Parallel blind digital image watermarking in spatial and frequency domains

Article *in* Telecommunication Systems · November 2013

DOI: 10.1007/s11235-013-9734-x

2 authors:

Piotr Lenarczyk
Military University of Technology
4 PUBLICATIONS **10** CITATIONS
SEE PROFILE

Zbigniew Piotrowski
Military University of Technology
44 PUBLICATIONS **110** CITATIONS
SEE PROFILE

Telecommun Syst
DOI 10.1007/s11235-013-9734-x

Parallel blind digital image watermarking in spatial and frequency domains

Piotr Lenarczyk · Zbigniew Piotrowski

Abstract The protection of copyrights of digital images authors is one of the most important tasks set before watermarking. What is especially important is to ensure the high robustness of a watermarked images against attacks, preventing the reading of additional information about the author. In addition, the used processing of the original image must be absolutely invisible. The presented algorithm embeds information in a parallel way—independently of the luminance and chrominance matrices in the spatial and frequency domains. The main factor motivating the use of a parallel watermark embedding via the proposed way was the mutual complementing of robustness, offered by processing in spatial and frequency domains. Additional information is recovered in a 2D cepstrum domain and in coefficients of the cosine transform. The article shows a description of a mathematical model, tests of invisibility, effectiveness and the robustness of the method were carried out. The robustness of the algorithm was shown against the following attacks: JPEG and JPEG2000 lossy compression, noise, median filtering, Low-Pass and High-Pass filtering, desynchronization, simple and inverse D/A conversion, majority cropping, photomontage and affine transforms—rotation, scaling, shearing, translation.

Keywords Watermarking · Hiding information · 2D cepstrum · 2D DCT

P. Lenarczyk (✉) · Z. Piotrowski
Faculty of Electronics, Military University of Technology, Warsaw, Poland
e-mail: Piotr.Lenarczyk@interia.pl

Z. Piotrowski
e-mail: Zbigniew.Piotrowski@wat.edu.pl

Published online: 23 October 2013

1 Introduction

The dynamic development of modern systems of distributing digital data, especially videos, photos, music and text enforce the rapid development of techniques which enable their control. They are known in the form of DRM which may be characterized as a system aimed at protecting digital data of high value, controlling their distribution and use [11]. The basic requirements set for the DRM system contain suitable protection of digital data against unauthorized access, suitable robustness for different types of multimedia (video, music, text, pictures), independent from the platform on which they will be used (PC, phones, TV, radio). DRM consists of two components: (1) a technology of the following type: digital watermarking, encoding, copy control, authentications, tamper-resistant hardware and software, integrity checking, revocation and risk management architectures, key management, fingerprinting (2) creating technologies which allow for the use of DRM on hardware platforms [11, 22].

Watermarking meets those challenges as a potential technique which allows for the control of digital data.

"Digital watermarking—means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm" Juergen Seitz [45].

Depending on the application, watermarking has different requirements. For example [6] mentions eight watermarking applications, taking into account their specific requirements: broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, device control and legacy enhancements. De-

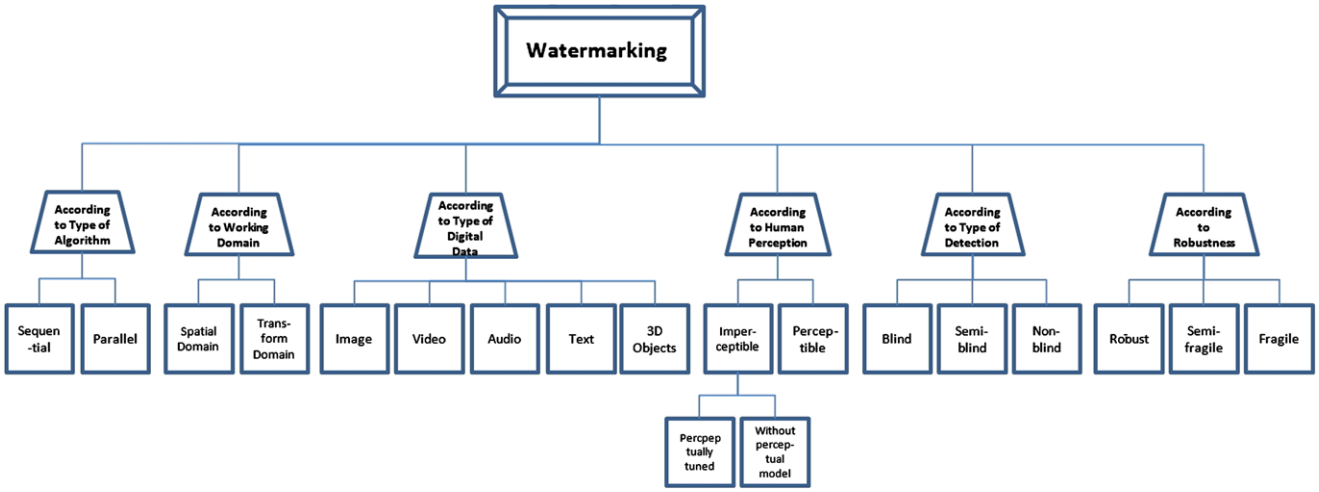

Fig. 1 Types of watermarking techniques

pending on the requirements set forward by a given application type, digital data watermarking may be divided according to several proposed categories (Fig. 1):

Referring to the type of algorithm, we take into account the character of the method—sequential or parallel. The potential proposed algorithm may be aimed at parallel processing which watermarks in two independent domains, [1, 3, 30] i.e. multichannel watermarking. Also embedding two different watermarks containing information about the owner of the image and the client using the digital image may be deemed as parallel watermarking [27]. An example of a sequential algorithm may be the use of the DWT transform to initially process the image, and then to embed the mark represented in the DCT frequency domain [21].

Referring to the domain in which additional information is embedded, we differentiate the spacial and transform domain used for watermarking. Because of the fact that it is easier to obtain a high algorithm robustness in the transform domain, this type of algorithms is more popular compared to spatial algorithms. Among numerous proposed methods one may notice the large number of algorithms in the DCT [10, 29, 32] and DWT [4, 26, 47, 51] domains (because of the fact that most popular lossy compression standards—JPEG and JPEG2000 operates in DCT and DWT). Also two transforms are used, e.g. DWT—DCT [18], DCT in connection with SVD [24] and many others, e.g. Counterlet [50], one-dimensional DWT [15], Shur [44] or Fourier—Mellin [56] transforms. Algorithms watermarking in the spatial domain appear much more rarely [3, 11, 38].

In terms of the type of digital data, we may divide them into four types: image, video, music, text and 3D objects. Among algorithms which watermark images we may find an interesting approach to the individual identification of the digital image's owner based on embedded biometric data of his voice [19]. Many articles undertake the issue of watermarking video data [36, 46], e.g. [52] use a 3D Wavelet transform for blind watermarking, taking into account the Human Visual System (HVS) properties. Proper use of the digital data watermarking technique [25] allows for advanced localization ways and, as a result, for the identification of a person who is copying a movie illegally. Thanks to the use of the geometric distortion estimation model, Min-Jeong Lee, Kyung-Su Kim and Heung-Kyu Lee obtained high accuracy of location of the in–theatre pirate, confirmed experimentally.

Watermarking of audio data is a noticeably less popular field when compared to watermarking of digital images or video. However, an example may be given of an interesting algorithm [42] which uses phase drift modulation, obtaining high robustness against different types of attacks, including transmissions through UKF data channels. Relatively smallest is the amount of articles on watermarking texts [20, 39, 54] and 3D objects [40].

In terms of human perception, digital data watermarking methods may be divided into perceptible and imperceptible algorithms. In addition, imperceptible methods may be further divided into those which use the perceptual models of a human being [4, 55]—the Watson model may be given as an example [16, 43]. There are many methods which do not take into account the perceptible models [9, 17, 18, 27].

In terms of the decoder type, we may differentiate between non-blind algorithms [21, 47] which require an original image and secret keys. Semi-blind algorithms [41] require secret keys and a watermark bit sequence. By analogy, blind algorithms (such as [11, 26]) do not require additional elements for decoding processing.

In terms of robustness, we may differentiate between robust, fragile and semi-fragile algorithms. Fragile algorithms aim at discovering and locating the changes introduced in a watermarked picture [18]. The aim of semi-fragile al-

gorithms is to detect and locate the area which has been changed in the watermarked picture, at the same time providing sufficient robustness so that the additional information is not removed by the most basic image processing (such as [8, 31]). In addition, it should be mentioned that the problem of algorithm robustness may not be based on the knowledge about the functioning of the encoder and decoder [6, 45].

The proposed algorithm may be referred to as parallel, imperceptible, blind, robust, digital images watermarking method. Parallel—because it embeds additional information in a parallel way in the spatial and frequency domain. The main factor motivating the use of a parallel watermark embedding via the proposed way was the mutual complementing of robustness, offered by processing in the spatial and frequency domains. For example, processing in the spatial domain gives weak robustness of the watermarked picture against lossy compression, but a very good one against cropping because of the fact that the watermark is spread over the entire picture. At the same time, when processing the original picture in the frequency domain we gain robustness of the watermarked picture against a change of resolution or the adding of noise. The decoder functions based on 2D cepstrum dependences and the dependences occurring between 2D coefficients of the cosine transform. The beginning of the cepstrum analysis is marked for the 60's [2]; analyzing the field of digital image watermarking we find a small number of examples of using the Cepstrum [23, 53, 57] (used mainly for processing audio signals [37, 49]).

The article is organized as follows: Sect. 2 provides the mathematical description of the algorithm—the processes of encoding and decoding; Sect. 3 describes invisibility, effectiveness and robustness tests of the method. Section 4 contains a summary of the article.

2 A description of mathematical algorithm

2.1 Coding process

The initial RGB representation of image I matrix is changed into the matrices of luminance and chrominance.

(A change of representation of the digital image from RGB to YCbCr results from strong correlations between the specific red, green and blue matrices. Using image conversions on the luminance and chrominance matrices, it is possible to separately process two matrices—that of luminance and chrominance).

