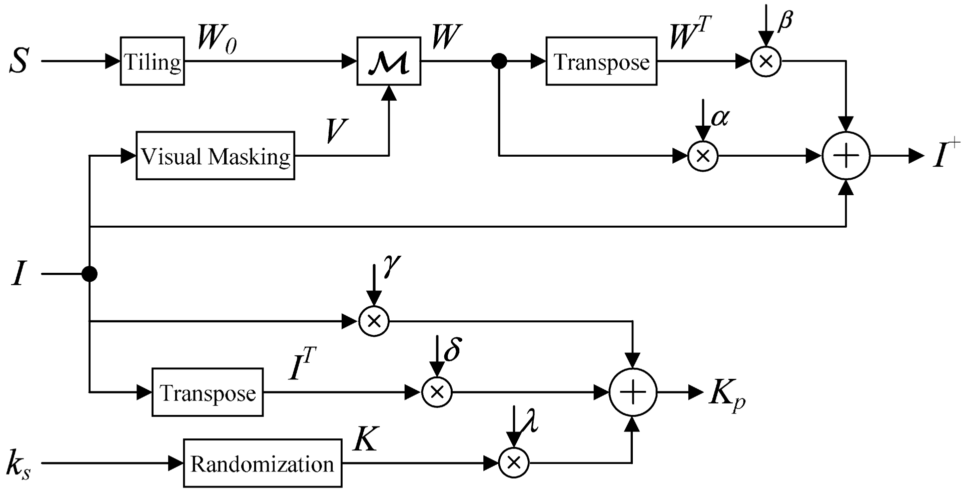


Fig. 3. The WMicaT embedding scheme.

generating a pseudo-random sequence such that $K = K^T$. A secret key k_s is used as the seed number to a pseudo-random number generator. The public image is computed by

$$K_P = \gamma I + \delta I^T + \lambda K. \tag{4}$$

The parameters γ, δ and λ are the 'key-image coefficients.' These parameters can be any nonzero values in the range of $[-1, 1]$. Without knowing the secret number k_s, one cannot extract the original image I using the public image K_P. The public image, therefore, can be made available online.

In this paper, we use the noise visibility function (NVF) technique [14] to compute the visual mask. The (m, n)th entry of the visual mask V is obtained from the original image I and is given by

$$V_{(m,n)} = \frac{1}{1 + \sigma_I^2(m, n)}, \tag{5}$$

where $\sigma_I^2(m, n)$ denotes the local variance of the image in a window centered on the pixel $I_{(m,n)}$. The local variance is calculated using a window of length $2L + 1$ as

$$\sigma_I^2(m, n) = \frac{1}{(2L+1)^2} \sum_{i=-L}^{L} \sum_{j=-L}^{L} \left(I_{(i+m,j+n)} - \bar{I}_{(m,n)}\right)^2, \tag{6}$$

where

$$\bar{I}_{(m,n)} = \frac{1}{(2L+1)^2} \sum_{i=-L}^{L} \sum_{j=-L}^{L} I_{(i+m,j+n)}. \tag{7}$$

In summary, with reference to Fig. 3, steps involved in the embedding process are as follows:

(1) Generate the initial watermark W_0 by tiling the owner's signature S.
(2) Generate a visual mask V from the original image using (5).
(3) Create the watermark W from W_0 and V using a modification function $\mathcal{M}$ given by

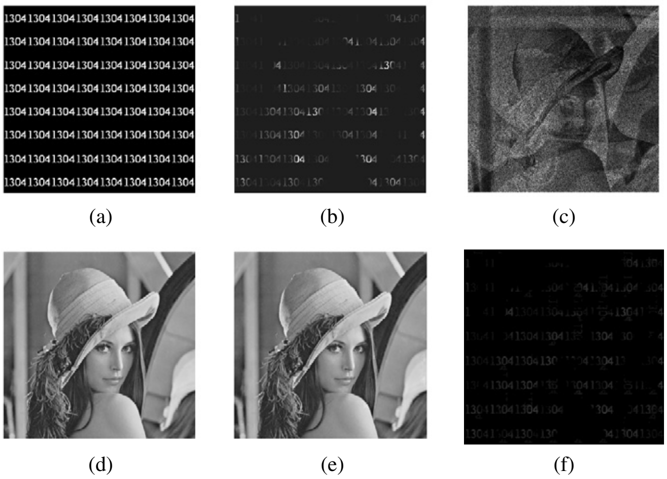
$$W = W_0 - W_0 \bullet V, \tag{8}$$

where '$\bullet$' denotes element-by-element product. For example, the (m, n)th entry of this product is given by $(W_0 \bullet V)_{(m,n)} = W_{0(m,n)} \cdot V_{(m,n)}$.
(4) Generate the watermarked image I^+ using (3).
(5) Compute key image K using the secret key k_s such that $K = K^T$.
(6) Generate the public image K_P using (4).

An example of the embedding scheme is provided in Fig. 4, which shows the original image, initial watermark, watermark, watermarked image and public image, all are 256 gray-scale images of size 512 × 512. The initial watermark was created from the owner's signature of size 64 × 64. In this example, the value of the coefficients were set at $\alpha = 0.06$, $\beta = 0.015$, $\gamma = -0.7$, $\delta = 0.49$, $\lambda = 0.82$ and $L = 10$. The last figure (Fig. 4f) illustrates the difference between original image I and the watermarked image I^+. This indicates that the distortion caused to the original image due to embedding of watermark is very little.

4. WMicaT extraction scheme

The goal of the extraction scheme is to extract the signature S from the watermarked image I^+. Besides the watermarked image, the other information available to us are the public image K_P and the secret key k_s. Using k_s, the seed to the pseudo-random generator, we are able to generate the key image K. Therefore, the task now is to extract the owner's signature S from the knowledge of I^+, K_P and K. The extraction scheme can be divided into three stages. The first stage is to extract the original image from K and K_P by applying ICA technique. The second stage applies ICA again on the estimated image and watermarked image to extract the watermark. After that, in stage three, a post processing scheme is applied to obtain the owner's signature from the estimated watermark. A WMicaT extraction scheme is depicted in Fig. 5.


