Technique for the hidden transfer of the color images

I. A. Reznik [1)], R. Kh. Sadykhov, A. Doudkin [2)]
1) BSUIR, 220013 Belarus Minsk P.Brovki str. 6, i.reznik@inbox.ru
2) UIIP, 220072 Belarus Minsk Sourganova str. 6, rsadykhov@gw.bsuir.unibel.by;
doudkin@newman.bas-net.by

Abstract. The steganographic system for hidden transfer of the graphic information is represented. For hiding the graphic information the digital correlations based on the complex BIFORE transform are used. A crypto stability of a technique is provided by a secret key, with that the hidden image is embedded in the container-image. The problems of efficiency, robustness, accuracy and performance of the suggested method are considered.

Key Words: steganography, BIFORE, spatial correlator.

1. Introduction

One of an important direction of the protection information from an unauthorized access is a steganography. The steganography is a science about hiding a fact of existing secret information. A digital steganography is based on methods of the digital signal processing. In this work the example of the combining methods of digital steganography with methods of the optical information processing is shown. Using of optical methods gives a good capability for encoding information [1,2,3,4].

The steganographic system for the hidden transfer the color image is proposed. The picture, in which the hidden image is embedded as a rule denominates a container image, and the container with embedded hidden image is the stego-image [5]. A core of our system is two-dimensional spatial correlator, which is used for encoding, embedding and reconstruction of the hidden image. Digital correlations are based on the complex BIFORE (BInary FOurier REpresentation) transform [6]. Note, that classical 2D spatial correlator is based on the complex Fourier transform (CFT). A choice of the complex BIFORE transform (CBT) is conditioned more fast computation performance in comparison with CFT. The secret key of the staganographic system is spatial filter of the correlator.

2. Complex BIFORE transform

The notion of binary Fourier representation (BIFORE) was introduced in [7]. Transform based on this representation names BIFORE transform (BT). In publications it also called Hadamard transform or Walsh-Hadamard transform.

CBT belongs to a family of a discrete orthogonal transforms [8]. While the Fourier bases are sinusoids with harmonic frequencies, the BIFORE bases are Walsh functions. Since the Walsh functions are square waves, they take only two values, namely, +1 and -1. The simplicity of square waves relative to sinusoids allows relatively easy process information [9]. Both CFT and CBT require $N \cdot \log_2 N$ arithmetical operations, but in case of CFT every arithmetical operation include, beside complex addition, the multiplying.

Sampling of Walsh functions at N equally spaced sample points in $(0;1)$ results in an $N \times N$ array of "-1" and "+1". The rows of any array obtained by this method can be rearranged to form a particular matrix of Hadamard $H(n)$, where $N = 2^n$ [8]. For example for $n = 3$

$$[H(3)] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}. \quad (1)$$

We can see that Hadamard matrices can be recursively generated as follows:

$$[H(0)] = [1]$$
$$[H(k+1)] = \begin{bmatrix} [H(k)] & [H(k)] \\ [H(k)] & -[H(k)] \end{bmatrix}. \quad (2)$$

For the complex case transform matrices can be generated as follows:

$$\begin{aligned}
&[M(0)] = 1 \\
&[M(1)] = [H(1)] \\
&[M(n)] = \begin{bmatrix} [M(n-1)] & [M(n-1)] \\ [L(1)] \otimes [H(n-2)] & -[L(1)] \otimes [H(n-2)] \end{bmatrix}
\end{aligned}, \qquad (3)$$

where $\otimes$ denotes Kronecker product and $[L(1)] = \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$.

So, CBT of the function $x(n)$ and its inverse transform ICBT is defined as:

$$\begin{aligned}
&\{X(n)\} = \frac{1}{N} \cdot [M(n)] \cdot \{x(n)\} \\
&\{x(n)\} = [M^*(n)]^T \cdot \{X(n)\}
\end{aligned}, \qquad (4)$$

where * and T denotes complex conjugate and transpose, respectively. $[M(n)]$ is matrix of transform (3). The signal flow graphs for CBT and ICBT for $n = 3$ are shown on Fig.1 and 2 respectively.