Then, to the matrix Y_I of image I_{ycbcr} we add the same luminance matrix translated by p_x, p_y (missing lines resulting from the translation are copied) with values reduced by the δ coefficient. This coefficient defines the energy of embedded watermark. To reduce the luminance changes in the watermarked image we have performed a compensation of matrix added. It results in creating the Y_I matrix of the host image while the information bits are contained in the translation values and the sign of the translated matrix.

$$\begin{aligned} Y_{Iw}(x,y) &= Y_I(x,y) \pm Y_I(x+p_x, y+p_y)\delta \\ &\quad \mp Y_I(x,y)[1-\delta]. \end{aligned} \tag{1}$$

During the tests it turned out that the maximum imperceptible values of horizontal and vertical translations could not exceed the value of 6 pixels for which the average PSNR value was 37,0799 dB. Then, on matrix $Cb_I(x,y)$ (sized X by Y) we perform a 2D, discrete cosine transform (DCT):

$$\begin{aligned} Cb_{DCT}(k,l) &= \sum_{x=0}^{X-1}\left[\sum_{y=0}^{Y-1} Cb_I(x,y)b_Y^*(l,y)\right]b_X^*(k,x) \\ Cb_{DCTXY} &= B_X^* Cb_{XY} B_Y^{*T} \\ 0 &< x, y < X-1, Y-1 \end{aligned} \tag{2}$$

x, y—indexes of the discrete spatial position of pixels
k, l—indexes of discrete, 2D frequencies in the image spectrum.

The frequency of changes in the pixels values of image I_w amounts to the sum of product of base matrices $B(k,l)$ multiplied by the corresponding cosine transform coefficients. The base matrices $B(k,l)$ have in their rows the orthogonal vectors of 1D cosine transform:

$$\begin{aligned} b(k,x) &= \alpha(k)\cos\left(\frac{\pi k}{X}(x+0,5)\right), \\ b(l,y) &= \beta(l)\cos\left(\frac{\pi l}{Y}(y+0,5)\right) \end{aligned} \tag{3}$$

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{X}} & \text{if } k=0, \\ \sqrt{\frac{2}{X}} & \text{if } k=1\ldots X-1 \end{cases}$$

$$\beta(l) = \begin{cases} \sqrt{\frac{1}{Y}} & \text{if } k=0, \\ \sqrt{\frac{2}{Y}} & \text{if } k=1\ldots Y-1 \end{cases}$$

Finally, the base matrices of the 2D cosine transform can be defined by the following relationship:

$$B(k,l) = b_X^T(k)b_Y(l) \tag{4}$$

Because part of the algorithm processing DCT uses Human Visual System (HVS), it will be presented in short.

The visual perceptual model is based on measuring three basic types of phenomena [6, 14]: (a) sensitivity, (b) masking, (c) pooling.

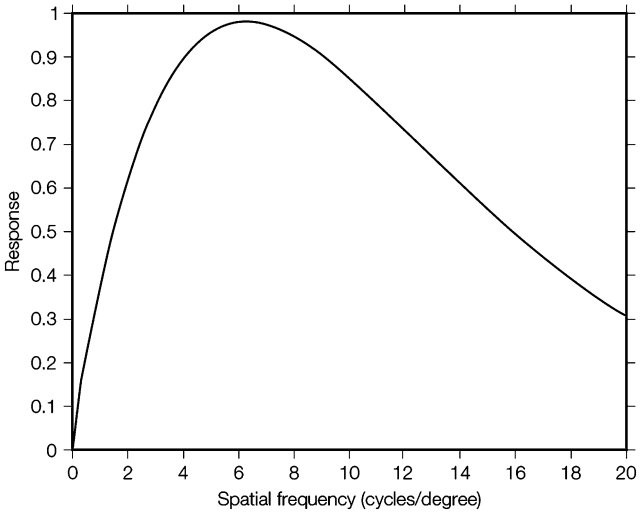

Fig. 2 The graph of the Contrast Sensitivity Function [35]

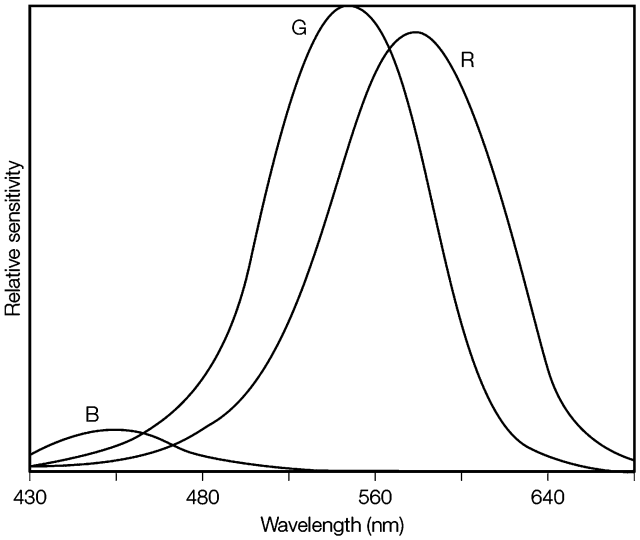

Fig. 3 The three color systems in normal human color vision [6]

Sensitivity refers to the eyes' response to a direct stimulus. In experiments measuring sensitivity, observers watch isolated stimuli and provide the level of their perception. However, in case of the HVS system there exist many stimuli, to which the human eye is sensitive. What is important in the perception ability is not only frequency and the brightness level but also colors, spatial orientation and other parametres. Frequency sensitivity for images is divided for three main frequency types: (a) spatial frequencies, (b) spectral frequencies, (c) temporal frequencies (temporal frequencies are perceived as motion and will not be presented in the article).

Spatial frequencies are perceived by the human being as consistency, image texture. Such a response is referred to as a Contrast Sensitivity Function (CSF) [35] and it has been illustrated at Fig. 2. 2D spatial frequencies of image elements may be presented as a frequency of different patterns, but also as their orientation. For example, prof. Campbeell [41] speaks of the eye's sensitivity to spatial frequency orientations. He proves that the human eye is most sensitive to horizontal and vertical line and edge changes. On the other hand, it is least sensitive to changes of lines and edges oriented by 45 degrees. Spectral frequencies are perceived as colors. The way of perceiving color by the human being may be divided into three separate color systems (Fig. 3). We notice that the human being best perceives the green and red colors, while blue—the least. This fact has been used in the second part of the algorithm in the part responsible for processing the 2D cosine spectrum. (Despite the fact that during the processing of the popular lossy compression—the JPEG standard—the Cb matrix is round down the strongest, coefficients in the algorithm are selected in such a way that the processed watermark coefficients were lost only at very low values of the Q coefficient).

Masking is the degree of the observer's response to a stimulus during the impact of a second "masking" stimulus. The content of the image influences its perception: one example might be a passport picture in which the main information is the face of the photographed person. The matter is different if we look for the same face in a photograph from a crowded shopping center. The same rule applies to masking in the perceptual visual model where one object (or a group of objects) may mask another object. There are two main types of masking in images: frequency and brightness masking.

Pooling is the degree to which the human being observes a combination of many frequencies. In the case of masking or sensitivity we have obtained a response to the change of a specific parameter, e.g. Fig. 2.

The phenomena of masking and pooling are used in Watson's model, described in the further part of the article.

Utilizing the properties of the above mentioned human visual system [6] we have chosen the spectrum of matrix Cb to embed information bits, because the human visual system is less sensitive to changes in both chrominances as compared to luminance. In addition, the encoding process took into account the Contrast Sensivity Function based on he model developed by Mannos and Sakrison [35], showing that the human capacity to perceive spatial changes in pixels is most sensitive to horizontal and vertical changes, while being less sensitive to changes occurring at an angle of 45 degrees.

Using the above-mentioned properties in the 2D cosine spectrum there is performed a change in the phase of rescaled coefficients with embedding the following se-

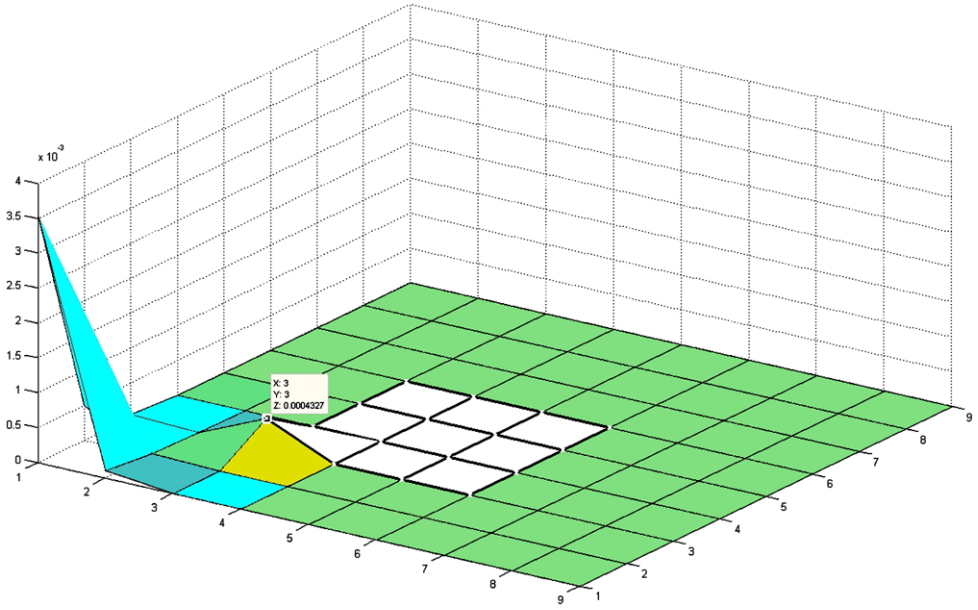

Fig. 4 The graph of two-dimensional cepstral matrix (first row ($p_y = 1$) and column ($p_x = 1$) low quenfrencies coefficients are excluded). Point (3, 3) shows the existence of translated luminance copy at watermarked image luminance matrix

quence of information i_{inf}:

$$Cb_{IwDCT}(k,l) = \begin{cases} |Cb_{DCT}(k,l)| + 256,41\delta & \text{if } bit = 1, \\ -|Cb_{DCT}(k,l)| - 256,41\delta & \text{if } bit = 0 \end{cases} \quad (5)$$

$$3 \leqslant k, l \leqslant 21$$

The δ coefficient value was chosen depending on decides of 17 persons group of observers. The embedded information is preceded by the preamble p_{inf} to provide robustness against false–positive errors.

The next step is to perform the inverse 2D cosine transform:

$$Cb_{Iw}(x,y) = \sum_{x=0}^{X-1}\left[\sum_{y=0}^{Y-1} Cb_{IwDCT}(k,l)b_Y(l,y)\right]b_X(k,x) \quad (6)$$

$$Cb_{IwXY} = B_X^T Cb_{IwDCTXY} B_Y$$

The last step is to change image representation $Cb_{Iw}(x,y)$ into RGB to create watermarked image.

