МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 9, № 1-2

Volume 9, No. 1-2

Одеса – 2019
Odesa – 2019

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 621.396.946

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 5-14

EFFECT OF BINARY ORTHOGONAL TRANSFORM TYPE ON THE CARDINALITY AND STRUCTURE OF CONSTANT AMPLITUDE CODES FOR THE MC-CDMA TECHNOLOGY

A.V. Sokolov

Odesa National Polytechnic University,
Shevchenko ave. 1, Odesa, 65044, Ukraine; e-mail: radiosquid@gmail.com

One of the most important multiple access technologies used in modern mobile telecommunication systems is MC-CDMA technology, in which Walsh-Hadamard transform coefficients are used as transmitted signals. Despite the significant advantages of MC-CDMA technology, its significant disadvantage is the high PAPR (Peak-to-Average Power Ratio) values of the transmitted signals. One of the most effective methods to overcome this disadvantage is the use of C-codes, each codeword of which has a strictly defined PAPR value. This paper is devoted to the research of the influence of the type of binary orthogonal transform on the structure and cardinality of C-codes, which can be built on its basis. It is established that the class of classical bent-sequences with respect to the Walsh-Hadamard matrix constructed using the Sylvester construction is only a special case of the class of binary bent-sequences. It was established that similar classes of bent-sequences exist for two other nonequivalent classes of Hadamard matrices, as well as for Hadamard matrices constructed on the basis of other perfect algebraic constructions: perfect binary arrays and, in fact, classical bent-sequences. So, in the paper, algebraic normal forms of bent-sequences constructed with respect to the second and third nonequivalent Hadamard matrices of order n=16 are listed. The structure and cardinality of classes of bent-sequences constructed with respect to Hadamard matrices synthesized based on perfect binary arrays and classical bent-sequences were researched. Using the found new classes of bent-sequences, as well as the concept of operative changing of the working orthogonal transform matrix, it will be possible to reduce the redundancy of C-codes used in MC-CDMA technology while maintaining the PAPR of the transmitted signals at a minimal level.

Keywords: Peak-to-Average Power Ratio, C-code, MC-CDMA, bent-sequence, perfect binary array.

Introduction and problem statement

The key technology used to build new generation mobile communication systems is Multi-Code Code Division Multiple Access (MC-CDMA) technology, in which communication channels have the same frequency band, but different code manipulation [1]. MC-CDMA technology has many advantages, such as high noise immunity, flexible distribution of resources among subscribers, high security level, and greater energy efficiency.

MC-CDMA technology is based on the coding model of the transmitted information using an orthogonal transform to implement the concept of code division of channels (Fig. 1).

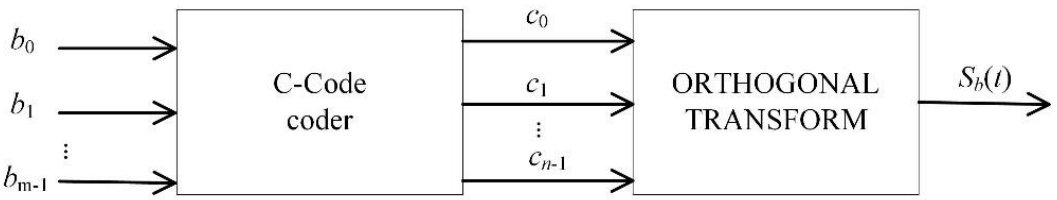


Fig. 1. Information coding model based on orthogonal transform

Thus, the original message d_i is encoded using a set of codewords c_j of the C-code, which are fed to the input of the Walsh-Hadamard orthogonal transform unit, and further to the transmitter.

One of the most significant requirements for the C-code is its ability to form output signals with an optimal PAPR value

$$\kappa = \frac{P_{\max}}{P_{av}} = \frac{1}{n} \max_t \left\{ \left| S_c(t) \right|^2 \right\}, \quad (1)$$

where $P_{\max}$ is the peak power of $S_c(t)$ signal; P_{av} is the average power of signal $S_c(t)$; n is the length of signal $S_c(t)$.

Achieving the optimal value of the PAPR can significantly increase the energy and spectral efficiency of the communication system, reduce the levels of out-of-band emissions, nonlinear distortion, and facilitate the reception and demodulation of the transmitted signal.

The researches [2] led to the conclusion that the optimal value of the PAPR $\kappa = 1$ can be achieved only by the use of such perfect algebraic constructions as bent-sequences [3], which have uniform absolute values of the Walsh-Hadamard transform coefficients. However, the number of bent-sequences is small, for example, for the length $N = 16$ their class cardinality is equal to $J_{16} = 896$ [4], which leads to significant redundancy of code, which is spent only on reducing the PAPR of the output signal. The possibility of increasing the cardinality of classes of available signals with an optimal value of the PAPR may lie in the consideration of new types of orthogonal transforms, but this issue has not been considered well in the literature.

The purpose of this paper is to research new classes of orthogonal transform matrices of order $\lambda = 16$ in terms of the possibility of the constructing the C-codes with an optimal PAPR value κ.

Definition 1 [5]. The Hadamard matrix A of order λ is a such matrix that all its elements take values from the set $\{\pm 1\}$ and the following identity is valid

$$A \cdot A = \lambda E,$$

where T is the transpose operator, E is the identity matrix.

As an orthogonal transform in communication systems with MC-CDMA technology, the well-known Hadamard matrices of order $\lambda = 2^k$ obtained using the recurrent rule are often used

$$A_{2^k} = \begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix}, \quad (2)$$

where $A_1 = 1$.

Equivalent classes of Hadamard matrices of order $N = 16$

Definition 2 [6]. The Hadamard matrices obtained from each other by repeated using of the operations of inversion and permutation of rows or columns are called as equivalent.

It was shown in [6] that for the orders of Hadamard matrices $\lambda = 1; 2; 4; 8$ there is only one class of equivalent Hadamard matrices, whose representative matrix can be obtained by using the recurrent rule (2). For the order $\lambda = 16$, there are 5 equivalent classes of Hadamard matrices, whose representatives are shown in Fig. 2.

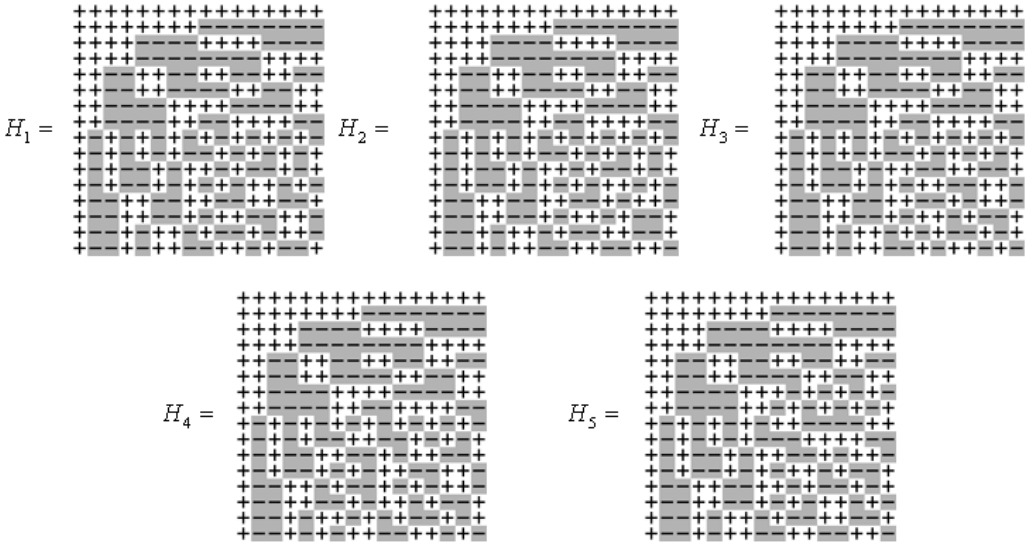


Fig. 2. Equivalent classes of Hadamard matrices

Using each of the Hadamard matrices shown in Fig. 2 as an orthogonal transform in the model (Fig. 1) and the full code as the C-code, we construct (Table 1) the PAPR distribution tables calculated in accordance with (1) [7].

Table 1.

The PAPR distribution for full code vectors for different non-equivalent matrices

No.	Absolute peak value $P_{\max}$	PAPR value κ	The number of vectors for the matrix				
			H_1	H_2	H_3	H_4	H_5
1	16	1	896	384	128	0	0
2	36	2,25	14336	14336	14336	14336	14336
3	64	4	28000	28512	28768	28896	28896
4	100	6,25	17920	17920	17920	17920	17920
5	144	9	3840	3840	3840	3840	3840
6	196	12,25	512	512	512	512	512
7	256	16	32	32	32	32	32

It is clear that of the greatest practical interest from the point of view of construction of the C-codes are the vectors from group No. 1 (Table 1), which have the optimal value of the PAPR $\kappa = 1$. For the matrix H_1, each such codeword is a bent-sequence of length $N = 16$, a regular synthesis method of which was developed in [4].

Definition 3 [7]. A binary sequence $B = [b_0, b_1, \cdots, b_i, \cdots, b_{n-1}]$ of length n, where $b_i \in \{\pm 1\}$ are the coefficients, $i = 0,1,...,n-1$, $n = 2^k, k = 2,4,6,8,...$, is called a bent-sequence, if it has a uniform Walsh-Hadamard spectrum $W_B(\omega)$.

We call a bent-sequence as classical if Definition 3 is valid for Walsh-Hadamard matrix of classical structure (2).

Thus, the number of bent-sequences is different for each nonequivalent class of orthogonal transform (Fig. 2). However, research have shown that the codewords of the C-code formed from the vectors of group No. 1 for the orthogonal transform matrix H_1 include the vectors for the matrix H_2 and H_3. In other words, the matrices H_2 and H_3 do not allow obtaining new structures of bent-sequences.

Definition 4 [8]. The algebraic normal form (ANF) $\varphi(x_1, x_2, ..., x_k)$ of a sequence T is a polynomial of $k \le \log_2 n$ variables with coefficients $a_i \in \{0,1\}$, where the AND operation is used as the multiplication, and the XOR operation is used as the addition operation

$$\varphi\left(x_1, x_2, ..., x_k\right) = \bigoplus_{i=0}^{n-1} a_i X_i^s,$$

where X_i^s are the terms of the ANF polynomial of degree $s = wt\{X\}$; wt is the Hamming's weight. The coefficients $a_i = \{a_0, a_1, ..., a_{n-1}\}$ can be found by performing the Reed-Muller transform [8], i.e. by multiplying the original sequence by the Reed-Muller matrix RM_v

$$\{a_i\} = TRM_v, T = \{a_i\}RM_v,$$

where the original sequence T is represented above the alphabet $\{0,1\}$ using a bijective mapping $+1 \leftrightarrow 0, -1 \leftrightarrow 1$, and the Reed-Muller matrix RM_v is determined using the following recurrent rule

$$RM_0 = [1], RM_v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes RM_{v-1} = \begin{bmatrix} RM_{v-1} & 0 \\ RM_{v-1} & RM_{v-1} \end{bmatrix},$$

where $\otimes$ is the Kronecker product.

Definition 5 [8]. Terms of ANF of the degree $s = wt\{X\} \le 1$ are called as affine.

For example, for sequence length $n = 16$ there are the following possible affine terms: $1, x_1, x_2, x_3, x_4$ on the basis of which corresponding affine codewords can be formed.

The modern approach to the classification, as well as the synthesis of bent-sequences, involves the use of the following proposition.

Proposition 1 [3]. The sum of a bent-sequence with an affine function (which is equivalent to adding one or several affine terms to the ANF coefficients sequence) leads to the formation of other bent-sequences.

The researches performed in this paper allowed us to establish that Proposition 1 is valid for bent-sequences, both on the basis of the orthogonal transform matrix H_1, and for the bent-sequences on the basis of the orthogonal transform matrices H_2 and H_3.

