УДК 004.056.5

ИССЛЕДОВАНИЕ СВОЙСТВ ЭЛЕКТРОННОГО ВОДЯНОГО ЗНАКА, ВСТРОЕННОГО В ЧАСТОТНУЮ ОБЛАСТЬ СТЕГОКОНТЕЙНЕРА

Шарова Мария Дмитриевна

Студентка;
ГБОУ ВПО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: mdsharova@gmail.com.

В данной статье рассмотрен способ обработки изображений, основанный на методе дискретного косинусного преобразования и технике быстрого преобразования Фурье. Исследования электронного водяного знака, встроенного в изображение с помощью данного преобразования и алгоритми Коха-Жао, доказывают, что данный метод обеспечивает робастность ЦВЗ к обработке стегоконтейнера (таких как сжатие, добавление шума, размытия по Гауссу, ряби и др.) и к аффинным преобразованиям (сжатию, растяжению и повороту). Также продемонстрировано, что ЦВЗ подписанного изображения устойчив к искажению, вызванному сохранением изображения в различных форматах.

Ключевые слова: стеганография, электронный (цифровой) водяной знак (ЦВЗ), двумерное дискретное косинусное преобразование (ДКП), техника быстрого преобразования Фурье (БПФ), робастность, аффинные преобразования, фильтры, формат изображения, сжатие *JPEG*.

RESEARCH OF DIGITAL WATERMARK EMBEDDED INTO THE FREQUENCY DOMAIN OF THE CONTAINER

Sharova Maria

Student;
Dubna International University of Nature, Society, and Man,
Institute of system analysis and management;
141980, Dubna, Moscow Reg., Universitetskaya St., 19;
e-mail: mdsharova@gmail.com.

In this article the method of processing image, based on of Discrete Cosine Transform method and Fast Fourier Transform technique, has been considered. Researches of watermark embedded into an image by this method and the Koch-Zhao algorithm, which are presented in this document, prove that insertion of a watermark by DCT watermarking method makes the watermark robust to image processing operations (such as lossy compression, adding noise, Gaussian blur and ripple, etc.), and affine transformation (such as scaling and rotation). It is also proved, that the watermarked image is robust to distortion caused by saving in different formats.

Keywords: steganography, digital watermark, 2D Discrete Cosine Transform, Fast Fourier Transform, robustness, affine transformation, filters, image format, JPEG compression.

Introduction

More and more often, especially in the Internet, you can see digital images with embedded electronic, or digital, watermarks. Using digital watermarks allows owners and creators of digital images and photos to protect their copyrights on this intellectual property. The development of computer technology in the last decade has given a new impetus to the development of computer steganography. It has made possible to embed the message into digital data: speech, audio, images and video. In addition, it is proposed to embed information into text files and executable programs.

The aim of this work is to construct a digital watermark and analize its resistance to changes of graphical container it is embedded into.

Discrete Cosine Transform Method, the Koch-Zhao Algorithm, Fast Fourier Transform Technique

The Discrete Cosine Transform Method, as well as the Fourier Transform Method, is based on a changing picture's structure by stego law, but so that standard programs for viewing pictures would stay indifferent to these changes.

The goal of the Discrete Cosine Transform is to replace processing original images by working with frequency domain of luminance and chrominance. These frequencies are related to the level of an image's details. The image, which is analyzed within the YCbCr color model, is divided into blocks of 8×8 pixels, then the Discrete Cosine Transformation is applied to every 8×8 block.

As a result of the Discrete Cosine Transform we obtain the 8×8 matrix, in which the very first element describes the basic color tone of this block, and the elements to the right and bottom describe tiny details of the image's block. The direct Discrete Cosine Transform is specified by the formula below:

$$F(u,v) = \frac{c(u,v)}{4} \cdot \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cdot \cos\left(\frac{2x+1}{16} \cdot v \cdot \pi\right) \cdot \cos\left(\frac{2x+1}{16} \cdot u \cdot \pi\right).$$

The inverse Discrete Cosine Transform is described by the formula:

$$f(x,y) = \frac{1}{4} \cdot \sum_{u=0}^{7} \sum_{v=0}^{7} c(x,y) \cdot F(u,v) \cdot \cos\left(\frac{2v+1}{16} \cdot x \cdot \pi\right) \cdot \cos\left(\frac{2u+1}{16} \cdot y \cdot \pi\right),$$

where: $c(0,0) = \frac{1}{2}, c(0,v) = c(u,0) = \frac{1}{\sqrt{2}}$, u ≠ 0 и v ≠ 0; c(u, v) = 1, u ≠ 0 и v ≠ 0.