In turns, matrices $YCbCr$ are changed into the RGB representation to create watermarked image I_w.

2.2 Decoding process

The first step is to change the range of watermarked image pixels from 24 to 48 bits and to increase the dynamics of pixel value:

$$I_w(x,y,z) = I_w(x,y,z)^2 \quad (7)$$

Then, a 2D discrete Fourier transform of image I_w luminance is performed:

$$Y_{DFT}(k,l) = \sum_{x=0}^{X-1}\left[\sum_{y=0}^{Y-1} Y_I(x,y)b^*_{DFTY}(l,y)\right]b^*_{DFTX}(k,x)$$

$$Y_{DFTXY} = B^*_{DFTX} Y_{XY} B^{*T}_{DFTY} \quad (8)$$

$$b_{DFT}(k,x) = \sqrt{\frac{1}{X}}\exp\left(j\frac{2\pi k}{X}x\right), \quad b_{DFT}(l,y) = \sqrt{\frac{1}{Y}}\exp\left(j\frac{2\pi l}{Y}y\right) \quad (9)$$

Another step is to transform $Y_{DFT}(k,l)$ into the 2D cepstrum domain (the cube of two-dimensional autocepstrum function of the matrix $Y_{DFT}(k,l)$):

$$Y_{cepstr} = \left(IDFT\left(\ln\left(\left|Y_{DFT}(k,l)\right|\right)\right)\right) \quad (10)$$

$$I_{IDFT}(x,y) = \sum_{x=0}^{X-1}\left[\sum_{y=0}^{Y-1} I_{DFT}(k,l)b_{DFTY}(l,y)\right]b_{DFTX}(k,x) \quad (11)$$

If in matrix $Y_{Iw}(x,y)$ there is a translated luminance copy $Y_I(x+p_x, y+p_y)$, then the coefficient with cepstral coordinates (quefrencies) that equals to translation $Y_{(p_x,p_y)} \leftrightarrow Y_{cepstr(p_x,p_y)}$ reaches considerably higher values than the matrix mean calculated in the 2D Cepstrum domain (excluding the low-frequency components—$p_x, p_y < 4$), (Fig. 4). If the value of this coefficient exceeds the threshold

τ then, the picture $I_w(x, y, z)$ is interpreted as watermarked. On one hand there is a limitation of maximum translation to 6 pixels (the changes become perceptible for insufficiently large pictures), on the other hand there's also a limitation for minimum translation to 3 pixels. It results from the property of non-linear Cepstrum transform that translates the low-frequency Fourier spectrum components into the low 2D quefrencies that cannot be exceeded by cepstral coefficient value (responsible for the translated luminance copy). Additionally the sign of added and translated matrix $Y_I(x + p_x, y + p_y)$ determines the phase of the coefficient $Y_{cepstr(p_x,p_y)}$. As a result, we receive a matrix in a 2D cepstral space with 4 rows and columns, preserving the coefficient phase and providing data payload of the method at a level of $L_{pinf} = 5$ bits. The hidden information is defined by spatial position $Y_{cepstr(p_x,p_y)} \geqslant \tau$ and the coefficient sign.

$$L_{pinf} = \log_2(32) = 5\text{bits} \tag{12}$$

When $Y_{(p_x,p_y)} \leqslant \tau$ there is calculated two-dimensional discrete cosine transform of chrominance Cr for image I_w, the sequence of preamble p'_{inf} is extracted according to the following rule:

$$p'_{inf} = \begin{cases} 1 & \text{if } Cb_{IwDCT}(k,l) \geqslant 0, \\ 0 & \text{if } Cb_{IwDCT}(k,l) < 0 \end{cases} \tag{13}$$

If p'_{inf} equals to p_{inf} (if it does not equal, the picture is rotated by 90°), then the extracted sequence i'_{inf} is the decoder's sense.

3 Tests

The tests have been performed by applying the detector to 100 images with a smaller picture size of 1000 pix. Attempting to analyze the tests there is a need of understanding what the following watermark attack types consist in affine transforms, responsible for translation, scaling, shearing and rotation. Let's consider digital image I sized X by Y pixels with a color depth of 24 bits represented as matrix:

$$I = i(x, y, z) \tag{14}$$

$i \in I; x, y \in X, Y; z$—$RGB$ matrix number

Geometrically distorted pixels of image I_g can be expressed in the following way:

$$\begin{bmatrix} x_g \\ y_g \\ 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

Coefficients a correspond to the matrix elements of affine transform (translation, scaling, shearing and rotation) of image I. Depending on their type they can adopt the following form:

$\begin{bmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{bmatrix}$ —translation matrix,

$\begin{bmatrix} s_x & 0 & 0 \\ 0 & s_y & 0 \\ 0 & 0 & 1 \end{bmatrix}$ —scaling matrix,

$\begin{bmatrix} 1 & sh_x & 0 \\ sh_y & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ —shearing matrix,

$\begin{bmatrix} \cos(q) & -\sin(q) & 0 \\ \sin(q) & \cos(q) & 0 \\ 0 & 0 & 1 \end{bmatrix}$ —rotation matrix of q angle

In addition, there are tests performed for robustness against: cropping—removing pixels lines and columns from the picture edges, desynchronization—removing lines and columns inside the image, lossy JPEG compression depending on the scaling coefficient for quantization matrix. Other attacks include adding noise to the watermarked image in the following three types (Gauss, speckle, salt & pepper and changing their variance) and median filtering depending on the mask size used.

3.1 PSNR, BER

To basically measure the differences between two digital images there is used the term of peak signal to noise ratio (PSNR) expressed in a logarithmic scale. It can be defined in the following way:

$$RMS = \frac{1}{XY} \sum_{i=1}^{N} \sum_{j=1}^{M} \left[\left(I(i, j) - I_w(i, j) \right)^2 \right] \tag{15}$$

$$PSNR = 20 \lg_{10} \left(\frac{I_p}{RMS} \right) [dB] \tag{16}$$

X, Y—spatial resolution of the images compared: the host and watermarked, I_p—peak value (number of color quantization levels), RMS—root mean square.

To define the transfer quality in telecommunications we use the Bit Error Ratio (BER) coefficient. This can be defined as the number of bits received divided by the total number of bits transferred.

3.2 False–positive tests

The tests begin from defining a probability of false-positive (FP) decoder error. The detection theory specifies that this error occurs in the case of the decoder that interprets an image as watermarked, in spite of the fact that the picture possesses no additional information. The probability of false–

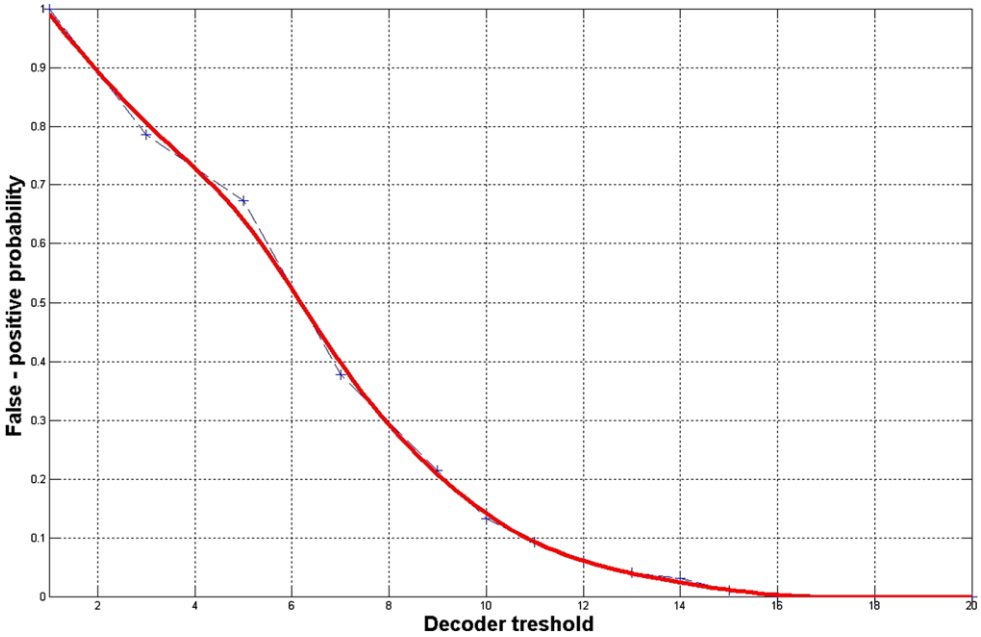

Fig. 5 The probability of false–positive error for decoder operation with unwatermarked pictures

positive error P_{FP} of the threshold method can be defined in the following way [28]:

$$P_{FP} = P\{D_{max} > \tau\} \tag{17}$$

D_{max}—decoder decisions for working on unwatermarked images, τ—decoder threshold.

False–positive test consists in testing 1000 unwatermarked images and checking whether the decoder has interpreted it as watermarked. Zero probability of false–positive error was obtained for decoder threshold $\tau = 16$ and this value was adopted in the algorithm (Fig. 5).

3.3 Imperceptibility

Imperceptibility is one of the trade off components (imperceptibility, data payload, robustness). In order to measure the imperceptibility of proposed algorithm there have been calculated the differences between two images. A more advanced criterion than PSNR was used—Watson's distance, calculated on the basis of Watson's model [6].

Watson's visual model is based on a two-dimensional discrete cosine transform and is block–oriented (the image is divided into blocks and calculations are performed for each block). It uses the perceptual visual model, however its aim is to set a Just Noticeable Difference (JND) between two images. At first this model was supposed to be used in the JPEG standard in order to choose a suitable compression level for a given image using JND between the uncompressed image and further compressed ones. It did not, however, find application in this standard.

The Watson visual model consists of four levels and each of them allows one to specify in a more exact way the manner of perceiving differences between images by a human being. After initial block–processing, the model consists of the following elements: (a) sensitivity, (b) luminance masking, (c) contrast masking, (d) Watson distance.

3.3.1 Watson model—sensitivity

The two-dimensional discrete cosine transform concentrates energy in low–frequency transform coefficients for each block. The DCT 2D coefficient with zero coordinates carries with it information about the image's mean intensity level. The model defines a t frequency sensitivity matrix of each transform coefficient for each block $G_{u,v}$.