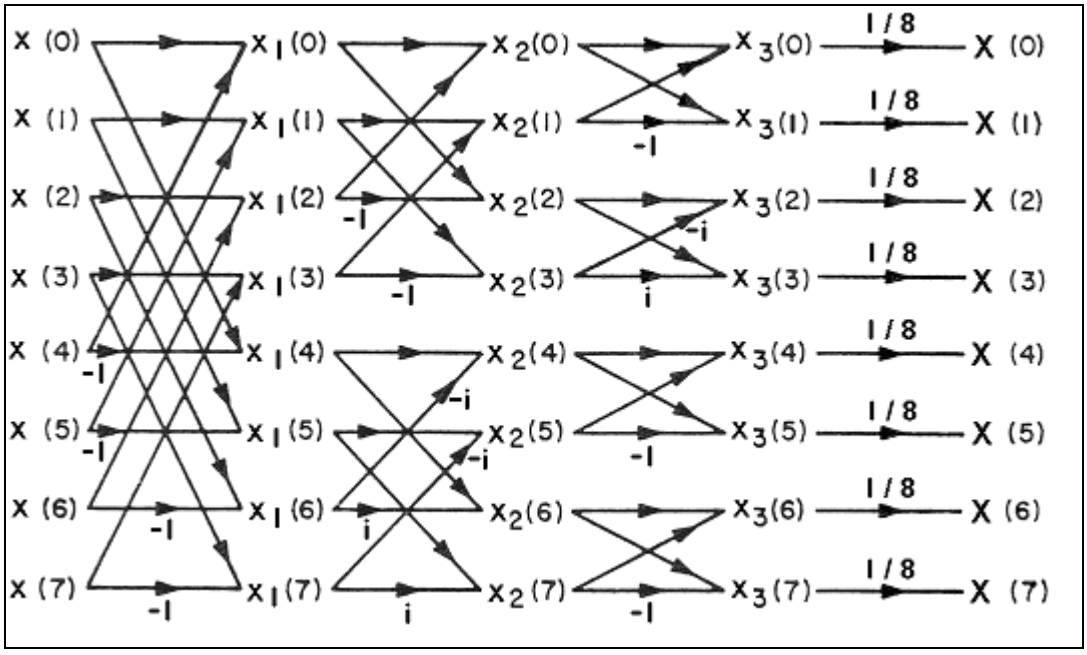

Fig.1. The signal flow graphs for CBT $(n = 3)$.

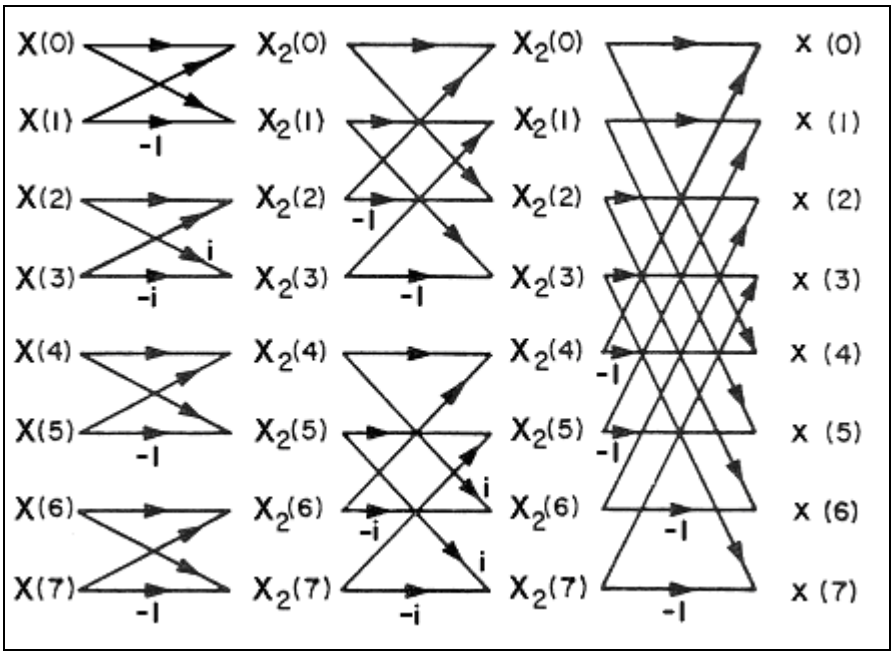

Fig.2. The signal flow graphs for ICBT $(n = 3)$.

