Proceedings of the 2013 Federated Conference on
Computer Science and Information Systems pp. 523–527

Design of Digital Watermarking System Robust to the Number of Removal Attacks

Sergey Anfinogenov
State University of Telecommunications,
St. Petersburg, Russia
Email: serganff@gmail.com

***Abstract*—In this paper it is proved that in fact the zero-bit digital watermarking system based on local maxima embedding in frequency area heuristically proposed recently is resistant to a number of removal attacks. It is shown how the watermark can survive after such conversions as shift cropping rescaling rotation and jpeg transform. The theoretical base of each transformation is given. Also it is shown how the image Fourier amplitude spectrum is affected by the image distortions and how the watermark can overcome those distortions and stay untouched.**

I. Introduction

THE MAIN idea of the watermarking method offered in [1] is an embedding of a zero-bit watermark (identification key) into the positions of maxima of the local areas, which are selected in the amplitude spectrum of the two dimensional discrete Fourier transform (DFT), calculated from the original image.

Now let us remember how this algorithm works step-by-step. First we generate a binary key K, which can be represented as the two dimensional matrix $K(n,m)$ where the number of columns N and rows M is equal to the width and height of the image respectively. Then we calculate the DFT of the image and get the amplitude spectrum. Next we change the amplitude spectrum according to the rule: If $K(n,m)=1$ we build the local area $(n-a..n+a, m-a..m+a)$ with the size (2a+1)x(2a+1) around this point, where a is a constant value which determines local area size. Then maximum of each local area is calculated. This maximum is multiplied by β value ($\beta > 1$) and placed in the point $K(n,m)$. Later we combine this new amplitude spectrum with a phase untouched before and perform the inverse DFT to get the watermarked image.

During the extraction process we calculate the amplitude again and using previously saved key K build the same local areas and verify if the maximum of each area is situated in the point $K(n,m)$. Next we count all positive answers and divide this value by the total number of local areas. Percepts of watermark are recognised if this value exceeds some threshold. If the watermarked image was untouched there would be no errors and all key points would be recognised. If some attack is applied to the watermark image, then some maxima can be lost, but the watermark will still be detectable sometimes.

The current method of zero-bit WM embedding and extraction seems to be robust against such transforms of an image as cyclic shifting, rotation, removal of rows and columns, noise addition, JPEG transform and cropping, but these conclusions have been based on simulation. In the next section we are going to present the proof of this claim based on the properties of DFT.

II. The proof of robustness of the proposed zero-bit WM system to different attacks

Now let us concentrate on the robustness of the algorithm and answer two main questions. After what image distortions a watermark can survive and why? The direct and inverse Fourier transforms for 2D signal $h(n,m)$(Image in our case) with N columns and M rows are as usually given by:

$$F(h) = \widehat{h}(k,l) = \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} e^{-i(\omega_k n+\omega_l m)} h(n,m) \quad (1)$$

$$h(F) = \frac{1}{NM}\sum_{k=0}^{N-1}\sum_{l=0}^{M-1} e^{-i(\omega_k n+\omega_l m)} \widehat{h}(k,l) \quad (2)$$

Often it is convenient to express frequency in vector notation with $\vec{k} = (k,l)^t$, $\vec{n} = (n,m)^t$, $\vec{\omega}_{kl} = (\omega_k, \omega_l)^t$ and $\vec{\omega}^t\vec{n} = \omega_k n + \omega_l m$. The vector form will help us when we talk about DFT properties. In this section we will show