Each $t(k,l)$ matrix element (Fig. 6) is approximately the smallest change of DCT 2D coefficients which does not introduce noticeable noise to the image after conducting the operation of inverse two-dimensional discrete cosine transform (IDCT 2D). Thus, it is assumed that each change of DCT 2D coefficients of each of the original image blocks introduces a single JND. When analyzing the t matrix it may be noted that the eye is more sensitive to low-frequency coefficients and to coefficients responsible for the image's vertical and horizontal elements (JND allows for a smaller scope of changes for these coefficients). The t matrix is a function of very many parameters [41], e.g. image resolution, lighting, distance from the image, imaging form (e.g. a picture on chalk overlay paper is perceived differently from one displayed on a screen), etc.

3.3.2 Watson visual model—luminance masking

In the second stage of the Watson model, the property of signal masking is used. Watson takes into consideration the

fact that the $t(k,l)$ can be changed by a greater value if the average intensity of $G_{u,v}$ is brighter. In order to numerically specify the scope of JND changes, sensitivity tables $t(k,l)$ are taken into account, as well as the luminance level against the mean image luminance for each block $G_{u,v}$ (Fig. 6).

$$t_L(k,l)_{u,v} = t(k,l)\left[X_{DCTu,v}(0,0)/X_{DCT}(0,0)\right]^{\alpha_T} \quad (18)$$

$X_{DCTu,v}(0,0)$—mean luminance of each block $G_{u,v}$, $X_{DCT}(0,0)$—mean luminance of the entire image I I, α_T—constant, its value has been determined experimentally and equals 0.649.

	l=0	l=1	l=2	l=3	l=4	l=5	l=6	l=7
k=0	1,40	1,01	1,16	1,66	2,40	3,43	4,79	6,56
k=1	1,01	1,45	1,32	1,52	2,00	2,71	3,67	4,93
k=2	1,16	1,32	2,24	2,59	2,98	3,64	4,60	5,88
k=3	1,66	1,52	2,59	3,77	4,55	5,30	6,28	7,60
k=4	2,40	2,00	2,98	4,55	6,15	7,46	8.71	10,17
k=5	3,43	2,71	3,64	5,30	7,46	9,61	11,58	13,51
k=6	4,79	3,67	4,60	6,28	8,71	11,58	14,50	17,29
k=7	6,56	4,93	5,88	7,60	10,17	13,51	17,29	21,15

Fig. 6 DCT 2D frequency coefficients sensitivity matrix $t(k,l)$ of specific DCT 2D coefficients

3.3.3 Watson visual model—contrast masking

Contrast masking is a change in the perception of the image by the observer through a frequency coefficient correction proportional to the energy occurring in it. Frequencies coefficients with higher values may be changed in a broader scope before achieving JND. Contrast masking is described as the function:

$$s(k,l)_{u.v} = \max\left(t_L(k,l)_{u,v}, \left|X_{DCTu,v}(k,l)\right|^{w(k,l)}\left|t_L(k,l)_{u,v}\right|^{1-w(k,l)}\right) \quad (19)$$

$w(k,l)$—is constant and is included in the scope between 0 and 1. A $w(k,l)$ change matrix may be separately assigned to each DCT 2D coefficient, however in his model Watson assumes the same value for all of them—0.7.

3.3.4 Watson distance

Watson distance is expressed with the formula (20), it is used to calculate the differences between two images, using a more advanced criterion than PSNR. Watson distance is described as the function:

$$D_W(I, I_W) = \left[\sum_{i,j_{u,v}}\left(\frac{I_W[i, j_{u,v}] - I[i, j_{u,v}]}{s(k,l)_{u,v}}\right)^4\right]^{\frac{1}{4}} \quad (20)$$

In the implemented method the value of δ coefficient was selected in such a way to make the watermark imperceptible in the method described. For $\delta = 0{,}78$ the average PSNR (for 100 pictures) after adding the translated luminance copy and Watson distance amounted to 39.31 dB and $4.89 \cdot 10^3$, processing DCT coefficients resulted as 46.84 dB and $1.39 \cdot 10^3$ (Fig. 7).

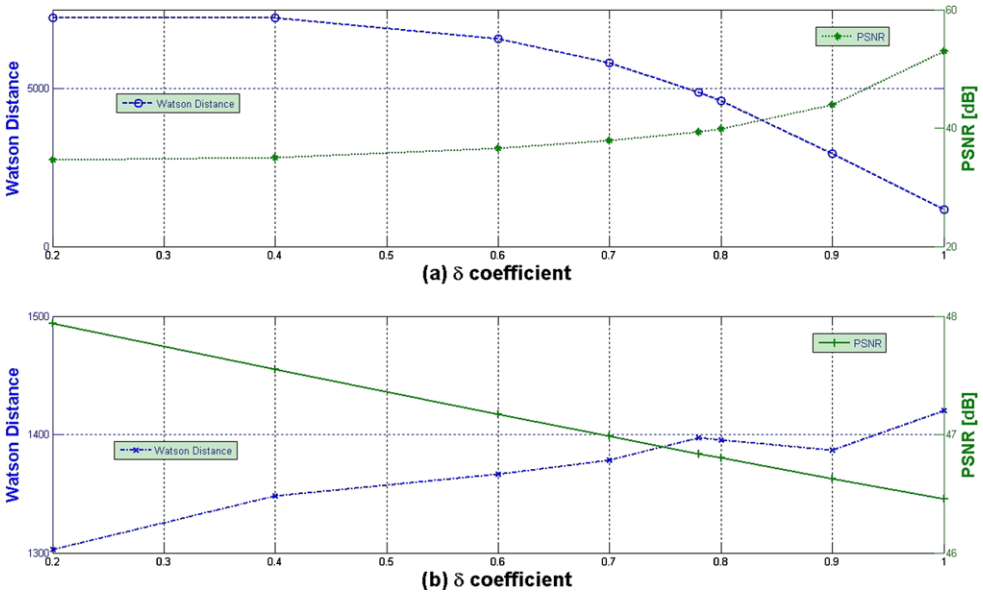

Fig. 7 The graph of Watson distance and PSNR for encoder spatial (**a**) and frequency (**b**) processing, measuring the imperceptibility of proposed algorithm for different δ coefficient values

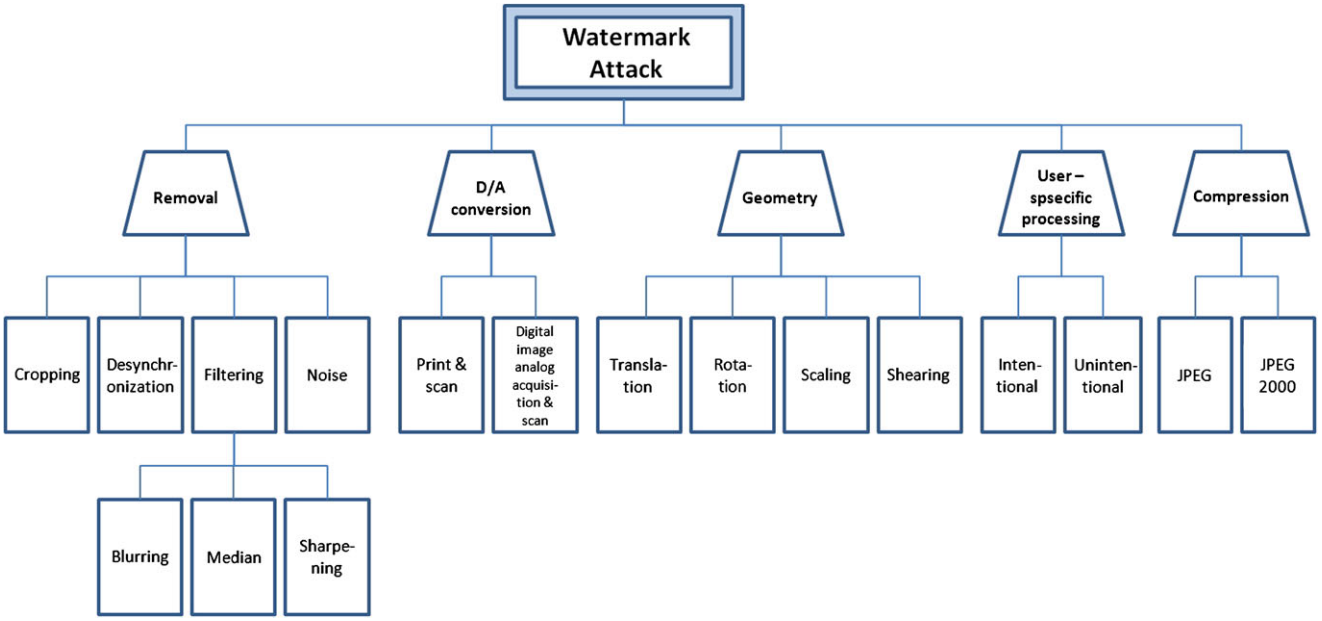

Fig. 8 Classification of watermarked image attacks

3.4 Effectiveness

"A receiver operating characteristics (ROC) graph is a technique for visualizing, organizing and selecting classifiers based on their performance." Tom Fawcett [13].

ROC have been used in detection theory for a long time in order to present the golden mean between two possible accurates and two possible erroneous decoder decisions [12].

The effectiveness of the proposed method is based on ROC curves [13], representing the probability of true–positives, versus the probability of false–positives associated with the preset decoder threshold τ. The translation attacks, cropping and shearing have a low impact on the watermark decoding process in the cepstrum domain. For the above-mentioned processes the probability of true–positives is higher than 90 % (shearing 10 %, translation 205 %, cropping 20 %), while for the probability of false–positives $P_{FP} = 1.0\ \%$.

3.5 Robustness

In order to properly determine the robustness of the method, a division of attacks according to five factors has been adopted. These attacks are illustrated in Fig. 8 (taking into account the analysis included in [5]).

Attacks oriented at removal are to process the watermarked image in such a way so as to prevent a simple deletion of the watermark signal from the attacked data. It is the most often tested type of attack for watermarking algorithms. This type of attacks may include a cropping attack (removing image fragments at its edges), desynchronizations (removing fragments inside the image, e.g. rows and columns), adding noise (adding noise to the watermarked image, e.g. salt & pepper, Gauss, Speckle) and filterings commonly used during image processing in photography—blurring corresponding to the two-dimensional low-pass filtration and sharpening corresponding to high-pass filtration. A special case of filtration is median filtering—non-linear, order–statistic. It is the most often one because it effectively reduces noise occurring in the image, thanks to which it is readily used for image smoothing. However, at the same time it may prevent the detection of embedded information due to the fact that the watermarking signal usually has low energy, introducing noise to the original image. Therefore, conducting median filtrations watermarking detection may be distorted.

