Fragile and Resistant Image Watermarking Based on Inverse Difference Pyramid Decomposition

Roumen Kountchev
Deptartment of Radio Communications
Technical University of Sofia
Bulgaria
rkountch@tu-sofia.bg
www.tu-sofia.bg

Vladimir Todorov
T&K Engineering
Mladost 3
Pob 12
Sofia 1712
Bulgaria
todorov_vl@yahoo.com

Roumiana Kountcheva
T&K Engineering
Mladost 3
Pob 12
Sofia 1712
Bulgaria
kountcheva_r@yahoo.com

Abstract: - In the paper is presented one approach for image content protection based on layered still image decomposition with Inverse Difference Pyramid (IDP) and digital watermark insertion. Unlike the famous pyramid decompositions (Laplacian, Gaussian, etc.), the IDP starts from the pyramid top, which comprises smallest number of coefficients, and continues with the next decomposition layers (i.e., it represents the processed image with consecutive approximations of increasing quality). The new approach permits the insertion of multiple watermarks in the consecutive decomposition layers (resistant and fragile) and their reliable extraction by authorized users only. The fragile watermark is added as additional information in the corresponding decomposition layers. Any change in the extracted fragile watermark indicates unauthorized image editing. The resistant watermark embedding is performed in the image spectrum phase domain. For this, the decomposition is accomplished with Complex Hadamard Transform (CHT). The resistant watermark is inserted in the transform coefficients' imaginary part, which permits the insertion of relatively large amounts of watermark data in the protected image. The images are transformed into new format, based on the IDP decomposition. This approach affords the opportunity for the successful developing of various applications – image content protection; historical heritage protection; telemedicine and healthcare; transfer of confidential information with restricted access and many others.

Keywords: - Image content protection, image watermarking, multilayer image decomposition, Complex Hadamard Transform, hierarchical access control.

1 Introduction

The contemporary practice for documents management in large enterprises, healthcare institutions, shops, etc., requires the management of huge amounts of documents in electronic form: texts, photos, etc. The traditional approach is to archive the documents, using compression, based on some of the famous standards: JPEG, JPEG 2000, etc. This is a reliable and efficient solution, but the use of documents in electronic form generates various problems, such as the ability for unauthorized access, editing, etc. A supplementary problem is the availability of too much software products, which provide successful image content editing. This state of the art requires the archived files to possess some additional security levels, which ensure reliable content protection, or to permit the detection of any kind of unauthorized edition. The existing digital image watermarking techniques [1, 2, 3, 9] solve these problems to a high degree. Two main kinds of watermarking are used – *resistant*, which usually proves the content ownership, and *fragile*, aimed at the creation of tools which to indicate any kind of image content editing. Various techniques for resistant watermark embedding had been developed and used. Some of them are based on watermarking in the image spectrum phase domain [4]. One similar technique is presented in [14]. This watermarking is based on an iterative phase retrieval algorithm and sine–cosine modulation in the discrete cosine-transform (DCT) domain. The original hidden image is first encrypted into two phase masks. Then the cosine and sine functions of one of the phase masks are introduced as a watermark to be embedded into an enlarged host image in the DCT domain. By extracting the watermark of the enlarged superposed image and decryption we can retrieve the hidden image. Other similar DCT-based methods with watermark insertion in the phase domain are presented in [5]

and [6]. They both confirm the method resistance against various attacks.

For some applications, the watermark extraction is performed without comparison with the original image (blind), while in other cases, the original should be available. The second approach is suitable for documents archiving, because the original image is easily available, when requested, and the comparison ensures reliable watermark extraction [4, 7].

One more approach is the use of a fragile watermark which hides the protected image (or its most important part) and is removed by authorized users only.

This paper presents methods for fragile and for resistant watermarking, based on the Inverse Difference Pyramid Decomposition (IDP) [10,11]. In accordance with this approach, the image is processed layer by layer, and approximations with increasing quality are generated. This permits the insertion of different watermark data in the consecutive decomposition layers.

The watermark technique is selected in accordance with the application: the fragile watermarking is aimed at the protection of medical visual information, because it does not influence the image data and (as a sequence – the image quality), and the resistant watermarking is more suitable for protection of documents and other confidential information. Any change, detected in the extracted fragile watermark proves un-authorized document editing. The resistant watermark should prove the document ownership and can identify unauthorized editing as well.

The paper is arranged as follows: Section 2 introduces the principles of the IDP decomposition; Section 3 is devoted to the method for multi-layer fragile watermarking; Section 4 presents the approach for resistant watermarking; Section 5 provides some experimental results obtained using the software implementations of the methods; Section 6 is the Conclusion.

2 IDP Decomposition

The essence of the IDP decomposition for 8-bit grayscale images is given in brief as follows.

The matrix [B(i,j)], which represents the digital halftone original image, is divided into K sub-images of size $2^n \times 2^n$, where n = 3, 4, 5, etc., depending on the image size.

The elements of the matrix $[L_{k_p}(i,j)]$ of the sub-image k_p from level p = 0,1,..,P-1 (1<P≤n) of the IDP of *P* layers are defined in accordance with the relations:

$$L_{k_p}(i,j) = \begin{cases} B_{k_0}(i,j) & \text{for} \quad p=0; \\ E_{k_{p-1}}(i,j) & \text{for} \quad p=1,2,...,P-1, \end{cases} \qquad (1)$$

k_p=1,2,..,4^pK, i, j = 0,1,2,..,2^{n-p}-1.

Here $B_{k_0}(i,j)$ is the pixel (i,j) from the sub-image k_0 = 1,2,..,K in the initial (zero) pyramid layer p=0, which corresponds to the pixel (i,j) of the input image, B(i,j); $E_{k_{p-1}}(i,j)$ (presented in detail in Eq.9) is the pixel (i,j) from the difference image k_p in pyramid layer p, obtained by subtracting the image approximation from the original.

