Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 685–689

ISBN 978-83-60810-22-4

Robust Digital Watermarking System for Still Images

Sergey Anfinogenov and Valery Korzhik (Member, IEEE)
State University of Telecommunications
St. Petersburg, Russia
serganff@gmail.com , korzhik@spb.lanck.net

Guillermo Morales-Luna
Computer Science, CINVESTAV-IPN
Mexico City, Mexico
gmorales@cs.cinvestav.mx

***Abstract*—Fast and wide-scale spreading of the image data on the Internet creates great opportunities for illegal access by the different kinds of intruders. In order to solve the problem of intellectual property protection, digital image watermarking can be successfully used. We describe a new method of digital watermarking based on the embedding of the local maxima into the Fourier transform area of the image. Simulation results are presented, which confirm that the proposed method is resistant to cyclic shifts, row and column removal, cropping, addition of noise, rotation and JPEG transforms.**

I. Introduction

DIGITAL watermarks (WM) can be effectively used for copyright protection to various products. However, intruders (the so-called *pirates*), who try to copy and spread illegally these products, attempt to remove the WM or to perform some transforms over the watermarked products which, without impairing the product itself, make impossible to extract the WM reliably by legal users. In this paper a new method of 0-bit WM system creation with *blind* decoder is proposed. This means that the system task is to find the fact that the WM is indeed present in the marked object. It is common to use the following criteria for the evaluation of the systems efficiency: the *probability of false detection* of the WM (P_{fa}) and the *probability of WM missing* (P_m).

There are two main approaches to provide resistance of WM against different deliberate transforms: the use of recovering transforms to reduce the attacked products to their original WM-ed forms, and the use of the invariant domain for such transforms which allow blind detection of WM's. The WM systems here introduced are based on the properties of mathematical conversions that establishes a domain which is invariant to the changes of the WM-ed products. Several such systems are based on the properties of the *Fourier-Mellin Transform*. As an example, we hold up the system introduced at [1], where the informed decoder has been used. However, that system cannot prevent the attacks that partly delete the cover image. There are attempts to refine the system characteristics by introducing a *Logarithmically-Polar Transform* (LPM). In [2] an example of such attempts is described. In theory, this method works properly, however in practice such system appears inapplicable. Even without embedding, the carrying out of direct and reverse LPM impairs seriously the quality of the image and therewith it demands considerable computing resources.

A good example of a robust watermarking system is constructed by the holographic method, proposed in [3]. Nevertheless, it has one essential drawback: in order to extract the WM, it is necessary to posses the original image. W. Luo *et al.* [4] have proposed a fast and robust JPEG domain image watermarking method but it cannot be used for automatic watermark detection.

Thus, the problem of robust WM systems design resistant to the whole complex of transforms has not been solved completely. Our new method, which is an alternative solution, is described in the following section.

II. Description of the robust WM system

The development of a WM system robust against a complex of natural and intentional conversions is not an easy problem, particularly when the *blind* decoder is used. In the previous section, a short description can be found of the basic approaches to fulfill this task. However, the problem has not been yet solved completely. Nevertheless, some progressive ideas have been borrowed by ourselves while developing the introduced new method.

There are some approaches, for instance [1], where the WM is embedded into the area of the Fourier amplitude spectrum, because this area is invariant under the image cyclic shift. Besides, it seems reasonable to embed the identification code of the owner into the position of some maxima, as proposed in [5]. However, the maxima in our method are located directly in the amplitude spectrum and do not undergo preliminary by log-polar conversion. According to the known recommendations, it is also necessary to select, not all frequency coefficients for an embedding, but only those of them which lie in the field of the middle frequencies.

The main idea of the proposed method consists in generating the local areas worked out by the stegokey, and replacing the center of each area by its amplitude spectrum maximum. The number of maxima should be chosen in such a way, on the one hand, to provide an acceptable quality of the image and, on the other hand, it should survive after a number of image deformations. If the position of the local area maximum coincides with the position given by the stegokey, then the maximum is considered to be recognized. The ratio of the

recognized maxima number and the total maxima number is compared with a threshold, and the decision about the presence or absence of a WM in the image can be outperformed.

The task of the local maxima formation can be solved as follows:

First, the matrix $\mathbf{G}$ of the mutual-independent random values (in the unit real interval $[0, 1]$) is generated. After that, the matrix $\mathbf{Z}$ of the same order is created according to the following rule:

$$\mathbf{Z}[i,j] = \begin{cases} 1 & \text{if } \mathbf{G}[i,j] > \lambda \\ 0 & \text{if } \mathbf{G}[i,j] \leq \lambda \end{cases}$$

where $i = 0, \ldots, M-1, j = 0, , N-1$, and λ is some real-valued threshold. The parameter λ defines an amount of the units in matrix $\mathbf{Z}$ and, therefore, the amount of the embedding areas as well. The higher is the value λ, the fewer units are there in $\mathbf{Z}$. The remaining positions are filled with zeros.