(a) (b) (c)

(d) (e) (f)

Fig. 4. An example of the WMicaT embedding scheme. (a) Initial watermark W_0, (b) watermark W, (c) public image K_P, (d) original image I, (e) watermarked image I^+ and (f) difference between I^+ and I. The size of all images is 512 × 512.

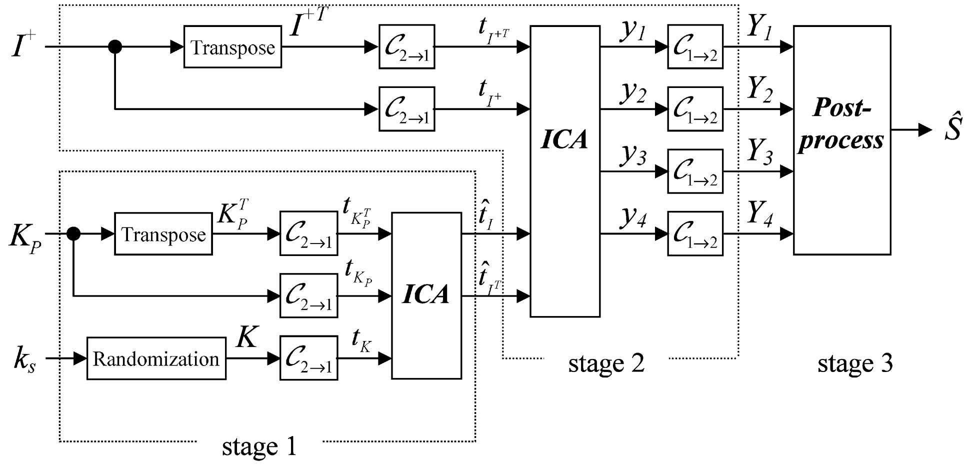
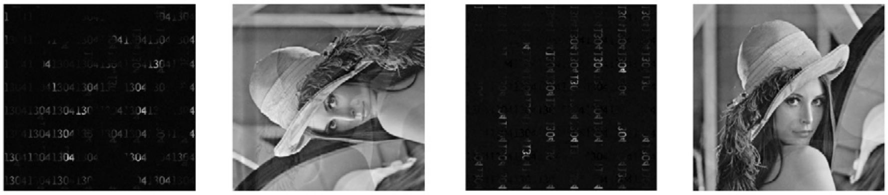


Fig. 5. The WMicaT extraction scheme. I^+, K_P and k_s are the watermarked image, public key image and secret key, respectively. $\mathcal{C}_{2\to1}$ and $\mathcal{C}_{1\to2}$ are 2D-to-1D and 1D-to-2D operators, respectively, and $\hat{S}$ is the estimate of the owner's signature.

As discussed earlier, the most important task in all ICA-based watermarking methods is to generate enough observations from the available data. Our solution is to use the image transpose. We have two images: K_P and I^+, and we need to generate at least four signals to extract the watermark. To do this, in the first stage, we reconstruct the key image K using a pseudo-random generator with secret key k_s. The three images K, K_P and K_P^T are converted by a 2D-to-1D operator $\mathcal{C}_{2\to1}$ into one-dimensional (1D) signals t_K, t_{K_P} and $t_{K_P^T}$, respectively. Applying (4) and noting that $K^T = K$, the inputs to the first ICA block can be expressed as

$$\begin{aligned}
t_{K_P} &= \mathcal{C}_{2\to1}(K_P) = \mathcal{C}_{2\to1}\big(\gamma I + \delta I^T + \lambda K\big),\\
t_{K_P^T} &= \mathcal{C}_{2\to1}\big(K_P^T\big) = \mathcal{C}_{2\to1}\big(\gamma I^T + \delta I + \lambda K\big),\\
t_K &= \mathcal{C}_{2\to1}(K).
\end{aligned} \tag{9}$$



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

Fig. 6. An example of the WMicaT extraction scheme. The four output images Y_1, Y_2, Y_3 and Y_4 are extracted by ICA technique.

Denote the 1D signal of I and I^T by t_I and t_{I^T}, respectively. The above equation (9) can be rewritten in a matrix form as

$$\begin{bmatrix} t_{K_P} \\ t_{K_P^T} \\ t_K \end{bmatrix} = \begin{bmatrix} \gamma & \delta & \lambda \\ \delta & \gamma & \lambda \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} t_I \\ t_{I^T} \\ t_K \end{bmatrix}. \tag{10}$$

Clearly, (10) represents an ICA mixing model. That is, by applying ICA technique on the observed signals $[t_{K_P}, t_{K_P^T}, t_K]^T$, we can estimate the 1D signals $\hat{t}_I$ and $\hat{t}_{I^T}$ of the original image and its transpose.

The second stage is the main step to extract the watermark. We have in total four 1D observations: t_{I^+}, $t_{I^{+T}}$, $\hat{t}_I$ and $\hat{t}_{I^T}$. Using (3) the four mixtures can be expressed as

$$\begin{aligned} t_{I^+} &= \mathcal{C}_{2\to 1}\big(I + \alpha W + \beta W^T\big), \\ t_{I^{+T}} &= \mathcal{C}_{2\to 1}\big(I^T + \alpha W^T + \beta W\big), \\ \hat{t}_I &= \mathcal{C}_{2\to 1}(I), \\ \hat{t}_{I^T} &= \mathcal{C}_{2\to 1}\big(I^T\big) \end{aligned} \tag{11}$$

or in the matrix format

$$\begin{bmatrix} t_{I^+} \\ t_{I^{+T}} \\ \hat{t}_I \\ \hat{t}_{I^T} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \alpha & \beta \\ 0 & 1 & \beta & \alpha \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} t_I \\ t_{I^T} \\ t_W \\ t_{W^T} \end{bmatrix}, \tag{12}$$

where t_W and t_{W^T} denote the 1D signals of the watermark W and its transpose W^T, respectively.

Equation (12) clearly matches the ICA mixing model $\mathbf{x} = \mathbf{A}\mathbf{s}$. Hence, applying ICA technique on $[t_{I^+}, t_{I^{+T}}, \hat{t}_I, \hat{t}_{I^T}]^T$ results in four outputs y_1, y_2, y_3, and y_4, which correspond to the 1D estimates of the original image I, the watermark W and their transposes I^T and W^T (but may not be in same order). From these 1D signals, we apply an 1D-to-2D operator $\mathcal{C}_{1\to 2}$ to generate four estimated images Y_1, Y_2, Y_3, and Y_4. Figure 6 illustrates the ICA output images obtained from the watermarked image and public key image shown in Fig. 4. We can see in the figure the original Lena image, the watermark and their transposes.