High frequencies correspond to the greater detail and are of little use for digital watermark embedding because even slight changes of container may cause the watermark distortion or destruction. In case of embedding bits to the range of the very low frequencies the distortion of the image will be too noticeable, and the digital watermark won't satisfy the condition of invisibility. That is why the range of frequencies close to the area of middle and low frequencies is the most appropriate for embedding watermark.

When the coefficients of the Discrete Cosine Transform matrix are obtained, the algorithms of changing some coefficients are applied, so that these coefficients would code some sequence of bits of the watermark. The Koch-Zhao algorithm is one of such algorithms.

The Koch-Zhao algorithm for hiding data in a frequency domain of container is used for relative replacing of coefficients of the Discrete Cosine Transform.

Information is embedded in the following way: for the bit "0" the difference between the absolute values of the coefficients should be larger than a positive value, whereas for the bit "1" this difference should be less than a negative value:

$$\left|\Omega_1(u_1,v_1)\right| - \left|\Omega_2(u_2,v_2)\right| > \varepsilon, \text{ if } s_i = 0,$$
$$\left|\Omega_1(u_1,v_1)\right| - \left|\Omega_2(u_2,v_2)\right| < -\varepsilon, \text{if } s_i = 1,$$

where $\varepsilon = \varepsilon(P)$ – a value which depends on a threshold P; $\Omega_1(u_1,v_1)$ – a coefficient of the matrix DCT with coordinates (u_1,v_1); $\Omega_2(u_2,v_2)$ – a coefficient of the matrix DCT with coordinates (u_2,v_2); s_i – a bit of the embedding information.

The magnitude of the changes for embedding information and the robustness of this steganosystem depends on the choice of parameters u_1, v_1, u_2, v_2 and P.

After embedding watermark in the blocks of DCT we make the inverse DCT, and, using the inverse formulas of transforming from the color model YCbCr, represent the image with the hidden watermark in the color model RGB.

For reading the hidden message in decoder the same procedure of choosing coefficients is made, and the decision about transferred bit is made by the following rule:

$$s_i = 0, \text{if } \left|\Omega_1(u_1, v_1)\right| > \left|\Omega_2(u_2, v_2)\right|,$$
$$s_i = 1, \text{ if } \left|\Omega_1(u_1, v_1)\right| < \left|\Omega_2(u_2, v_2)\right|,$$

where $\Omega_1(u_1, v_1)$ – a coefficient of the matrix DCT with coordinates (u_1, v_1); $\Omega_2(u_2, v_2)$ – a coefficient of the matrix DCT with coordinates (u_2, v_2); s_i – a bit of the hidden information [6].

To estimate the overlap of the embedded and recovered information the correlation coefficient is calculated by the formula:

$$\rho = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \hat{w}_i^2}},$$

where $w_i, \hat{w}_i$ – elements of the original and recovered message; N – a count of message bits.

For the method of Discrete Cosine Transform the algorithm of Fast Fourier Transform can be written as follows (considering a one-dimensional case)

1) a sequence y_m is generated from the original sequence x_m:

$$\begin{cases} y_m = x_{2m}, \\ y_{N-1-m} = x_{2m+1}, \end{cases}$$

where $0 \le m \le N/2$;

2) then DFT Y_n of y_m is obtained using FFT (as y_m is real, only half of the data points need be computed):

$$Y_n = F(y_m),$$

where F means FFT;

3) DCT X_n is calculated from Y_n by the formula:

$$X_n = \mathrm{Re}(e^{-jn\pi/2N} Y_n).$$

The most obvious way to make inverse DCT on the obtained set is to reverse the order of the mathematical operations of the three steps for the forward DCT:

1) Y_n is obtained from X_n:

$$Y_n = X_n e^{jn\pi/2N};$$

2) y_m is calculated from Y_n by inverse DFT using FFT:

$$y_m = \mathrm{Re}(F^{-1}(Y_n));$$

3) then x_m is obtained from y_m:

$$\begin{cases} x_{2m} = y_m, \\ x_{2m+1} = y_{N-1-m}, \end{cases}$$

where $0 \le m \le N/2$.

One of the most popular implementations of the FFT technique is the Cooley-Tukey algorithm. This algorithm makes two equal sets of points from the original set (the size of the input must be a power of two). Every set is divided for two subsets and so on. The FFT is calculated on every obtained set [1].