Now it is necessary to create a new matrix $\mathbf{L}$ according to the following expression:

$$\mathbf{L}[i,j] = \begin{cases} 1 & \mathbf{Z}[i,j] = 1 \ \& \ S[a,i,j] < 1 \\ 0 & \text{otherwise} \end{cases}$$

where

$$S[a,i,j] = \sum_{m=i-a}^{i+a} \sum_{n=j-a}^{j+a} \mathbf{Z}[m,n]$$

and a is a predetermined integer which defines the size of the local areas.

The matrix $\mathbf{L}$ forms a mask with randomly allocated values 1 which lie in the centers of not intersecting areas of size $(2a+1) * (2a+1)$.

Next, the values 1 at the matrix $\mathbf{L}$ are replaced with 0's in those frequencies where the embedding is not performed. It is worth to note that in order to make real the image brightness values after the embedding of a WM, it is necessary to preserve the symmetry of the matrix. Therefore the lower half of the amplitude spectrum matrix should be replaced with a mirror display of the upper half of the matrix, that requires to restrict the embedding area with the upper half of the matrix $\mathbf{L}$ only. Let us denote as $\mathbf{K}$ the matrix thus obtained from $\mathbf{L}$, which is considered as a stegokey, useful in order to detect the WM.

After the performing of all previous steps we should change the amplitude matrix $\mathbf{A}$ according to the matrix $\mathbf{K}$. For this purpose, we select areas δ of size $(2a+1) * (2a+1)$ in the amplitude matrix $\mathbf{A}$. The centers of these areas are allocated on the same positions as the 1's in the matrix $\mathbf{K}$. We replace the values of an amplitude in the center of each area by the maximum amplitude over this area multiplied by some coefficient β, where $\beta \geq 1$. The remaining values of the matrix $\mathbf{A}$ are not changed. The coefficient β is selected in such a way that the new image does not differ visually from the original one. This process can be presented by the equation:

$$\mathbf{A}_w[i,j] = \begin{cases} \beta \ \max_{(m,n) \in I_a(i,j)} \mathbf{A}[m,n] & \text{if } \mathbf{K}[i,j] = 1 \\ \mathbf{A}[i,j] & \text{if } \mathbf{K}[i,j] = 0 \end{cases}$$

where

$$I_a(i,j) = \{(m,n) | \ \max\{|m-i|, |n-j|\} \leq a\},$$

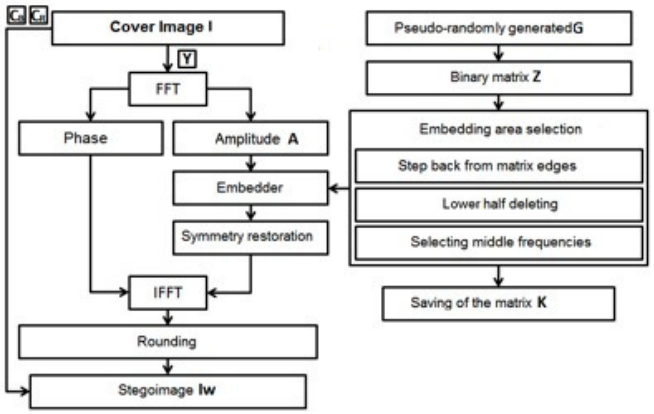

Fig. 1. Diagram of the watermark embedding method.

and $\mathbf{A}[i,j]$ is the value of the two-dimensional Fourier amplitude at the point with coordinates (i,j).

Let us restore the symmetry of the amplitude matrix. For this purpose we transform the first row in the matrix according to the formula:

$$\forall i = 2, \ldots, M: \quad \mathbf{A}_w[M-i+2, 1] = \mathbf{A}_w[i, 1],$$

where i is the x-coordinate of the matrix current element. Then, we transform the first column in the matrix according to the formula:

$$\forall j = 2, \ldots, N: \quad \mathbf{A}_w[1, N-j+2] = \mathbf{A}_w[1, j],$$

where j is the y-coordinate of the matrix current element. For all remaining elements of the matrix we use the ratio: $\forall i = 2, \ldots, M, \ j = 2, \ldots, N$:

$$\mathbf{A}_w[M-i+2, N-j+2] = \mathbf{A}_w[i,j].$$

After that, let us apply the inverse Fourier transform, connect three color components of the image and save it as the image after embedding.