Thus, the full set of bent-sequences of cardinality $J = 896$ can be classified into $896/32 = 28$ affine non-equivalent classes, in each of which it is possible to distinguish a bent-sequence that does not have affine terms

$b_1 = x_2x_3 + x_1x_4;$
$b_2 = x_2x_3 + x_1x_4 + x_1x_2;$
$b_3 = x_2x_3 + x_1x_4 + x_1x_3;$
$b_4 = x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2;$
$b_5 = x_2x_4 + x_1x_3;$
$b_6 = x_2x_4 + x_1x_3 + x_1x_2;$
$b_7 = x_2x_4 + x_1x_4 + x_1x_3;$
$b_8 = x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2;$
$b_9 = x_2x_4 + x_2x_3 + x_1x_3;$
$b_{10} = x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2;$
$b_{11} = x_2x_4 + x_2x_3 + x_1x_4;$
$b_{12} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2;$
$b_{13} = x_3x_4 + x_1x_2;$
$b_{14} = x_3x_4 + x_1x_3 + x_1x_2;$
$b_{15} = x_3x_4 + x_1x_4 + x_1x_2;$
$b_{16} = x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2;$
$b_{17} = x_3x_4 + x_2x_3 + x_1x_2;$
$b_{18} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2;$
$b_{19} = x_3x_4 + x_2x_3 + x_1x_4;$
$b_{20} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3;$
$b_{21} = x_3x_4 + x_2x_4 + x_1x_2;$
$b_{22} = x_3x_4 + x_2x_4 + x_1x_3;$
$b_{23} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_2;$
$b_{24} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3;$
$b_{25} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_2;$
$b_{26} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3;$
$b_{27} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4;$
$b_{28} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2.$

Similarly, we can represent all bent-sequences relating to the matrix H_2 up to an affine term

$$
\begin{array}{ll}
b_1 = x_2x_3 + x_1x_4; & b_7 = x_2x_4 + x_2x_3 + x_1x3; \\
b_2 = x_3x_4 + x_2x_3 + x_1x_4; & b_8 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3; \\
b_3 = x_2x_4 + x_2x_3 + x_1x_4; & b_9 = x_2x_4 + x_1x_4 + x_1x_3; \\
b_4 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4; & b_{10} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3; \\
b_5 = x_2x_4 + x_1x_3; & b_{11} = x_2x_3 + x_1x_4 + x_1x_3; \\
b_6 = x_3x_4 + x_2x_4 + x_1x_3; & b_{12} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3.
\end{array}
$$

We also represent a set of bent-sequences relating to the matrix H_3 up to an affine term

$$
\begin{array}{ll}
b_1 = x_2x_3 + x_1x_4; & b_3 = x_2x_4 + x_2x_3 + x_1x_4; \\
b_2 = x_3x_4 + x_2x_3 + x_1x_4; & b_4 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4.
\end{array}
$$

Let us consider the well-known regular rules for constructing matrices of orthogonal transforms on the basis of perfect algebraic constructions and research their influence on the type and cardinality of the code.

The matrices of orthogonal transforms based on perfect binary arrays

Definition 6 [9]. A perfect binary array (PBA) is a two-dimensional matrix sequence

$$H(N) = \left\| h_{i,j} \right\|, \quad i, j = \overline{0, N-1}, \quad h_{i,j} \in \{-1, 1\},$$

having an ideal two-dimensional Periodic Autocorrelation Function (PACF), whose elements

$$R(m,\tau) = PACF\left(m,\tau\right) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} h_{i,j}h_{i+m,j+\tau} = \begin{cases} N^2, & for \;\; m = \tau = 0; \\ 0, \text{ for any other } m \text{ and } \tau. \end{cases}$$

It is known that the generating $P(N)$ PBA class of order $N = 4$ consists of 12 arrays [9]

$$
\begin{array}{llll}
P_1(4) = \begin{bmatrix} -&+&-&- \\ -&-&+&- \\ +&+&+&- \\ +&-&-&- \end{bmatrix}, & P_2(4) = \begin{bmatrix} +&+&-&+ \\ +&-&-&- \\ -&-&+&- \\ +&-&-&- \end{bmatrix}, & P_3(4) = \begin{bmatrix} -&+&-&- \\ -&+&+&+ \\ -&+&-&- \\ +&-&-&- \end{bmatrix}, & P_4(4) = \begin{bmatrix} +&+&+&- \\ -&-&+&- \\ -&+&-&- \\ +&-&-&- \end{bmatrix}, \\
P_5(4) = \begin{bmatrix} +&-&+&+ \\ +&-&-&- \\ -&+&-&- \\ +&-&-&- \end{bmatrix}, & P_6(4) = \begin{bmatrix} -&-&+&- \\ +&+&-&+ \\ +&-&-&- \\ +&-&-&- \end{bmatrix}, & P_7(4) = \begin{bmatrix} +&+&-&+ \\ -&-&+&- \\ +&-&-&- \\ +&-&-&- \end{bmatrix}, & P_8(4) = \begin{bmatrix} -&+&+&+ \\ +&-&-&- \\ +&-&-&- \\ +&-&-&- \end{bmatrix}, \\
P_9(4) = \begin{bmatrix} +&-&-&+ \\ -&+&-&+ \\ +&+&-&- \\ -&-&-&- \end{bmatrix}, & P_{10}(4) = \begin{bmatrix} -&+&+&- \\ -&+&-&+ \\ +&+&-&- \\ -&-&-&- \end{bmatrix}, & P_{11}(4) = \begin{bmatrix} +&-&-&+ \\ +&-&+&- \\ +&+&-&- \\ -&-&-&- \end{bmatrix}, & P_{12}(4) = \begin{bmatrix} -&+&+&- \\ +&-&+&- \\ +&+&-&- \\ -&-&-&- \end{bmatrix}.
\end{array}
\qquad (3)
$$

On the basis of each of the arrays (3) of the generating $P(N)$-class, an orthogonal matrix can be constructed by successively concatenating (joining) the rows of the original array and all its cyclic shifts in rows and columns. As an example, we give an orthogonal matrix constructed on the basis of the PBA $P_1(4)$

$$\psi_1 = \begin{bmatrix} -+----+-+++-+--- \\ --+-----+-+++-+-- \\ ---+++---+-+-+--+- \\ +----+--+++-+---+ \\ +----+-----+-+++- \\ -+----+-----+-+++ \\ --+-----+---+-+++ \\ ---+++----+--+++- \\ +++-+----+----+-- \\ -+++-+----+----+- \\ +-+++--+----+--- \\ ++-+---+----+--- \\ --+-+++-+----+-- \\ ---+-+++-+----+- \\ +---+-+--+----+- \\ -+--+++--+----+- \end{bmatrix}.$$

Our experiments show that if the full code is used as a C-code each matrix $\psi_1,...,\psi_{12}$ gives the same PAPR value distribution as the matrix H_1 (Table 1).

So, if using the orthogonal transform based on the PBA it is possible to construct 896 sequences that have uniform absolute values of the Walsh-Hadamard transform coefficients.

Thus, the matrices $\psi_1,...,\psi_{12}$ produce $12 \cdot 896 = 10752$ bent-sequences. Considering each of them in comparison with the classical definition of a bent-sequence it was established that from the set of 10752 bent-sequences there are only 5120 unique ones, and there are $5120 - 896 = 4224$ ones that do not coincide with the class of classical bent-sequences. Let us give a classification of all newly discovered bent-sequences classes (Table 2).

Table 2.

Classes of bent-sequences based on PBA $P(N)$ class

Class Number	1	2	3	4	5	6
The orthogonal transform matrix	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6
Cardinality of the bent-sequences class	896	896	896	896	896	896
The number of bent-sequences, that coincide with the classical bent-sequences	128	384	128	128	128	128
The number of bent-sequences, that do not coincide with the classical bent-sequences	768	512	768	768	768	768
Class Number	7	8	9	10	11	12
The orthogonal transform matrix	ψ_7	ψ_8	ψ_9	ψ_{10}	ψ_{11}	ψ_{12}
Cardinality of the bent-sequences class	896	896	896	896	896	896
The number of bent-sequences, that coincide with the classical bent-sequences	128	384	128	128	128	128
The number of bent-sequences, that do not coincide with the classical bent-sequences	768	512	768	768	768	768

As an example, let us consider Class 1 of bent-sequences constructed on the basis of the matrix ψ_1 (Fig. 3). Based on this matrix, it is possible to build 768 new structures of bent-sequences that do not coincide with classical bent-sequences.

The performed researches have also shown that Proposition 1 is not valid in this class of bent-sequences. Thus, the sum of a bent-sequence with an affine codeword does not necessarily form a bent-sequence. However, in this paper, the following property of the class of bent-sequences relating to the matrix ψ_1 was established:

Property 1. The sum of a bent-sequence relating to matrix ψ_1 with an affine terms $1, x_4, x_2, x_1$ leads to the formation of other bent-sequences.

Using *Property 1* we can represent this set of bent-sequences relating to matrix ψ_1 in the $896/16=56$ ANF up to affine terms $1, x_4, x_2, x_1$

$b_1 = 0;$
$b_2 = x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_3 = x_1x_4 + x_1x_2;$
$b_4 = x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_5 = x_2x_3 + x_1x_2;$
$b_6 = x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_7 = x_2x_3 + x_1x_4 + x_1x_2;$
$b_8 = x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_9 = x_2x_4;$
$b_{10} = x_2x_4 + x_1x_3 + x_1x_2x_4;$
$b_{11} = x_2x_4 + x_1x_4 + x_1x_2;$
$b_{12} = x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{13} = x_2x_4 + x_2x_3 + x_1x_2;$
$b_{14} = x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4;$
$b_{15} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2;$
$b_{16} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{17} = x_3x_4;$
$b_{18} = x_3x_4 + x_1x_2;$
$b_{19} = x_3x_4 + x_1x_3 + x_1x_2x_4;$
$b_{20} = x_3x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{21} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4;$
$b_{22} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{23} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{24} = x_3 + x_3x_4;$
$b_{25} = x_3x_4 + x_2x_4;$
$b_{26} = x_3x_4 + x_2x_4 + x_1x_2;$
$b_{27} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{28} = x_3;$
$b_{29} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{30} = x_3 + x_1x_3 + x_1x_2x_4;$
$b_{31} = x_3 + x_1x_4 + x_1x_2;$
$b_{32} = x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{33} = x_3 + x_2x_3 + x_1x_2;$
$b_{34} = x_3 + x_2x_3 + x_1x_3 + x_1x_2x_4;$
$b_{35} = x_3 + x_2x_3 + x_1x_4 + x_1x_2;$
$b_{36} = x_3 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{37} = x_3 + x_2x_4;$
$b_{38} = x_3 + x_2x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{39} = x_3 + x_2x_4 + x_1x_4 + x_1x_2;$
$b_{40} = x_3 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{41} = x_3 + x_2x_4 + x_2x_3 + x_1x_2;$
$b_{42} = x_3 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{43} = x_3 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2;$
$b_{44} = x_3 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{45} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{46} = x_3 + x_3x_4 + x_1x_2;$
$b_{47} = x_3 + x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{48} = x_3 + x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{49} = x_3 + x_3x_4 + x_2x_4;$
$b_{50} = x_3 + x_3x_4 + x_2x_4 + x_1x_2;$
$b_{51} = x_3 + x_3x_4 + x_2x_4 + x_1x_3 + x_1x_2x_4;$
$b_{52} = x_3 + x_3x_4 + x_2x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{53} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4;$
$b_{54} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4;$
$b_{55} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4;$
$b_{56} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4.$

Orthogonal transform matrices based on the full class of classical bent-sequences

In [10] it was shown that the construction of orthogonal transform matrices is also possible on the basis of the classical bent-sequences themselves by applying a regular dyadic shift operator

$$Dyad(N) = \begin{bmatrix} Dyad(N/2), & Dyad(N/2)+N/2 \\ Dyad(N/2)+N/2, & Dyad(N/2) \end{bmatrix},$$

where $Dyad(2) = \begin{bmatrix} 1, 2 \\ 2, 1 \end{bmatrix}$. For example, for a value $N = 16$, we get

$$Dyad(16) = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\
3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\
4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\
5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\
6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\
7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\
8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
10 & 9 & 12 & 11 & 14 & 3 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\
11 & 12 & 9 & 10 & 15 & 16 & 3 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\
12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\
13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\
14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\
15 & 16 & 13 & 14 & 11 & 2 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\
16 & 15 & 14 & 13 & 12 & 1 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}. \quad (4)$$

Performing the permutation of the elements of the bent-sequence in accordance with the rules (lines) of the dyadic shift matrix, we obtain a binary matrix γ of the orthogonal transform.

It is known [3] that the cardinality of the class of classical bent-sequences of length $n=16$ is $J_{16}=896$. Thus, based on the dyadic shift operator (4), it is possible to construct the same number of orthogonal transform matrices $\gamma_1,\gamma_2,...,\gamma_{896}$. It is clear that with respect to each of these orthogonal matrices there are their own bent-sequences classes — binary vectors with uniform absolute values of transform coefficients. Researches have shown that the number of such bent-sequences relating to each of the orthogonal transform matrices is also 896. Thus, there was constructed $896*896=802816$ bent-sequences.

It was discovered that just 1152 of these differs in structure from the classical bent-sequences [3].

Conclusion

Let us summarize the main results achieved in this paper:

- the method of synthesis of C-codes classes with uniform Walsh-Hadamard transform coefficients was further developed, it was established that the cardinality and the specific type of C-code strongly depends on the type of selected orthogonal transform.
- the using of methods for the synthesis of orthogonal matrices based on perfect binary arrays, a dyadic shift operator and classical bent-sequences allowed us to construct new families of bent-sequences that can be used as C-codes, and each of the sets of bent-sequences possesses optimal error correction ability.
- it was found that the existence of various structures of bent-sequences relating to orthogonal matrices based on perfect binary arrays, a regular dyadic shift operator and classical bent-sequences, allows to improve the MC-CDMA technology in the following aspects: by combining the found classes of bent-sequences and dynamically changing the orthogonal transform matrix depending on the data vectors arriving to its input, it is possible to reduce redundancy of the code that is spent on achieving the optimal PAPR value; by dynamically changing the orthogonal transform matrices using a pseudo-random sequence, which is unknown to the third party, it is possible to implement a secret communication system with a minimal computational cost for data encryption and decryption.