The elements of the sub-image $[L_{k_p}(i,j)]$ are transformed, using "truncated" 2D orthogonal transform (DCT, WHT, Haar, etc.), i.e., using a restricted number of coefficients only. The transform coefficients are calculated in accordance with the relations:

$$s'_{k_p}(u,v) = \begin{cases} s_{k_p}(u_r,v_r) & \text{for} \quad m_p(u,v)=1; \\ 0 & \text{for} \quad m_p(u,v)=0, \end{cases} \qquad (2)$$

for p = 0,1,.,P-1;

$$s_{k_p}(u_r,v_r) = \frac{1}{4^{n-p}} \sum_{i=0}^{2^{n-p}-1} \sum_{j=0}^{2^{n-p}-1} L_{k_p}(i,j)\, t_p(i,j,u_r,v_r)$$

for r=1, 2, .., R_p;

$m_p(u,v)$ – the elements of the binary matrix-mask $[M_p]$ of size $2^{n-p} \times 2^{n-p}$ for the layer p, which defines the retained coefficients, $s_{k_p}(u_r,v_r)$;

$R_p = \sum_{i=0}^{2^{n-p}-1} \sum_{j=0}^{2^{n-p}-1} m_p(i,j)$ - the number of the retained coefficients in the layer *p*, chosen within the range $1 \le R_p < 4^{n-p}$. The number of retained coefficients defines the quality of the approximated image after restoration (more coefficients ensure higher quality).

$t_p(i,j,u_r,v_r)$ - the element (i,j) from the "basic" image (the kernel of the orthogonal transform) with spatial frequency (u_r,v_r) in decomposition level p.

The elements $m_p(u,v)$ from Eq. 2 are defined in the following four steps:

- Calculation of the modules of the spectrum coefficients of every sub-image in pyramid layer *p*:

$$|s_{k_p}(u,v)| = \frac{1}{4^{n-p}} \left| \sum_{i=0}^{2^{n-p}-1} \sum_{j=0}^{2^{n-p}-1} L_{k_p}(i,j)\, t_p(i,j,u,v) \right| \qquad (3)$$

for u, v = 0,1, 2,..,2^{n-p}-1

- Calculation of the modules of the coefficients of the mean transform for the layer *p*:

$$|\bar{s}_{k_p}(u,v)|=\frac{1}{4^p K}\sum_{k_p=1}^{4^p K}|s_{k_p}(u,v)| \quad (4)$$

- Arrangement of the modules of the mean coefficients in uniform decreasing order:

$$|\bar{s}(u_1,v_1)|\geq|\bar{s}(u_2,v_2)|\geq\ldots\geq|\bar{s}(u_{R_p},v_{R_p})| \quad (5)$$

- Calculation of the elements $m_p(u,v)$ is performed in accordance with Eq. 5, as follows:

$$m_p(u,v)=\begin{cases}1-\text{for } u=u_r \text{ and } v=v_r \text{ for } r=1,2,..R_p;\\ 0 \quad - \quad \text{in all other cases.}\end{cases} \quad (6)$$

The approximation $\tilde{L}_{k_p}(i,j)$ for the sub-image k_p in pyramid level p is obtained, using the inverse orthogonal transform:

$$\tilde{L}_{k_0}(i,j)=\tilde{B}_{k_0}(i,j)=\sum_{u_r}\sum_{v_r}s'_{k_0}(u,v)\,t_0(i,j,u,v) \quad (7)$$

for p=0 and i, j=0,1,..,2^n-1,

$$\tilde{L}_{k_p}(i,j)=\tilde{E}_{k_p}(i,j)=\sum_{u_r}\sum_{v_r}s'_{k_p}(u,v)\,t_p(i,j,u,v), \quad (8)$$

for p=1,..,P-1 and i, j=0,1,..,2^{n-p}-1

Here $t_p(i,j,u,v)$ is the kernel of the selected orthogonal transform for the level p.

The elements of the difference image k_p in pyramid level p are defined by the relation:

$$E_{k_p}(i,j)=\begin{cases}B_{k_0}(i,j)-\tilde{B}_{k_0}(i,j) & \text{for } p=0;\\ L_{k_{p-1}}(i,j)-\tilde{L}_{k_{p-1}}(i,j) & \text{for } p=1,2,..,P-1.\end{cases} \quad (9)$$

i, j = 0,1,2,..,2^{n-p}-1.

The coefficients $s^q_{k_p}(u_r,v_r)$ from all sub-images in the pyramid level p are arranged in R_p two-dimensional massifs in accordance with their spatial frequency (u_r,v_r) for r=1,2,..,R_p. Each two-dimensional massif of coefficients for the corresponding decomposition levels is then transformed into one-dimensional, following the recursive Hilbert scan. The so obtained one-dimensional data massif is processed with special lossless coding method, developed by the authors [12, 13], which comprises two main steps: adaptive coding of the lengths of the series of equal symbols (run-length encoding), and modified adaptive Huffman coding. As a result is obtained the one-dimensional compressed data sequence Z_p for the decomposition level p. The so compressed image is transformed into a new format, which has special header comprising the global decomposition data: the number of decomposition layers; the kind of orthogonal transform, used for each layer (2D Walsh-Hadamard Transform, DCT, etc.); the number of retained coefficients and the way of coefficients' values arrangement.

3 Multi-Layer Fragile Watermarking

The IDP decomposition permits the insertion of a different watermark (an image or a data sequence), in each consecutive pyramid level p. This is performed by processing the coded image data $Z_p(r)$ (r = 1, 2,.., l_p) for the corresponding level together with the coded watermark data. For this, the data sequence $Z_p(r)$ is arranged in accordance with the relation:

$$Z_p(r)=\begin{cases}X_p(r) & \text{for } r=1,2,..,l_p;\\ W_p(r) & \text{for } r=l_p+1,l_p+2,..,l_p+l_{wp},\end{cases} \quad (10)$$

Here $W_p(r)$ is the data, representing the compressed watermark of length l_{wp} and inserted in the decomposition layer p, using the password Y_p. The password is a code of length $l_p^y \leq l_p$. Each watermark has a corresponding number N_{wp}, defined by the relation:

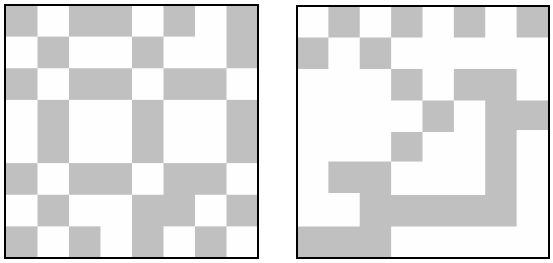
$$N_{wp}=l_p\oplus Y_p=\sum_{i=0}^{l_p^y-1}(l_i^p\oplus y_i^p)2^p, \quad (11)$$

where l_i^p and y_i^p are respectively the i^{th} binary digits of the numbers l_p and Y_p, and the sign "⊕" represents the operation "exclusive OR". The number N_{wp} is included in the header of the compressed image data.