Analysis of robustness of the watermark embedded by the Discrete Cosine Transform

A digital image of the water snake was selected as a stegocontainer (see Fig. 1, on the left; the author of this document is also the author of the picture). The original image size is 400 × 900 pixels, the image format is JPEG. Thus, a watermark up to 50 × 112 pixels can be embedded in this image. The black-and-white image 32 × 32 pixels size (see Fig. 1, on the right) was selected as a watermark.

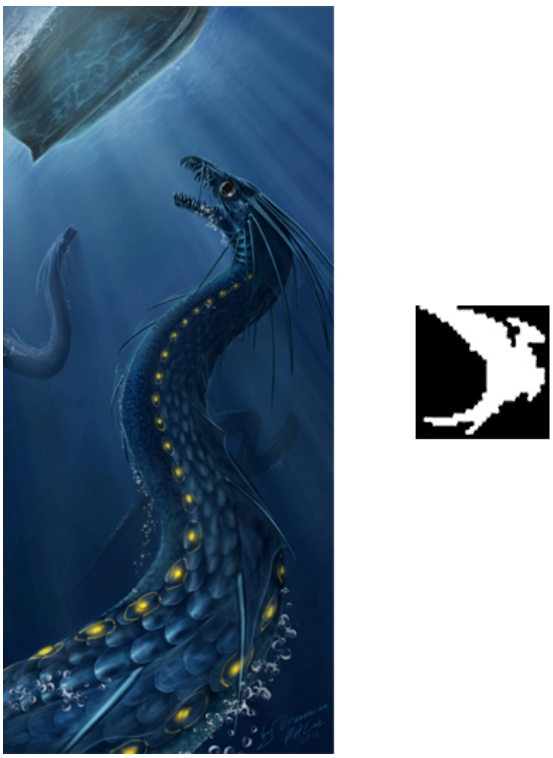
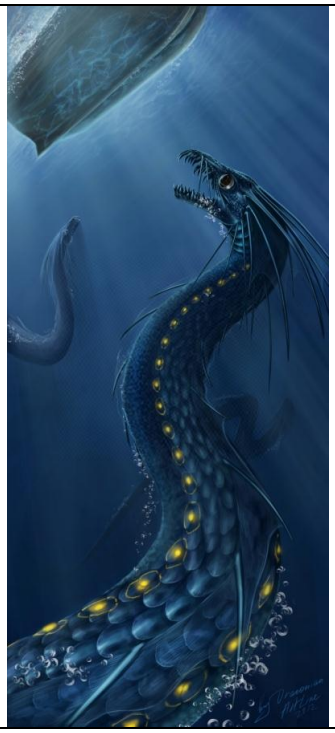
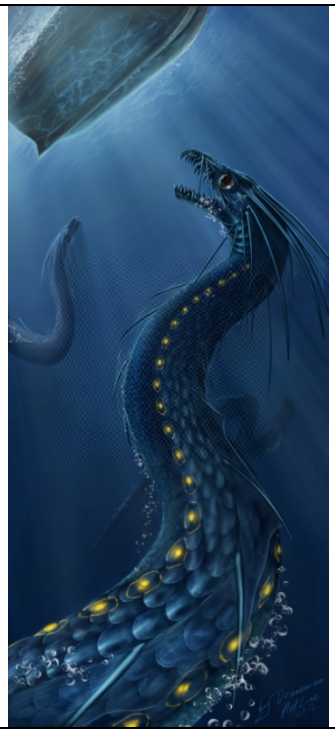
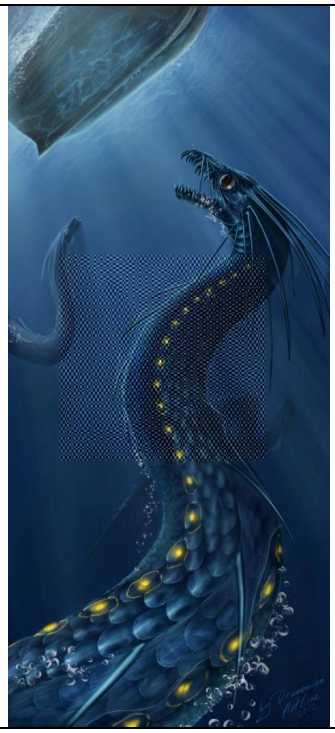


Fig. 1. The stegocontainer and the image of the embedding watermark

First, the impact of the embedding threshold on the image quality was analyzed. The higher was the embedding threshold, the more conspicuous were the image manipulations. So, at the threshold of $P = 15$ the embedded tracks of the watermark can be noticed only on closer examination and comparison with the original image, at $P = 50$ we can already notice strong distortion of the picture, and an attentive attacker will clearly see the region of embedding. When the threshold of P reaches 250, the trace of the watermark is seen almost up to the distinction between the «black» and «white» embedded bits. A further embedding threshold increase worsens the image and does not make sense. The results of this analysis are presented in Table 1.