We also note that, in the case of other values of n, the problem of finding existing full classes of bent-sequences relating to the all regularly constructed orthogonal transforms, which is relevant from the point of view of MC-CDMA technology, remains unresolved and may be continued in the future.

References

1. Paterson, K.G. On codes with low peak-to-average power ratio for multicode CDMA / K.G. Paterson // IEEE Transactions on Information Theory. – 2004. – Vol. 50, No. 3. – Pp. 550 -559.
2. Paterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory / K.G. Paterson // Sequences and their applications, Seta 2001: Second Int. Conference, May 13–17 2001 : proceedings. – Bergen, Norway : Springer, 2002. – Pp. 46-71.
3. Tokareva, N. Bent Functions: Results and Applications to Cryptography / N. Tokareva. – Academic Press, 2015. – 220 p.
4. Mazurkov, M.I. The regular rules of constructing the complete class of bent-sequences of length 16 / M.I. Mazurkov, A.V. Sokolov // Proceedings of ONPU. – 2013. – No. 2(41). – Pp. 231-237.
5. Mazurkov, M.I. Broadband radio communication systems / M.I. Mazurkov. – Odessa: Science and Technology, 2010. – 340 p.
6. Hadamard matrices of order 16: Research Summary: Vol I, No. 36–10 / Jet Propulsion Laboratory; M.Jr. Hall. – 1961. – Pp. 21-26.

7. Mazurkov, M.I. On the effect of the type of orthogonal transform on PAPR of signal spectrum in CDMA systems / M.I. Mazurkov, A.V. Sokolov, N.A. Barabanov // Informatics and Mathematical Methods in Modeling. – 2015. – Vol. 5, No. 1. – Pp. 28-37.
8. Logachev, O.A. Boolean Functions in Coding Theory and Cryptography / O.A. Logachev, A.A. Salnikov, V.V. Yashchenko. – Amer Mathematical Society, 2012. – 334 p.
9. Mazurkov, M.I. Classes of equivalent and generating perfect binary arrays for CDMA technologies / M.I. Mazurkov, V.Ya. Chechelnitsky // Proceedings of the universities. Radioelectronics. – 2003. – Vol. 46, No. 5. – Pp. 54-63.
10. Mazurkov, M.I. Fast orthogonal transforms based on bent-sequences / M.I. Mazurkov, A.V. Sokolov // Informatics and mathematical methods in modeling. – 2014. – No. 1. – P. 5 -13.

ВПЛИВ ТИПУ ДВІЙКОВОГО ОРТОГОНАЛЬНОГО ПЕРЕТВОРЕННЯ НА ПОТУЖНІСТЬ І СТРУКТУРУ КОДІВ ПОСТІЙНОЇ АМПЛІТУДИ ДЛЯ ТЕХНОЛОГІЇ MC-CDMA

А.В. Соколов

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Однією з найважливіших технологій множинного доступу, яка використовується в сучасних мобільних телекомунікаційних системах є технологія MC-CDMA, в якій в якості сигналів, що передаються використовуються коефіцієнти перетворення Адамара. Незважаючи на істотні переваги технології MC-CDMA, її значним недоліком є високий пік-фактор сигналів, що передаються. Одним з найбільш ефективних методів подолання даного недоліку є використання С-кодів, кожне кодове слово яких має строго визначене значення пік-фактора. Ця стаття присвячена дослідженню впливу виду бінарного ортогонального перетворення на структуру і потужність С-кодів, які можуть бути побудовані на його основі. У статті встановлено, що клас класичних бент-послідовностей щодо матриці Адамара, побудованої за допомогою конструкції Сильвестра, є лише окремим випадком класу бінарних бент-послідовностей. Встановлено, що подібні класи бент-послідовностей існують для двох інших нееквівалентних класів матриць Адамара, а також для матриць Адамара, побудованих на основі інших досконалих алгебраїчних конструкцій: досконалих двійкових решіток і, власне, класичних бент-послідовностей. Так, в статті виписані алгебраїчні нормальні форми бент-послідовностей, побудованих щодо другої і третьої нееквівалентних матриць Адамара порядку n=16. Проведено дослідження структури і потужностей класів бент-послідовностей, побудованих відносно матриць Адамара, синтезованих на основі досконалих двійкових решіток і класичних бент-послідовностей. Використання знайдених нових класів бент-послідовностей, а також концепції оперативної зміни робочої матриці ортогонального перетворення, дозволить отримати зменшення надмірності С-кодів, що застосовуються в технології MC-CDMA при збереженні пік-фактора сигналів, що передаються на мінімальному рівні.
Ключові слова: пік-фактор, С-код, MC-CDMA, бент-послідовність, досконала двійкова решітка.

ВЛИЯНИЕ ТИПА ДВОИЧНЫХ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ НА МОЩНОСТЬ И СТРУКТУРУ КОДОВ ПОСТОЯННОЙ АМПЛИТУДЫ ДЛЯ ТЕХНОЛОГИИ MC-CDMA

А.В. Соколов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: anna-odessitka@mail.ru

Одной из важнейших технологий множественного доступа, используемой в современных мобильных телекоммуникационных системах является технология MC-CDMA, в которой в качестве передаваемых сигналов используются коэффициенты преобразования Уолша-Адамара. Несмотря на существенные преимущества технологии MC-CDMA, её значительным недостатком является высокий пик-фактор передаваемых сигналов. Одним из наиболее эффективных методов преодоления данного недостатка является использование С-кодов, каждое кодовое слово которых имеет строго определенное значение пик-фактора. Настоящая статья посвящена исследованию влияния вида бинарного ортогонального преобразования на структуру и мощность С-кодов, которые могут быть построены на его основе. В статье установлено, что класс классических бент-последовательностей относительно матрицы Уолша-Адамара, построенной с помощью конструкции Сильвестра, является лишь частным случаем класса бинарных бент-последовательностей. Установлено, что подобные классы бент-последовательностей существуют для двух других неэквивалентных классов матриц Уолша-Адамара, а также для матриц Уолша-Адамара, построенных на основе других совершенных алгебраических конструкций: совершенных двоичных решеток и, собственно, классических бент-последовательностей. Так, в статье выписаны алгебраические нормальные формы бент-последовательностей, построенных относительно второй и третей неэквивалентных матриц Адамара порядка n=16. Проведены исследования структуры и мощности классов бент-последовательностей, построенных относительно матриц Адамара, синтезированных на основе совершенных двоичных решеток и классических бент-последовательностей. Использование найденных новых классов бент-последовательностей, а также концепции оперативной смены рабочей матрицы ортогонального преобразования, позволит получить уменьшение избыточности С-кодов, которые применяются в технологии MC-CDMA при сохранении пик-фактора передаваемых сигналов на минимальном уровне.

Ключевые слова: пик-фактор, С-код, MC-CDMA, бент-последовательность, совершенная двоичная решетка.

УДК 004.051

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 15-23

РОЗРОБКА АЛГОРИТМУ СТВОРЕННЯ ПАНОРАМНОГО ВІДЕО

О.Ю. Лебедєва, Д.О. Золотарьова, В.М. Ситник

Одеський національний політехнічний університет,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@opu.ua, allacia.gilbert@gmail.com, apeorin@gmail.com

У роботі розглядається алгоритм створення панорамного відео з декількох відеопослідовностей. Алгоритм розроблено для систем відеоспостреження. За останні роки системи відеоспостереження стали основою надійної системи безпеки. Системи відеоспостереження дозволяють отримати інформацію про поточний стан об'єкту, що охороняється, шляхом збору, обробки, архівування, зберігання, відображення та аналізу цієї інформації. Розроблений алгоритм обробляє відеопослідовності з декількох камер та створює єдину відеопослідовність, яка містить всю інформацію з оброблених відеопослідовностей, базується на алгоритмах пошуку особливої точки на зображеннях. Особливі точки – це такі точки, за якими можна класифікувати зображення, розпізнати його. Вони визначають особливість зображення, його унікальність. У роботі розглядаються найбільш відомі і широко використовуванні алгоритми пошуку особливої точки – як SIFT (Scale Invariant Feature Transform) та SURF (Speeded Up Robust Features). Метод SIFT шукає особливі точки за допомогою піраміди гауссіанів та різниці гауссіанів. Дескриптори будуються за допомогою обчислення гістограми орієнтованих градієнтів в околі особливої точки. Для пошуку особливих точок метод SURF використовує матрицю Гессе. Розглядаються основні кроки розробленого алгоритму: пошук особливих точок, відбір однієї або декількох особливих точок за критерієм, зшивання кадрів відео. Наведено приклади роботи розробленого алгоритму створення панорамного відео для перших кадрів. Проведено дослідження методів SIFT та SURF в ситуаціях, коли зображення масштабується, обертається, затемняється та розмивається і наводиться порівняння методів SURF та SIFT. У роботі надаються висновки про використання методів SURF та SIFT у розробленому алгоритмі створення панорамного відео.

Ключові слова: відео, панорамне відео, зображення, особливі точки на зображенні, пошук особливої точки, SIFT, SURF, зшивання кадрів.

Вступ

На сьогоднішній день відеоспостереження можна зустріти майже усюди: на маленькому чи великому підприємстві, у магазинах, на залізничних вокзалах та навіть на вулиці. Адже головне призначення системи відеоспостереження – отримання інформації про поточний стан об'єкту, що охороняється, шляхом збору, обробки, архівування, зберігання, відображення та аналіз цієї інформації.

Метою установки системи відеоспостереження зазвичай є перегляд місць, які важливо контролювати з точки зору збереження матеріальних цінностей (автостоянки, полиці супермаркетів, склади тощо), контролю за проникненням на об'єкт (прохідні, паркани, двері, ворота та інше), стеження за переміщенням об'єктів (вокзали, офіси, підприємства тощо). Відеоспостереження в сучасному світі, в тому числі в Україні, успішно використовується для моніторингу та управління технологічними процесами на виробництві, у сфері послуг.

На жаль, на підприємствах досі використовуються стандартні камери, які добре себе зарекомендували раніше. Але їх головний недолік – маленький кут огляду, тому підприємству потрібно налаштувати багато камер для огляду усієї території. Крім того, потрібно багато моніторів для перегляду інформації з цих камер, або об'єднати

відеоінформацію з камер на одному моніторі. Це призводить до виникнення труднощів в спостереженні у служби охорони.

Один з варіантів вирішення цієї проблеми – створення панорамного відео, яке б об'єднувало у собі кадри з декількох камер, а на екран монітору служби охорони виводилися лише одне відео.

Мета роботи

Метою роботи є розробка забезпечення систем відеоспостереження шляхом розробки алгоритму створення панорамного відео з використанням методів пошуку особливих точок на зображенні.

Для досягнення мети в роботі були вирішені наступні *задачі*:

- вибір методів пошуку особливих точок на зображенні;
- розробка алгоритму створення панорамного відео з використанням обраного методу;
- програмна реалізація розробленого алгоритму створення панорамного відео з використанням обраного методу.

Основна частина

Створення панорам, стереопари, розпізнавання зображень і знаходження на них об'єктів потребують співставлення декількох зображень. Для цього необхідно застосувати методи пошуку точок, які є загальними на обох зображеннях, а також пошук дескрипторів (описів) цих точок.

Особливі точки – такі точки, за якими можна класифікувати зображення, розпізнати його, які визначають якусь особливість зображення, унікальність. Як правило – це кутові точки, або ті, де різко змінюється колір, яскравість тощо. Потрібно вибирати такі точки, які вносять певний вклад в характеристику зображення, також необхідно вважати особливими такі точки, які з великою ймовірністю будуть знайдені на іншому зображенні. Кожен метод виявлення особливих точок повинен гарантувати інваріантність щодо будь-яких перетворень зображення [1].

Існує багато методів для пошуку особливих точок на зображенні. Вони відрізняються алгоритмом пошуку, побудовою дескрипторів та інваріантністю до масштабу чи повороту. Найбільш відомими і широко використовуваними алгоритмами пошуку особливих точок є метод SIFT (Scale Invariant Feature Transform) та метод SURF (Speeded Up Robust Features).

Метод SIFT (Scale Invariant Feature Transform) шукає особливі точки за допомогою піраміди гауссіанів та різниці гауссіанів. Дескриптори будуються за допомогою обчислення гістограми орієнтованих градієнтів в околі особливої точки [2]. Цей метод інваріантний до масштабу та повороту. Дескриптори також стабільні до змін у висвітленні, шумів і невеликих змін точки спостереження.