The image, used as a watermark, is losslessly compressed. In order to get the shortest possible coded data sequence, it is suitable to use a relatively small watermark (256x256 or 512×512 pixels) and to apply it over the original document image as many times as necessary, until the entire document is covered. For every IDP layer is created an individual data sequence $Z_p(r)$, in which the watermark image data is inserted. The coded data (the compressed image together with the inserted watermark) is processed as one common file.

The special method for lossless image coding permits the grayscale image watermarks to be compressed very efficiently, depending on the image content. Example grayscale watermark images are shown in Fig. 1. The sizes of the losslessly compressed files are correspondingly:

369B for the image in Fig.1.a (compression ratio more than 177) and 390B for the image in Fig.1.b (compression ratio more than 190). The size of the compressed watermarks is negligible, when compared to the protected document size (usually several MB for a scanned paper document of size A4): after compression, the electronic files of paper documents are still very large, because the quality of the restored image has to be good and high compression ratios are not acceptable.



256 × 256 pixels, 8 bpp 256 × 256 pixels, 8 bpp

Fig. 1. Example watermark images

In systems, using such kind of documents protection the watermark images are kept in a special library and for every document is used the watermark, whose number corresponds to the number of bits obtained after the document coding. The watermark invisibility and the password ensure high security for the processed images, because users, who have the decoding software, are not aware of the existence of the embedded watermark, and will not be able to visualize it without having the password. The content of the visualized image with the visible watermark could be changed, if anyone wants to do this, but the unauthorized user will not be able to change the hidden watermark. There are two reasons for this. The first is that in result of the modified lossless run-length and Huffman coding of the image data, the length of the compressed file is never known in advance. The compressed data varies with the change of the image content and influences the compressed data file length, l_p. As a result, the first indication, that the image has been changed, is the change of the compressed data file length. The second indication for unauthorized editing is the embedded hidden watermark, because the code, which corresponds to the new file length, will point at another watermark number from the library, unknown for the password owner. The same approach is used in the next (higher) decomposition layer in which could be inserted one more watermark. The watermark could be applied so that to cover (hide) a part of the protected image and the original would be then recovered only after the watermark extraction (removal). The example in Fig. 2 demonstrates that the original text cannot be understood until the inserted watermark is removed. In this case, instead of invisible, a visible watermark had been inserted, which hides the original image.

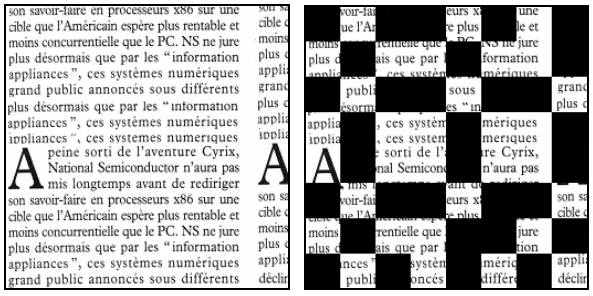


Fig. 2. a) Example text image; b) Watermarked image

The watermark used for the presented method should satisfy the following requirement: it must consist of relatively large brightness segments (8x8 pixels or larger) of constant brightness, which to ensure very efficient lossless compression of the watermark data.

The image decoding and watermark extraction are performed in reverse order, as follows:

- The components $X_p(r)$ and $W_p(r)$ are extracted from the coded data $Z_p(r)$ and after that the watermark data W_p for the level p is restored;
- The data $X_p(r)$, obtained in result of the image coding, is decoded;
- The sub-image approximation is calculated using the inverse orthogonal transform, in accordance with Eqs. 7-9;
- The elements $B'(i, j)$ of the restored image, which can contain one, two or even more watermarks, are calculated for each of the consecutive pyramid layers p = 0, 1, etc., in correspondence with the equation:

$$[B'_k(i,j)] = [\tilde{B}_{k_0}(i,j) || W_{k_0}(i,j)] + [\tilde{E}_{k_1}(i,j) || W_{k_1}(i,j)] + \sum_{p=2}^{P-1} [\tilde{E}_{k_{p-1}}(i,j)] \quad (12)$$

for i, j = 0,1, . ., 2^n-1 and k =1, 2, .., K.

The sign || means "concatenation" of the two data sequences (the coded data for the decomposition layer and the corresponding watermark).

The IDP decomposition permits the use of one more method for fragile watermarking – to insert the uncompressed watermark image into the last (highest) decomposition layer. In this case the watermark should be very pale (the brightness change should be lower than the perceptual threshold of the human visual system, which in the general case means less than 2-4 brightness levels

(for the range 0-255). This ensures the watermark transparency, retaining the ability for its successful extraction. He watermark should answer the following requirements:

- The amplitude of the invisible watermark should be relatively small. When applied on the bright parts of the document, its amplitude should be lower than the perception threshold of the human visual system (2-4 levels). In other cases, when the brightness in the corresponding part of the document is lower, the watermark brightness amplitude could be higher. Such approach requires intelligent, adaptive algorithms for watermark insertion. The easiest way is to use watermarks with low brightness, applied across the entire document and in the process of watermark insertion to check for eventual distortions in case that the maximum or minimum brightness values are violated.

The watermark should consist of relatively large brightness segments (8x8 pixels or larger) of constant brightness. This will permit its detection and recognition after JPEG compression.

The watermark visualization in this case is performed with image histogram modification (enhancement), in result of which the inserted watermark becomes easily visual.

4 Resistant Watermarking

The resistant watermarking is performed in one of the decomposition layers. In this case is used the specific feature of the IDP decomposition that it permits to use different orthogonal transform in each consecutive layer. One of the middle layers is usually used for resistant watermark embedding. The watermark data is inserted in the phases of selected spectrum coefficients, obtained with 2D Complex Hadamard Transform (2D-CHT). The decomposition layer, selected for the resistant watermarking, is presented as a square matrix [B(N)] of size N×N elements ($N=2^n$), which is transformed using 2D-CHT with "arranged" complex Hadamard matrix.