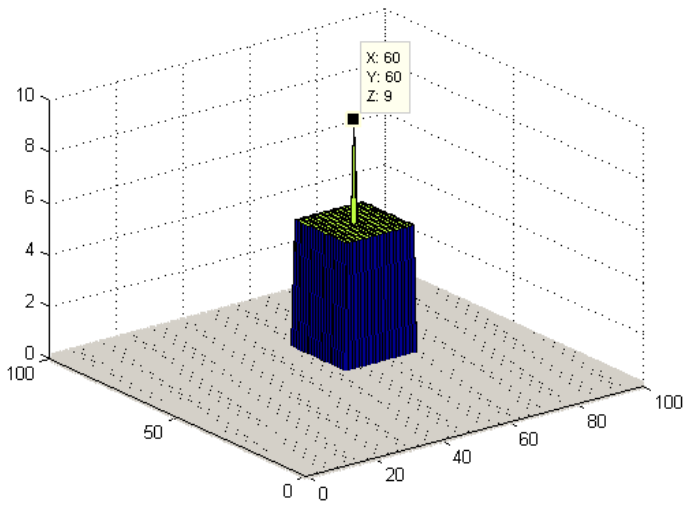

Fig. 1. Test amplitude spectrum

how the proposed watermarking algorithm can stand against different transformations. The set of transformations that are usually performed to remove a watermark are described in [5] and [4]. Now let us discuss each transformation one by one. To show an effect of each transformation we generate a test amplitude spectrum Fig. 1 where we have only one local area with maximum in the center. Such model differs from the real situation where there are many local maxima, but this simplified model helps us to show how each transformation affects on the behaviour of local maxima positions in each local area.

A. Translation

Using the shift property of the Fourier transform

$$F[f(\vec{x}-\vec{x}_0)] = \exp(-i)\vec{\omega}^t\vec{x}_0)\widehat{f}(\vec{\omega}) \tag{3}$$

it is easy to see that only phase of the DFT is affected by the translation of the image. The amplitude spectrum where the watermark is embedded remains untouched. So that transformation has no impact on a watermark detection.

B. Rotation

According to FFT property a rotation of the image causes the rotation of the FFT amplitude.

$$F(x,y) \rightarrow F(x\cos\theta + y\sin\theta, x\sin\theta + y\cos\theta) \tag{4}$$

To overcome a rotation problem if the watermark is not found initially the detection process is repeated after rotation of the image on a small angle. Another solution can be used with a normalisation algorithm described in [3] where the image is converted to the domain invariant to rotation. In fact, the image rotation on more than 10 degrees can be distinguished from the original. So it is possible to reduce number of calculations and image rotations. The last way to deal with rotation is to extend the size of local areas and detect maxima not in one certain point but in several points around the embedded maxima. That will help especially in case of small rotation angles.

C. Noise Addition

Let us define a set of n points $x_1, x_2, x_3, ...x_n$ with constant amplitude A and a point $x0$ with amplitude $\beta A(\beta > 1)$. At all points we add zero mean i.i.d Gaussian noise. The probability that the maximum stay in the previous position after the addition of noise is the following:

$$P = Pr(\tilde{x_0} \geq x_1, \tilde{x_0} \geq x_2 ... \tilde{x_0} \geq x_n) = ? \tag{5}$$

where

$\tilde{x_0} = \beta A + n_0, \tilde{x_i} = A + n_i$

$i = 1, 2..n..n_i \in i.i.dN(0, \sigma^2)$

It is easy to see that:

$$P = \int_{-\infty}^{+\infty} \omega_0(y) \prod_{i=1}^{n} (P_\tau(x_i) \leq y)dy \tag{6}$$

where

$$Pr\{\tilde{x} \leq y\} = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{y} e^{-\frac{t-A^2}{2\sigma^2}} dt, \tag{7}$$

$$\omega_0(y) = \frac{1}{\sqrt{2\pi, \sigma^2}} e^{-\frac{(y-\beta A)^2}{2\sigma^2}} \tag{8}$$

Substituting (7) and (8) in (6) we get:

$$P = \frac{1}{\sqrt{2\pi, \sigma^2}} \int_{-\infty}^{+\infty} e^{-\frac{(y-\beta y)^2}{2\sigma^2}} \cdot (\int_{-\infty}^{y} e^{-\frac{(t-A)^2}{2\sigma^2}})^n dy, \tag{9}$$

It is easy to find the lower bound of that probability using the equation:

$$P \geq \prod_{i=1}^{n} P_\tau\{\tilde{x_0} \geq \tilde{x_i}\} = (P_\tau\{\tilde{x_0} \geq \tilde{x_i}\})^n \tag{10}$$

where $(P_\tau\{\tilde{x_0} \geq \tilde{x_i}\})^n = (P_\tau\{\tilde{x_0} - \tilde{x_i}\} \geq 0)^n$

$$(P_\tau\{\tilde{x_0} - \tilde{x_i}\} \geq 0)^n = (\frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{+\infty} e^{-\frac{t-A(\beta-1)}{2\sigma^2}} dt)^n \tag{11}$$

But unfortunately it is the most interesting for us to find the upper bound of that probability, because we want to know when the local maximum changes its position. Taking into account that a calculation by (9) is very tedious procedure, we can try to solve it by simulation. Fig. 2 shows the effect of noise addition and Table I demonstrates the results of correct maxima recognition for $A = 100$, $\beta = 1.5$, $\sigma = 0.097927$.In the similar manner we can calculate the results for other embedding parameters.