5. The post-processing scheme

The ICA technique, however, only provides a set of images that contains the watermark, but is not able to identify which one is the estimate of the watermark. It means that the output Y_1 does not necessarily correspond to the estimate of original image I. It can be the estimate of any one of the four source signals I, I^T, W or W^T. For this reason, in the third stage of the extraction scheme, we develop a post-processing algorithm to obtain the owner's signature from the images Y_1, Y_2, Y_3 and Y_4. We apply the correlation coefficients in post-processing scheme to identify which output, Y_i, corresponds to which source signal.

The detail scheme of the post-process is shown in Fig. 7. It includes two stages, an identifying stage and a refining stage. The first stage filters out the watermarks from the four image inputs. The second stage uses the estimated watermarks to extract the owner's signature. To identify the watermarks, we use the correlation coefficients between

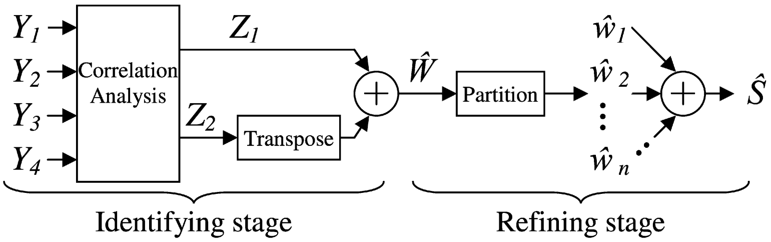


Fig. 7. The WMicaT post-processing scheme.

each output and the watermarked image. Let us consider two images X and Y, each of size $M \times N$. The absolute correlation coefficient $|r_{X,Y}|$ between two images $X_{M\times N}$ and $Y_{M\times N}$ is defined as

$$|r_{X,Y}| = \frac{|s_{xy}|}{\sqrt{s_{xx}s_{yy}}}, \tag{13}$$

where

$$s_{xy} = \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{(i,j)} - \bar{X})(Y_{(i,j)} - \bar{Y}), \qquad s_{xx} = \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{(i,j)} - \bar{X})^2, \qquad s_{yy} = \sum_{i=1}^{M}\sum_{j=1}^{N}(Y_{(i,j)} - \bar{Y})^2 \tag{14}$$

and

$$\bar{X} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}X_{(i,j)}, \qquad \bar{Y} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}Y_{(i,j)}. \tag{15}$$

The absolute correlation coefficient $|r_{X,Y}|$ measures the similarity between two images X and Y. When two images are totally different $|r_{X,Y}| \approx 0$, and, on the other hand, when X and Y are identical to each other $|r_{X,Y}| \approx 1$.

Our identification method is based on the following observations. In watermarking, the watermarked image I^+ is supposed to be highly correlated with the original image I, i.e., $|r_{I,I^+}| \approx 1$. Similarly, the absolute correlation coefficient between their transposes, $|r_{I^T,I^{+T}}|$ is also near to 1. On the other hand, the watermark, W is considered to be independent from both I^+ and I^{+T}. The values of $|r_{W,I^+}|$ and $|r_{W,I^{+T}}|$, therefore, are close to 0. That is, by evaluating the absolute correlation coefficient between an output Y_i and the watermarked image I^+, we can identify which output is the estimate of the watermark.

Let us denote the absolute correlation coefficient between the watermarked image I^+ and the output Y_i by $|r_{I^+,Y_i}|$. Similarly, denote the absolute correlation coefficient between the transpose of the watermarked image I^{+T} and the output Y_i by $|r_{I^{+T},Y_i}|$, for $i = 1, \ldots, 4$. Let $\bar{r}_i$ be the sum of these two values, i.e., $\bar{r}_i = |r_{I^+,Y_i}| + |r_{I^{+T},Y_i}|$. From the above observations, it is clear that the sum, $\bar{r}_i$ will be close to 0 if its corresponding output, Y_i is the estimate of the watermark or the watermark transpose. Thus, by computing all the sum, $\bar{r}_i$, $i = 1, \ldots, 4$, we can find out the estimates of the watermark and its transpose.

A numerical example of the correlation coefficients for the results shown in Fig. 6 are provided in Table 1. From Table 1, it can be seen that the ICA outputs Y_1 and Y_3 are the estimates of W and W^T.

After successfully estimating the watermark and its transpose by choosing the two outputs that yield the smallest correlation coefficient sum, $\bar{r}_i \approx 0$, we continue to the next stage. The aim of this refining stage is to compute owner's signature from the two extracted watermarks. From the fact that the watermark is a multiple duplication of the owner's signature, we apply a reverse process, splitting the watermark estimate into sub-images and then averaging them to retrieve the owner's signature.

Now let us denote by Z_1 and Z_2 the two outputs that are the estimates of the watermark and its transpose. First, we calculate an average watermark, $\hat{W}$, by

$$\hat{W} = \left(Z_1 + Z_2^T\right)/2. \tag{16}$$

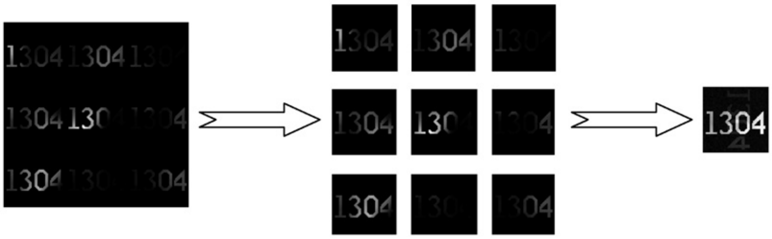


Fig. 8. An example of the refining stage. The average watermark $\hat{W}$ is partitioned into small images. These sub-images are then averaged to generate the estimate of the owner's signature $\hat{S}$.