4.1 Watermark embedding

The watermark embedding comprises the following steps:

Step 1: The image matrix $[B(2^n)]$ is transformed, using the direct 2D-CHT:

$$[S(2^n)] = [CH(2^n)][B(2^n)][CH(2^n)] \qquad (13)$$

Here $[CH(2^n)]$ is an arranged matrix of size $2^n \times 2^n$ and $[S(2^n)]$ - a matrix of same size, representing the image discrete spectrum (transform). The matrix $[CH(2^n)]$ is defined using the natural complex Hadamard matrix $[CH_0(2^n)]$, whose elements are calculated in accordance with the relation:

$$ch_0(t,q) = j^{tq}\, h_0(t,q) \qquad (14)$$

for t, q = 0,1,..,2n -1,

where:

$$h_0(t,q) = \begin{cases} 1 & \text{for} \quad n = 2; \\ (-1)^{\sum_{r=3}^{n} \left\lfloor \frac{t}{2^{r-1}} \right\rfloor \left\lfloor \frac{q}{2^{r-1}} \right\rfloor} & \text{for } n = 3,4,., \end{cases}$$

is the sign function of the element (t,q) from the matrix $[CH_0(2^n)]$;

$\left\lfloor \frac{*}{*} \right\rfloor$ - Operator used for the calculation of the integer part, obtained as a result of the division;

$j = \sqrt{-1}$; $n = \lg_2 N$.

Instead of the regular way for CHT implementation based on the natural transform matrix, in this work is offered a modification with "arranged" CHT matrix. In result is obtained higher energy concentration in the low-frequency area of the image spectrum.

On Fig. 3 are shown the 2D-CHT Basic functions for arranged matrix of size 4 x 4.

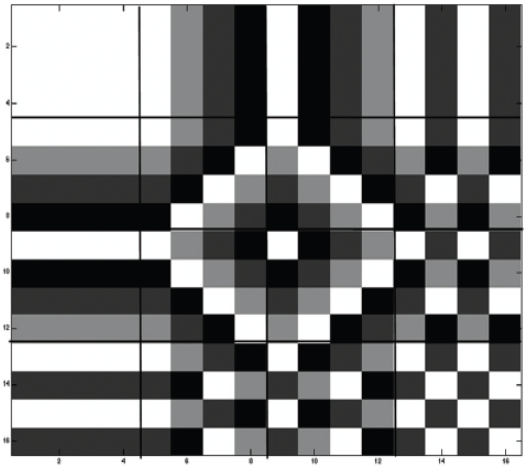


Fig.3. Basic 2D-CHT for arranged matrix of size 4x4 (white = 1, light gray = j, dark gray = - 1, black = - j)

On Fig. 4 are shown the 2D-CHT Basic functions for arranged matrix of size 16×16 and on Fig. 5 - the 2D amplitude spectrum obtained with arranged CHT for the test image "Peppers", of size 64×64 pixels. This graphic represents very well the high energy concentration in the low-frequency part of the image spectrum and the smooth energy decrease toward the high-frequency area.

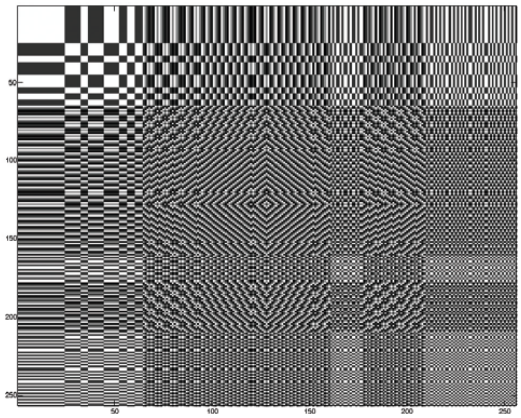


Fig.4. Basic 2D-CHT for arranged matrix of size 16x16 (white = 1, light gray = j, dark gray = - 1, black = - j)

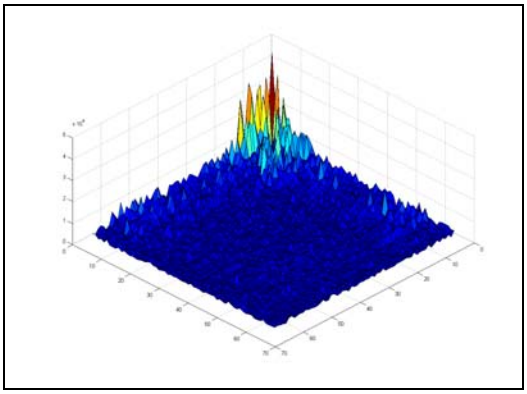


Fig.5. Arranged 2D-CHT spectrum obtained for the test image "Peppers" of size 64×64 pixels.

The arranged matrix $[CH(2^n)]$ is obtained from the natural one, $[CH_0(2^n)]$ after rearranging its rows in such a way, that the number of sign changes $\Sigma_{sign}(q)$ for the elements in the row q to be increased by one in the next row, (q+1). Then for each q = 0,1,..,2^n-1 is obtained:

$$1+\Sigma_{sign}(q)=\Sigma_{sign}(q+1), \tag{15}$$

where

$$\Sigma_{sign}(q)= =\frac{1}{2}\sum_{p=0}^{2^n-2}|sign[ch_0(p,q)]-sign[ch_0(p+1,q)]| \tag{16}$$

Step 2: Each coefficient of the matrix $[S_0(2^n)]$, is then represented as:

$$s_0(u,v)=\sum_{i=0}^{2^n-1}\sum_{k=0}^{2^n-1}B(i,k)e^{-j\frac{\pi}{2}(ui+vk)}h_0(u,i)h_0(v,k) \tag{17}$$

for u,v = 0,1,..,2^n-1

where B(i,k) is the element of the original image matrix $[B(2^n)]$.