The scheme of a WM embedding for a color image is presented in Fig. 1.

In order to extract a WM, firstly the fast Fourier Transform (FFT) of the luminance component of the image is performed and the amplitudes $\mathbf{A}_w$ are calculated. Next, the areas of the size $(2a+1)*(2a+1)$ with the centers in positions of the matrix $\mathbf{K}$ values 1 are created. After that we count how many areas contain a maximum at their centers. This number is divided by the total number of the areas and compared with some threshold Δ. In case the threshold is exceeded, the presence of a WM is detected, otherwise its absence is declared.

Besides, some modification of the extraction algorithm is made, allowing to detect a WM even after an image rotation. For this purpose, the image is sequentially rotated with the step 0.5° up to 180°, and the detection process described above is repeated each time. If the threshold is not exceeded at any step, then no WM is detected (see Fig. 2).

From the algorithms of the WM embedding and extraction given above we can see how the local maxima principle works.

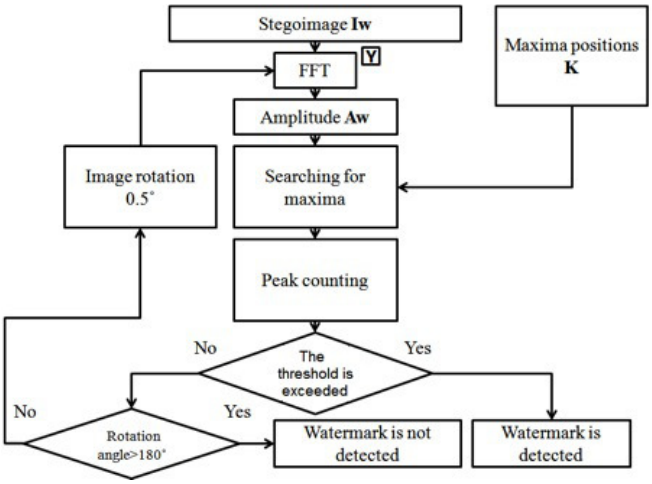

Fig. 2. Diagram of the watermark detection method.

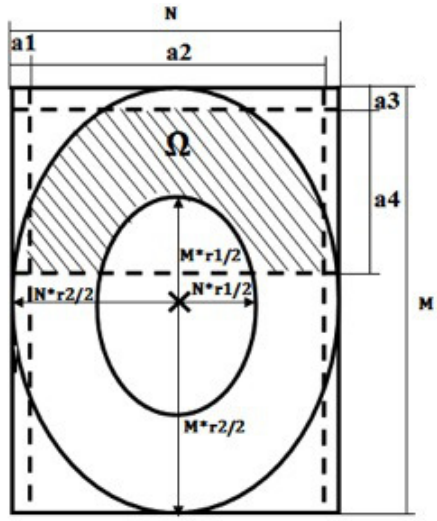

Fig. 3. The shape of the area Ω.

On the one hand, the substitution of brightness amplitude in the centers of the areas for maxima with some coefficient ($\beta \geq 1$) should not considerably worsen the image quality. And on the other hand, it is expected that various conversions of the image which do not worsen it considerably, will not change the position of maxima in local areas. However, in order to provide this expectations it is necessary to correctly select the main parameters of the proposed method. These parameters are the coefficient β, the area size $(2a+1)*(2a+1)$ and the threshold value Δ.

The experimental research of the method for various images has shown that the optimal size of the local areas is $5*5$. The parameters of the embedding area were selected experimentally as well. The geometry of the optimally selected area of embedding is shown in Fig. 3. Here, `a1` is the number of rows from the left boundary of the matrix to the beginning of the area Ω, `a2` is the width of the area Ω, `a3` is the number of columns from the upper boundary of the matrix to the beginning of the area Ω, `a4` is the height of the area, `r1` is the coefficient defining the sizes of an internal oval, `r2` is the coefficient defining the sizes of an external oval. As far to the choice of the parameter β, its best value (by the results of many experiments with various images) has appeared to be equal to 1.2. The choice of the optimal detectability threshold is made in such a way to minimize the probability of false detection of a WM, and for each specific image the parameters of embedding can be chosen individually, just before the embedding of a WM.