Під гауссіаном розуміється зображення, яке було розмите за допомогою фільтра Гаусса (1):

$$L(x,v,\sigma) = G(x,v,\sigma) * I(x,v), \tag{1}$$

де $L(x,y,\sigma)$ – значення гауссіанів у точці з координатами (x,y) та радіусом розмиття σ; $G(x,y,\sigma)$ – гауссове ядро; $I(x,y)$ – значення вихідного зображення.

Під різницею гауссіанів розуміється зображення, яке отримується попіксельним віднімання гауссіана початкового зображення з гауссіана, у якого інший радіус розмиття $k\sigma$ (2):

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma), \quad (2)$$

де $D(x, y, \sigma)$ – значення різниці гауссіанів у точці з координатами (x, y) та радіусом розмиття σ; $L(x, y, k\sigma)$ – значення гауссіанів у точці з координатами (x, y) та радіусом розмиття $k\sigma$; $L(x, y, \sigma)$ – значення гауссіанів у точці з координатами (x, y) та радіусом розмиття σ.

Інваріантність щодо масштабу зображень в дескрипторах SIFT досягається за рахунок знаходження характерних точок на оригінальному зображенні, взятому в різних масштабах [2]. Саме для цього потрібна піраміда гауссіанів. Всі масштабовані простори (набори різних варіацій вихідного зображення, згладжених будь-яким фільтром) діляться на ділянки, які називаються октавами. При переході від однієї октави до наступної розміри зображення в два рази зменшуються. Далі добудовуються ще два гауссіана, що виходять за межі октави.

Одночасно з пірамідою гауссіанів будується і піраміда різниць гауссіанів, кількість зображень в якій буде на одне менше, ніж в першій.

Після побудови пірамід визначаються особливі точки. Точка вважається особливою, якщо вона є локальним екстремумом різниці гауссіанів. Кожна точка поточного зображення різниці гауссіанів порівнюється зі своїми вісьмома сусідніми точками і з дев'ятьма сусідніми точками, розташованими на рівень старше і молодше в піраміді.

Далі проводиться перевірка, яка визначає координати особливої точки з підвищеною точністю. Для цього треба апроксимувати функції різниць гауссіанів многочленом Тейлора другого порядку. Екстремум многочлена Тейлора обчислюється за допомогою прирівнювання похідної до нуля.

Коли визначено точки екстремуму, то проводиться перевірка на малість величини різниці гауссіанів в цій точці. Якщо ця перевірка точкою не буде пройдена, то вона теж виключається зі списку особливих.

Після попередніх двох перевірок проводиться остання. Якщо особлива точка лежить на контурі об'єкта, або ж ця точка погано освітлена, то її теж слід виключити.

У методі SIFT дескриптором є вектор. Як і напрямок особливої точки, дескриптор визначається на гауссіані, максимально наближеному за масштабом до особливої точки, і виходячи з градієнтів в деякій області особливої точки. Для початку ця область повертається на певний кут напрямку особливої точки, чим домагається інваріантності щодо операції повороту.

Метод SURF вирішує одночасно два завдання: пошук особливих точок зображення та створення їх дескрипторів, інваріантних до масштабування та обертання. Це означає, що дескриптор (опис) ключової точки завжди буде однаковим, навіть якщо зразок змінить свій розмір та/або буде повернений (тут і далі мова йде про обертання в площині зображення). Окрім того, сам пошук ключових точок також є інваріантним, у тому сенсі, що повернутий об’єкт сцени має той же набір ключових точок, що й зразок [2].

Для пошуку особливих точок метод використовує матрицю Гессе (3). Детермінант матриці Гессе досягає екстремуму в точках максимальної зміни градієнта яскравості. Завдяки цьому алгоритм добре виявляє плями, кути і края ліній [4].

$$H(f(x, y)) = \begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{vmatrix}, \quad \det(H) = \frac{\partial^2 f}{\partial x^2} \frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y} \right),$$

де $\frac{\partial^2 f}{\partial x^2}$, $\frac{\partial^2 f}{\partial x \partial y}$, $\frac{\partial^2 f}{\partial y^2}$ – похідні другого порядку.

Гессіан є інваріативним відносно обертання, але не є інваріативним масштабу. З цієї причини SURF використовує різномасштабні фільтри для знаходження гессіанів.

Для кожної ключової точки розраховує напрям максимальної зміни градієнту яскравості і масштаб, що береться з scale-коефіцієнта матриці Гессе. Градієнт в точці розраховується за допомогою фільтрів Хаара.

Для ефективного розрахунку фільтрів Гессе і Хаара використовується інтегральне представлення зображень. Інтегральне представлення – це матриця, розмірність якої співпадає з вимірністю початкового зображення, а елементи розраховуються за формулою

$$II(x,y) = \sum_{i=0,\, j=0}^{i \le x,\, j \le y} I(i,j),$$

де $I(i,j)$ – яскравість пікселя вихідного зображення.

Після знаходження ключових точок SURF формує їх дескриптори. Дескриптор представляє собою набір з 64 (або 128) чисел для кожної ключової точки. Ці числа відображають напрям градієнта навколо ключової точки. Оскільки ключова точка представляє собою максимум гессіана, то це гарантує, що в околі точки мають бути ділянки з різними градієнтами. Таким чином, забезпечується дисперсія (відмінність) дескрипторів для різних ключових точок.

Напрямок градієнта околів ключової точки розраховується відносно напрямку градієнта навколо точки в цілому (по всьому околу ключової точки). Таким чином, досягається інваріантність дескриптора відносно обернення. Одночасно з цим, розмір ділянки, на котрій розраховується дескриптор, визначається масштабом матриці Гессе, що забезпечує інваріантність відносно масштабу. Напрямок градієнту також розраховується за допомогою фільтра Хаара.

а

б

Рис. 1. Результат роботи методів пошуку ключових точок: а – результат роботи методу SIFT; б – результат роботи методу SURF

Алгоритм створення панорамного відео складається з таких трьох основних етапів:

- пошук особливих точок;
- відбір однієї або декількох особливих точок за критерієм;
- зшивання кадрів відео.

Для створення панорамного відео потрібно мати два та більше відео. Відео, що використовується, повинно мати області перехрестя друг з другом. Пошук особливих точок виконується на перших кадрах вхідних відео (рис. 1).

В результаті роботи методів SIFT або SURF маємо пари дескрипторів. Необхідно вибрати одну або декілька пар для подальшого зшивання кадрів.

Панорамне зображення буде зшиватися по одній точці. Але у результаті роботи алгоритму SIFT ми отримуємо декілька особливих точок. Для вибору однієї з них використовуємо певний критерій (рис. 2).

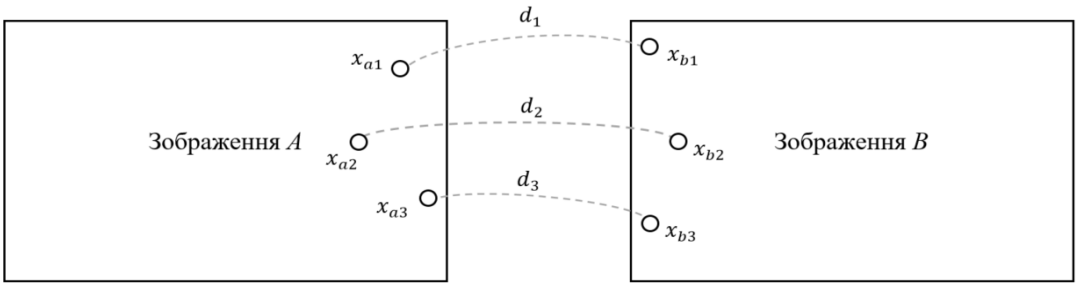


Рис. 2. Критерій відбору особливої точки

Для кожної пари $\{x_{a1}, x_{b1}\}, \{x_{a2}, x_{b2}\} \ldots \{x_{an}, x_{bn}\}$ дескрипторів знаходимо відстань d_i:

$$d_i = \left|(x_{ai} + m) - x_{bi}\right|, i = 1, \ldots, n,$$

де a – зображення A; b – зображення B; n – номер пари $\{x_a, x_b\}$; x_{an} – значення координати x на зображенні A; x_{bn} – значення координати x на зображенні B; m – довжина зображення.

Серед отриманих відстаней d_i знаходимо найменшу відстань, позначимо її d_j. Відповідна їй пара $\{x_{aj}, x_{bj}\}$ буде потрібною особливою точкою.

Маємо особливі точки на зображеннях $\{x_{aj}, y_{aj}\}$ та $\{x_{bj}, y_{bj}\}$. Тепер переходимо до зшивання кадрів. Ми будемо зшивати їх по горизонталі. Але для цього потрібно позбутися області, яка дублюється на обох зображеннях.

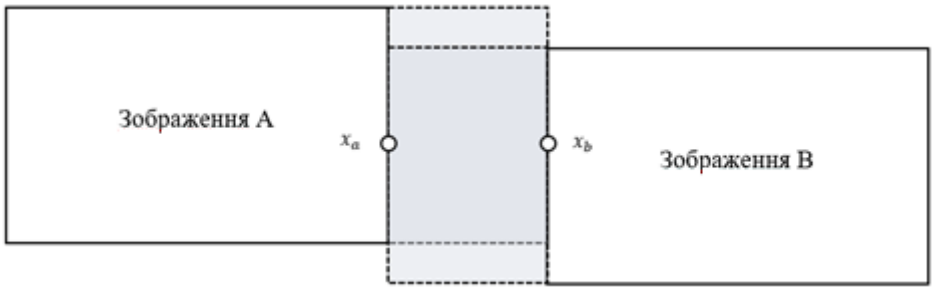


Рис. 3. Зшивання кадрів по обраній точці

Розглянемо основні кроки алгоритму створення панорамного відео:

Крок 1. Маємо два відео $A=\{a^1,...,a^l\}$ та $B=\{b^1,...,b^l\}$, де l – кількість кадрів в відео.

Крок 2. Маємо два перших кадра a^1 та b^1, розміру m x k.

Крок 3. Для зображень a^1 та b^1 використовуємо метод SIFT для пошуку особливих точок. Нехай знайдені особливі точки є пари $\{x_{a1},x_{b1}\},\{x_{a2},x_{b2}\}...\{x_{an},x_{bn}\}$, де x_{ai} – координата x особливої точки на зображенні a^1, x_{bi} – координата x особливої точки на зображенні b^1.

Крок 4. Для кожної пари особливих точок, знайдених на кроці 2 обчислюємо відстані $d_i=\left|(x_{ai}+m)-x_{bi}\right|, i=1,...,n$.

Крок 5. Серед знайдених відстань d_i знаходимо найменшу відстань, позначимо її d_j, якій відповідає особлива точка $\{x_{aj},x_{bj}\}$.

Крок 6. Для кожної пари кадрів з відео $A=\{a^1,...,a^l\}$ та $B=\{b^1,...,b^l\}$ виконуємо:

- об'єднуємо зображення a^f та b^f у точках x_{aj} та x_{bj} відповідно;
- маємо новий кадр c^f;

Крок 7. Маємо панорамне відео $C=\{c^1,...,c^l\}$.

Результат роботи розробленого алгоритму продемонстровано на рисунку 4.

а

б

в

Рис. 4. Результат зшивання перших кадрів з двох відео: а – перший кадр першого відео; б – перший кадр другого відео; в – панорамний кадр з перших кадрів

Для того щоб оцінити роботу методів SIFT та SURF проведемо дослідження та розглянемо ситуації, коли зображення масштабується, обертається, затемняється та розмивається. Також розглянемо, за який час впораються методи, якщо зображень буде 1, 50 чи навість 100. Для цього візьмемо перші кадри відео, що досліджується. Результати досліджень представлені на рисунку 5 та в таблиці 1.