Attacks of simple and inverse digital-analog conversion consist of print and scan-type attacks and attacks which include an analog obtaining of the digital image and processing it to a digital form. There are algorithms dedicated to robustness against simple and inverse D/A conversion attacks [48, 56]. This type of attacks is deemed as complex in which many factors influence a watermarked image—in case of a print and scan-type attack of considerable importance are the properties of printing and scanning processes, as well as the resulting distortions of pixels included in affine transform matrices.

Geometric attacks, as opposed to removal attacks, are aimed mainly at distorting the decoding process or causing the search for signal watermark by the decoder to become fruitless and slow.

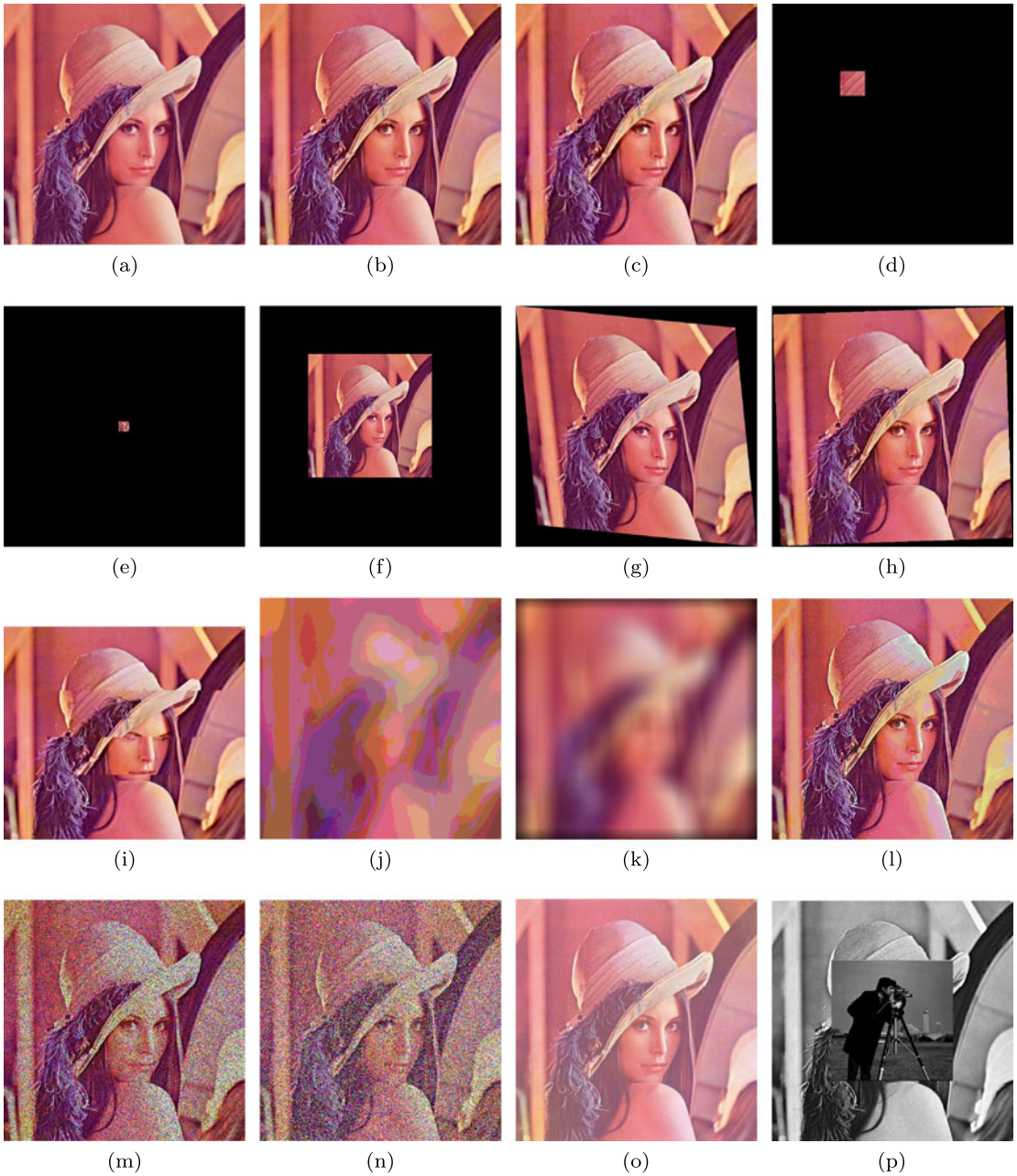

Fig. 9 Pictures: (**a**) host image; (**b**) watermarked image. Types of attacks performed: (**c**) JPEG compression, $Q = 20$; (**d**) XY cropping [10 % 10 %]; (**e**) XY change of resolution 4 %; (**f**) translation 200 %; (**g**) XY shearing 10 %; (**h**) 2° rotation; (**i**) 60 rows desynchronization; (**j**) Low Pass filtering; (**k**) average filtering, mask size [50 50]; (**l**) High Pass filtering; (**m**) speckle noise $mean = 0$, $var = 0.4$; (**n**) salt & pepper noise, $var = 0, 4$; (**o**) simple & inverse D/A conversion attack; (**p**) photomontage attack, coefficient equal 0.5; (**d**) and (**e**) attacked pictures are compared to host image resolution

Lossy compression attacks are especially important—because of its special popularity—another compression of the watermarked image cannot erase the additional information. In the case of images we may distinguish two compressions: JPEG (currently the most popular one because of its simplicity and good effectiveness) and JPEG2000 (with bigger possibilities than JPEG, e.g. better image compression coefficients with a considerably better quality; however, it is not yet popular because of its calculating complexity).

Attacks dependent on the user may be divided into two types—unintentional when the authorized user processes an image during normal use and intentional aimed at removing or hindering the decoding of a watermark. These attacks may be presented as a multielement composition of removal, geometric and lossy compression attacks.

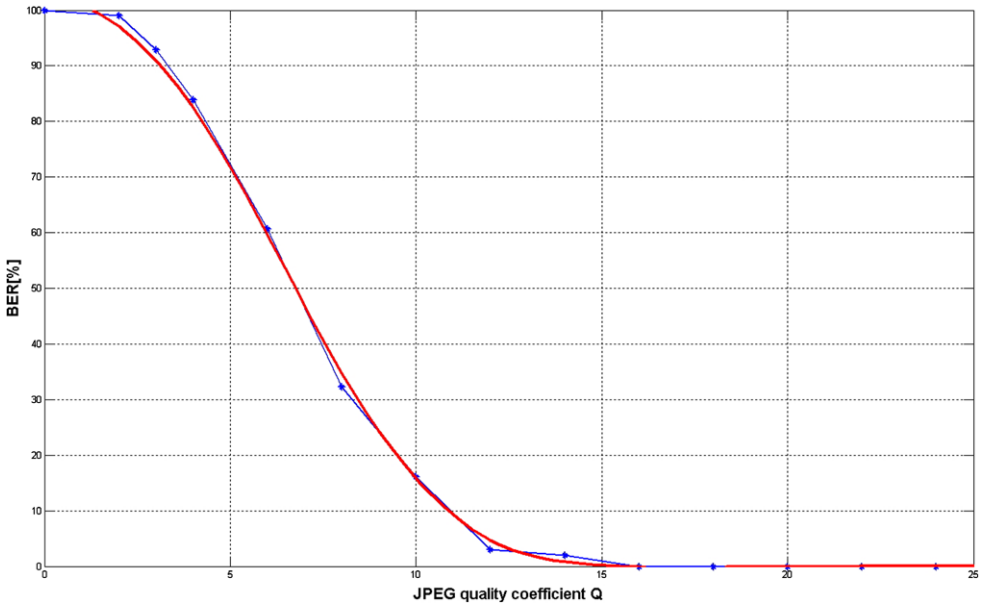

Fig. 10 The graph of BER versus JPEG compression factor

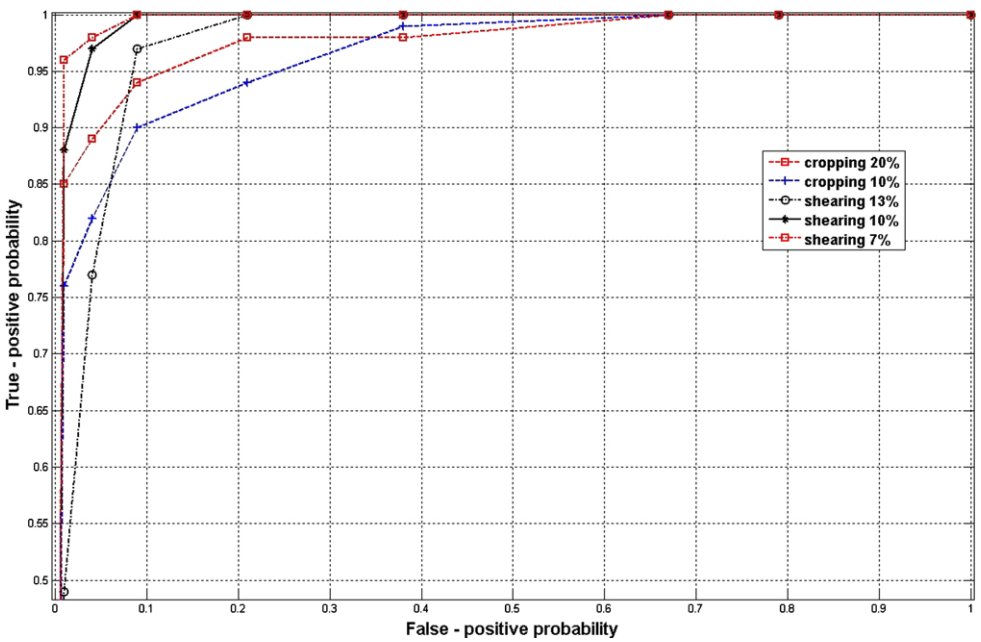

Fig. 11 ROC curves: cropped watermarked image (BER equals 4.29 % and 8.59 % for 20 % and 10 % cropping ratio) sheared watermarked image (BER equals 5.1 % and 0 % for 10 % and 7 % shearing)

The tests of robustness cover the attacks of rotation, scaling, shearing, translation, cropping, lossy JPEG compression, desynchronization, adding noise to the signal and median filtering. In addition, we have performed the test of digital/analog and analog/digital conversion (for *lena* image). Figure 9 presents some examples of the attacks performed (for each distorted watermarked image BER equals 0 %).