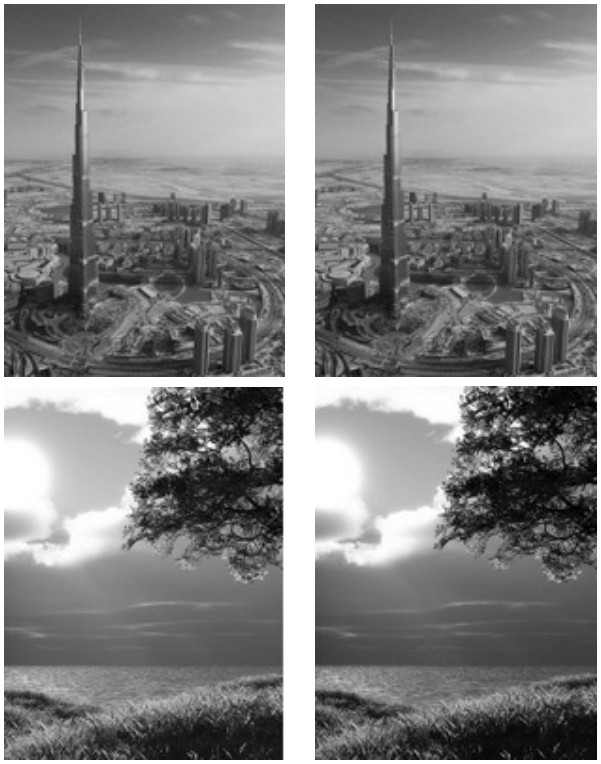

Fig. 4. Cover images (left column) and stegoimages (right column) ($a = 5, \beta = 1.2$).

In Fig. 4 the examples of two images without embedding and with embedding of a WM are shown. We can see that the images before and after embedding of a WM do not differ visually, which testifies indeed a high quality saving of the image after the WM embedding.

On the other hand, the choice of the threshold $\Delta = 0.076$ allows us to make the decision about the presence or absence of a WM with an absolute reliability (i.e. $P_m = 0$, $P_{fa} = 0$).

III. Investigation of Algorithm Robustness

The results of the experiments presented in Table I show that for the choice of the threshold value $\Delta = 0.076$, the probability of false detection appears equal to zero. The probability of successful detection of a WM is equal to one also after the cyclic shift on 50% on a vertical and a horizontal, by the removal of 50% rows or columns, after rotation of the image on the angle up to $50°$.

TABLE I
EXPERIMENTAL RESULTS.

(1)	(2)	With embedding of a WM						
		(3)	(4)	(5)	(6)	(7)	(8)	(9)
max Δ	0.07242	1	1	0.67864	0.53232	0.40438	0.25889	0.42827
min Δ	0.03508	0.175	0.15009	0.04403	0.05653	0.05487	0.07753	0.076459
Δ	0.058344	0.92828	0.92675	0.28575	0.24798	0.22337	0.11703	0.12692
Threshold Δ_D	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076
Probability of successful WM detection	0	1	1	0.95	0.94	0.98	1	1

(1): Parameters
(2): No embedding
(3): Without distortions
(4): Cyclic shift of 50% on a vertical and a horizontal axis
(5): Noise adding 5%
(6): Removal of 10% of rows and columns
(7): Cropping
(8): Rotation on 5°
(9): Rotation on 50°

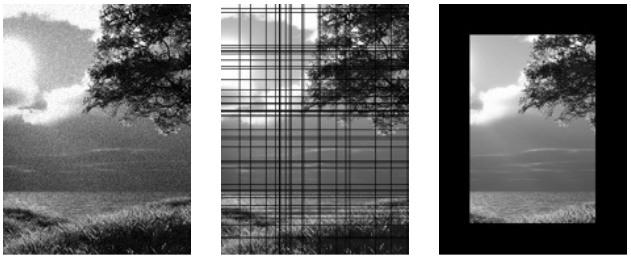

Fig. 5. Pictures after adding of the 10% noise, rows and columns removal and cropping.

In the Table I the normalized values Δ of the recognized maxima number ratio to their total number of values 1 are presented, calculated as a result of 100 various images testing. For all experiments the parameters $a = 5$, $\beta = 1.2$ have been selected.

The probability is less than one, but it remains still acceptable after adding as noise 5% of the image brightness range. However, looking at the images after such strong conversions (Fig. 5) we can see that their commercial value is low, and it is very unlikely to be applied to the images by pirates.

Let us now recall that the Kerkhoffs principle with respect to steganography means that the attacker knows everything except the stegokey, i.e., first of all, the algorithm of embedding and extraction of a WM. Therefore, the attacker can apply more sophisticated attacks with the purpose of making impossible the reliable detection of a WM by the owner, but simultaneously, with saving its high quality.

In particular, knowing of the offered WM method, the attacker can try to add false maxima in Fourier amplitude spectrum in a hope that in this case a threshold Δ_D will not be exceeded and, hence, the legal embedding will be not detected.