We can see from Table I that maxima are recognised whenever signal-to-noise ratio $\frac{\beta^2}{\sigma^2}$ is greater than 0.49808 ($\sigma < 2.1254$).

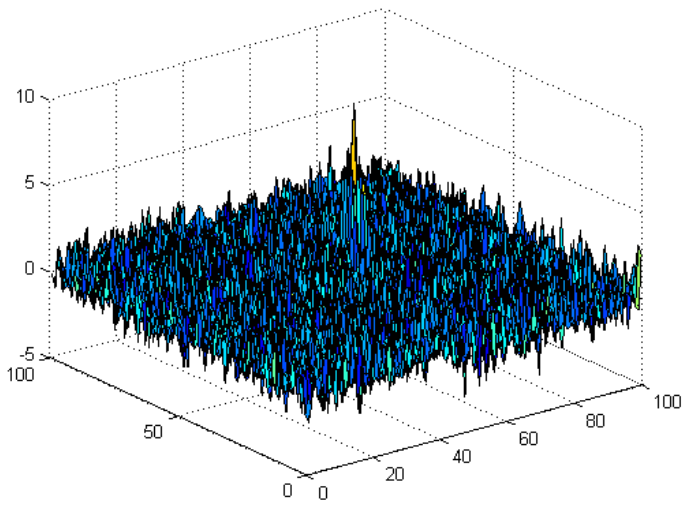

Fig. 2. Amplitude spectrum after noise addition for $A = 100$, $\beta = 1.5$, $\sigma = 0.097927$

TABLE I
THE RESULTS OF CORRECT MAXIMUM RECOGNITION AFTER NOISE ADDITION PERFORMED BY SIMULATION

Variance	Detected
0.097927	Y
0.19737	Y
0.26537	Y
0.38688	Y
0.56174	Y
0.56124	Y
0.72913	Y
0.72439	Y
0.9224	Y
0.98988	Y
1.2446	Y
1.292	Y
1.3197	Y
1.5344	Y
1.6075	Y
1.8164	Y
2.1254	N
1.8201	N
2.1679	N
2.259	Y
2.225	N
2.4485	N
2.5048	N

D. Cropping

During the cropping process some parts of the image are removed, and as the result some frequency components can be changed. Let's analyse this process in more details.

We can present cropping of the image as a multiplication of window by raster image. That is represented in one dimensional form (for the simulation) as one local area of the image amplitude Fig. 4 where cropping is given by the rectangular window function. According to the convolution theorem of the Fourier transform [2] the Fourier transform of the product of the two functions is equal to the convolution of their individual transforms.

So we get:

$$f(n,m)h(n,m) \rightarrow F(n',k') * *H(n',k') \tag{12}$$

where $f(n,m)$ - raster image,
$h(n,m)$ - the window of cropping. So now we can look on those functions separately.

In the frequency domain window function (in the 1-D case) is defined as follows:

$$h(t) = \frac{\sin\frac{\omega t}{2}}{\frac{\omega t}{2}} \tag{13}$$

The frequency ω is defined by the size of the window. Let's calculate the convolution between $h(t)$ and the test function with one local area (rectangular impulse with the maxima in the center) as follows:

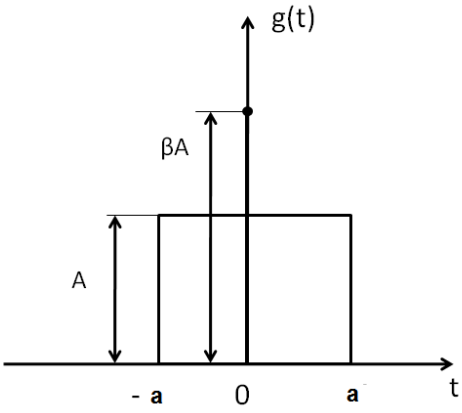

Fig. 3. Local area of the amplitude spectrum

$$y(t) = g(t) * h(t) \tag{14}$$

$$y(t) = FT[I_w(x,y)Rect(c_x(x-x_0), c_y(y-y_0))] \tag{15}$$

where c_x, c_y, x_0, y_0 - cropping parameters.