3. Two-dimensional spatial correlator in basis of complex BIFORE transform

The two-dimensional spatial correlator consists of three planes. Input plane is described by complex function $a(x, y) = c(x, y) \cdot e^{i\theta(x,y)}$, where $c(x, y)$ is the container image, $\theta(x, y)$ is the phase function of the input domain. The frequency plane is described by key function $K(u, v) = e^{i\phi(u,v)}$, where $\phi(u, v)$ is a random function uniformly distributed on the interval $(-\pi, \pi)$ [10], $K(u, v)$ is a phase-only function. The computational problem is to find such phase function $\theta(x, y)$ to having placed function $a(x, y)$ in input plane, receive in output plane complex function with magnitude that is equal to the hidden image $h(x, y)$. Then output plane is described by the complex function $b(x, y) = h(x, y) \cdot e^{i\psi(x,y)}$, where $\psi(x, y)$ is the phase function of the output domain. Therefore the output correlation function is

$$b(x, y) = ICBT\left[CBT\{a(x, y)\} \cdot K(u, v)\right], \tag{5}$$

From Eq.5, the input function is given by

$$a(x, y) = ICBT\left[CBT\{b(x, y)\} \cdot K^*(u, v)\right], \tag{6}$$

where $K^*(u,v)$ denotes complex conjugation to $K(u,v)$. CBT and ICBT are the complex BIFORE transform and the inverse complex BIFORE transform, respectively.

To calculate phase function $\theta(x,y)$ we have used the projection-onto-constraint-sets (POCS) algorithm. The version of this algorithm, optimized for correlation between two images, is described in [11]. POCS starts with random initialization of the phase function $\theta(x,y)$. On each iteration of the algorithm, function $a(x,y)$ from the input domain is transformed to function $b(x,y)$ from the output domain according to (5), and then function $b(x,y)$ is transformed backward to $a(x,y)$ according to the correlation described in (6). At each iteration complex functions $a(x,y)$ and $b(x,y)$ are projected onto the constraint sets in every of the two domains. In the input domain constraint sets describe probability of the getting container image $c(x,y)$, in the output domain constraint sets describe probability of the getting hidden image $h(x,y)$. In the output plane the projection P_1 is obtained as:

$$P_1\left[b_j(x,y)\right]=\begin{cases} h(x,y)\cdot e^{i\varphi_j(x,y)}, if\ (x,y)\in W \\ b_j(x,y), otherwise \end{cases}, \tag{7}$$

where W is a window contained hidden. In the input plane projection P_2 is obtained as:

$$P_2\left[a_j(x,y)\right]=c(x,y)\cdot e^{i\theta_j(x,y)}. \tag{8}$$

The algorithm is ended on *n-th* iteration, when average mean square errors down relatively to average mean square value of an original images less then predefined threshold (in percent). The necessary conditions of the convergence these errors are considered in [12]. This threshold must provide enough approximation magnitude $|b_n(x,y)|$ to the hidden image $h(x,y)$, and magnitude $|a_n(x,y)|$ to $c(x,y)$. Average mean square values of original images are described as:

$$c_{cp}=\frac{1}{D^2}\sum_x\sum_y c^2(x,y) \tag{9}$$

$$h_{cp}=\frac{1}{D_W{}^2}\sum_x\sum_y h^2(x,y). \tag{10}$$

Note that key function $K(u,v)$ is generated once before iterations and it never changes within the iteration process. The block diagram of the POCS algorithm is shown on Fig.3.