For the calculation of the $s(u,v)$ elements, obtained using the matrix $[CH(2^n)]$, is necessary to rearrange the $s_0(u,v)$ coefficients, defined in accordance with Eq. (17). For example for n = 2 and after rearrangement is obtained:

$$[S(4)]=\begin{bmatrix} s(0,0) & s(0,1) & s(0,2) & s(0,3) \\ s(1,0) & s(1,1) & s(1,2) & s(1,3) \\ s(2,0) & s'(2,1) & s(2,2) & s(2,3) \\ s(3,0) & s(3,1) & s(3,2) & s(3,3) \end{bmatrix}= \tag{18}$$

$$=\begin{bmatrix} s_0(0,0) & s_0(0,1) & s_0(0,3) & s_0(0,2) \\ s_0(1,0) & s_0(1,1) & s_0(1,3) & s_0(1,2) \\ s_0(3,0) & s_0(3,1) & s_0(3,3) & s_0(3,2) \\ s_0(2,0) & s_0(2,1) & s_0(2,3) & s_0(2,2) \end{bmatrix}$$

Step 3: Each spectrum coefficient $s_0(u,v)$ is represented as a vector in the complex space:

$$s_0(u,v)=s_{0,Re}(u,v)-js_{0,Im}(u,v)= =M_0(u,v)e^{-j\varphi_0(u,v)}. \tag{19}$$

The components of the coefficient $s_0(u,v)$ are defined by the relations:

$$s_{0,Re}(u,v)= =\sum_{i=0}^{2^n-1}\sum_{k=0}^{2^n-1}B(i,k)h_0(u,i)h_0(v,k)\cos[\tfrac{\pi}{2}(ui+vk)], \tag{20}$$

$$s_{Im}(u,v)= =\sum_{i=0}^{2^n-1}\sum_{k=0}^{2^m-1}B(i,k)h_0(u,i)h_0(v,k)\sin[\tfrac{\pi}{2}(ui+vk)] \tag{21}$$

$$M_0(u,v)=\sqrt{s_{0,Re}(u,v)]^2+[s_{0,Im}(u,v)]^2} \quad \text{and}$$

$$\varphi_0(u,v)=-\text{arctg}\left[\frac{s_{0,Im}(u,v)}{s_{0,Re}(u,v)}\right] \tag{22}$$

Step 4: From all spectrum coefficients, defined in accordance with Eq. (1) for further processing are chosen the complex-conjugated couples $s(u,v)$ and $s^*(u,v)$ only, whose phases are inverse $\varphi(u,v)=-\varphi^*(u,v)$, and the modules - equal, i.e. when $|M(u,v)|=|M^*(u,v)|$.

On Fig. 6 are shown the 2D-CHT coefficients for sub-image block of size 4 × 4.

Here R_1 –R_4 are the real coefficients; C_1-C_6 – the complex coefficients; C_1*-C_6* - the corresponding complex-conjugated coefficients. For the further

processing (watermarking) are used the couples (C_1,C_1*), …, (C_6,C_6*) only. It is easy to notice that the number of complex coefficients is equal to ¾ of the total number of transform coefficients and ½ of them (the complex-conjugated couples) are suitable for watermark data embedding.

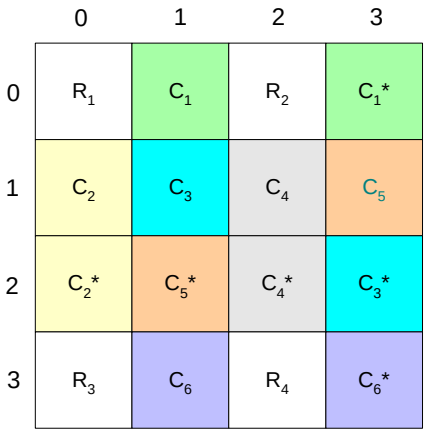


Fig. 6. Graphic representation of the 2D-CHT coefficients for sub-image block of size 4 × 4

Step 5: Every bit $w_r(p)$ of the watermark data p is inserted in the phases of the coefficients $s(u,v)$ and $s^*(u,v)$ only, in correspondence with the relation:

$$\varphi_{w_r(p)}(u,v) = -\varphi^*_{w_r(p)}(u,v) = \\ = \begin{cases} \varphi(u,v)+\Delta, & \text{if} \quad w_r(p)=1; \\ \varphi(u,v)-\Delta, & \text{if} \quad w_r(p)=0. \end{cases} \tag{23}$$

Here $\varphi_{w_r(p)}(u,v)$ and $\varphi^*_{w_r(p)}(u,v)$ are the phases of the watermarked coefficients $s_{w_r(p)}(u,v)$ and $s^*_{w_r(p)}(u,v)$, and the watermark is represented by the binary sequence $w_r(p)$ for r = 1,2,.., R (R is the number of the watermark binary elements). The parameter Δ is the angle, which defines the watermark "depth", its "transparency" and the resistance against pirates' attacks as well.

The sequence of bits $w_r(p)$ is obtained after performing the function "XOR" both for each bit of the watermark and the corresponding bit from a pseudorandom sequence, which represents a secret (private) or public key, used for the watermark encryption. In this case the autocorrelation function of the sequence $w_r(p)$ is chosen to be of the kind "delta-pulse". This ensures high accuracy for the watermark detection and ability for its successful extraction. In case that the currently processed complex spectrum coefficient, which should be watermarked, has zero amplitude, the corresponding binary value of the watermark is omitted and the binary symbol from the pseudorandom sequence only remains, because the operation "XOR" is not applied. In result, the errors in the elements of the extracted watermark are reduced, because the spectrum coefficients of zero amplitude have zero phases as well, and they are practically not suitable for watermark elements extraction. This is of high importance for images with large homogenous areas, for which significant number of complex coefficients have zero amplitudes. Very important for the process is no complex coefficients to be missed, because in such case the synchronization could be lost in the process of the watermark elements extraction.

Step 6: The elements $B_w(i,k)$ of the watermarked image $[B_w(2^n)]$ are calculated in accordance with Eqs. (22, 23). The coefficients of the rearranged spectrum matrix $[S_w(2^n)]$ are calculated in accordance with the relation:

$$s_{w_r(p)}(u.v) = M(u,v)e^{-j\varphi_{w_r(p)}(u,v)} \tag{24}$$

The matrix $[S_w(2^n)]$ is processed with inverse 2D-CHT and as a result is obtained:

$$[B_w(2^n)] = \frac{1}{4^n}[CH(2^n)]^*[S_w(2^n)][CH(2^n)]^* \tag{25}$$

Here

$$[CH(2^n)]^{-1} = \frac{1}{2^n}[CH(2^n)]^* \tag{26}$$

is the inverse arranged CHT matrix of size $2^n \times 2^n$, whose elements are complex-conjugated with these of $[CH(2^n)]$.

The elements of the natural complex-conjugated matrix $[CH_0(2^n)]^*$ are defined by the relation:

$$ch_0^*(t,q) = j^{-tq}\, h_0(t,q) \quad \text{for} \quad t, q = 0,1,..,2^n\text{-}1 \tag{27}$$

where $h_0(t,q)$ is the sign function of the element (t,q) in the matrix $[CH_0(2^n)]$. The arranged matrix $[CH(2^n)]$ is obtained from $[CH_0(2^n)]$ after rearrangement of its rows in correspondence with the number of sign change growth.