However, such attack appears unsuccessful because, although even if a WM is not detected the image is distorted significantly (Fig. 6).

Of course if the attacker gets a stegokey, he could have changed the position of local maxima and thereby he could provide the impossibility of the WM detection without distortion of the image. Although the stegokey is secure, pirates can try to find it by an analysis of the Fourier amplitude spectrum

Fig. 6. Pictures before and after adding false maxima.

with an embedded WM. However, in this way they face with insuperable difficulties because maxima are formed only in local areas and do not exceed the other maxima connected with the peculiarities of the original image.

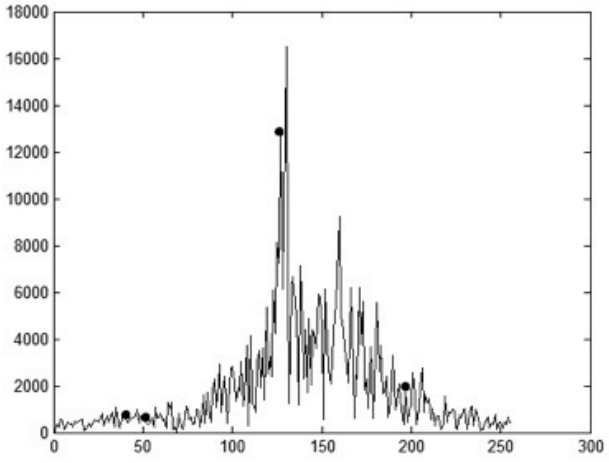

Fig. 7. One line of the amplitude coefficients of the Fourier transform.

In Fig. 7 one line of the amplitude matrix of the image with embedding is given as an example. Coefficients which form

the local maxima are marked with a filled small circle. We can see that even for a single line it is impossible to recognize the positions of maxima.

Simulation shows that after saving the WM-ed image in JPEG format, it is still possible to extract the WM for not very low quality (not worse than 30%). When the JPEG quality is worsened, the possibility of a WM extraction decreases and depends on a particular type of the image. It is possible to improve the robustness of the system by introducing an adaptive algorithm that will embed the maxima only into the frequency areas that will not change their values even after a strong JPEG compression. We can highlight the three main steps of such an adaptive algorithm:

1) Compare the FFT for the original image and the FFT of the same image after the JPEG compression at 5% quality factor.
2) Find the areas where amplitude changes are minimal.
3) Embed the local maxima only in those areas.

The performed experiments have shown that such an algorithm made it possible to extract the watermark after a 5% quality JPEG compression.

It is worth to note that if a WM is embedded in the luminance channel of the image, then it survives even after an stronger JPEG attack.

IV. Conclusions

A new method of WM embedding and extraction is proposed, that occurs to be robust against such transforms of an image as cyclic shifting, rotation, removal of rows and columns, noise addition and cropping. The important advantage of this method is that it does not require the original image for WM detection.

It is reasonable to improve the method by conducting further research of the given method in order to provide better WM extraction after strong JPEG compression and collusion attacks [6]. One way to overcome the collusion attacks is to embed some additional maxima that would be the same for the same images and would not be erased after making an averaged copy.

References

[1] J. J. O. Ruanaidh, T. Pun, and J. J. K, "Rotation, scale and translation invariant digital image watermarking," in *IEEE Int. Conf. on Image Processing ICIP1997*, 1997, pp. 536–539.

[2] C. Woo, J. Du, and B. Pham, "Geometric invariant domain for image watermarking," in *Proceedings of the International Workshop on Digital Watermarking, IWDW '06*. Springer LNCS Vol. 4283, 2006, pp. 294–307.

[3] A. Bruckstein and T. Richardson, "A holographic transform domain image watermarking method," *CSSP Journal Special Issue*, vol. 17, no. 3, pp. 361–389, 1998.

[4] W. Luo, G. L. Heileman, and C. E. Pizano, "Fast and robust watermarking of JPEG files," in *Proceedings of the Fifth IEEE Southwest Symposium on Image Analysis and Interpretation*. Washington, DC, USA: IEEE Computer Society, 2002, pp. 158–. [Online]. Available: http://portal.acm.org/citation.cfm?id=882499.884595

[5] R. Ridzon and D. Levicky, "Robust digital watermarking based on the log-polar mapping," *Radioengineering*, vol. 16, no. 4, pp. 76–81, 2007.

[6] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, and H. Zhao, "Multimedia fingerprinting forensics for traitor tracing," in *EURASIP on Signal Processing and Communications*. Hindawi, 2005.