Table 1
The correlation coefficient table used for WMicaT post-processing scheme

	Y_1	Y_2	Y_3	Y_4
$\lvert r_{I^+,Y_i}\rvert$	0.0034	0.0895	0.0374	0.9953
$\lvert r_{I^{+T},Y_i}\rvert$	0.0408	0.9762	0.0059	0.2130
$\bar{r}_i$	**0.0442**	1.0657	**0.0433**	1.2083

Second, we partition the image $\hat{W}$ into l sub-images, $\hat{W}_{s1}, \hat{W}_{s2}, \ldots, \hat{W}_{sl}$ each of size $M_S \times M_S$, where $M_S \times M_S$ is the size of the owner's signature. Third, we compute the estimate of the owner's signature as the average of these sub-images, given by

$$\hat{S} = \frac{1}{l}(\hat{W}_{s1} + \hat{W}_{s2} + \cdots + \hat{W}_{sl}). \tag{17}$$

An illustration of the refining process is shown in Fig. 8. The average watermark is divided into 9 sub-images. These images are then averaged to generate the estimate of the owner's signature. As it can be seen in the figure, the quality of the estimated signature is very good.

6. WMicaT performance analysis

We carried out several experiments to verify the robustness of the proposed method under different attacks with different original images and watermarks. We implement the first and second experiments on a medium-textured Lena image with two different watermarks. The first watermark was an image of a university logo and the second watermark was an image containing three letters 'NTU.' In the third experiment, the same 'NTU' image was selected and embedded in a highly-textured Baboon image.

6.1. Simulation setup

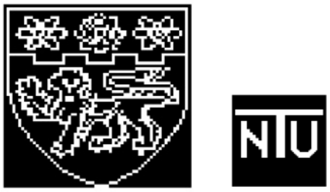
The original images (Lena and Baboon) are gray-scale images of size 512 × 512 with 256 intensity levels. The owner's signatures are binary images: the university logo is of size 128 × 128 and the university's name, 'NTU,' is of size 64 × 64. The embedding strengths α and β were controlled so that the watermarked images have a high quality in term of the peak signal-to-noise ratio (PSNR). The peak signal-to-noise ratio between an original image I and the modified image $\hat{I}$ is computed by

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{(i,j)} - \hat{X}_{(i,j)})^2}}\right), \tag{18}$$

where $I_{(i,j)}$ and $\hat{I}_{(i,j)}$ denote the (i, j)th pixel intensity (gray) level of the original and modified images, respectively. The numerical values used for different parameters in the three experiments are provided in Table 2. With the chosen parameter values, the watermark was generated and embedded into the host images. The owner's signatures used in the three experiments are shown in Fig. 9.

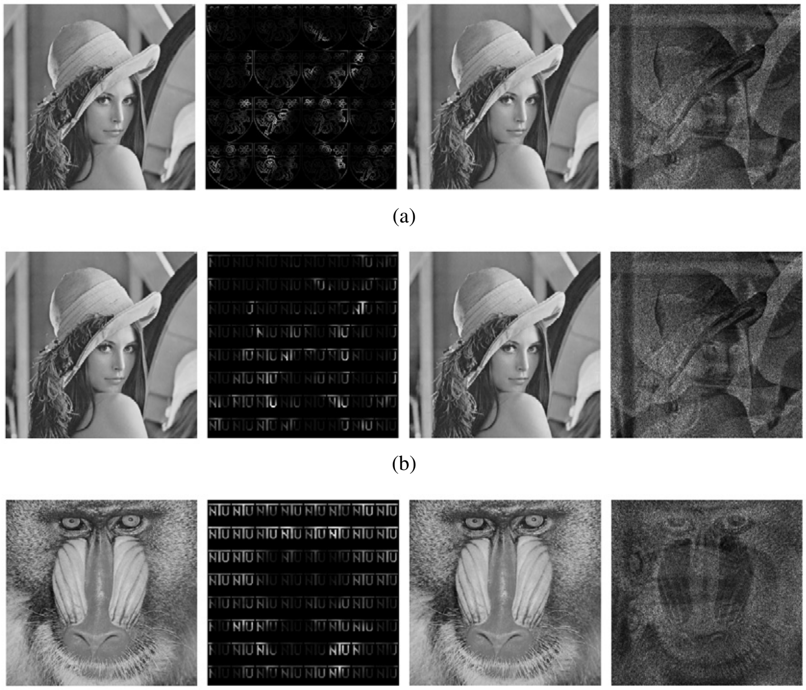
Table 2
The configuration table for the three experiments

	α	β	γ	δ	λ	L	PSNR (dB)
Expt1	0.073	−0.010	−0.70	0.49	0.82	10	41.45
Expt2	0.060	0.015	−0.70	0.49	0.82	10	43.99
Expt3	0.040	−0.010	−0.70	0.49	0.82	10	42.91



(a) (b)

Fig. 9. The owner's signatures used in WMicaT experiments. (a) Size 128 × 128 used in Expt1 and (b) size 64 × 64 used in Expt2 and Expt3.



(a)

(b)

(c)

Fig. 10. The images used in WMicaT experiments. From left to right: original image (I), watermark (W), watermarked image (I^+) and public image (K_P). (a) Expt1, (b) Expt2 and (c) Expt3.

An illustration of the original image I, watermark W, the watermarked image I^+ and the public image K_P are shown in Fig. 10. With the help of the visual mask and the selected embedding strengths (Table 2), we are able to produce a high quality watermarked images (PSNR > 40 dB). The watermarked images are almost identical to the original ones and the embedded marks are invisible to normal eyes.

We conduct the simulations by letting the watermarked images undergo various modifications before carrying out watermark extraction. We have applied several typical linear ICA methods for the extraction, such as SOBI (second-order blind identification) [16], JADETD (joint approximate diagonalization of eigen matrices with time delays) [17], and FPICA (fixed-point ICA) [11]. Since results of these methods were almost identical, we only provide the outcomes

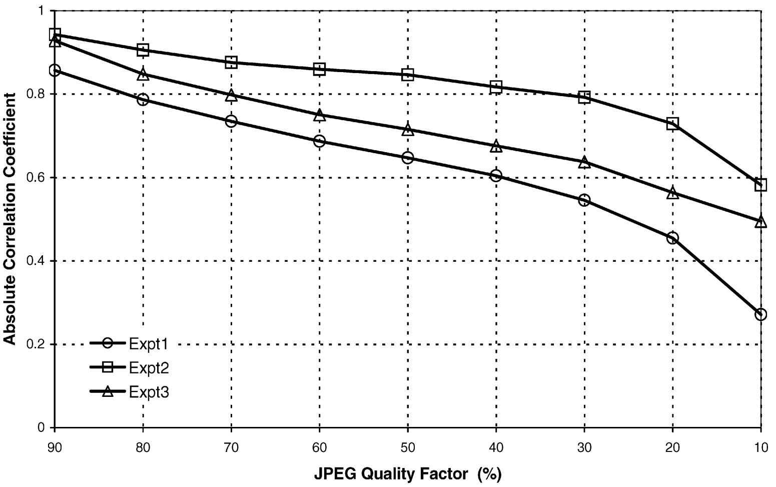


Fig. 11. WMicaT results for the JPEG compression test. The compression quality ranges from 90% to 10%.