In correspondence with Eq. (25) the pixels of the watermarked image are defined by the relation:

$$B_w(i,k) = \sum_{u=0}^{2^n-1}\sum_{v=0}^{2^n-1} s_w(u,v)e^{j\frac{\pi}{2}(ui+vk)}h(u,i)h(v,k) \tag{28}$$

for i, k = 0,1,..,2^n-1.

4.2 Watermark detection

For the watermark detection in unknown image are performed the steps 1 – 4 of the algorithm, presented above. After that the process continues as follows:

Watermark detection Step 1: Should be checked if in the image had been inserted the watermark p, which is one of the known D possible signs. The check is performed by evaluation of the coefficient of the mutual correlation $C_{m,p}$ between the m^{th} and p^{th} watermark, the first of which is one of the D possible, and the second is used for watermarking of the complex-conjugated spectrum coefficients $s(u,v)$ and $s^*(u,v)$ of the unknown image. The coefficient of the mutual correlation is defined by the relation:

$$C_{m,p} = \sum_{r=1}^{R}[\varphi(u,v) + \Delta_r(p)]\Delta_r(m) = \\ = A(m) + B(m,p) \qquad (29)$$

for m, p = 1,2,..,D

where D is the number of the searched watermarks; $[\varphi(u,v)+\Delta_r(p)] = \varphi_{w_r(p)}(u,v)$ is the phase of the mafrked coefficient $s_{w_r(p)}(u,v)$ of the matrix $[S_w(2^n)]$, which contains the p^{th} watermark;

$$\Delta_r(p) = (-1)^{w_r(p)}\Delta = \begin{cases} +\Delta & \text{if } w_r(p) = 1; \\ -\Delta & \text{if } w_r(p) = 0, \end{cases} \qquad (30)$$

for r = 1,2,..,R

$w_r(p)$ - the r^{th} bit from the pseudorandom sequence of length R, which describes the p^{th} watermark;

$$A(m) = \sum_{r=1}^{R}\varphi(u,v)\Delta_r(p), \\ B(m,p) = \sum_{r=1}^{R_p}\Delta_r(p)\Delta_r(m) \qquad (31)$$

For big values of R from Eq. (31) follows that

$$A(m) = \varphi(u,v)\sum_{r=1}^{R}\Delta_r(p) \approx 0. \qquad (32)$$

In case that the spectrum coefficients, obtained in accordance with Eq. 24 are not marked, $\Delta_r(p) = 0$. Then, from Eq. 29 follows that $C_{m,b}(p) \approx 0$; in case that these spectrum coefficients are marked, is obtained:

$$C_{m,p} \approx \begin{cases} \sum_{r=1}^{R}[\Delta_r(m)]^2 = R\Delta^2 & \text{if } m = p; \\ \sum_{r=1}^{R}\Delta_r(m)\Delta_r(p) \approx 0 & \text{if } m \neq p. \end{cases} \qquad (33)$$

Watermark detection Step 2: The decision for the detection of the watermark p is:

$$p = \begin{cases} \text{Yes,} & \text{if } \rho(\Delta) = [C_{m,p}/R\Delta^2)] \geq \theta; \\ \text{No,} & \text{-} \quad \text{in other cases.} \end{cases} \qquad (34)$$

for m, p = 1, 2,…, D

Here θ is a pre-defined threshold, whose value is in the range $0 < \theta < 1$. The value of θ should satisfy two contradictory requirements: to minimize the possibility for watermark missing and for false watermark detection. The so described *watermark detection* is "blind", i.e. it does not need the original image.

For the *watermark extraction* is needed the original image. It is supposed, that the owner is the person, authorized to do this. After the phase spectrums of the original and the watermarked images had been calculated, the phases of the corresponding coefficients are subtracted and is defined the sequence, obtained after applying the "XOR" operation on the watermark and the pseudorandom sequence, which is the encryption key. The watermark is obtained after performing XOR for the phase differences sequences and the key.

5 Experimental results

5.1 Fragile watermarking

The presented methods are designed to support the safe storage of the digital copies of various documents.

This application area defines some restrictions in the fragile watermarking application:

- The watermark extraction requires the use of a password;
- The method requires the document creator to have a library of watermark images, one or more of which to be inserted in the document image in accordance with the described algorithm;
- The size of the compressed data, representing the original document, is increased with the watermark insertion. As a result, the compression ratio and the storage efficiency are slightly reduced.

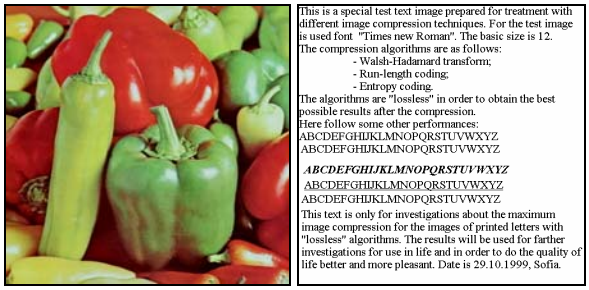
The ability of the IDP decomposition to permit the insertion of different fragile watermark in every

decomposition layer ensures the identification of any image change or it's editing in case of un-authorized access. The inserted watermark ensures, that images, contained in the image databases had not been changed, or edited.

The specific requirements for the image storage could be defined as follows:

- The authenticity of the compressed images should be surely proved. The image content authenticity is proved with the extracted watermark, which should be unchanged. In case, that the picture had suffered some kind of unauthorized editing, the changes in the extracted watermark will prove this.
- The stored information must ensure authorized access only. For this purpose is usually applied a masking watermark, whish is removed by using a special password. The method permits the insertion of invisible watermark together with the masking one as well, without affecting the protected image quality.
- The method offers the ability to create large database management systems with hierarchical access control: the authorized users are permitted to access the images without overlapped masking fragile watermark.

In the presented example with the test image "Peppers" on Fig. 7 as a watermark was used the image of a scanned text of same size.



a. Original image "Peppers" b. Watermark image

c. Watermarked test image d. Extracted watermark

Fig. 7. Example test image "Peppers" (24 bpp, 512 × 512 pixels).