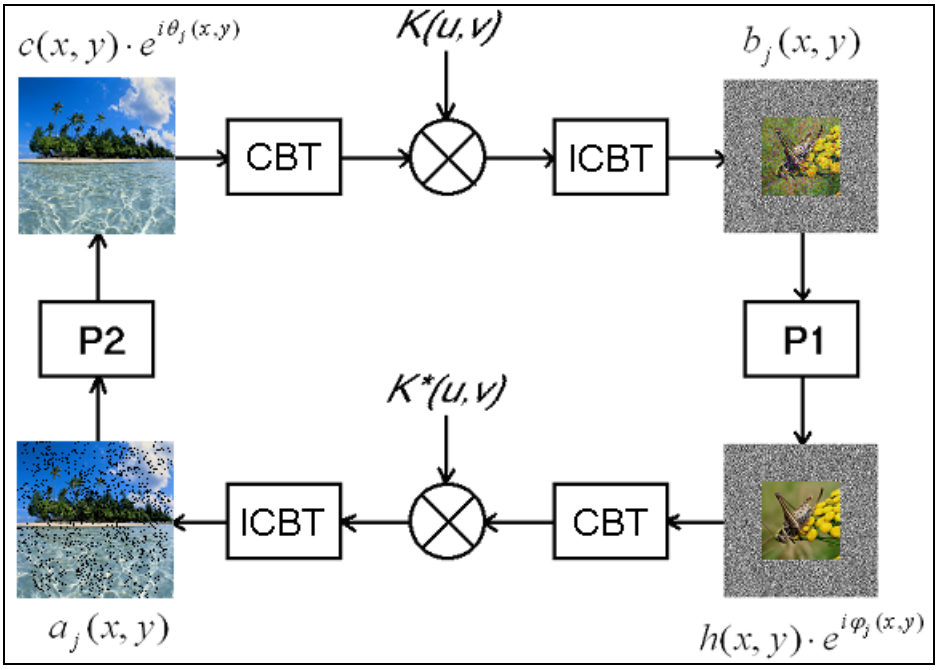

Fig.3. Block diagram of the POCS algorithm.

4. Embedding and extracting hidden image

We grouped respectively colour components (red, green and blue) of the container image and hidden image. And then the correlator is learnt for each these pairs. In result of this operations for each colour component we have received complex function $a_n(x,y)$ described by two linear functions $c_n(x,y)$ and $\theta_n(x,y)$, where n - count of the iterations spent for training. Now it is required to generate color component of the stego-image on the basis of these two functions.

Let m is a number of bits, required for storage every color component. Let the $Ph(x,y)$ is approximation to the function $\theta_n(x,y)$, that was received by quantization on 2^r levels $(r<m)$, where r is a number of bits for storage the phase function $\theta_n(x,y)$. The every color component of the stego-image is constructed by the following algorithm. The brightness of every pixel for each color component equals the brightness respectively pixel of the halftone container image, except for r lower bits. These r lower bits are replaced by value of the function $Ph(x,y)$. This replacement is possible since modification several lower bits does not heavily distort total picture of the image. Obviously that r must be not more than half m. Number of bits used for storage phase, is directly

proportional to quality of the reconstructed hidden image, but on the other hand it is inversely proportional to quality of the stego-image. The stego-image that is received in such way we can send by open telecommunication channels.

On the receiving side from each color component stego-image we get two functions $Ph(x, y)$ and $c'(x, y)$. $Ph(x, y)$ is described by r lower bits of the color component of the stego-image, and $c'(x, y)$ is described by $(m-t)$ lower bits. After normalization $Ph(x, y)$ and $c'(x, y)$ the next correlation is calculated:

$$b(x, y) = ICBT\left[CBT\left\{c'(x, y) \cdot e^{iPh(x,y)}\right\} \cdot K(u, v)\right]. \quad (11)$$

The magnitude of the received complex function $|b(x, y)|$ is approximately equal to respectively color component of the hidden image $h(x, y)$.

5. Experimental results

We have tested the system for three pairs images (hidden and the container- image). As the container and hidden images for all three cases, we used color (24 bits per pixel) pictures in the size 512×512 and 256×256 of pixels, respectively.

Training of the correlator was stopped, during that moment when the total mean-square error made less than 1% of average value of the image for every picture (7), (8). The algorithm of training was taken on the average 9 iterations for each color pair. The technique was tested with various count of the bits used for storage of a phase (parameter r - see section 3). Results of experiment are represented on Fig. 4.

During experiment the next parameters have been determined: a) the degree of difference of the transmitted stego-image from the container-image; b) the degree of difference of the extracting hidden image from original hidden image. The measure of difference was defined as average total distinction between all pixels of pair images. Results first pair of images are displayed in Table 1.