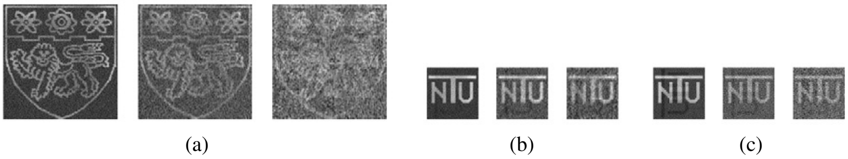


Fig. 12. The estimated signatures of WMicaT in JPEG compression test. (a) Expt1, (b) Expt2 and (c) Expt3. In each figure, from left to right: the outputs of JPEG compression test with quality factor of 90%, 50% and 20%.

that were carried out with SOBI. Finally, to measure and compare the quality of the estimated signature, we evaluate the absolute correlation coefficient $|r_{S,\hat{S}}|$ between the original owner's signature S and its estimate $\hat{S}$.

6.2. JPEG compression test

The watermarked image I^+ was compressed using JPEG compression tool with different quality factors (from 90% down to 10%). The watermark extraction was done on the compressed image. The performance index, $|r_{S,\hat{S}}|$ was computed for each quality factor and is shown in Fig. 11. As it is shown, the proposed algorithm provided very good performance on all experiments. The quality of the estimated signatures were high even when the JPEG quality factor was lowered drastically. Only in Expt1 where the watermark was a relatively complex image (university logo), and when the compression quality factor was reduced to the lowest level (=10%), the estimated signature was unrecognizable. Illustrations of the estimated signatures are shown in Fig. 12.

6.3. Gray scale reduction test

In this test, the intensity (gray) level of the watermarked image I^+ was reduced from original 256 level down to $128, 64, \ldots, 8$ level. As it is shown in Fig. 13, the algorithm offered excellent results in the gray-scale reduction test. The performance index $|r_{S,\hat{S}}|$ in all experiments were high, showing a strong correlation between the estimated image and the owner's signature. It can be seen that WMicaT was able to extract the signature successfully in all the cases where the gray level is greater or equal 8. When the gray level went down to 4, however, the performance of WMicaT degraded and the signature was not recognizable. Figure 14 shows examples of the estimated signatures extracted from the test images with gray level of 128, 32 and 8.

When comparing the results among the three experiments, we found out that Expt1's results were inferior to the others because of the relatively complex signature and the watermark. However, unlike the previous JPEG compression test, Expt3 yielded a slightly better performance in comparing with Expt2, especially when the gray level was low.

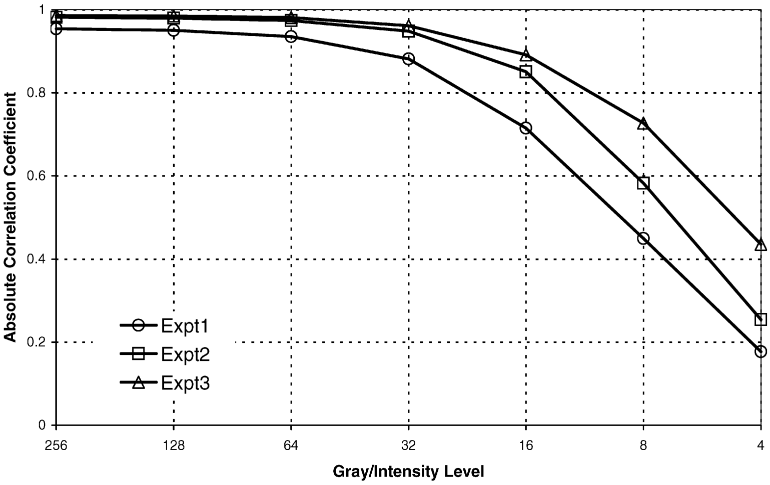


Fig. 13. WMicaT results for the gray-scale reduction test. The pixel gray level of the watermarked image is reduced from 256 down to 4 level.

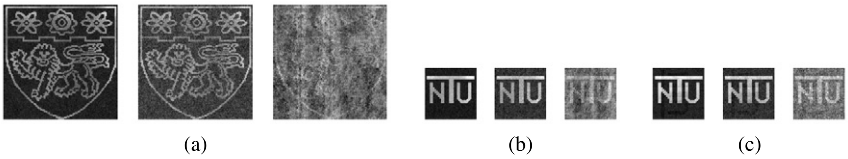


Fig. 14. The estimated signatures of WMicaT in gray level reduction test. (a) Expt1, (b) Expt2 and (c) Expt3. In each figure, from left to right: the outputs of the test with gray level reduced to 128, 32 and 8.

The difference is partially because there is no distortion in the gray level test. Therefore, the experiment on Baboon image (Expt3), where the watermark was more strongly embedded in textured areas, provided a better result.

6.4. Image resizing test

Image resizing is one of the most common modification to an image. In this test, we resized the watermarked image to different sizes and then applied WMicaT to estimate the signature. Since the image is resized, we needed to synchronize all the input images (the watermarked image and the public image) to the same size before executing the extraction scheme. There are two approaches for the synchronization. In the first approach, we resize all images to the size of the test image I^* before doing the ICA-based extraction. After that, the outputs of ICA process Y_1, Y_2, Y_3, Y_4 are resized again to the size of the public image and the post-process scheme is carried out. In the second approach, the test image I^* was resized to the public image's size and the whole extraction scheme was executed normally.