Table 1. The impact of the embedding threshold on the image quality

	Embedding threshold , *P*		
	15	50	250
A picture with an embedded watermark			

Also the quality of the embedded watermark was analyzed in the range $1 \geq P \geq 50$ (see Table 2).

Table 2. The impact of the embedding threshold on the quality of the embedded watermark

	Embedding threshold, *P*											
	—	50	45	40	35	30	25	20	15	10	5	1
Water-mark												
ρ	—	0,9960	0,9960	0,9660	0,9933	0,9920	0,9907	0,9868	0,9766	0,9583	0,9332	0,8006

It can be easily seen that the higher is the embedding threshold, the higher is the correlation coefficient between the original and restored watermark. Moreover, the higher is the embedding threshold, the more resistant to distortion is the watermark.

Thus, the increasing *P* worsens the visual quality of the picture and the embedded watermark is getting more likely to be detected. With decreasing *P* the image stays almost unchanged, however, the outer influences on the container may cause severe distortion of the watermark itself. Nevertheless, the exact optimal embedding threshold P cannot be specified, because it may vary with every image, and the value of *P* staying the same, the watermark in one image can be more noticeable than in the other one. The easiest way to detect manipulation on the image is when the watermark is embedded into the monotonous part of the image that is why a lower embedding threshold should be chosen for such images in this algorithm.

In further analysis for this image-container (Fig. 1) the threshold value 15 was used, as with the given threshold value the image structure interference is yet hardly noticeable and the recovered watermark is still sharp.

To test the safety of the watermark in each of the four formats – JPEG, BMP, GIF and PNG, the signed image with the threshold of 15 was separately saved in JPEG, BMP, GIF and PNG formats.

Then each of the resulting images was loaded into the embedding application, and for each of these containers the watermark was restored. Table 3 shows a comparison of the restored watermarks and presents correlation coefficients for each of the four image formats.

Table 3. Restoring watermark from the images in four formats

	PNG	BMP	GIF	JPEG
Restored watermark				
ρ	0,9766	0,9766	0,9304	0,9842

As seen from Table 3, the watermark is well preserved if the images are saved in formats PNG, BMP and JPEG, but slightly worse in the format GIF. This is due to bit representation of each format.

Then these four images were saved in the formats different from the original to check the distortion of the watermark signature when container is translated into another format. As an example, the results of four trials are presented in Table 4.

Table 4. Saving four images in formats different from the original

	Original format — result format			
	PNG – BMP	BMP – JPEG	GIF – PNG	JPEG – GIF
Restored water-mark				
ρ	0,9766	0,9791	0,9304	0,9804

From these results we can conclude that the watermark is preserved when the image in one format is translated into another format, the correlation coefficient having the previous value in case of saving in the format with the quality preserved, and lower one if the target format uses compression that worsens the image quality.

One of the most important characteristics of the JPEG image is compression ratio, and attempts to change the compression ratio can seriously affect the container. Therefore, the JPEG container was saved with different compression percentage, ranging from 10% to 80% in steps of 10%. From each obtained image the attempts to allocate the watermark were made.

According to the results in Table 5, we can say that after 50% compression the watermark is too distorted, and at 80% it is almost indiscernible.

Table 5. The impact of JPEG compression on the watermark

	Compression, %								
	—	10	20	30	40	50	60	70	80
Restored watermark									
ρ	—	0,9571	0,9868	0,9814	0,9364	0,7392	0,6134	0,6149	0,4092

It should be noted that at 30-40% compression the original image is still of acceptable quality, and after compression above 60% the quality leaves much to be desired, so attempts to destroy the watermark in this way do not make sense.

Let us consider the effect of different filters and transformations used to destroy or severely distort the watermark, the overall image quality staying generally the same.

JPEG container with the embedding threshold of 15 was subjected to multiple filters that are available in Adobe Photoshop CS5 graphic editor. The following filters and transformations were used: Desaturation, Noise 3%, Ripple 40%, Blur, Blur more, Gaussian Blur 0,5 and the combined effect of three filters: Noise 3%, Blur and Sharpen. The results can be seen in Table 6.