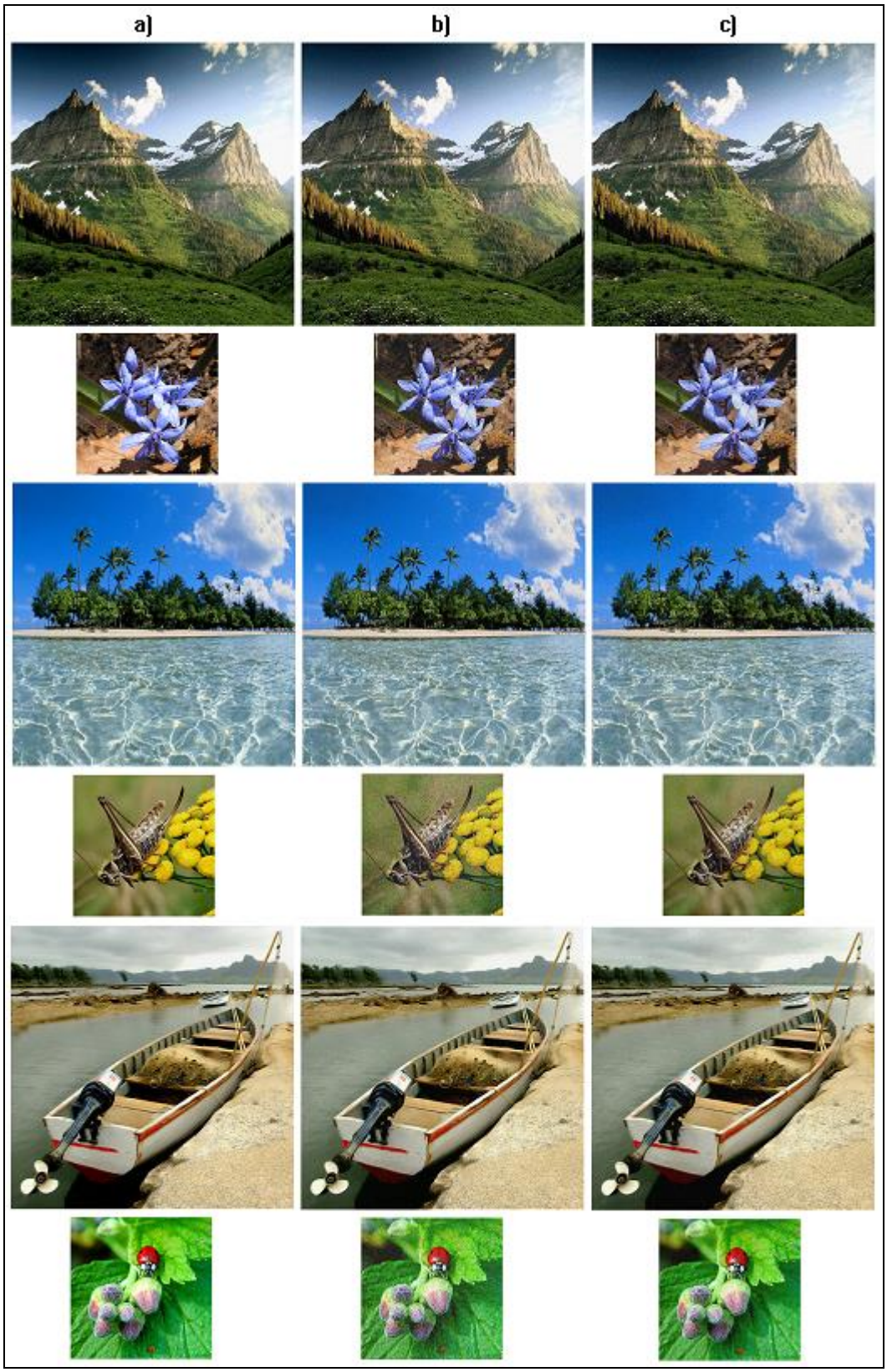

Fig.4. a) Original container and stego images;

b) Stego image and reconstructed hidden image (number of bits for coding phase r=3);

c) Stego image and reconstructed hidden image (number of bits for coding phase r=4);

Table 1. Degree of difference of pairs images.

	Number of bits needed for storage phase	
	$r = 3$	$r = 4$
Stego-image and container-image	1.9%	2.5%
Extracting image and hidden image	6.9%	4.5%

Besides the basic experiment we have tested the system for stability to losses or purposely damage part of the information by transfer of the stego-image. Stability of system was checked as follows: in the transmitted image were emulated losses a part (15 %, 30 % and 45 %) of pixels - area with zero intensity. The result of experiment is shown on Fig.5.