$$y(t) = \frac{1}{c_x c_y} I'_w(u,v) * e^{-i2\pi(c_x x_0 + c_y y_0)} e^{-i\pi(\frac{u}{c_x}+\frac{v}{c_y})} \times sinc\frac{\pi u}{c_x} sinc\frac{\pi v}{c_y} \tag{16}$$

where $sinc(x) = \frac{sin(x)}{x}$ if $x \neq 0$, $sinc(x) = 1$ if $x = 0$.

Now we can represent $I'_w(u,v)$ as the sum of amplitude of the original image and key $K(u,v)$ multiplied by β', where β' is the max value of local area multiplied by a constant β.

$$y(t) = [K(u,v)\beta' + I(u,v)] * * \frac{e^{-i2\pi(c_x x_0 + c_y y_0)}}{c_x c_y} e^{-i\pi(\frac{u}{c_x}+\frac{v}{c_y})} sinc\frac{\pi u}{c_x} sinc\frac{\pi v}{c_y} \tag{17}$$

To make the equation more simple we will denote the expression $\frac{e^{-i2\pi(c_x x_0 + c_y y_0)}}{c_x c_y} e^{-i\pi(\frac{u}{c_x}+\frac{v}{c_y})} sinc\frac{\pi u}{c_x} sinc\frac{\pi v}{c_y}$ as E and use the distributivity property.

$$y(t) = [K(u,v)\beta'] * E + [I(u,v)] * E \tag{18}$$

The key $K(u,v)$ can have only two values 0 and 1.

If $K(u,v) = 0$ then $y(t) = I(u,v) * E$

else $y(t) = \beta' * E + I(u,v) * E$

If we want the maxima to survive the value of the amplitude in where $K(u,v) = 1$ should be greater than the other points.

$$\beta' * E + [I(u,v)] * E > [I(u,v)] * E \tag{19}$$

$$\beta' * \frac{e^{-i2\pi(c_x x_0 + c_y y_0)}}{c_x c_y} e^{-i\pi(\frac{u}{c_x}+\frac{v}{c_y})} sinc\frac{\pi u}{c_x} sinc\frac{\pi v}{c_y} > 0 \tag{20}$$

Let us substitute the cropping parameters and see when the maximum would be recognised. Table II shows the results of calculation for the different size of the window function. We

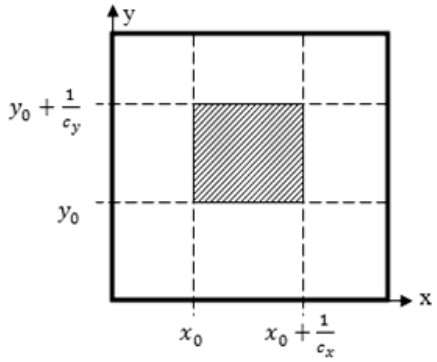

Fig. 4. Cropped area of an image

TABLE II
RESULTS OF MAXIMA RECOGNITION AFTER CROPPING BY WINDOW WITH COORDINATES x_0, $x_0 + \frac{1}{c_x}$, y_0, $y_0 + \frac{1}{c_y}$ AND TOTAL IMAGE SIZE 100X100

x_0	$x_0 + \frac{1}{c_x}$	y_0	$y_0 + \frac{1}{c_y}$	Detected
1	99	1	99	Y
2	98	2	98	Y
3	97	3	97	Y
4	96	4	96	Y
5	95	5	95	Y
6	94	6	94	Y
7	93	7	93	Y
8	92	8	92	Y
9	91	9	91	Y
10	90	10	90	Y
11	89	11	89	Y
12	88	12	88	Y
13	87	13	87	Y
14	86	14	86	Y
15	85	15	85	Y
16	84	16	84	Y
17	83	17	83	Y
18	82	18	82	Y
19	81	19	81	Y
20	80	20	80	N
21	79	21	79	N
22	78	22	78	N
23	77	23	77	N
24	76	24	76	N
25	75	25	75	N
26	74	26	74	N
27	73	27	73	N
28	72	28	72	N
29	71	29	71	N
30	70	30	70	N

gradually reduce the size of the window Fig. 4 and check how the detection process is performed. We can see that the maxima can be still detected after removing a half of an image.

