International Journal of Computer Science and Applications

Vol. 9 No. 3, pp. 37 - 46, 2012

A MULTIPLE ROBUST DIGITAL WATERMARKING SYSTEM FOR STILL IMAGES

SERGEY ANFINOGENOV
State University of Telecommunications, St. Petersburg, Russia
serganff@gmail.com

VALERY KORZHIK
State University of Telecommunications, St. Petersburg, Russia
val-korzhik@yandex.ru

GUILLERMO MORALES-LUNA
Computer Science, CINVESTAV-IPN, Mexico City, Mexico
gmorales@cs.cinvestav.mx
http://delta.cs.cinvestav.mx/∼gmorales

Fast and wide-scale spreading of the image data on the Internet creates great opportunities for illegal access by different intruder kinds. In order to solve the problem of intellectual property protection, digital image watermarking can successfully be used. We extend the previously proposed method of digital 0-bit watermarking based on the embedding of the local maxima into the Fourier transform area of the image to multiple watermarking. Simulation results are provided confirming that the proposed method is resistant to cyclic shifts, row and column removal, cropping, addition of noise and JPEG transforms.

1. Introduction

Digital watermarks (WM) can effectively be used for copyright protection of various products. However, intruders (the so-called *pirates*), trying to illegally copy and spread 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 multiple WM system creation with *blind* decoder is proposed. This means that the system task is not only to test the fact that the WM is indeed present in the marked object, but to embed some data that can help to trace illegal distributors of products (fingerprinting).

There are two main approaches which provide resistance of WM against different deliberate transforms: to use the recovering geometric transforms which will restore the attacked products to their original WM-ed forms, and to use the invariant do-

main for transformations and blind WM detection. The WM systems introduced here are based on the properties of mathematical conversions that establish a domain 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 [Ó Ruanaidh (1997)], where an 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 [Woo *et al* (2006)] an example of such attempts is described. In theory, this method works properly, however in practice such system appears to be inapplicable. Even without embedding, the image quality is seriously impaired by carrying out direct and reverse LPM, and besides these transforms demand considerable computing resources.

A good example of a robust watermarking system is constructed by the holographic method [Bruckstein (1998)]. Nevertheless, it has one essential drawback: in order to extract the WM, it is necessary to possess the original image. In [Luo *et al* (2002)], the authors 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 completely solved. Our method, which is an extension of the method proposed in [Anfinogenov *et al* (2011)], is described in the following section.

2. Description of the robust multiple WM system

The development of a WM system which is robust against a complex of natural and intentional conversions is not an easy problem, particularly when the *blind* decoder is used, as discussed in the short description of the previous section. However, the problem has not yet been solved completely. Nevertheless, some progressive ideas have been borrowed in the current paper when developing our new method.

There are some approaches, for instance [Ó Ruanaidh (1997)], 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 [Ridzon (2007)]. 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 highlighting the local areas, which have the size $(2a+1) \times (2a+1)$ where a is a predetermined integer defining the size of the square area. This area encloses nearly located amplitude spectrum values. The position of each local area is worked out by the stegokey. We replace one of the values in each area by the amplitude spectrum maximum of that area.

The number of maxima should be chosen in such a way that an acceptable image quality is provided and an equivalent quality survives after a series of eventual image deformations. The position of the local area maximum is chosen depending on the data to be embedded. For example in order to embed 1 the local area maxima is placed in the first position of the local area, to embed 2 it is placed in the second position and so on. Then the embedded data is extracted as follows: The same local areas are built as in the embedding process according to the given stegokey. Then the positions of the local maxima at each area are found. We build the same local areas as in the embedding process according to the given stegokey. Then we find the positions of the local maxima in each area. After all the maxima positions are detected, the position appearing most frequently in all the areas is found and the decision about the embedded data is made.

In the current realization the same data is embedded in each local area and 25 different values (for local area size 5×5) can be embedded, but this can be enlarged significantly by embedding different data in each group of local areas as follows: At first let us divide the whole number of the local areas into several groups. Then the decision about the embedded data is made using the results for each group. Then the errors may be corrected using Reed-Solomon (RS) codes. There are about 300 generated by stegokey local areas in a typical 320×240 image. If we increase the size of local area till 6×6, then we can use the RS code with parameters $q = 32$, $n = q - 1 = 31$, $k = 5$.This RS code is able to correct at least 13 errors in each block, hence we can embed about 250 bits in total. The task of the local maxima formation can be solved as follows:

First, let $\mathbf{G} = (\mathbf{G}[i,j])_{0 \le i \le M-1}^{0 \le j \le N-1}$, where M and N are respectively the width and height of the image in pixels, be a matrix consisting of mutually-independent random values (in the unit real interval $[0,1]$). A matrix $\mathbf{Z}$ of the same order is created according to the following rule:

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

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 $\mathbf{Z}$ 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 $\mathbf{L}$ as:

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

where

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

The matrix $\mathbf{L}$ forms a mask with randomly allocated values 1 lying in the centers of disjoint areas of size $(2a+1) \times (2a+1)$. Next, the values 1 at $\mathbf{L}$ 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 of the original image denoted by ($\mathbf{A}$) should be replaced with a mirror display of the upper half of the matrix. This imposes to restrict the embedding area to the upper half of $\mathbf{L}$ only. Let $\mathbf{K}$ be the matrix thus obtained from $\mathbf{L}$, which is considered as a stegokey, useful to detect the WM.

After all previous steps, the amplitude matrix $\mathbf{A}$ should be changed according to $\mathbf{K}$ and the data to be embedded. For this purpose, let us select submatrices δ of size $(2a+1) \times (2a+1)$ in $\mathbf{A}$. The centers of these areas are allocated on the same positions as the 1's in $\mathbf{K}$. Let us replace the values of the amplitude, in the positions representing data at each area, by the maximum amplitude over that area multiplied by some coefficient $\beta \geq 1$. The remaining entries of $\mathbf{A}$ 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 stated as:

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

where

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

and $\mathbf{A}[i,j]$ is the value of the two-dimensional Fourier amplitude at the point with coordinates (i,j). The coordinates (i_d, j_d) depend on the embedding data and represent the position of the current local area maxima.

Let us restore the symmetry of the amplitude matrix. For this purpose let us transform the first row in the matrix as:

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

where i is the x-coordinate of the matrix current element. Then, let us transform the first column in the matrix as:

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

where j is the y-coordinate of the matrix current element. For all remaining entries, let

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

After that, it is necessary to perform the inverse Fourier transform and connect three color components of the image.

The scheme of a WM embedding 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.

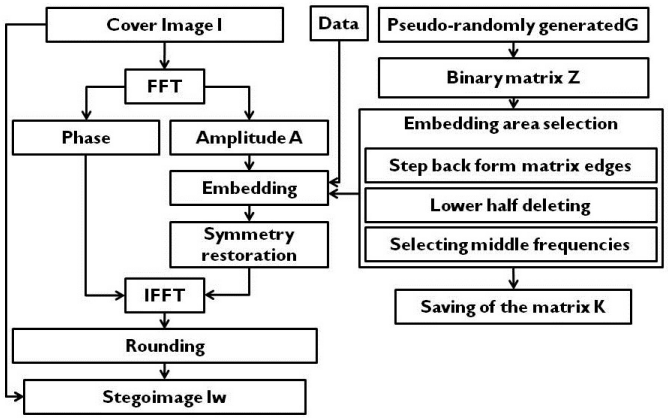

Fig. 1. Diagram of the multiple watermark embedding method.

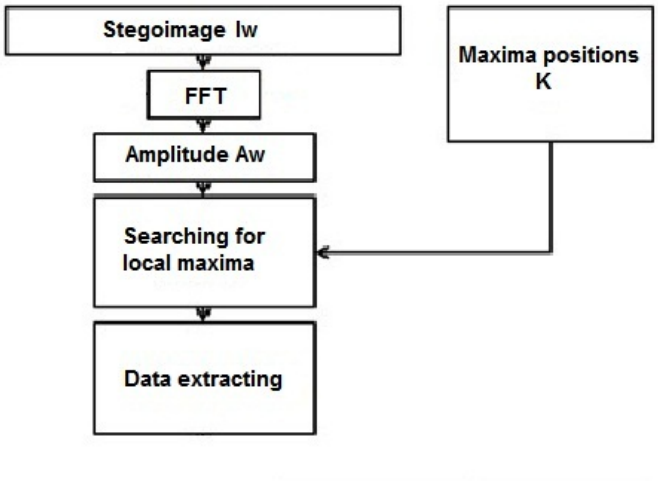

Fig. 2. Diagram of the multiple watermark detection method.

Next, the areas of size $(2a+1)\times(2a+1)$, centered at positions where the matrix $\mathbf{K}$ has entry 1, are created. After that, we count how many areas contain a maximum at the same position and decide which data are embedded (see Fig. 2).