We down-scaled the watermarked image I^+ to different sizes: 384 × 384 (75%), 256 × 256 (50%), 192 × 192 (37.5%), 128 × 128 (25%), 96 × 96 (18.75%) and 64 × 64 (12.5%), and then carried out all the three experiments with both synchronization approaches. The experiment results are illustrated in Fig. 15. The difference in size synchronization results in different performance of WMicaT. The first approach $m1$ in which the test image, I^* is kept intact displays a superior result (Fig. 16) in comparison with the second approach $m2$ where the test image is resized before going through the extraction. In fact, with $m2$, the test image has been resized two times, one during the attack and another one during the synchronization. The interpolation technique which is usually involved in the resizing process has modified or even removed most of the watermark content that was embedded in the image. Hence, as it is shown in Fig. 16, WMicaT algorithm performed poorly in all three experiments with the second size synchronization approach.

The interpolation applied in the resizing test also results in an interesting observation. A closer look on Fig. 15 reveals that, when the test image is resized to 256 × 256, the performance (measured by the absolute correlation coefficient) of Expt2 with synchronization $m2$ approach is better than the performance of Expt3 with $m1$ approach. However, in Fig. 16, the estimated signature of Expt2.m2 (Fig. 16b, row 2, column 2) is much worse than the estimated

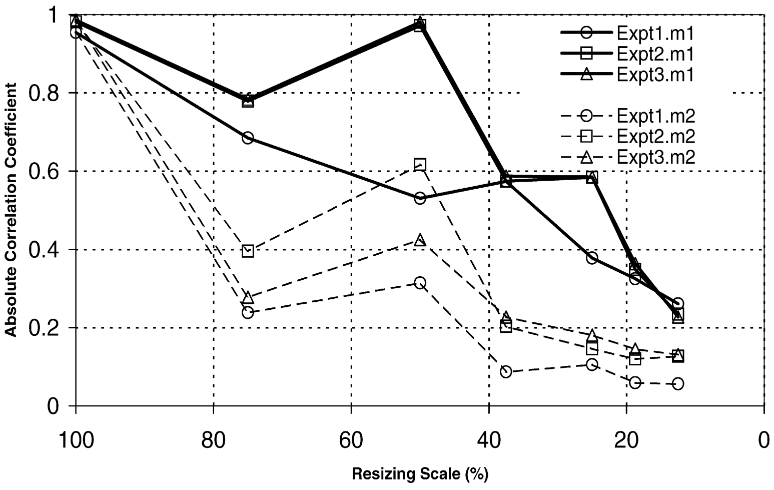


Fig. 15. WMicaT results for the resizing test. The image is resized from 512 × 512 (100%) down to 64 × 64 (12.5%). In the figure, $m1$ and $m2$ denote the two synchronization approaches.

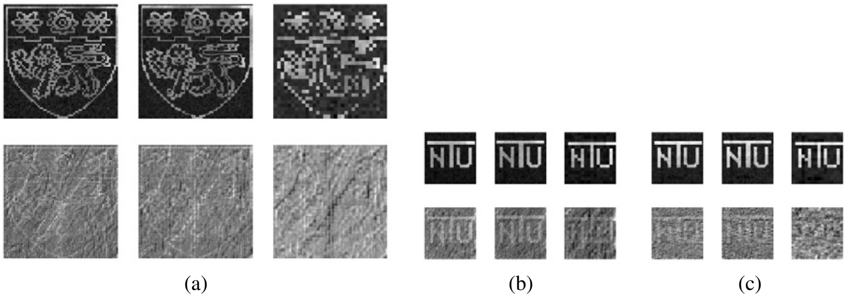


Fig. 16. The estimated signatures of WMicaT in resizing test. (a) Expt1, (b) Expt2 and (c) Expt3. In each figure, from left to right: the extracted owner's signature with test image of size 384 × 384, 256 × 256 and 128 × 128. First row: the first resizing approach $m1$, and second row: the second resizing approach $m2$.

signature of Expt3.m1 (Fig. 16c, row 1, column 2). So, what is the reason for the performance contradiction between numerical measure and visual observation?

The answer is because of the inevitable interpolation that is applied in all image resizing process. This interpolation can make several (or every) pixels in the reconstructed image shift one or two row/column(s) from their location in the original image. For example, a pixel at (10, 10) in the original image can be moved to (9, 10) or (11, 11) in the reconstructed image. Such pixel shifting effect does not make any visible difference. However, for the point-to-point numerical measure, like the absolute correlation coefficient, it makes a big difference, resulting in low performance. A classic example is when you take a chessboard image (black and white pixels interleaving each other), shift the image one column to the left, and do the correlation calculation. You will get a number that is close to zero, which means the old image and the new one are almost totally different.

In addition, the shifting effect is also the cause of the sudden depression in performance of WMicaT (shown in Fig. 15) at 75% size-reduction test, for example. The effect happens not only on WMicaT but also on other algorithms, as we will see it in Section 6.5. Hence, for a better conclusion, we should consider the performance of an watermarking algorithm both by visual inspection and by numerical measures.

6.5. Comparison with other methods

For further investigation, we compared the proposed WMicaT method with other watermarking techniques that work on different processing domains [18]. These techniques include two discrete cosine transform algorithms *Cox-DCT* [19] and *Koch-DCT* [20], two spatial-domain algorithms *Langelaar-spa* [21] and *Kutter-spa* [22], and two

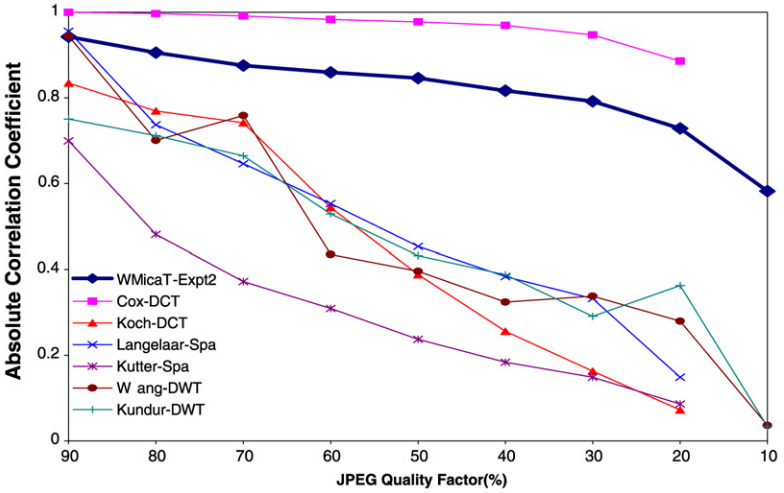


Fig. 17. Performance comparison between WMicaT and other techniques for JPEG compression test.