The JPEG compression standard makes it possible to increase the compression ratio of digital pictures with perceptible loss in image quality Fig. 9(c). At (Fig. 10) there is presented a BER diagram versus the scaling coefficient of quantization matrix, it is easy to note that for JPEG compression factor $Q > 20$, the BER amounts to 0 %.

Robustness against cropping attack results from the fact that the watermark (reduced energy luminance copy) is added to the whole luminance matrix and its cropping has a low effect on the decoding process. After strong XY cropping of approx. [10 % 10 %] decoder is still possible to obtain 80 % probability of true–positive, at 1.0 % false–positives errors. It is clearly shown at Fig. 11.

Because of the fact that picture low-frequency DCT spectrum coefficients are changed, the watermarked image is robust to a wide range of scaling (Fig. 14). Downscaling does not result in removing them, while up scaling results in the redundancy of spectrum matrix and has no effect on the decoding process.

The attacks of desynchronization involved removing 60 rows (numbers: 156 : 166, 256 : 266, 356 : 366), as a result is obtained the perfect effect of embedded information decoding, BER = 0 % (an example is shown at Fig. 9(i)).

Robustness tests of the method against sharpening—corresponding to high-pass filtering—were carried out. For the filtering matrix, calculated based on the formula (21), all the images have been correctly decoded ($BER = 0$ %, $PSNR = 25.49$ dB, $\alpha = 2$).

$$\frac{1}{(\alpha+1)}\begin{bmatrix} -\alpha & \alpha-1 & -\alpha \\ \alpha-1 & \alpha+5 & \alpha-1 \\ -\alpha & \alpha-1 & -\alpha \end{bmatrix} \tag{21}$$

Blurring tests were carried out—corresponding to low-pass filtration. For the filtering matrix presented in Fig. 13, the obtained BER equaled 0 %, the mean PSNR—30.21 dB.

A photomontage attack differs from a cropping attack in that to a watermarked image there is add another one; therefore the results for photomontage are considerably worse than for cropping although in both cases the watermark's energy becomes reduced. This results from the fact that in a photomontage attack an additional signal, distorting the decoding process, is added to the watermarked signal. In this type of attack a photomontage coefficient was used, calculated from the formula (22) showing the absolute number of

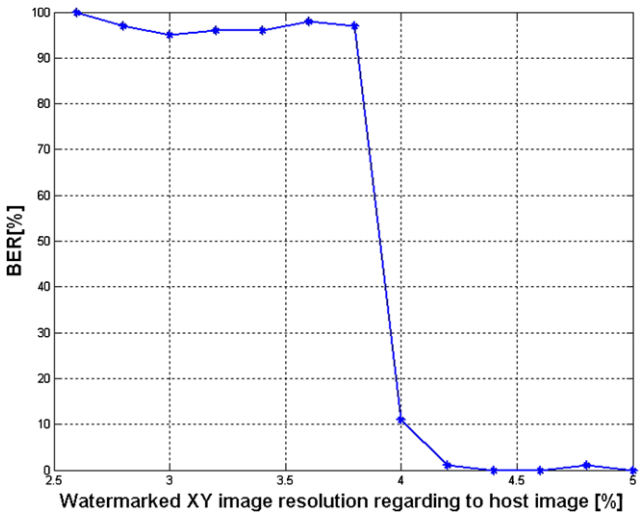

Fig. 12 BER versus watermarked image scaling ratio

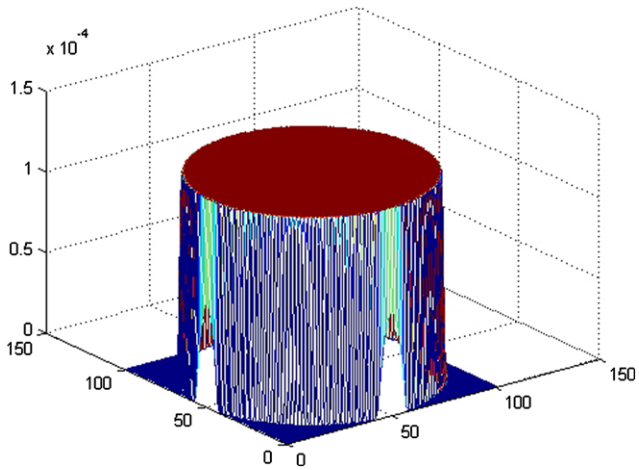

Fig. 13 Low Pass filter used for blurring attack

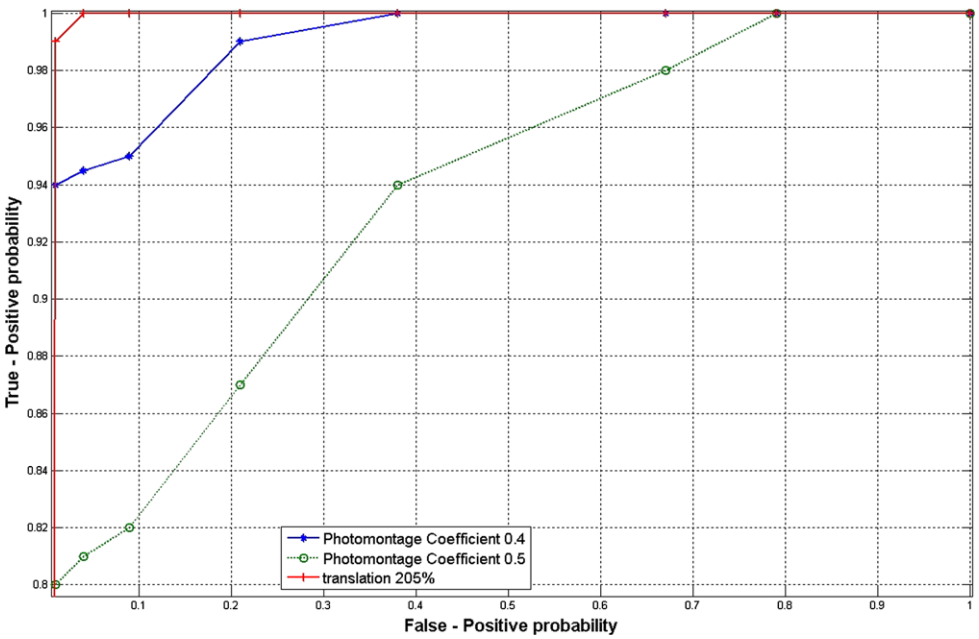

Fig. 14 ROC curves for watermarked image after photomontage attack and translation attack (BER equals 0.93 % for 205 % translation and 2.2 % and 7.27 % for 0.4 and 0.5 photomontage coefficient value)

the embedded image to the watermarked image.

$$C_p = \frac{I_p}{I_{wm}} \tag{22}$$

I_p—coefficient of the embedded image $(x_p y_p)$, I_{wm}—coefficient of the watermarked image $(x_{wm} y_{wm})$. The obtained ROC characteristics for this type of attack are illustrated in Fig. 14.

Robustness tests were carried out of the algorithm against a JPEG2000 compression attack. The results are illustrated in Fig. 15 showing a high algorithm robustness.

The algorithm is robust against median filtering attack. Filtering has been performed for the averaging filter mask sized [50 50]. The obtained BER is 0 %.

For experimental reasons there have been performed the process of digital/analog conversion and vice versa. Three pictures were printed on regular A4 size paper (with 300 dpi print resolution), and then they were scanned at a resolution of 300 dpi. The results were as follows: BER = 5.56 %, PSNR = 28.21 dB (after rescaling to the host image resolution).

The robustness against the translation attack, like in the case of cropping and shearing, results from using the cepstral processing. After 205 % translation attack decoder is still possible to obtain 98 % probability of true–positive, at 1.0 % false–positive (Fig. 14).

Also algorithm is robust against shearing attack. For shearing ratio of 10 % (Fig. 16) BER equals 5.1 %, for 7 %