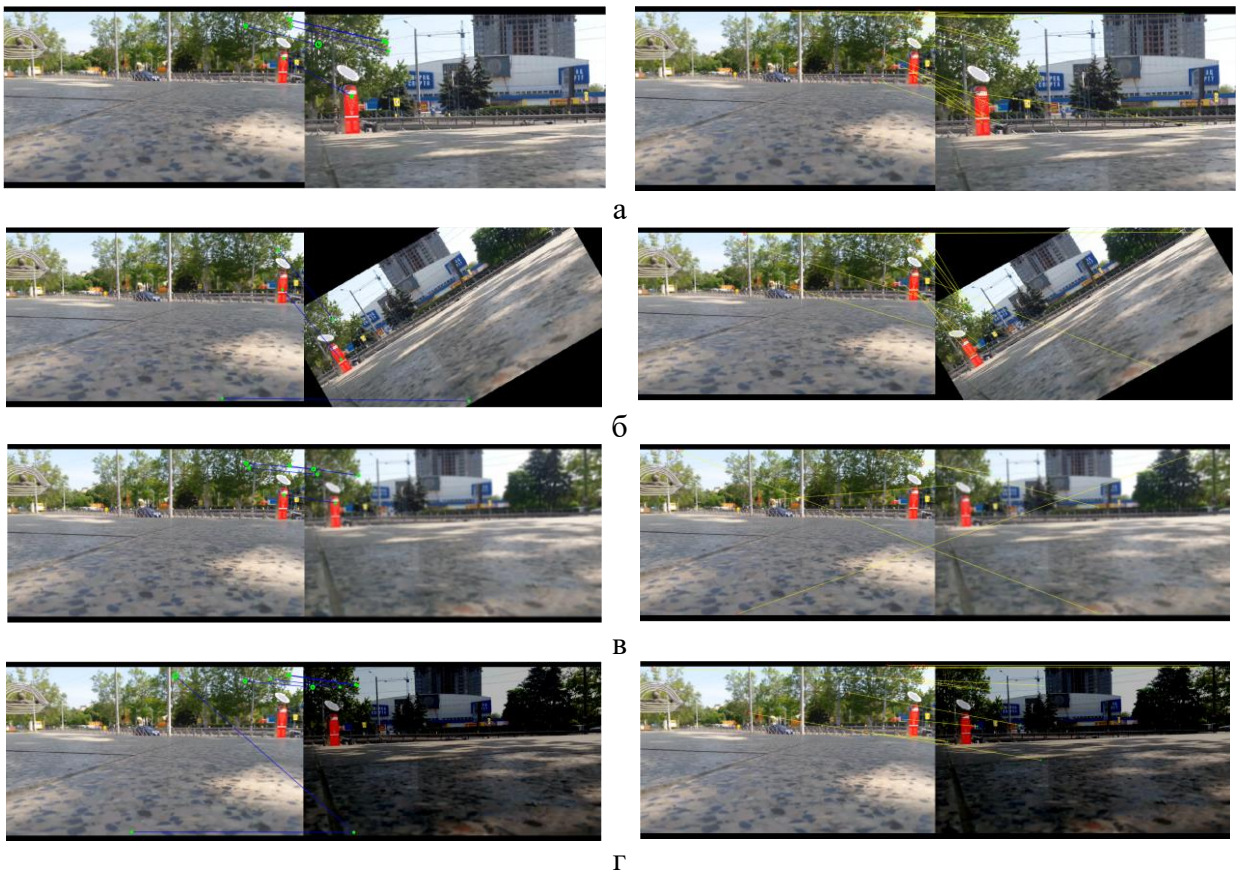


Рис. 5. Результат роботи методу SIFT (ліво) та методу SURF (право) при: а – масштабуванні; б – повороті; в – розмитті; г – зміні яскравості

Таблиця 1.

Порівняння методів SURF та SIFT

Кількість особливих точок		
Критерій	Метод SURF	Метод SIFT
Звичайні зображення	22	6
Масштаб	17	5
Поворот	13	4
Розмиття	5	5
Затемнення	15	6
Час роботи		
Кількість зображень	Метод SURF	Метод SIFT
1	0.33 секунди	0.95 секунд
50	18 секунд	56 секунд
100	40 секунд	1 хвилина 51 секунда

Таким чином, два методи працюють швидко, але метод SURF виявився швидше методу SIFT. Тому для використання цих методів у реальному часі рекомендується використовувати саме метод SURF. Також він знаходить більше особливих точок. Але з розмиттям краще справиться метод SIFT.

Список літератури

1. Ивашечкин А. П. Методы нахождения особых точек изображения и их дескрипторов / А. П. Ивашечкин, А. Ю. Василенко, Б. Д. Гончаров // Молодой ученый. – 2016. – №15. – С. 138-140.
2. Золотых Н.Ю., Кустикова В.Д., Мееров И.Б. Обзор методов поиска и сопровождения транспортных средств на потоке видеоданных / Н.Ю. Золотых, В.Д. Кустикова, И.Б. Мееров // Вестник ННГУ – 2012. – №5-2. – С. 348-358.
3. Афиногенов Е.И. Метод автоматизированного формирования цифровой модели рельефа / Е.И. Афиногенов // Машиностроение и компьютерные технологии – 2013. – №12. – С. 375-400.
4. Джгаркава Г.М., Лавров Д.Н. Использование метода Surf для обнаружения устойчивых признаков изображения при создании сферических панорамных снимков / Г.М. Джгаркава, Д.Н. Лавров // МСиМ. – 2011. – №1 (22). – С. 95-99.

РАЗРАБОТКА АЛГОРИТМА СОЗДАНИЯ ПАНОРАМНОГО ВИДЕО

Е.Ю. Лебедева, Д.О. Золотарева, В.М. Сытник

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: o.y.lebedieva@opu.ua,
allacia.gilbert@gmail.com, apeorin@gmail.com

В работе рассматривается алгоритм создания панорамного видео с нескольких видеопоследовательностей. Алгоритм разработано для систем видеонаблюдения. За последние годы системы видеонаблюдения стали основой надежной системы безопасности. Системы видеонаблюдения позволяют получить информацию о текущем состоянии охраняемого объекта, путем сбора, обработки, архивирования, хранения, отображения и анализа этой информации. Разработанный алгоритм обрабатывает видеопоследовательность из нескольких камер и создает единую видеопоследовательность, которая содержит всю информацию из обработанных видеопоследовательностей, базируется на алгоритмах поиска особой точки на изображениях. Особые точки — это такие точки, по которым можно классифицировать изображения, распознать его. Они определяют особенность изображения, его уникальность. В работе рассматриваются наиболее известные и широко использовании алгоритмы поиска особой точки. SIFT (Scale Invariant Feature Transform) и SURF (Speeded Up Robust Features). Метод SIFT ищет особые точки с помощью пирамиды гауссианов и разницы гауссианов. Дескрипторы строятся с помощью вычисления гистограммы ориентированных градиентов в окрестности особой точки. Для поиска особых точек метод SURF использует матрицу Гессе. Рассматриваются основные шаги разработанного алгоритма: поиск особых точек, отбор одной или нескольких особых точек по критерию, сшивания кадров видео. Приведены примеры работы разработанного алгоритма создания панорамного видео первых кадров видео. Проведено исследование методов SIFT и SURF в ситуациях, когда изображение масштабируется, вращается, затемняется и размывается, и приводится сравнение методов SURF и SIFT. В работе приводятся выводы об использовании методов SURF и SIFT в разработанному алгоритму создания панорамного видео.

Ключевые слова: видео, панорамное видео, изображения, особые точки на изображении, поиск особой точки, SIFT, SURF, сшивания кадров.

DEVELOPMENT OF AN ALGORITHM FOR CREATING PANORAMIC VIDEO

E.Y. Lebedeva, D.O. Zolotareva, V.M. Sytnik

Odessa National Polytechnic University,
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: o.y.lebedieva@opu.ua,
allacia.gilbert@gmail.com, apeorin@gmail.com

This paper discusses the developed algorithm for creating a panoramic video of several video sequences. The algorithm was developed for video surveillance systems. In recent years, CCTV systems have become the basis of a robust security system. CCTV systems allow you to obtain information about the current status of a protected object by collecting, processing, archiving, storing, displaying, and analyzing this information. The developed algorithm processes a video sequence of several cameras and creates a single video sequence, which contains all the information from the processed video sequences, based on the search algorithms for a singular point in the images. Special points are those points by which you can classify images, recognize it. They determine the peculiarity of the image, its uniqueness. The paper considers the most well-known and widely used algorithms for finding a singular point. The SIFT (Scale Invariant Feature Transform) and SURF (Speeded Up Robust Features). The SIFT method looks for special points using the Gaussian pyramid and the Gaussian difference. Descriptors are constructed by computing a histogram of oriented gradients in the vicinity of a singular point. To find special points, the SURF method uses the Hessian matrix. The basic steps of the developed algorithm are considered: search of special points, selection of one or more special points by criterion, stitching of video frames. Here are some examples of how to create a panoramic video algorithm for the first video frames. SIFT and SURF methods have been investigated in situations where the image is scaled, rotated, dimmed and blurred and a comparison of SURF and SIFT methods is made. The paper presents conclusions about the use of SURF and SIFT methods in the developed algorithm for creating panoramic video.

Keywords: video, panoramic video, images, special points in the image, special point search, SIFT, SURF, frame stitching.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 24-37

ВИЯВЛЕННЯ ЛОКАЛЬНОГО ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.О. Хорошко[1], І.І. Бобок[2]

[1]Національний авіаційний університет,
пр-т Космонавта Комарова, 1, Київ, 03058, Україна;
[2]Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

На практиці порушення цілісності цифрового зображення (ЦЗ) часто відбувається локально, у межах якоїсь (невеликої) області. Такі локальні зміни відбуваються, як правило, внаслідок клонування або фотомонтажу, при цьому при клонуванні порушення цілісності має місце локально лише в області клону (при відсутності якої-небудь додаткової обробки ЦЗ), тому актуальною є задача відокремлення клону від прообразу, яка не має на цей час задовільного рішення. В відкритих джерелах відсутня інформація про методи, алгоритми, які б дозволили виявити область клону в умовах його геометричних перетворень (ГП): відбиття відносно вертикальної або/і горизонтальної осі, повороту на кут, кратний 90 градусам, відбиття відносно діагоналі (головної, побічної) відповідної матриці, яким клон часто піддається на практиці. Метою є підвищення інформативності результатів виявлення локальних порушень цілісності ЦЗ шляхом розробки методу відокремлення області клону від області прообразу малого розміру в ЦЗ в умовах ГП клону. Розроблений в роботі метод заснований на забезпеченні незалежності міри відмінності відповідних блоків клону і прообразу від ГП клону шляхом використання в якості цієї міри відмінність сингулярних чисел блоків, враховуючи те, що сингулярні числа блоку не змінюються при його згаданих ГП. В результаті дослідження властивостей матриць мінімальних блокових відмінностей околів клону/прообразу малого радіуса визначені параметри цих матриць, які дозволяють відокремити клон від прообразу в умовах ГП клону: максимальні значення елементів згаданих матриць та значення, які найчастіше приймаються їх елементами. При оцінці алгоритмічної реалізації розробленого методу при виявленні клону, лінійні розміри якого порівнянні з l=4, 8, 16, кількість помилок склала 10.8, 11.2, 13% відповідно.

Ключові слова: цифрове зображення, локальне порушення цілісності, клонування, клон, прообраз, сингулярні числа, матриця мінімальних блокових відмінностей

Вступ

Цілісність поряд з доступністю і конфіденційністю є основною категорією стандартної моделі безпеки будь-якого інформаційного контенту [1], зокрема цифрового зображення (ЦЗ).

На практиці порушення цілісності ЦЗ часто відбувається локально, в межах якоїсь (невеликої) області, не змінюючи ніяк інші його частини. Такі локальні зміни відбуваються, як правило, внаслідок клонування [2,3] або фотомонтажу [4,5]. І якщо розв'язок питання виявленням фотомонтажу чітко вказує на область порушення цілісності – «чужу» для зображення, що піддається експертизі, то в результаті виявлення результатів клонування визначаються області клону й прообразу, причому, як правило, без відокремлення однієї від іншої. Але в останньому випадку порушення цілісності відбувається локально лише в області клону (при відсутності будь-якої додаткової обробки ЦЗ), а область прообразу залишається оригінальною, тому виявлення порушення цілісності тут – це не тільки визначення областей клону й прообразу, але й відокремлення однієї від іншої. І якщо задачі виявлення областей

клону й прообразу приділяється багато уваги в сучасному науковому світі, то друга задача в силу своєї складності залишається маловивченою.

Існуючі нечисленні методи для розв'язку задачі відокремлення клону від прообразу, інформація про які є доступною з відкритих джерел, ґрунтуються на двох принципово різних підходах до організації такого відокремлення.

Перший підхід ґрунтується на використання цифрових водяних знаків (ЦВЗ), які вбудовуються у ЦЗ для організації його захисту від несанкціонованого порушення цілісності [6,7], як правило, стійкими до атак проти вбудованого повідомлення стеганоалгоритмами. Цей підхід дозволяє ефективно відокремлювати клон від прообразу, коли розміри цих областей не є дуже малими в абсолютному сенсі, але у світлі проблеми виявлення порушень цілісності ЦЗ, що розв’язується в роботі, не є шуканим в силу наступної основної причини: на формальному рівні процес вбудови ЦВЗ сам по собі порушує цілісність оригінального зображення.