E. Resize

Resizing the image results in inverse resizing of an amplitude spectrum. Resize can be represented as a multiplication of the coordinates on a corresponding constant value. If we look on the similarity theorem:

$$f(an, bm) \rightarrow \frac{1}{|ab|} F\left(\frac{n'}{a}, \frac{m'}{b}\right) \tag{21}$$

we can see that the resize in spatial domain causes frequency shift in the spectra. In combination with the resize maxima remains on the same distance from the center. So the maxima in the amplitude spectra will not change their positions.

F. Jpeg transform

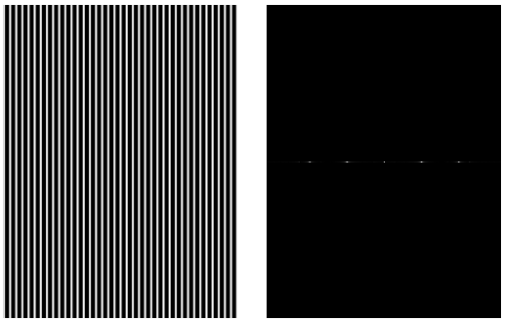

Fig. 5. Image after JPEG transform and the amplitude spectrum

Converting an image using JPEG algorithm produce specific kind of distortions. Many watermarking algorithms can not stand against such transform. The proposed algorithm can survive after JPEG transform performed with up to 30 present quality factor. This value may vary from image to image depending on image type and especially image size. Looking on the amplitude of the image after such transform we can see that some extra maxima appeared Fig. 5 right image. But all the values of those additional maxims are as the result much smaller than original ones. As long as we are searching for the max values those additional maxima give small effect on the extraction. We can see it only when additional maxima appear in the neighbour local areas with the smaller main maxima. Another effect of the JPEG transform is a removal of the high frequencies. After such transform most of the high frequencies are erased including the embedded maxima. The total number of maxima in the real system is about 350 for 100x100 pixel image. But the number of survived maxima is enough to detect the watermark.

The results of the experiments presented in Table III 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 III the recognised maxima number ratio to their total number of embedded maxima are presented. Total number of the embedded and extracted maxima is a mean value of the number of maxima, calculated as a result of 100

TABLE III
EXPERIMENTAL RESULTS

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

(1): No embedding
(2): Without distortions
(3): Cyclic shift of 50% on a vertical and a horizontal axis
(4): Noise adding 5%
(5): Removal of 10% of rows and columns
(6): Cropping 20% of the image

images testing. For all experiments the parameters $a = 2$, $\beta = 1.5$ 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, the commercial value of the images after such strong conversions is low, and it is very unlikely to be applied to the images by pirates.

III. CONCLUSION

So in this paper we tried to explain why the watermarking system can survive after image distortions. We showed that in spite of the fact, that image distortions affect on the amplitude spectra the most part of local maxima survives and therefore zero-bit watermark can be recognised with great probability.

ACKNOWLEDGMENT

The author would like to thank Dr. Valery Korzhik for help and support.

REFERENCES

[1] S. Anfinogenov, V. Korzhik, and G. Morales-Luna. Robust digital watermarking system for still images. In *FedCSIS*, pages 685–689, 2011.
[2] C. Solomon. *Fundamentals of Digital Image Processing.* Wiley-Blackwell, 2011.
[3] Dong, P., Brankov, J., Galatsanos, N., Yang, Y., Davoine, F. *Digital watermarking robust to geometric distortions*, IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2140–2150, 2005.
[4] Liu, K. J. R., Trappe, W., Wang, Z. J. *Multimedia fingerprinting forensics for traitor tracing.* Hindawi, 2011.
[5] Ingemar J. Cox, Miller M.L, Bloom J.A, Fridrich J, Kalker T. *Digital Watermarking and Steganography.* Morgan Kaufmann Publishers, 2008.