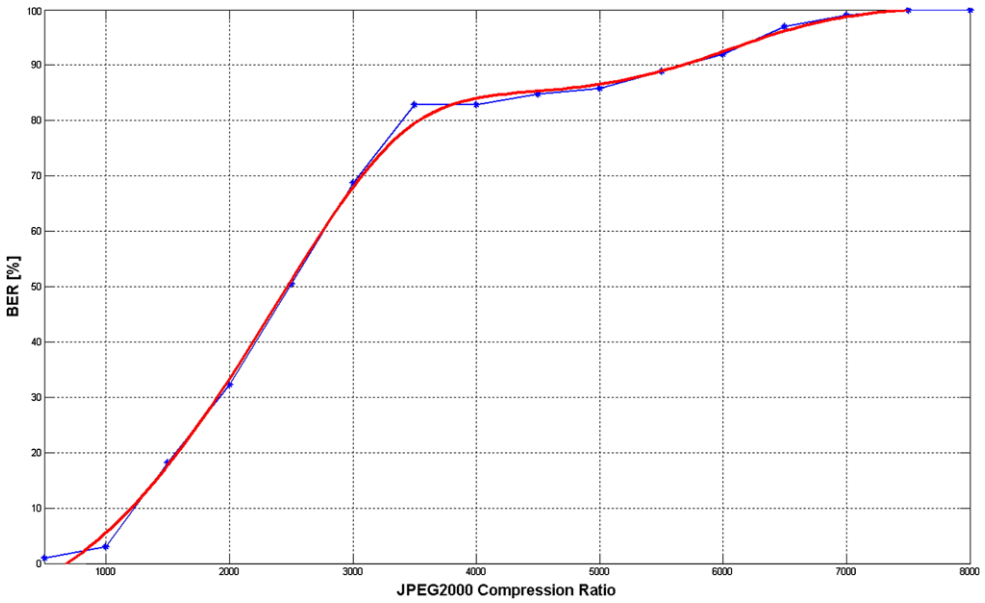

Fig. 15 The graph of BER versus JPEG2000 compression ratio

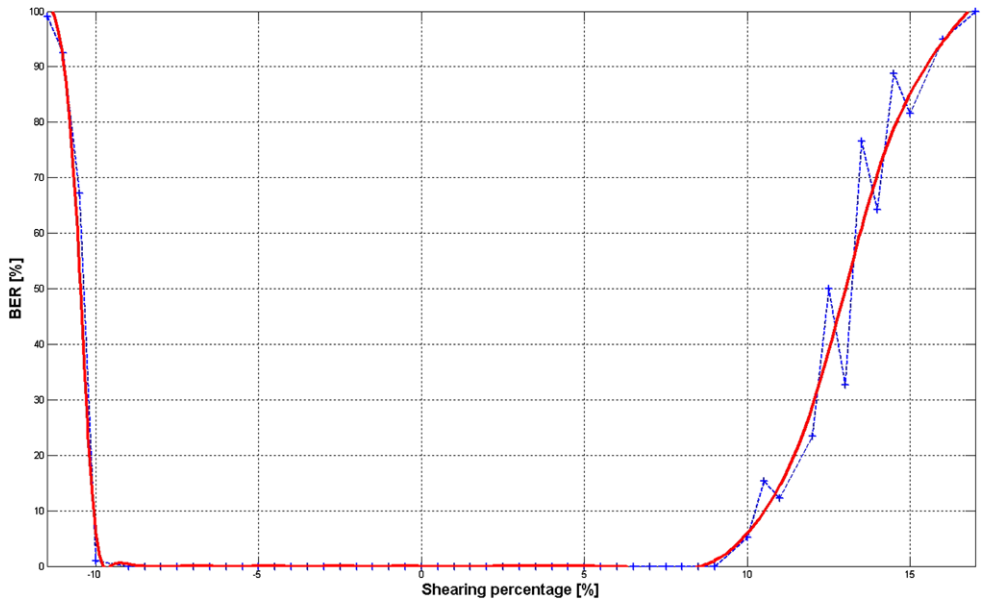

Fig. 16 BER versus the ratio of XY shearing

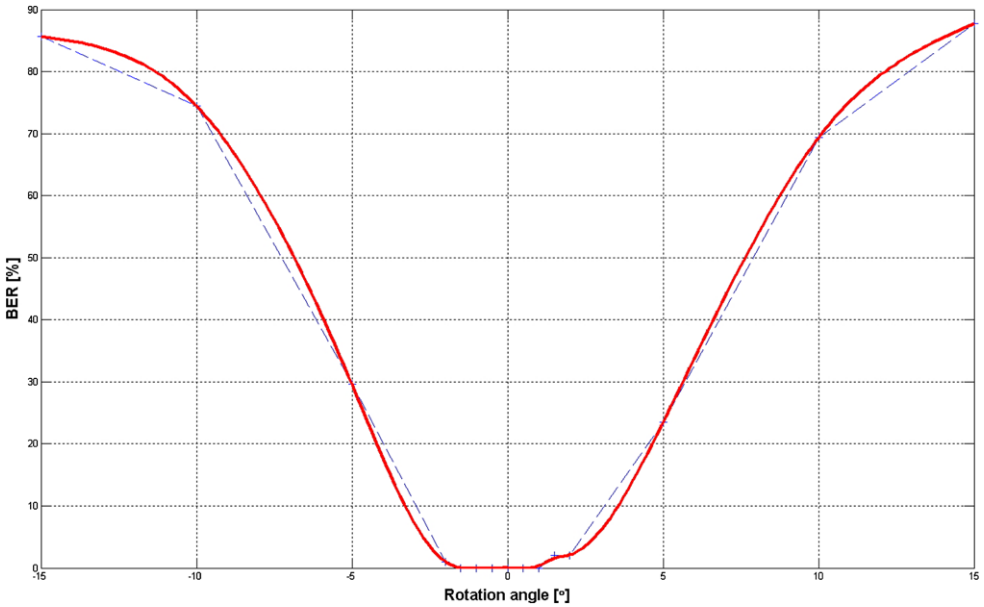

Fig. 17 BER versus the angle of watermarked image rotation attack

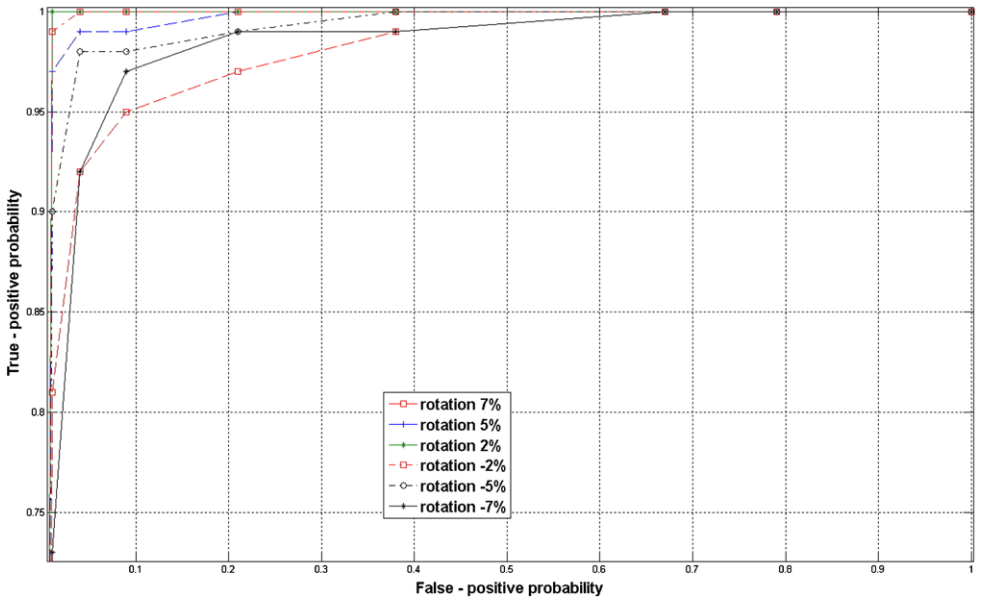

Fig. 18 ROC curves for watermarked images after rotation attack (BER equals 0 % for ± 2 % rotation angle)

shearing ratio the decoding process does not produce errors (Fig. 16), (example is shown at Fig. 9(g)).

The algorithm is robust against the attack of watermark image rotation of maximum rotation angle $\pm 2°$—obtained result is 0 % BER (Fig. 17). Receiver Operating Curves for rotation attack are shown at Fig. 18. Also decoder is robust against trivial attack of 90° rotation.

There have been performed the tests of adding noise to the watermarked image. Algorithm is highly robust against this kind of attack. Examples are shown at Fig. 9(m) for speckle and Fig. 9(n) salt & pepper noises. BER results are shown at Table 1.

Moreover, a comparison was carried out of the described algorithm with three methods of watermarking pictures, including Cox's [7] and Malvar's [34] algorithm for a standard Lena picture. The results are illustrated in Table 2: and show that the proposed algorithm is more robust against the most typical attack, i.e. JPEG lossy compression. Furthermore, the robustness of the proposed algorithm against a change

Table 1 BER versus adding noise to the watermarked image

Noise type	Salt & pepper	Gauss	Speckle
Parameters	$var = 0.4$	$mean = 0$; $var = 0.4$	$mean = 0$; $var = 0.4$
BER [%]	0.10	$2.00 \cdot 10^{-3}$	$4.00 \cdot 10^{-2}$

Table 2 Test results for the Lena picture, showing the percentage of properly decoded pictures

Attacks	Our scheme (%)	[7] (%)	[34] (%)	[33] (%)
JPEG ($Q = 50$)	100	88.5	91.5	95.5
Gaussian Low Pass Filter	100	100	100	100
Gaussian Noise (0.006)	100	94.5	95	99
Salt & Pepper Noise (0.4)	90	93	92	96
Rotation (40°)	0	84	86.5	100
Resizing (1.2)	100	76	71	100

of resolution, Gauss noise and low-pass filtering exceeds the remaining three algorithms.

4 Conclusions

Modern techniques of protecting digital data copyrights are related to the subject of digital watermarking. The key element is to work out a suitable algorithm which fulfill high requirements of the DRM application. The article presents a mathematical description of a robust parallel watermarking algorithm, embedding additional information in the spatial and frequency domain. Results were presented of the method's invisibility measurements, thorough effectiveness tests and robustness tests. High robustness was shown of the algorithm to attacks of desynchronization, low-pass filtering, high-pass filtering, median filtering, noise, translation attacks, rotation, shearing, lossy compressions—JPEG and JPEG2000, simple and inverse D/A conversion. Attention should be drawn to the high robustness of the algorithm against cropping and scaling attacks. In addition, a division was presented of watermarking techniques, attack types, and a photomontage–type new attack was proposed and tested, dependent on the photomontage coefficient.