а

б

Рис. 1. Ілюстрація можливості здійснення клонування в ЦЗ без використання будь-якої постобробки клону: а – оригінальне ЦЗ; б – ЦЗ, що отримано в результаті клонування

Другий підхід базується на виявленні відмінностей у результатах обробки клону й прообразу [8], яка може застосовуватися при клонування. При проведенні клонування області клону/прообразу можуть бути різних абсолютних/відносних розмірів. Якщо область клону значна (у порівнянні з усім ЦЗ), то в такому випадку практично

достовірною подією буде деяка обробка клону (повністю або частково (наприклад, розмиття по контуру)) для його «візуальної адаптації» у новій для нього області ЦЗ. Виявлення такої обробки й буде непрямим покажчиком на клон, дозволяючи його відокремити від прообразу. Саме виявлення результатів розмиття по контуру і є непрямим покажчиком на клон в [8]. Але якщо розміри клону малі, то його додаткова обробка може бути взагалі відсутньою, оскільки при малих розмірах вона, частіше за все, не потрібна для «візуальної адаптації» клону (рис.1(б) – у результаті клонування з ЦЗ усунуто прапор, після чого ЦЗ без будь-якої постобробки збережено без втрат (Tif); артефакти на ЦЗ не виявлені). Для такого випадку запропоновані методи відокремлення клону від прообразу в [9,10]. Але часто при несанкціонованих змінах ЦЗ, що робляться з нерозважальними цілями, клон піддається деяким геометричним перетворенням без зміни безпосередніх значень елементів відповідної частини матриці та зміни розмірів: відбиттю відносно вертикальної або/і горизонтальної осі (рис. 2), повороту на кут, кратний 90 градусам, відбиттю відносно діагоналі (головної, побічної) відповідної матриці. Саме ці геометричні перетворення нижче будемо позначати ГП. Геометричні перетворення клону часто мають значеннєву необхідність для зацікавленої сторони (рис.2), наслідком чого при невиявленні можуть стати фінансові збитки підприємства, фірми, банку, прийняття хибного рішення в судових розслідуваннях тощо. Для випадку наявності ГП клону в відкритих джерелах не знайдено жодного методу (алгоритму) для відокремлення клону від прообразу, що залишає задачу, яка розглядається, актуальною.

а

б

Рис. 2. Ілюстрація проведення клонування в ЦЗ з попередньою обробкою клону: а – оригінальне ЦЗ; б – результат проведеного клонування, у ході якого клон був підданий послідовному відбиттю щодо горизонтальної й вертикальної осей

Мета статті та постановка досліджень

Метою роботи є підвищення інформативності результатів виявлення локальних порушень цілісності ЦЗ шляхом розробки методу відокремлення області клону від області прообразу малого розміру в ЦЗ в умовах ГП.

Для досягнення мети в роботі розв'язуються наступні *задачі*:

- визначити можливості забезпечення незалежності міри відмінності відповідних блоків клону і прообразу від ГП клону;
- дослідити властивості матриць мінімальних блокових відмінностей околів клону/прообразу малого радіуса при різних принципах формування елементів цих матриць для забезпечення можливості відокремлення клону від прообразу в умовах ГП клону з урахуванням відмінностей в цих властивостях;
- розробити метод відокремлення області клону від області прообразу малого розміру в ЦЗ в умовах ГП клону та його алгоритмічну реалізацію;
- провести оцінку ефективності алгоритмічної реалізації розробленого методу.

Основна частина

Нещодавно в [10] був запропонований метод *KPM* відокремлення клону від прообразу малих абсолютних розмірів в умовах відсутності відмінностей при їх постобробці, зокрема в умовах відсутності будь-яких додаткових до клонування збурних дій, заснований на аналізі матриць мінімальних блокових відмінностей (ММБВ) для виявлених попередньо областей клону і прообразу. ММБВ ставиться у відповідність аналізованому зображенню (можливо частині зображення) за наступним правилом [11,12]. Нехай F - $n\times m-$матриця ЦЗ, для аналізу якого використовуються блоки розміру $l\times l$. Кожному елементу f_{ij}, $i=\overline{1,n-l+1}$, $j=\overline{1,m-l+1}$, матриці F ставиться в співвідношення $l\times l$-блок B_{ij}, який є підматрицею F, для якого на місці (1,1) знаходиться елемент f_{ij}. Елементи g_{ij} $(n-l+1)\times(m-l+1)$-ММБВ G, яка ставиться в співвідношення ЦЗ, відображають величину найменшої відмінності $l\times l$-блоку B_{ij} від будь-якого іншого $l\times l$-блоку B_{kl} матриці F в сенсі величини

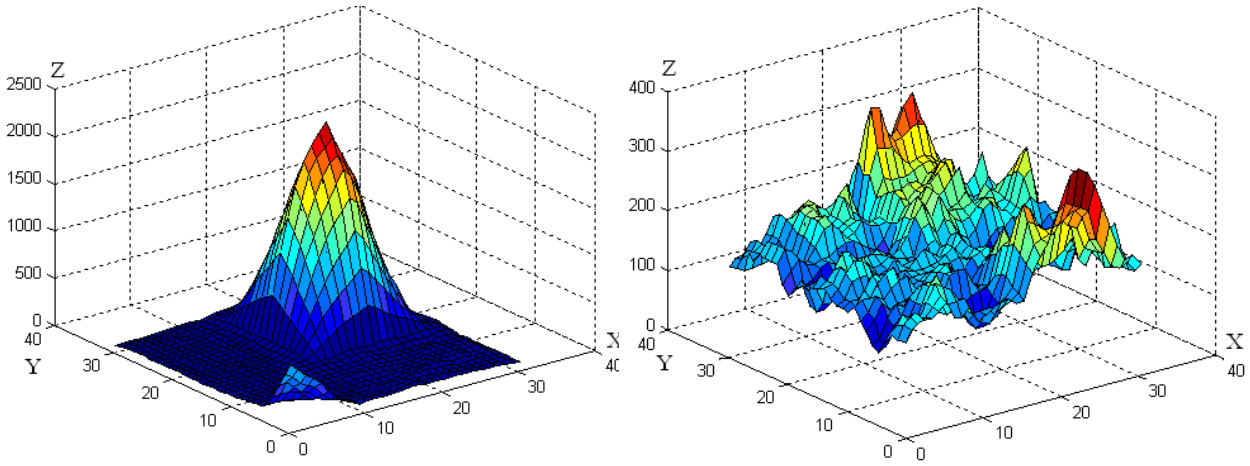
$$\sum_{t,p=1}^{l} r_{tp}, \tag{1}$$

де $r_{tp}, t,p=\overline{1,l}$, — елементи $l\times l-$матриці R,

$$R=\left|B_{ij}-B_{kl}\right| \tag{2}$$

співвідношення (2) розуміється в поелементному сенсі.

Основна ідея методу *KPM* полягала в використанні встановленого в [10] факту, що для значного числа ЦЗ, що зазнали клонування з малою областю клону, графіки функцій, що інтерполюють елементи ММБВ, які побудовані для околів незначного радіусу для областей клону і прообразу, мають специфічний вигляд у випадку клону, визначаючи блок клону (або блок, що відповідає пікселю, який відстоїть від пікселя, що відповідає блоку клона, на 1,2,3 позиції) як локальний (глобальний) максимум (рис. 3(а)), що взагалі не має місця в випадку прообразу (рис. 3(б)). Але співвідношення (1), (2) за своїм змістом є такими, що ефективно працюють лише в умовах відсутності відмінностей в постобробці клона і прообраза [11,12]. При наявності геометричних перетворень клону, що не стосуються прообразу, метод *KPM*, використовуючи (1), (2) для побудови ММБВ, не в змозі бути систематично відокремлювати клон від прообразу.



а Б

Рис. 3. Типовий вигляд графіків функцій, що інтерполюють елементи ММБВ, для околів клону й прообразу ЦЗ: а – ММБВ для околу клону, б – ММБВ для околу прообразу

В [13] нещодавно було доведено, що сингулярний спектр (множина сингулярних чисел (СНЧ)) квадратної матриці не змінюється при зазначених вище ГП, що робить доцільним використання при формуванні ММБВ для кількісної характеристики відмінності між блоками матриці ЦЗ замість (1), (2), відмінність їх сингулярних спектрів (у деякому сенсі). Побудована за запропонованим принципом ММБВ теоретично має властивості, аналогічні тим, що були їй притаманні у первісному варіанті [11,12], однак її елементи тепер належать множині дійсних, а не цілих чисел. Це приведе до значного впливу округлень на результати обчислень у системі чисел з плаваючою точкою. З врахуванням цього в [14] в якості кількісного показника відмінності блоків з залученням їх сингулярних спектрів, що використовується при побудові ММБВ G відповідного розміру з елементами g_{ij}, пропонується наступний:

$$g_{ij} = \min_{B_1}\left(round\left(\sum_{i=1}^{l} \left| \sigma_i(B) - \sigma_i(B_1) \right| \right) \right), \qquad (3)$$

де функція $round(\cdot)$ округлює аргумент до найближчого цілого значення, g_{ij} несе в собі інформацію про найменшу відмінність конкретного блоку B, який відповідає елементу f_{ij} матриці (підматриці) F, від будь-якого іншого блоку B_1 матриці (підматриці) F.

Як показано в [14], елементи матриці G, що побудовані відповідно до (1), (2), мають значення, що (часто значно) перевищують елементи G, побудовані за правилом (3). Це приводить до деяких негативних наслідків, які не дозволяють простою заміною в методі *KPM* принципу побудови ММБВ отримати метод відокремлення клону від прообразу в умовах ГП клону. А саме, часто порушується картина локального (глобального) максимуму для функції, що інтерполює елементи ММБВ в околі клону, який визначає блок клону, ілюстрація якої представлена на рисунку 3(а). Це є очікуваним і пояснюється наступним чином. Елементи ММБВ за принципом (3) будуються по значенням СНЧ відповідних блоків – $\sum_{i=1}^{l} \left| \sigma_i(B) - \sigma_i(B_1) \right|$, які є дійсними числами і обчислюються в системі чисел з плаваючою точкою, маючи в своєму остаточному значенні накопичену обчислювальну похибку. Ця похибка може відіграти ключову роль при виконанні округлення $round\left(\sum_{i=1}^{l} \left| \sigma_i(B) - \sigma_i(B_1) \right| \right)$, оскільки елементи

ММБВ у випадку (3) незначно відрізняються один від одного, руйнуючи картину локального (глобального) максимума (рис. 4(а) – значення $G(5,5)$ не є локальним максимумом ММБВ, оскільки в його околі радіуса 1 є елементи, що перевищують $G(5,5)$ (всього) на (1). І хоча для переважної більшості ЦЗ картина залишиться такою, як і повинна (рис. 5(а,б)), можливість попередньої ситуації значно збільшує кількість помилок при відокремлені клону від прообразу, якщо в *КРМ* просто замінити (1), (2) на (3), в порівнянні з *КРМ* в первісному вигляді.

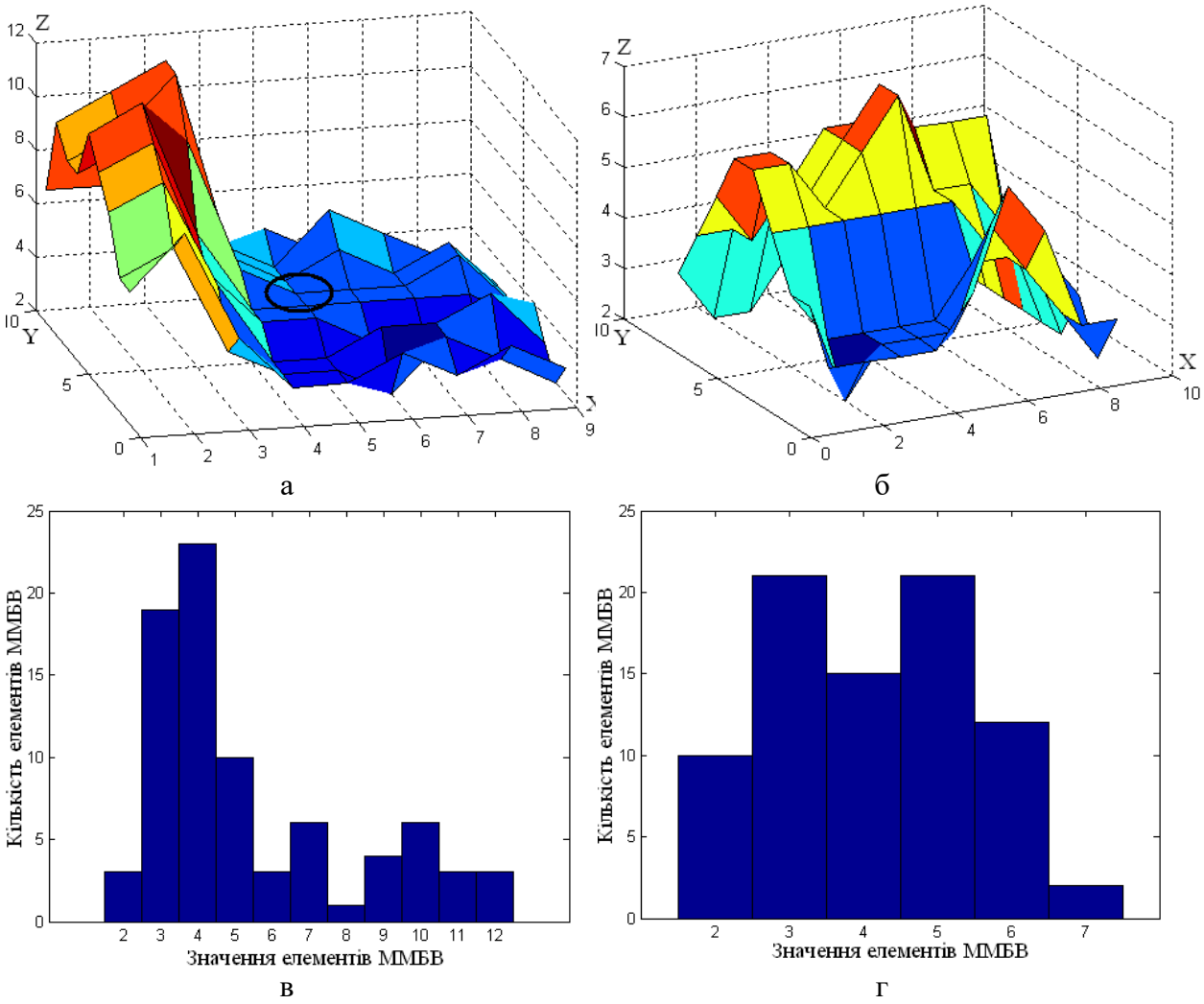


Рис. 4. Приклад клонованого ЦЗ, що ілюструє можливість відсутності для функції, що інтерполює елементи ММБВ, які побудовані у відповідності з (3), в околі клону, локального (глобального) максимуму в точці, що відповідає клону: а – ММБВ для околу радіуса 4 блоку клону (16×16) з позначенням відсутності локального максимуму; б – ММБВ для околу радіуса 4 блоку прообразу (16×16); в – гістограма значень ММБВ для околу клону; г – гістограма значень ММБВ для околу прообразу