From the algorithms for WM embedding and extraction given above, we can see how the local maxima principle works. On the one hand, the substitution of brightness amplitude at the center 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 some transforms of the image, not worsening it considerably, do not change the position of the maxima in local areas. However, in order to fulfil these

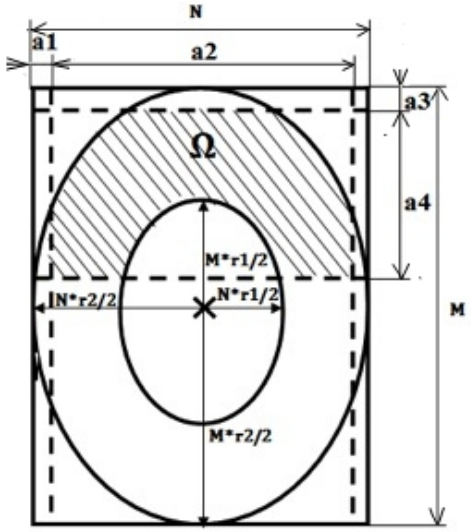

Fig. 3. The shape of the area Ω.

expectations, it is necessary to correctly select the main parameters of the proposed method. These parameters are the coefficient β and the area size $(2a+1)\times(2a+1)$.

The experimental research of the method for several images has shown that the optimal size of the local areas is 5×5. The parameters of the embedding area, that we defined as Ω, 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 which determines 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 which determines 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. Experimentally we found than we can get best results when $\texttt{a1} = a$, $\texttt{a2} = N - 2a$, $\texttt{a3}$, $\texttt{a4} = M/2.28$, $\texttt{r1} = 0.248$, and $\texttt{r2} = 0.83$. As far to the choice of β, its best value (by the results of many experiments with several 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.

In Fig. 4 the examples of two images without embedding and with embedding of a WM are shown. It can be seen 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.

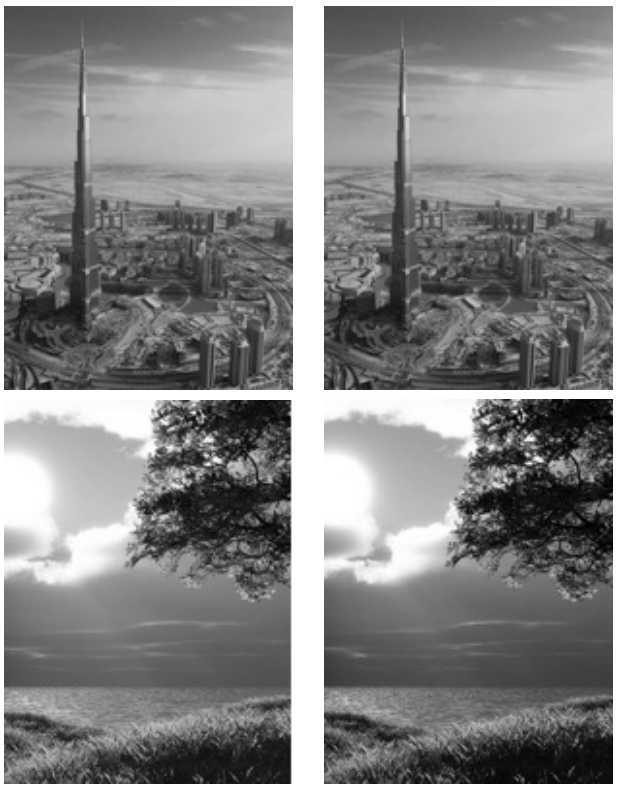

Fig. 4. Cover images (left column) and stegoimages (right column) ($a = 5, \beta = 1.2$).

3. Investigation of algorithm robustness

The results of the experiments presented in Table 1 show that the probability of false detection appears equal to 0. The probability of successful detection of a WM is equal or close to 1 also after the cyclic shift on 50% on a vertical and a horizontal, and removal of 10% of the rows and columns.

In the Table 1 the recognized maxima number ratio to their total number of embedded maxima are presented. Total number ofthe embedded and extracted maxima is a mean value of the number of maxima, calculated as a result of 100 images testing. For all experiments the parameters $a = 5$, $\beta = 1.2$ have been selected.

The probability of successful data extraction is sometimes less than 1, but it remains still acceptable, for the thing after adding a 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 area means that the attacker knows everything except the stegokey, i.e., first of all,

Table 1. Experimental results.