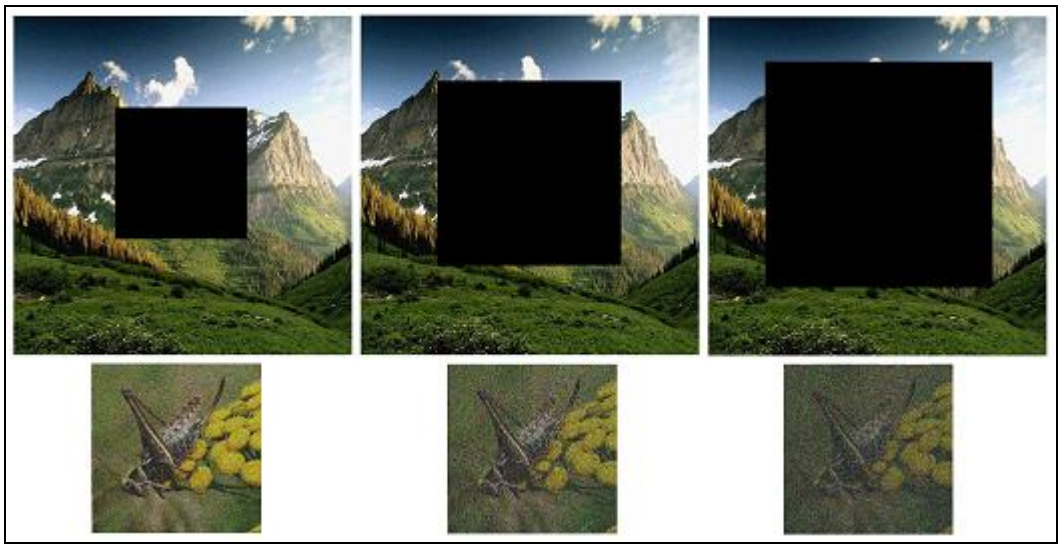

Fig.5. Stego-images with loss a part of pixels and the hidden images taken from them (the number of bits for storage the phase $r = 4$).

6. Conclusion

The steganographic system of the hidden transfer of color pictures optimized on computing complexity is offered. The algorithm of embedding and extracting is based on the modified model of the two-dimensional spatial correlator. Digital correlations are based on complex BIFORE transform. The secret key of stego-system is embedded into the correlator as the spatial filter.

Experiments for three pairs images and various values of parameter r (number of the bits needed for storage of a phase in the transmitted stego-image) are conducted. Such important qualitative characteristics of system, as a degree of difference of the transmitted stego-image from the original container- image and a degree of difference of the taken hidden image from original hidden image, for various parameters r are calculated. The optimum ratio of quality is shown for a case $r = 4$.

Stability of algorithm to losses or purposely damage of a part of the transmitted information is checked up. It is established, that images recognizable even at loss of 30 % of pixels of the stego-image. Thus, proposed steganographic system allows steadily and safely to transfer color pictures.

References

1. B. Javidi; "Securing information with optical technologies," *Phys. Today* 50(3), (1997), pp. 27–32.
2. B. Javidi and E. Ahouzi; "Optical security system with Fourier plane encoding," *Appl. Opt.* 37, (1998), 6247–6255.
3. B. Javidi, L. Bernard, and N. Towghi; "Noise performance of double-phase encryption compared to XOR encryption," *Opt.Eng.* 38, (1999), 9–19.
4. S. Kishk, B. Javidi; "Information hiding technique with double phase encoding", *Applied Optics* (Vol.41, No.26) 10 September 2002, pp.5462-5470.
5. V.G. Gribunin; „Digital steganography", St.-Petersburg, OOO Solon-Press, 2002.
6. N. Ahmed, K. R. Rao; "A decomposition technique for complex N-periodic sequences", IEEE Trans. Audio Electroacoust., Dec. 1971, pp. 324-326.
7. F. R. Ohnsorg; "Binary Fourier representation", presented at the Spectrum Analysis Techniques Symp., Honeywell Res. Cen., Hopkins. Minn., Sept. 20-21, 1996.
8. N. Ahmed, K. R. Rao, R. B. Schultz; "Generalized discrete transform", IEEE Trans., vol.59, Sept. 1971, pp.1360-1362.
9. N. Ahmed, K. R. Rao, and A. L. Abdussattar; "BIFORE or Hadamard transform", IEEE Trans. Audio Electroacoust., vol. AU-19, Sept. 1971, pp. 225-234.
10. J. Rosen; "Learning in correlators based on projections onto constraint sets," *Opt. Lett*.18, (1993), pp.1183–1185.
11. Y. Li, K. Kreske, and J. Rosen; "Security and encryption optical systems based on a correlator with significant output images," *Appl. Opt.* 39, (2000), pp.5295–5301.

12. J. Rosen, B. Javidi; “Hidden images in halftone pictures”, Applied Optics (Vol.40, No.20) 10 July 2001, pp.3346-3353.

The research is partially supported by the Belarussian Republican Foundation of Fundamental Research, grant T0 3- 0 52.