Таким чином, врахування наявності/відсутності локального (глобального) максимуму ММБВ для околів клону, прообразу є недостатнім в умовах, що розглядаються. Але наявність локального (глобального) максимуму є не єдиною умовою, що відрізняю ММБВ для околів клону і прообразу. Дійсно, значення елементів ММБВ для околу клону більші ніж в ММБВ для околу прообразу, оскільки «чужорідна» частина – клон очевидно буде мати більші відмінності від блоків свого нового, але оригінального для первісного ЦЗ околу, ніж оригінальний прообраз від

блоків свого оригінального околу, що витікає з [15]. Ілюстрацією даного факту є порівняння на рисунках 4(а) і 4(б), 5(а) і 5(б) (для наочності на рисунках 4,5 наведені гістограми значень елементів відповідних ММБВ; як видно при порівнянні на рисунках 4(в) і 4(г), 5(в) і 5(г), максимальні значення елементів ММБВ для околу клону перевищують максимальні значення в ММБВ для околу прообразу). Така ситуація має місце для переважної більшості ЦЗ, що зазнали клонування. Але приблизно для 5% розглянутих в ході роботи ЦЗ спостерігалася ситуація, коли максимальні значення ММБВ для околів клону і прообразу співпадали (рис. 6). Для таких ЦЗ потрібен був додатковий параметр для організації відокремлення клону від прообразу.

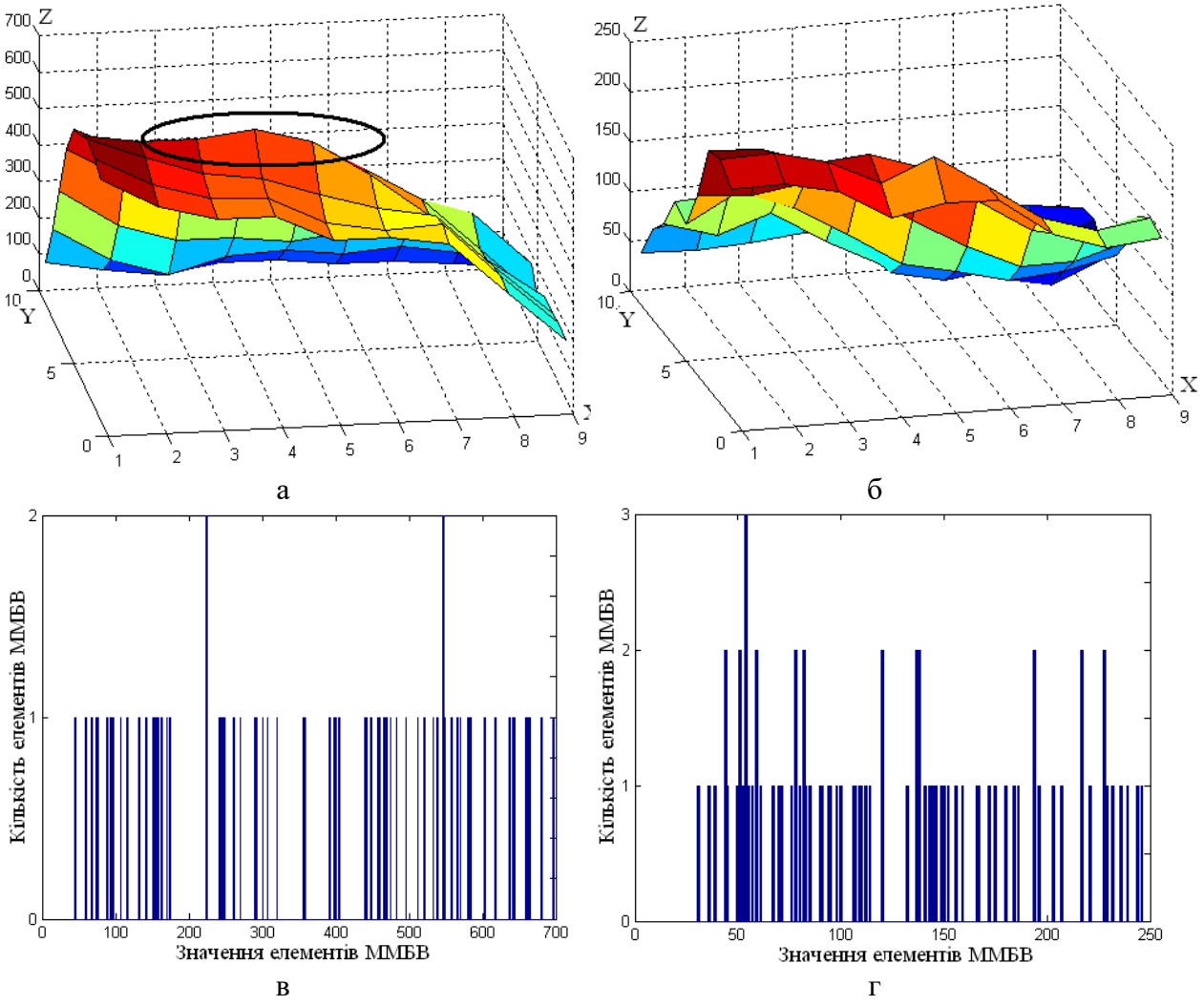


Рис. 5. Типовий приклад вигляду ММБВ для клонованого ЦЗ в умовах ГП клону: а – ММБВ для околу радіуса 3 блоку клону (16×16) з позначеним наявним локальним максимумом, що відповідає клону; б – ММБВ для околу радіуса 3 блоку прообразу (16×16); в – гістограма значень ММБВ для околу клону; г – гістограма значень ММБВ для околу прообразу

Розглянемо ситуацію, коли максимальні значення елементів ММБВ, що відповідають околу клону і прообразу, однакові. З врахуванням того, що, як вже було зазначено вище, клон є «чужорідною» областю в своєму новому місці розташування, його відмінність в переважній більшості випадків від блоків-сусідів буде більше, ніж для прообразу. Крім цього, відмінність для блоків-сусідів клону від інших блоків в околі клону теж в більшості випадків зросте в порівнянні з відмінністю блоків в околі прообразу. Дійсно, в окіл клону цей клон додався, зруйнувавши кореляцію між

пікселями, стовпцями, рядками, що є сусідніми з пікселями, стовпцями, рядками границі клону [15]. І хоча максимальні значення елементів ММБВ, що відповідають околу клону і прообразу, однакові, все вищенаведене очевидно приведе до зростання значення відмінності для більшості блоків з околу клону від інших блоків з цього ж околу, що відобразиться в збільшенні моди гістограми значень ММБВ для околу клону в порівнянні з модою гістограми ММБВ для околу прообразу, ілюстрацією чому є приклад, наведений на рис.6: при порівнянні гістограм на рисунках 6(в) і 6(г) мода для випадку клону дорівнює 18, у той час як мода гістограми для випадку прообразу дорівнює 9, що говорить про те, що більшість блоків околу клону має мінімальну блокову відмінність у сенсі (3) в 2 рази більшу, ніж більшість блоків околу прообразу.

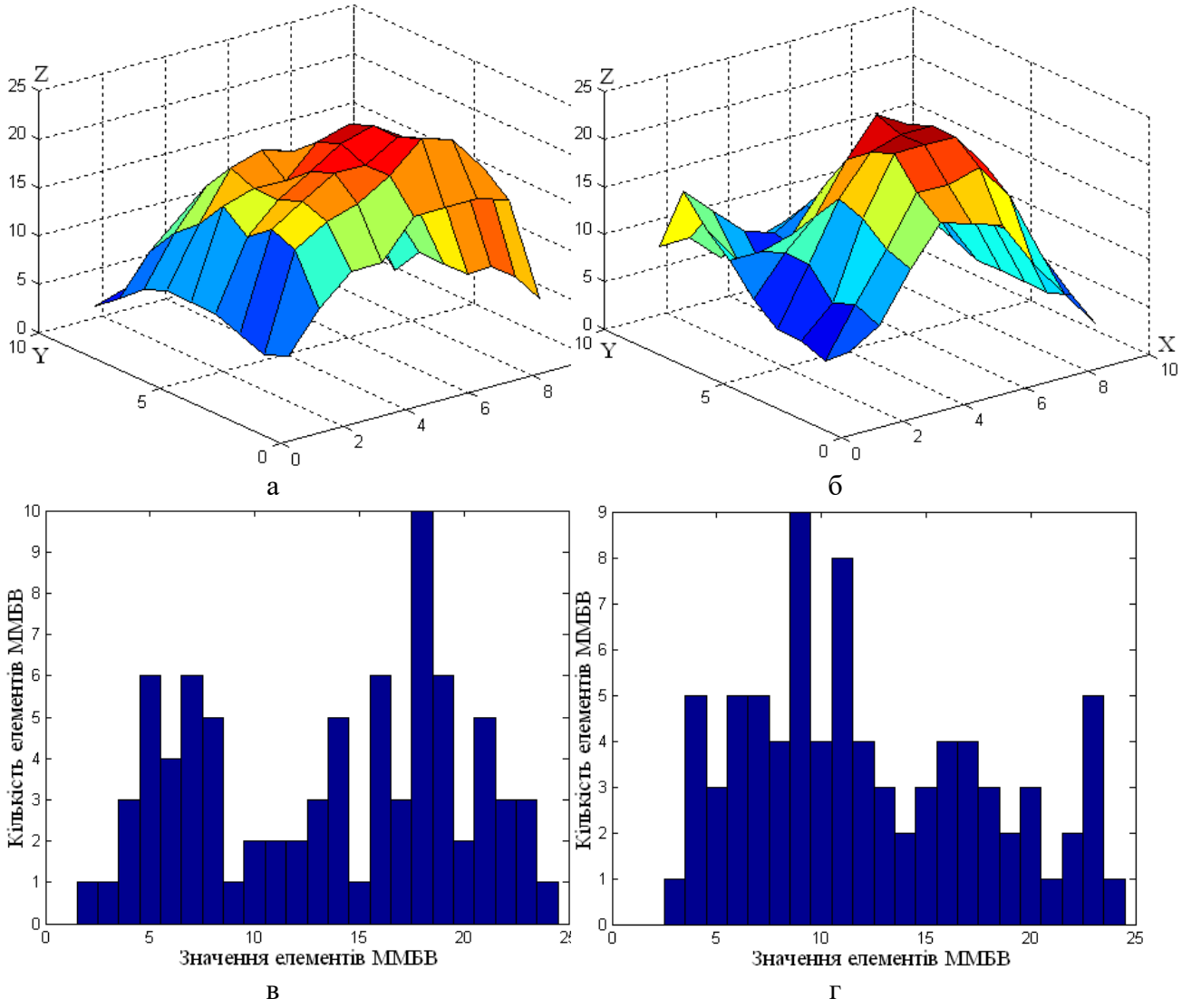


Рис. 6. Приклад ЦЗ, для якого значення максимумів ММБВ для околів клону і прообразу співпадають: а – ММБВ для околу радіуса 3 блоку клону (8×8); б – ММБВ для околу радіуса 3 блоку прообразу (8×8); в – гістограма значень ММБВ для околу клону; г – гістограма значень ММБВ для околу прообразу

З урахуванням всього вищенаведеного основні кроки методу відокремлення клону від прообразу в умовах ГП клону виглядають наступним чином. Перші два кроки аналогічні методу, запропонованому в [10]

Крок 1. Нехай T_1 і T_2 - виявлені деяким алгоритмом області клону й прообразу, що мають малі абсолютні розміри. Визначити B_1 і B_2 - $l \times l$ – блоки матриці F аналізованого ЦЗ як можна меншого розміру такі, що

$$T_1 \subseteq B_1,\ T_2 \subseteq B_2,\ B_1 \bigcap B_2 = \varnothing.$$

Крок 2. Побудувати O_1 і O_2 - прямокутні $p \times p$ – околи B_1 і B_2 відповідно, розміри яких порівнянні з розмірами B_1 і B_2, такі, що

$$B_1 \subseteq O_1,\ B_2 \subseteq O_2, O_1 \bigcap B_2 = \varnothing,\ O_2 \bigcap B_1 = \varnothing. \quad (4)$$

Крок 3. Для O_1 і O_2 побудувати ММБВ, використовуючи блоки розміру $l \times l$: M_1 (з елементами $m_{ij}^{(1)}$) і M_2 (з елементами $m_{ij}^{(2)}$) відповідно. При побудові ММБВ як кількісний параметр, що характеризує відмінність між блоками, використовувати (3).