The inserted watermark is invisible, but after its visualization with the software implementation of the method, the quality of the extracted watermark is sufficient to prove its presence. The extracted watermark, shown in Fig. 7.d was obtained after JPEG compression with Quality Factor = 70 (Microsoft Photo Editor). The fragile watermarking performed by adding an additional layer in the IDP decomposition is performed for images, transformed into the new format "tk", developed for the implementation of this decomposition. The watermark embedding does not influence the coded image data contents. This approach permits the use of a watermark of size equal or smaller than that of the processed image. In the second case the watermark is overlapped on the protected image (while it is decoded) as many times, as necessary to cover it.

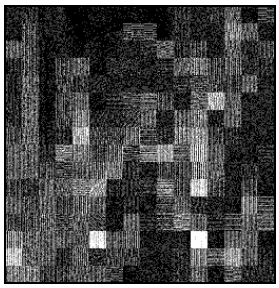
The comparison of the method with other contemporary techniques confirm the method advantages. The experimental results obtained using the method for geometric invariant semi-fragile image watermarking with real symmetric matrix [8] show that in result of the watermarking the restored image quality is changed significantly: the PSNR of the watermarked test images "Lena", "Baboon" and "Peppers" is in the range 39-40 dB. The size of digital watermark in this case was 32×32 pixels and the watermark was a binary sequence of 0's and 1's. The PSNR values show that the visual quality of the processed image is retained, but anyway there is a change. Unlike this, the quality of the images with inserted fragile watermark as an additional IDP layer is not changed at all.

5.2 Resistant watermarking

The software implementation of the resistant watermarking was used for the experiments and the evaluation of the method.

On Fig. 8 is shown the original test grayscale image "Lena" of size 256×256 pixels. For the resistant watermarking were used sub-blocks of size 16×16 pixels and phase angle Δ=12. The watermarked image, shown on Fig. 8.b contains watermark of 184 bits.

a. Original image "Lena" b. Watermarked image with phase angle Δ = 12



c. The absolute difference amplified 64 times

Fig. 8. Example for resistant watermarking

On Fig.8.c is shown the image of the absolute difference between the original and the watermarked image, amplified 64 times for better visibility. This example shows that in accordance with the presented algorithm the watermark data are inserted into the non-homogenous areas of the processed image and do not produce visible distortions.

In Table 1 below are presented the results obtained for the number of bits embedded in 4 test images. The quality of all watermarked images was higher than 35 dB, which means that the watermark is practically invisible.

Table 1

Image name 256×256 pixels, 8 bpp	Watermark capacity [bits]
Lena	184
Baboon	182
Cameraman	105
Peppers	179

On Fig. 9 are given the results obtained for the influence of the parameter Δ (the change of the phase angle for the selected spectrum coefficients) on the value of the Peak-Signal-to-Noise-Ratio (PSNR) for the test image "Baboon".

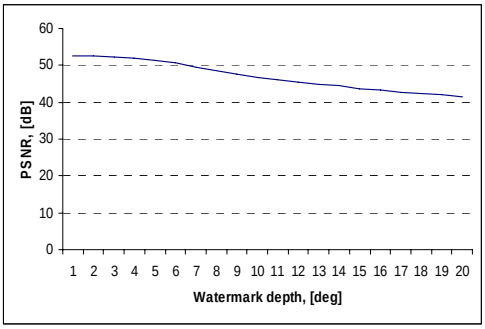
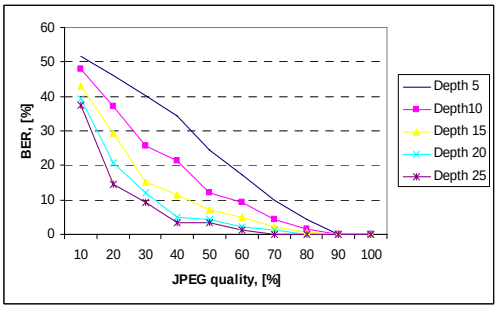


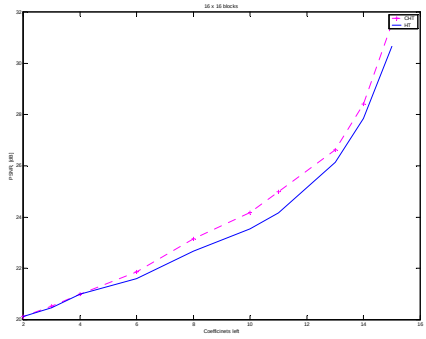
Fig.9. The watermarked image PSNR in a function of the angle Δ

On Fig. 10 is shown the relation between the Bit Error Rate (BER) and the JPEG compression value, when the image quality factor was changed in the range 10-100 (Microsoft Photo Editor) for several values of the phase angle Δ , for the test image "Baboon". The results obtained confirm the watermark resistance against compression and the watermark transparency for different watermark depth.



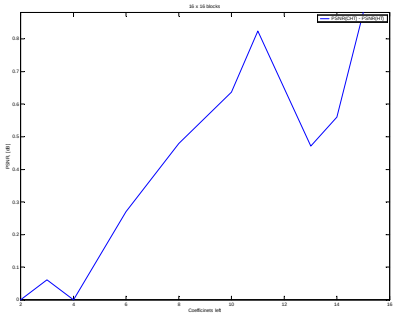
Фиг.10. Graphic presentation of BER dependence from JPEG compression quality

The same approach was used for watermarking based on the Hadamard Transform (HT). On Fig. 11 is shown the influence of the number of selected coefficients on the watermarked image quality for CHT and HT for the test image "Baboon". The size of the image sub-blocks was 16x16 pixels.



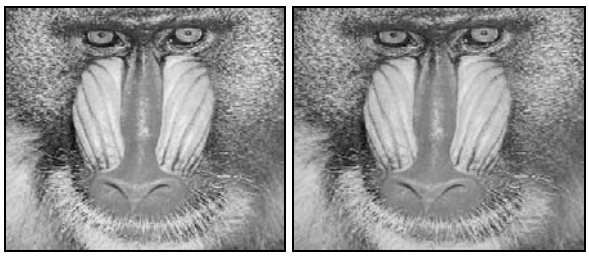
Фиг. 11. Relation of PSNR [dB] from the number of retained spectrum coefficients for test image "Baboon".

On Fig. 12 is given the graphic representation of the difference for the watermarked image quality obtained for the two transforms (CHT and HT) after JPEG compression.