(1)	(2)	With embedding of a WM				
		(3)	(4)	(5)	(6)	(7)
Detected maxima number	25	295	209	252	240	231
Detected maxima %	8	100	72	85	81	78
Probability of successful data extraction	0	1	1	0.92	0.93	0.97

(1): Characteristics (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

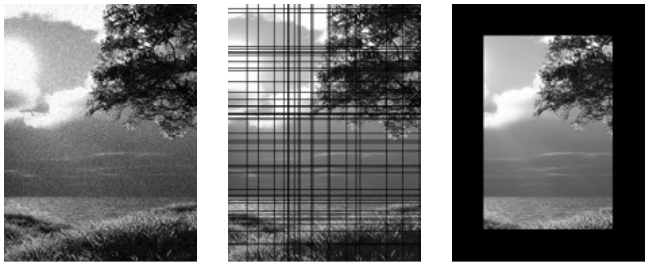

Fig. 5. Pictures after adding of the 10% noise, rows and columns removal and cropping.

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, with the knowledge of the offered WM method, the attacker can try to add false maxima in the Fourier amplitude spectrum in a hope that in this case the embedded data would be corrupted. However, such an attack appears unsuccessful because, although the WM would even not be detected, the image is distorted significantly (Fig. 6).

Of course if the attacker gets a stegokey, he could change 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 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

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

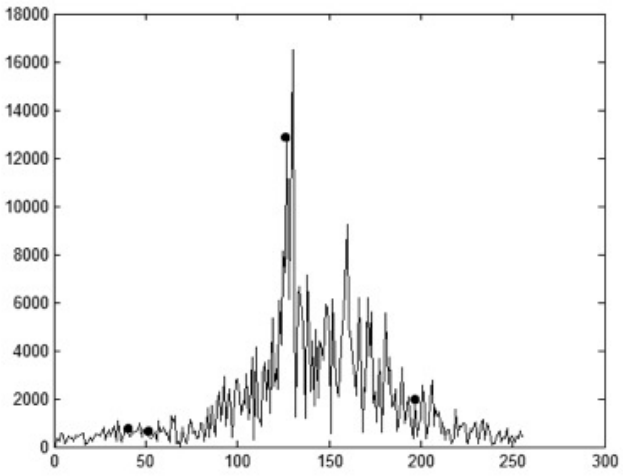

Fig. 7. One line of the amplitude coefficients of the Fourier transform matrix.

of the original image. 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 even after saving of the WM-ed image in JPEG format, it is still possible to extract data for not very low JPEG 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 a normalisation algorithm proposed

in [Dong *et al* (2005)]. The scheme would involve normalisation of the image before the FFT and inverse normalisation after IFFT during the embedding process. It is necessary to perform the normalisation of the image before the FFT in the extracting process. That improvement will help to extract data after rotation and complicated transforms as shearing. We plan to make a research in this direction.

4. Conclusions

A new method of 0-bit WM embedding and extraction that occurs to be robust against such transforms of an image as cyclic shifting, rotation, removal of rows and columns, noise addition and cropping has been proposed in [Anfinogenov *et al* (2011)]. The important advantage of this method is that it does not require the original image for WM detection. In the current paper we extend this method to the case of multiple watermarking. It is based on the selection of maxima depending on the embedded data. We have shown by simulation that such multiple WM system still occurs to be robust against such transforms of an image as cyclic shifting, removal of rows and columns, noise addition and cropping. In order to increase the number of the embedded bits it is possible to select different maxima positions in different areas and to correct errors by *Reed Solomon* codes.

It is reasonable to improve further the method by conducting research of the given method in order to provide better WM extraction after strong JPEG compression and collusion attacks [Liu *et al* (2005)]. 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

Anfinogenov, S., Korzhik, V., Morales-Luna, G. (2011). Robust digital watermarking system for still images, in *FedCSIS*, pp. 685–689.

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

Dong, P., Brankov, J., Galatsanos, N., Yang, Y., Davoine, F. (2005). Digital watermarking robust to geometric distortions, *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2140–2150,.

Liu, K. J. R., Trappe, W., Wang, Z. J. (2005). Multimedia fingerprinting forensics for traitor tracing," in *EURASIP on Signal Processing and Communications*. Hindawi.

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

Ó Ruanaidh, J., Pun, T. (1997)., Rotation, translation and scale invariant digital image watermarking, in *IEEE Int. Conf. on Image Processing ICIP1997*, pp. 536–539.

Ridzon, R., Levicky, D. (2007). Robust digital watermarking based on the log-polar mapping, *Radioengineering*, vol. 16, no. 4, pp. 76–81.

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