Table 6. The restored watermarks after filtrating

	Filters							
	no	Desaturation	Noise, 3%	Ripple, 40%	Blur	Blur more	Gaussian blur (0,5)	Noise (3%) + Blur + Sharpen
Water-mark								
ρ	—	0,9490	0,8990	0,9473	0,9728	0,9501	0,9650	0,9086

Almost everywhere a high correlation coefficient of the restored watermark can be noted. The filter Noise distorts the watermark most, but it also sufficiently alters the image. Thus, the watermark is quite resistant to the use of filters, whose purpose is the destruction or distortion of this watermark with the general preservation of image quality.

One of the criteria of watermark robustness is resistance to affine transformations of the image-container.

The original container with the embedding threshold 15 in the JPEG format is 400 × 900 size. Three variations of this image with the following dimensions 222 × 500, 356 and 533 × 800 × 1200 were obtained. Attempts to allocate the watermark were made on these three images. As the number of 8 × 8 blocks changed, the watermark was allocated incorrectly, and correlation coefficients indicate the absence of the watermark. However, when all the three modified images were converted back to the 400 × 900 size, the watermark stood out with a fairly high correlation coefficient and precision (see Table 7).

So, the size of the original signed picture being known, it is possible to detect the watermark even in a compressed or stretched image.

Table 7. The impact of resizing picture on the watermark

	Container size, *px*						
	Original 400 × 900	222 × 500	222 × 500, enlarged to 400 × 900	356 × 800	356 × 800, enlarged to 400 × 900	533 × 1200	533 × 1200, reduced to 400 × 900
Restored watermark							
ρ	0,9842	0,3927	0,9434	0,4566	0,9454	0,4687	0,9766

The last analysis considers the impact of rotation of the image on the recognizability of the watermark embedded by DCT algorithm.

The container with the watermark was then rotated by 15 ° clockwise, and then an attempt to obtain the watermark from this transformed image was made. As it can be seen from the table, after the image rotation it is impossible to restore the watermark, the correlation coefficient being only 0.4843. However, it is possible to restore the image by rotating it back to the same angle, if the angle is known. And then the watermark stands almost as distinct (see Table. 7).

If the angle is unknown, it is still possible to detect the watermark manually. For example, the author of the original may try to overlap the original and the rotated image so that they will match most closely (e.g. by using the Photoshop graphical editor). Even if the reverse rotation is imprecise, it is still possible to allocate the watermark or understand that it is there (see Table 8).

Table 8. The impact of the rotation on the watermark

	Original	After rotation by 15°	After rotation back by 15°	After imprecise rotation (about 13°)
Watermark				
ρ	—	0,4843	0,9741	0,7452

Literature

1. Инструменты параллельного программирования в системах с общей памятью: Учебник для вузов / Корняков К.В., Кустикова В.Д., Мееров И.Б. [и др.]. – М.: Издательство Московского университета, 2010. – С. 272.
2. Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, Talal Shamoon. Secure Spread Spectrum Watermarking for Multimedia // IEEE Transactions on image processing. – December 1997. – Vol. 6. – №. 12. – P. 14.
3. Gaurav Gupta, Himanshu Aggarwal. Digital image Watermarking using Two Dimensional Discrete Wavelet Transform, Discrete Cosine Transform and Fast Fourier Transform // International Journal of Recent Trends in Engineering. – May 2009. – Vol. 1. – № 1. – P. 3.
4. Борисова С.Н., Боброва Е.М. Стеганографические методы встраивания информации // Научно-методический журнал: XXI век: итоги прошлого и проблемы настоящего. – Пенза: Пенз. гос. технол. акад., 2011. – 03/2011. – С. 18-24.
5. Прохожев Н.Н. Методы и алгоритмы повышения устойчивости информации, встроенной в графические стеганоконтейнеры, к сжатию с потерями: автореферат диссертации ... кандидата технических наук / СПбГУ ИТМО. – Санкт-Петербург, 2010. – С. 22.
6. Михайличенко О.В., Прохожев Н.Н. Алгоритм встраивания цифровых водяных знаков в единичный коэффициент матрицы дискретно-косинусного преобразования // Сборник трудов конференции молодых учёных, выпуск 6: Информационные технологии – СПб: СПбГУ ИТМО, 2009. – С. 644-649.
7. Старченко А.П. Методы встраивания и идентификации скрытых водяных знаков: автореферат диссертации ... кандидата технических наук / СПбГУ ИТМО. – Санкт-Петербург, 2011. – С. 17.
8. Корытова М.В. Диофантовы алгоритмы при обработке и передаче видеоданных: диссертация ... кандидата технических наук / ОГУ им. Ф.М. Достоевского. – Омск, 2007. – С. 14-18.