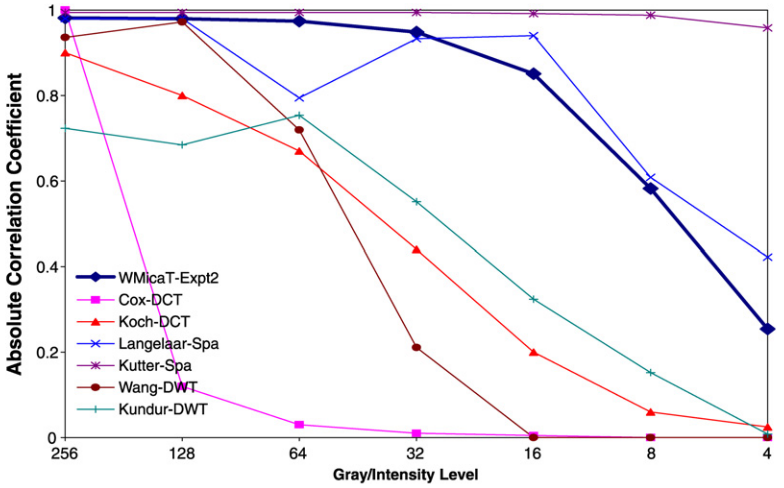


Fig. 18. Performance comparison between WMicaT and other techniques for gray-scale reduction test.

discrete wavelet transform algorithms *Kundur-DWT* [23] and *Wang-DWT* [24]. The result of these techniques are taken from [18] and compared with the result of our second experiment, Expt2 (the Lena embedded with ‘NTU’ signature).

Illustrations in Figs. 17, 18, and 19 show impressive results of WMicaT in comparison with the other techniques. It outperforms most of the referenced algorithms in all three image attacking tests: JPEG compression, gray-scale reduction and image resizing. Unlike some methods that are only robust against several specific attacks, the proposed method provides a steady performance throughout all the tests. In JPEG compression test, WMicaT outperforms the other algorithms and only inferior to on DCT-based method (the *Cox-DCT*). It is an advantage of WMicaT since the spatial-based techniques usually perform poorly on JPEG test [1].

Again, in the gray-scale reduction test (Fig. 18), the WMicaT provides good performance and is one of the three methods that yields the best result while the *Cox-DCT* method could not provide adequate result. A similar situation can be observed in the third test in Fig. 19 on image resizing, WMicaT is again one of the top three methods that provide the best estimation of the owner’s signature.

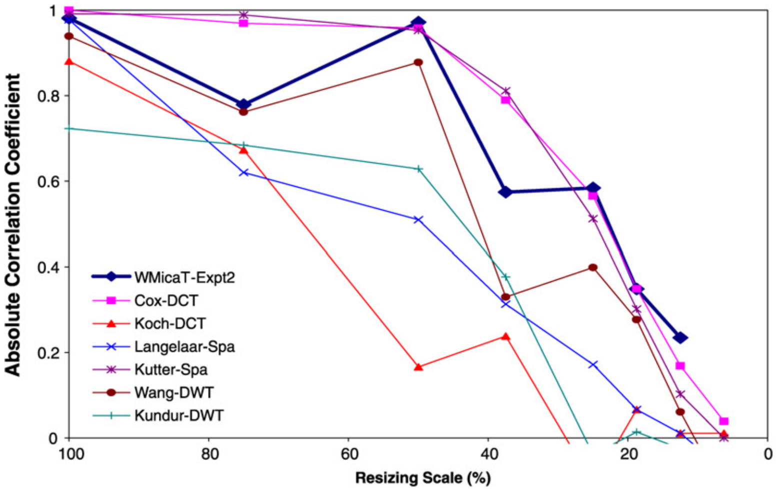


Fig. 19. Comparison of WMicaT performance on resizing test with other watermarking algorithms.

7. Conclusion

In this work, we have proposed a novel watermarking method which uses a single key image for extracting different watermarks. The utilization of ICA technique in watermark extraction brings advantages to our WMicaT because the supporting image K_P can be publicly available and no original image is required. In addition, the use of secret key k_s protects the original image without any degradation to the robustness of the algorithm and to the quality of the extracted watermark. We have observed that by using different secret key k_s to generate different public image K_P does not affect the performance of the proposed algorithm.

Throughout various simulations, the WMicaT has shown an impressive result against common attacks such as JPEG compression, gray-scale reduction and image resizing. It provides a consistent performance on different host images in all the experiments. In comparison with other watermarking methods, WMicaT illustrates very good performance with high quality estimation of the owner's signature.

The effect of watermark content on the extraction algorithm can be observed from the experiment results. An image embedded by a complex watermark that contains curves and discontinued areas seems to be more vulnerable to the attack than that embedded by a watermark with straight lines or smooth areas. Therefore, in the same test, the quality of the estimates of complex watermarks (the university logo, for example) is not as high as those of a simple watermark (the 'NTU' words, for example). However, the performance of WMicaT in the experiments with complex watermark is still very good. The estimated images are highly correlated with the owner's signature. The algorithm fails to recognize the signature only when the test image is modified severely.

Since the WMicaT embedding and extraction are carried out directly on spatial domain, the computational workload is similar to other spatial domain-based watermarking algorithm. The workload does not contain any complex calculation. For the experiment with 512 × 512 images presented in the simulation, it took less than 30 seconds to complete the extraction test set which includes 1 no-attack test, 9 JPEG compression tests, 6 gray reduction tests and 6 resizing tests.

WMicaT, however, also has its disadvantage that needs further improvement. The size of the public image is as big as the size of the original image, therefore, storing and transferring this supporting image is not very convenient in some situations. We might address this issue by exploiting some special watermarks. In addition, applying WMicaT in transformed domain is another interesting study. And finally, we are experimenting the use of multiple overlapping watermarks in order to increase the security of the watermarks. However, this approach may reduce the robustness of the algorithm.