References

1. Barni, M., Bartolini, F., & Piva, A. (2002). Multichannel watermarking of color images. doi:10.1109/76.993436.
2. Bogert, B. P., Healy, M. J. R., & Tukey, J. W. (1963). The quefrency analysis of time series for echoes: cepstrum, pseudo autocovariance, cross-cepstrum and saphe cracking. In M. Rosenblatt (Ed.), *Proceedings of the symposium on time series analysis* (pp. 209–243). New York: Wiley. Chap. 15.
3. Cheung, W. N. (2010). Digital image watermarking in spatial and transform domains. In *TENCON 2010*. doi:10.1109/TENCON.2000.892292.
4. Chou, C.-H., & Liu, K.-C. (2010). A perceptually tuned watermarking scheme for color images. doi:10.1109/TIP.2010.2052261.
5. Chunlin, S., Sudirman, S., Merabti, M., & Llewellyn-Jones, D. (2010). Analysis of digital image watermark attacks. In *CCNC 2010*. doi:10.1109/CCNC.2010.5421631.
6. Cox, I. J., & Miller, M. L. *Digital watermarking and steganography* (2nd ed.). MK; ISBN 978-012-372585-1.
7. Cox, I. J., Kilian, J., Leighton, J., & Shamoon, F. T. (1997). Secure spread spectrum watermarking for multimedia. doi:10.1109/83.650120.
8. Cruz, C., Reyes, R., Nakano, M., & Perez, H. (2008). Image content authentication system based on semi-fragile watermarking. In *MWSCAS 2008*. doi:10.1109/MWSCAS.2008.4616797.
9. Deshpande, N., Rajurkar, A., & Manthalkar, R. (2010). Robust DCT based video watermarking algorithms for assorted watermarks. In *ICSPS 2010*. doi:10.1109/ICSPS.2010.5555632.
10. Deshpande, N., Rajurkar, A., & Manthalkar, R. (2010). Robust DCT based video watermarking algorithms for assorted watermarks. In *ICSPS 2010*. doi:10.1109/ICSPS.2010.5555632.
11. Dorairangaswamy, M. A., & Padhmavathi, B. (2009). An effective blind watermarking scheme for protecting rightful ownership of digital images. In *TENCON 2009*. doi:10.1109/TENCON.2009.5395812.
12. Egan, J. P. (1975). *Signal detection theory and ROC analysis*. *Series in cognition and perception*. New York: Academic Press.
13. Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, *27*, 861–874. doi:10.1016/j.patrec.2005.10.010.
14. Gonzalez, R. C. (2002). *Digital image processing* (2nd ed.). Englewood Cliffs: Prentice Hall. ISBN 0201180758.
15. Hu, T., & Wei, J. (2010). A digital video watermarking scheme based on 1D-DWT. In *ICBECS 2010*. doi:10.1109/ICBECS.2010.5462403.
16. Hu, R., Chen, F., & Yu, H. (2010). Incorporating Watson's perceptual model into patchwork watermarking for digital images. In *ICIP 2010*. doi:10.1109/ICIP.2010.5652638.
17. Hu, X., Tian, W., Zheng, Y., Lian, X., & Ruan, W. (2010). A blind digital watermarking algorithm based on chaotic systems. In *ICECE 2010*. doi:10.1109/iCECE.2010.11.
18. Hua, Y., Wu, B., & Wu, G. (2010). A color image fragile watermarking algorithm based on DWT-DCT. In *CCDC 2010*. doi:10.1109/CCDC.2010.5498711.
19. Inamdar, V. S., & Rege, P. P. (2010). Speech as a biometric watermark for digital images using stationary wavelet transform. In *ICCTD 2010*. doi:10.1109/ICCTD.2010.5646076.
20. Jalil, Z., Aziz, H., Bin Shahid, S., Arif, M., & Mirza, A. M. (2010). A zero text watermarking algorithm based on non-nowel ASCII characters. In *ICEIT 2010*. doi:10.1109/ICEIT.2010.5607625.
21. Kang, G. S. (2010). Blind digital image watermarking using adaptive casting energy in different resolutions of wavelet transform. In *ICCCT 2010*. doi:10.1109/ICCCT.2010.5640527.
22. Kerr, I. (2007). Hacking@privacy: Why we need protection from the technologies that protect copyright. In *Proc. of conference on privacy and identity*.
23. Koda, H., Ogawa, T., & Sakata, S. (2003). A scheme of oblivious ghost-watermarking based on cepstral analysis and correlation techniques. In *Communications, computers and signal processing (PACRIM 2003)*. doi:10.1109/PACRIM.2003.1235952.
24. Lai, C.-C., & Yeh, C.-H. (2010). A hybrid image watermarking scheme based on SVD and DCT. In *ICMLC 2010*. doi:10.1109/ICMLC.2010.5580777.
25. Lee, M.-J., Kim, K.-S., & Lee, H.-K. (2010). Digital cinema watermarking for estimating the position of the pirate. doi:10.1109/TMM.2010.2061221.
26. Lian, H., Hu, B.-N., Zhao, R.-M., & Hou, Y.-L. (2010). Design of digital watermarking algorithm based on wavelet transform. In *ICMLC 2010*. doi:10.1109/ICMLC.2010.5580639.

27. Liao, Y., & Liu, Q. (2010). Applying dual digital watermarking technology in digital rights management. In *ICIS 2010*. doi:10.1109/ICICIS.2010.5534674.
28. Lin, C., Wu, M., Lui, Y. M., Bloom, J. A., Miller, M. L., & Cox, I. J. (2001). Rotation, scale, and translation resilient public watermarking for images. *IEEE Transactions on Image Processing*. doi:10.1109/83.918569.
29. Ling, L., Sun, X., & Cai, L. (2010). A robust image watermarking based on DCT by Arnold transform and spread spectrum. In *ICACTA 2010*. doi:10.1109/ICACTE.2010.5579033.
30. Liu, K.-C. (2009). Multichannel watermarking for color images by using quantization visibility thresholds. In *IMVIP 2009*. doi:10.1109/IMVIP.2009.19.
31. Liu, X., Lv, X., & Wang, Y. (2008). A semi-fragile digital watermarking algorithm based on integer wavelet matrix norm quantization for medical images. In *ICBBE 2008*. doi:10.1109/ICBBE.2008.189.
32. Liu, G.-q., Zheng, X.-s., Zhao, Y.-l., & Li, N. (2010). A robust digital video watermark algorithm based on DCT domain. In *ICCASM 2010*. doi:10.1109/ICCASM.2010.5619019.
33. Lu, W., Sun, W., & Lu, H. (2011). Novel robust image watermarking based on subsampling and DWT. In *Multimedia tools and applications 2011*. doi:10.1007/s11042-011-0794-1.
34. Malvar, H. S., & Florencio, D. A. F. (2003). Improved spread spectrum: a new modulation technique for robust watermarking. In *TSP 2003*. doi:10.1109/TSP.2003.809385.
35. Mannos, J. L., & Sakrison, J. J. (1974). The effects of a visual fidelity criterion on the encoding of images. *IEEE Transactions on Information Theory*. doi:10.1109/TIT.1974.1055250.
36. Marcinak, M. P., & Mobasseri, B. G. (2005). Digital video watermarking for metadata embedding in UAV video. In *MILCOM 2005*. doi:10.1109/MILCOM.2005.1605909.
37. Marnani, E. K., Karami, Z., & MolavianJazi, E. (2009). A comparison of some audio watermarking methods. In *Electrical engineering, computing science and automatic control (CCE 2009)*. doi:10.1109/ICEEE.2009.5393484.
38. Megalingam, R. K., Nair, M. M., Srikumar, R., Balasubramanian, V. K., & Sarma, V. S. V. (2010). Performance comparison of novel, robust spatial domain digital image watermarking with the conventional frequency domain watermarking techniques. In *ICSAP 2010*. doi:10.1109/ICSAP.2010.79.
39. Meng, Y., Guo, T., Guo, Z., & Gao, L. (2010). Chinese text zero-watermark based on sentence's entropy. In *ICMT 2010*. doi:10.1109/ICMULT.2010.5631421.
40. Nishchal, N. K., Pitkaaho, T., & Naughton, T. J. (2010). Digital Fresnel hologram watermarking. In *WIO 2010*. doi:10.1109/WIO.2010.5582496.
41. Okada, M., Okabe, Y., & Uehara, T. (2010). A web-based privacy-secure content trading system for small content providers using semi-blind digital watermarking. In *CCNC 2010*. doi:10.1109/CCNC.2010.5421697.
42. Piotrowski, Z. (2010). Drift correction modulation scheme for digital audio watermarking. In *Proceedings 2010 second international conference on multimedia information networking and security MINES 2010*. ISBN 978-0-7695-4258-4.
43. Qiao, L. & Cox, I. J., (2007). Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking. doi:10.1109/TIFS.2007.897266.
44. Seddik, H., Sayadi, M., & Fnaiech, F. (2009). A new blind image watermarking method based on Shur transformation. In *IECON 2009*. doi:10.1109/IECON.2009.5414857.
45. Seitz, J. *Digital watermarking for digital media*. Information Science Publishing. ISBN 1-59140-518-1.
46. Singh, R., Vatsa, M., Singh, S. K. b. & Upadhyay, S. (2009). Integrating SVM classification with SVD watermarking for intelligent video authentication. *Telecommunications Systems*, *40*(1–2), 5–15.
47. Subramanyam, A. V., Emmanuel, S., & Kankanhalli, M. S. (2010). Compressed-encrypted domain JPEG2000 image watermarking. In *ICME 2010*. doi:10.1109/ICME.2010.5583571.
48. Tang, Y.-L., & Huang, Y.-T. (2010). Print-and-scan resilient watermarking for authenticating paper-based certificates. In *PCSPA 2010*. doi:10.1109/PCSPA.2010.93.
49. Wei, F. S., & Qi, D. (2009). Audio watermarking of stereo signals based on echo—hiding method. In *Information, communications and signal processing (ICICS 2009)*. doi:10.1109/ICICS.2009.5397487.
50. Wei, J., Yong, S., & Ma, X. (2010). Blind digital watermarking algorithm based on quantization in contourlet domain. In *EBISS 2010*. doi:10.1109/EBISS.2010.54735944.
51. Yuan, X.-C., & Pun, C.-M. (2010). Digital image watermarking scheme based on histogram in DWT domain. In *IDC 2010*. ISBN 978-1-4244-7607-7.
52. Zamanidoost, A., Mirzakuchaki, S., Atani, R. E., Hesabi, Z. R., & Ayat, M. (2010). A novel 3D wavelet-based method for blind digital video watermarking. In *ISIEA 2010*. doi:10.1109/ISIEA.2010.5679471.
53. Zhang, M.-r., & Zhang, Z. Y. (2009). Color image watermarking algorithm in cepstrum domain. In *Intelligence and security informatics (ISI 2009)*. doi:10.1109/ISI.2009.5137310.
54. Zhang, Y., Qin, H., & Tao, K. (2010). A novel robust text watermarking for word document. In *CISP 2010*. doi:10.1109/CISP.2010.5648007.
55. Zhao, H. (2010). Algorithm of digital image watermarking technique combined with HVS. In *ICCSIT 2010*. doi:10.1109/ICCSIT.2010.5563684.
56. Zhou, J., & Pang, M. (2010). Digital watermark for printed materials. doi:10.1109/ICNIDC.2010.5657884.
57. Ziang, M.-r., Lu, C.-h., & Yi, K.-c. (2004). Cepstrum digital image watermarking algorithm. In *Industrial electronics, IEEE international symposium*. doi:10.1109/ISIE.2004.1571821.

Piotr Lenarczyk received the M.S. degree in telecommunication from Military University of Technology, Warsaw, Poland in 2011 and has been participating in the National Network-Centric System Program. His research interests are focused on digital image and real-time video watermarking.

Zbigniew Piotrowski received the M.Sc. and Ph.D. degrees in communications from the Military University of Technology (MUT), Warsaw, in 1996, and 2005 (with honours), respectively. At present he is a DSP engineer in the Telecommunication Institute (EF MUT). His main areas of interest are speech and audio processing, telecommunication systems engineering and information hiding technology.