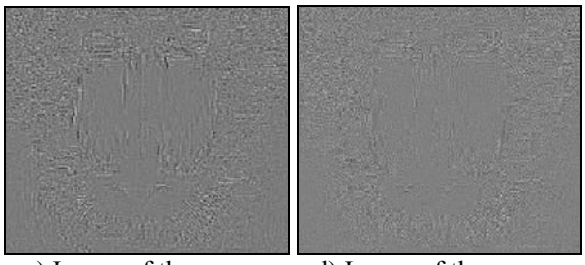


Фиг. 12. The PSNR [dB] difference obtained for CHT and HT in correspondence with Fig. 11.

On Fig. 13 are shown the results obtained for the test grayscale image "Baboon" of size 256×256 pixels (sub-block size 8×8).



а) original image б) watermarked image with 4 phase angles



c) Image of the error for 4 phase angles d) Image of the error for 8 phase angles

Фиг. 13. Test image "Baboon"

The experimental results, shown on Figs. 11, 12 and 13, which represent the change of the watermarked image quality (PSNR) depending on the number of the used spectrum coefficients and the number of the discrete phase angles, confirm the relatively low influence of the phase quantization on the restored image quality. The results shown on Fig. 10 prove the resistance of the presented method for digital watermarking based on the phase modification of the complex-conjugated coefficients in the image CHT.

The comparison of the method with other similar techniques, based on the watermark insertion in the image spectrum phase domain [4, 14], confirmed that this approach is very efficient and the so inserted watermark has significant resistance against various attacks. The new method, presented in this paper possesses these properties and together with this, has much lower computational complexity, because the IDP is based on the Walsh-Hadamard transform, while the other techniques use the DCT [14] or the wavelets transform [6]. The quality of the watermarked images is similar for all these methods.

6 Conclusions

The IDP decomposition permits easy watermark insertion in the consecutive image layers with increasing resolution. The resistant watermark data is added to the coded image data and does not influence the restored image quality. The software implementation in C++ (Windows environment) of the presented approach proved the method efficiency.

The most important applications are for content protection of any kind of documents, medical images, etc., i.e. – all cases, when the image quality should not be changed and the confidential information is preserved. The new method offers significant resources for efficient content protection of images in large databases. The method permits the insertion of multiple watermarks in the consecutive decomposition layers, which suits very well the aims of the visual data content protection.

The main advantages of the method for *fragile watermarking* are:

- The watermark is inserted as an additional decomposition layer and does not influence the protected image quality;
- Any change in the extracted watermark evidences unauthorized access and image editing;
- The knowledge of the algorithm and the possession of the decoding tools do not permit the watermark extraction without having the password.
- The ability to insert more than one watermark in the same image ensures higher security for the original image content and permits the creation of information systems with hierarchical access control.

The main advantages of the presented algorithm for *resistant watermarking* are:

- The ability for "blind" watermark detection (without using the original image);
- The watermark "transparency";
- The resistance of the inserted watermark against various attacks, such as compression and high-frequency filtration;
- The high efficiency – more than 100 bits for halftone images of size 256 × 256 pixels with retained visual quality.

The so developed methods for multiple watermarking offer wide abilities for implementation in various application areas.

Acknowledgements

This work was supported by the National Fund for Scientific Research of the Bulgarian Ministry of Education and Science, Contract VU-I 305.

References

[1] J. Tzeng, W. L. Hwang, I. L. Chern. Enhancing Image Watermarking Methods with/without Reference Images by Optimization on Second-

order Statistics. *IEEE Trans.on Image Processing*, Vol. 11, No. 7, July 2002, pp. 771-782.

[2] M. Barni, F. Bartolini. *Watermarking Systems Engineering*. Marcel Deccer, New York-Basel, 2004.

[3] M. Arnold, S. Wolthusen, M. Schmucker. *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House Publishers, 2003.

[4] F. Ahmed, I. Moskowitz. Phase Signature-based Image Authentication Watermark Robust to Compression and Coding. *Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications, Mark S. Schmalz (Ed.), Proc. of SPIE,* Vol. 5561 (SPIE, Bellingham, WA, 2004), pp. 133-144.

[5] C. Vural, S. Kazan. Analysis of the Moment Based Image Normalization Effects on Watermarking Capacity in DCT and DWT Domains. *WSEAS Intern. Conf. SP*, Istanbul, Turkey, 2009, pp. 99-103.

[6] W. Huang, S. Tan, Y. Chang, C. Chen. A Discrete Wavelet Transform Based Robust Watermarking for Copyright Protection. *WSEAS Intern. Conf. Recent Advances in Networking, VLSI and Signal Processing,* Cambridge, UK, Feb. 2010, pp. 39-43.

[7] B. J. Falkowsky, Lip-San Lim. Image Watermarking Using Hadamard Transforms. *Electr. Letters,* Feb.3, 2000, Vol. 36, No.3, pp. 211-213.

[8] Ch. Hsieh, Y. Wu. Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix. *Proc. of the 5th WSEAS Intern. Conf. on Signal Processing,* Istanbul, Turkey, May 27-29, 2006, pp. 70-75.

[9] M. Hartung, M. Kutter. Multimedia Watermarking Techniques. *Proc. of the IEEE, Vol. 87*, No. 7, July 1999, pp. 1079-1086.

[10] R. Kountchev, V. Haese-Coat, J. Ronsin. Inverse Pyramidal Decomposition with multiple DCT. *Signal Processing: Image Communication*, Vol. 17, Jan. 2002, pp. 201-218.

[11] R. Kountchev, Vl. Todorov, M. Milanova, R. Kountcheva. Documents Image Compression with IDP and Adaptive RLE. *Proc. of the 32d Annual Conf. of the IEEE IE Society*, Paris, Nov. 2006.

[12] R. Kountchev, M. Milanova, C. Ford, Vl. Todorov and R. Kountcheva. Detection and Lossless Compression of Texts and Graphics in Compound Images. *Intern. Symp. on Innovations in Intelligent Systems and Applications*, June 2005, Istanbul, Turkey, pp. 1-4.

[13] R. Kountchev, Vl. Todorov, R. Kountcheva, M. Milanova. Lossless Compression of Biometric Image Data. *WSEAS Intern. Conf. on SP*, Istanbul, Turkey, 2006, pp. 185-190.

[14] H. Zhang, L. Cai, X. Meng, X. Xu, X. Yang, X. Shen, G. Dong. Image Watermarking Based on an Iterative Phase Retrieval Algorithm and Sine–cosine Modulation in the Discrete Cosine-transform Domain. *Optics Communications 278*, Elsevier, 2007, pp. 257–263.