References

[1] I.J. Cox, M.L. Miller, J.A. Bloom, in: E. Fox (Ed.), Digital Watermarking, first ed., Morgan Kaufmann, 2001.

[2] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su, Attacks on digital watermarks: Classification, estimation based attacks, and benchmarks, IEEE Commun. Mag. 39 (8) (2001) 118–126.
[3] A. Cichocki, S.-I. Amari, Adaptive Blind Signal and Image Processing, John Wiley & Sons, 2002.
[4] S. Zhang, P.K. Rajan, Independent component analysis of digital image watermarking, in: Proc. IEEE Int. Sympos. Circ. Syst. (ISCAS'02), vol. 3, 2002, pp. 217–220.
[5] F.J. Gonzalez-Serrano, H.Y. Molina-Bulla, J.J. Murillo-Fuentes, Independent component analysis applied to digital image watermarking, in: Proc. IEEE Int. Conf. Acoust. Speech Signal Process. 2001 (ICASSP'01), vol. 3, 2001, pp. 1997–2000.
[6] S. Bounkong, B. Toch, D. Saad, D. Lowe, ICA for watermarking digital images, J. Mach. Learn. Res. 4 (2003) 1471–1498.
[7] M. Shen, X. Zhang, L. Sun, P.J. Beadle, F.H.Y. Chan, A method for digital image watermarking using ICA, in: Proc. Int. Sympos. Independent Component Analysis and Blind Signal Separation (ICA'03), Nara, Japan, 2003, pp. 209–214.
[8] D. Yu, F. Sattar, K.-K. Ma, Watermark detection and extraction using independent component analysis method, EURASIP J. Appl. Signal Process.—Special Issue on Nonlinear Signal Image Process. II 2002 (1) (2002) 92–104.
[9] P. Comon, Independent component analysis, a new concept? Signal Process. 36 (3) (1994) 287–314.
[10] A.J. Bell, T.J. Sejnowski, An information-maximisation approach to blind separation and blind deconvolution, Neural Comput. 7 (6) (1995) 1129–1159.
[11] A. Hyvärinen, Fast and robust fixed-point algorithms for independent component analysis, IEEE Trans. Neural Netw. 10 (3) (1999) 626–634.
[12] S.A. Cruces, A. Cichocki, Combining blind source extraction with joint approximate diagonalization: Thin algorithms for ICA, in: Proc. Int. Sympos. Independent Component Analysis and Blind Signal Separation (ICA'03), Nara, Japan, 2003, pp. 463–468.
[13] D. Yu, F. Sattar, A New Blind Image Watermarking Technique Based on Independent Component Analysis, in: Springer-Verlag Lecture Notes Comput. Sci., vol. 2613, 2003, pp. 51–63.
[14] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, T. Pun, A stochastic approach to content adaptive digital imagewatermarking, in: Proc. Int. Workshop on Information Hiding, Dresden, Germany, 1999, pp. 212–236.
[15] M. Kutter, S.K. Bhattacharjee, T. Ebrahimi, Towards second generation watermarking schemes, in: 6th Int. Conf. Image Process. (ICIP'99), vol. 1, Kobe, Japan, 1999, pp. 25–28.
[16] A. Belouchrani, K. Abed-Meraim, J.F. Cardoso, E. Moulines, A blind source separation technique using second-order statistics, IEEE Trans. Signal Process. 45 (2) (1997) 434–444.
[17] P.G. Georgiev, A. Cichocki, Robust independent component analysis via time-delayed cumulant functions, IEICE Trans. Fundament. E86-A (3) (2003) 573–579.
[18] P. Meerwald, Digital watermarking in the wavelet transform domain, Master's thesis, University Salzburg, Austria, 2001.
[19] I.J. Cox, J. Kilian, T. Leighton, T.G. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.
[20] E. Koch, J. Zhao, Towards robust and hidden image copyright labeling, in: Proc. IEEE Int. Workshop Nonlinear Signal Image Process., Marmaras, Greece, 1995, pp. 452–455.
[21] G.C. Langelaar, R.L. Lagendijk, J. Biemond, Robust labeling methods for copy protection of images, in: Proc. SPIE Conf. Storage Retrieval for Image and Video Databases, vol. 3022, San Jose, USA, 1997, pp. 289–309.
[22] M. Kutter, F. Jordan, F. Bossen, Digital signature of color images using amplitude modulation, in: Proc. SPIE Conf. Storage and Retrieval for Image and Video Databases, vol. 2952, San Jose, USA, 1997, pp. 518–526.
[23] D. Kundur, D. Hatzinakos, Digital watermarking using multiresolution wavelet decomposition, in: Int. Conf. Acoust. Speech Signal Process. (ICASSP'98), vol. 5, Washington, USA, 1998, pp. 2969–2972.
[24] H.-J. Wang, P.-C. Su, C.-C.J. Kuo, Wavelet-based digital image watermarking, Opt. Express 3 (12) (1998) 491–496.

Thang Viet Nguyen received his B.Sc. degree in computer science from the Vietnam National University, Hanoi, Vietnam in 2000. He obtained Ph.D. degree in computer science from the School of Computer Engineering, Nanyang Technological University, Singapore in 2007. His research interests include independent component analysis, neural networks, and genetic algorithms.

Jagdish C. Patra obtained B.Sc. (Engg) and M.Sc. (Engg) degrees, both in electronics and telecommunication engineering, from Sambalpur University, India in 1978 and 1989, respectively. He received Ph.D. degree in electronics and communication engineering from Indian Institute of Technology, Kharagpur, in 1996. After completion of Bachelor's degree, he worked in various R&D, teaching and government organizations for about 8 years. In 1987, he joined Regional Engineering College, Rourkela, Orissa, as a lecturer, where he was promoted to assistant professor in 1990. In April 1999, he went to Technical University, Delft, Netherlands as a Guest Teacher (Gastdocent) for six months. Subsequently, in October 1999, he joined the School of EEE, Nanyang Technological University (NTU), Singapore, as a research fellow. Currently he is serving as an assistant professor in the School of Computer Engineering, NTU, Singapore. His research interests include neural network-based intelligent signal processing in the area of data security, sensor networks, image processing, and bioinformatics. He is a member of IEEE and Institution of Engineers (India).