Крок 4. В M_1 і M_2 визначити значення максимальних елементів:

$$m^{(1)}{}_{max} = \max_{i,j} m_{ij}^{(1)},\ m^{(2)}{}_{max} = \max_{i,j} m_{ij}^{(2)}$$

Крок 5 *(відокремлення клону від прообразу)*.

Якщо

$$m^{(1)}{}_{max} > m^{(2)}{}_{max},$$

то

T_1 - клон, T_2 - прообраз,

Якщо

$$m^{(1)}{}_{max} < m^{(2)}{}_{max},$$

то

T_1 - прообраз, T_2 - клон,

Якщо

$$m^{(1)}{}_{\max} = m^{(2)}{}_{max},$$

то

побудувати гістограми Γ_1, Γ_2 значень M_1, M_2 відповідно; знайти $mod\,a(\Gamma_1)$ і $mod\,a(\Gamma_2)$ - моди Γ_1, Γ_2 відповідно

якщо

$$mod\,a(M_1) \geq mod\,a(M_2)$$

то

T_1 - клон, T_2 - прообраз,

інакше

T_1 - прообраз, T_2 - клон.

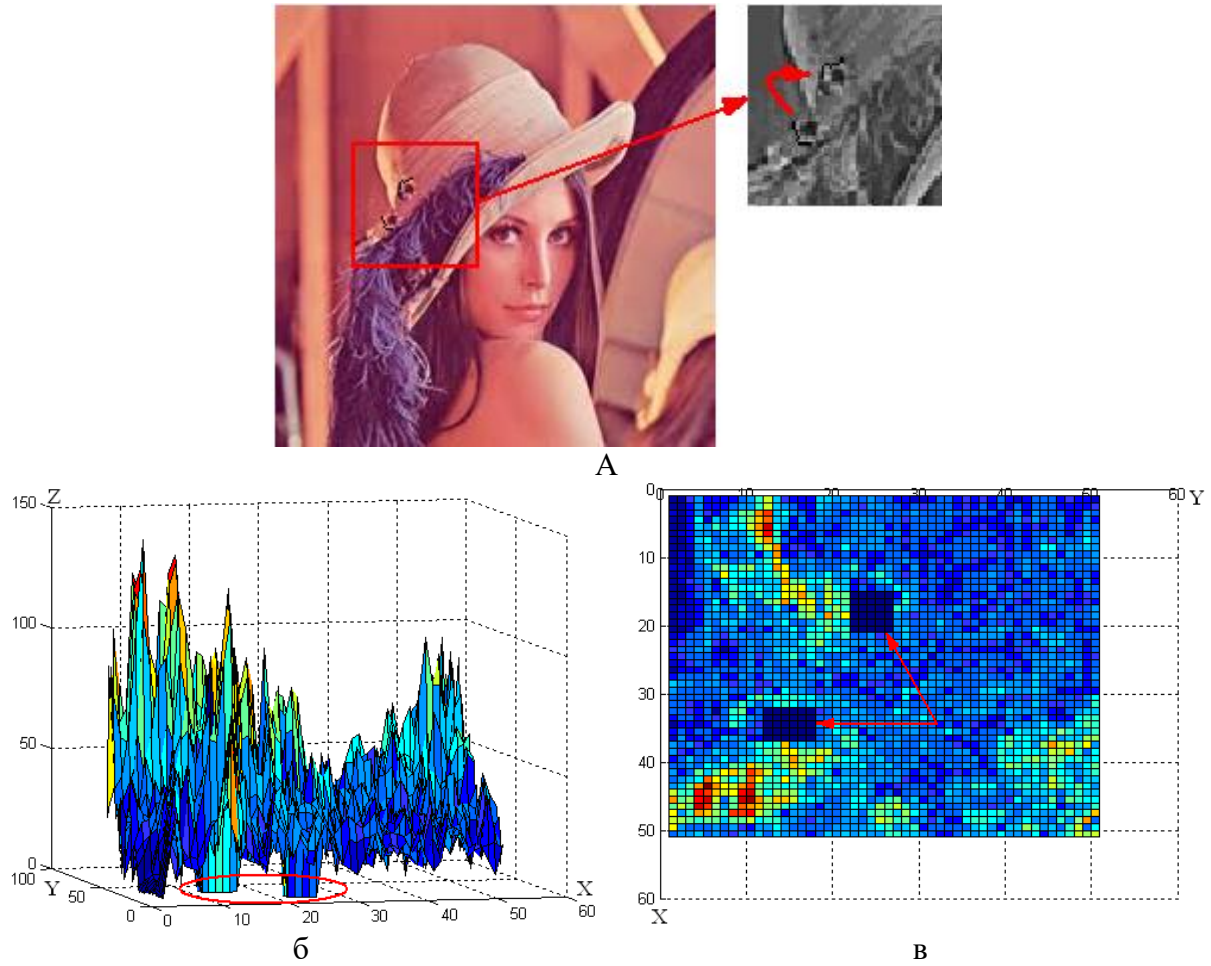
Для оцінки ефективності розробленого методу використовувалися наступні значення параметрів: $l \in \{4,8,16\}$, $p = l + 10$, при цьому O_1 і O_2 обиралися так, щоб клону/прообразу відповідали центральні елементи матриць M_1 і M_2 відповідно (хоча це не є обов'язковим), при побудові Γ_1, Γ_2 крок дорівнював одиниці. В експерименті було задіяно: 200 ЦЗ з бази img_Nikon_D70s [16], 300 ЦЗ з бази 4cam_auth [17]. В ході експерименту клони піддавалися різним ГП. Розміри клону/прообразу обиралися малими в абсолютному сенсі: $l \in \{4,8,16\}$. Результати експерименту представлені в таблиці 1. Причини зростання кількості помилок із збільшенням *l* викладені в [15].

Таблиця 1.

Помилки при відокремленні клону від прообразу (%)

L		
4	8	16
10.8	11.2	13

При проведені експерименту для виявлення областей клону і прообразу в умовах ГП клону використовувався метод *UKL*, запропонований в [14], заснований на аналізі ММБВ, яка будується за принципом (3). Повний цикл експертизи продемонстровано на прикладі ЦЗ Lenna, яке зазнало клонування в умовах повороту клону на 90 градусів в від'ємному напрямку (рис. 7(а)). За допомогою *UKL* вірно знайдено області клону і прообразу (рис. 7(б)), більш явно місце розташування яких в межах зображення видно на рисунку 7(в).

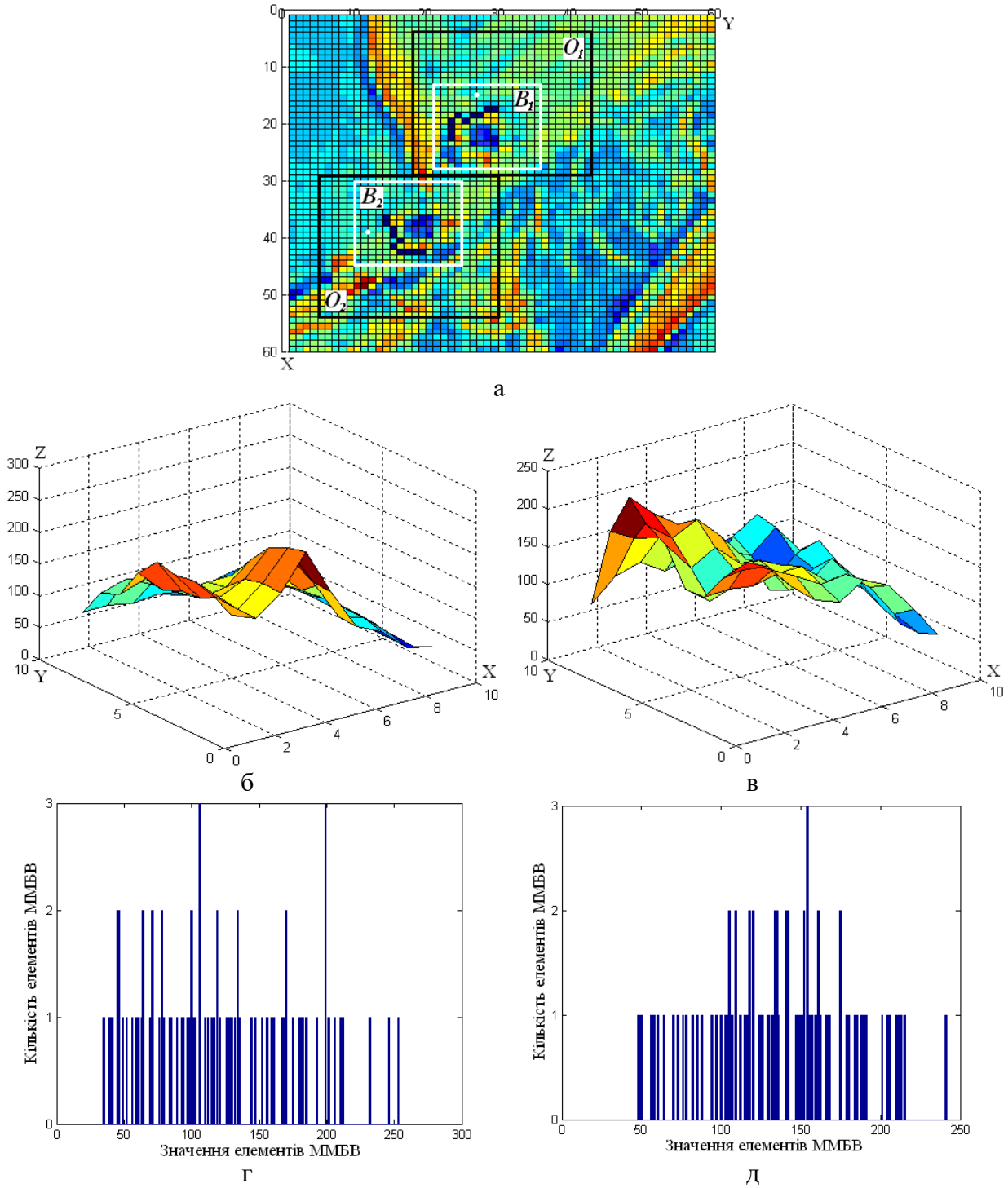


а б в

Рис. 7. Виявлення результатів клонування в ЦЗ Lenna методом *UKL*: а – ЦЗ, що зазнало клонування в умовах ГП клону, з виділеною частиною розміром 60×60 пікселів, яка піддається експертизі; б – графік функції, що інтерполює елементи ММБВ, побудованої з використанням 8×8-блоків для виділеної частини ЦЗ (позначені частини ММБВ відповідають T_1 і T_2); в – проекція поверхні, що є графіком функції, яка інтерполює елементи ММБВ, на площину ХОУ з вказаними T_1 і T_2

Результат 1-го і 2-го кроків розробленого методу представлені на рисунку 8(а): B_1, B_2 – 16×16-блоки; O_1, O_2 – 26×26-блоки. Треба зазначити, що відносне розташування B_1, B_2 в межах O_1, O_2 не обов'язково повинно бути однаковим,

обов'язковою для взаємного розташування B_1, B_2, O_1, O_2 є лише умова (4). Наступні кроки алгоритму знайшли своє відображення на рисунку 8(б)-(д). Отриманий результат, що виявляє як клон B_1, тобто T_1, відповідає дійсності.



а

б

в

г

д

Рис. 8. Результати експертизи виділеної частини ЦЗ (рис. 7(а)), яка містить клон, прообраз, розробленим алгоритмом: а – проекція поверхні, що є графіком функції, яка інтерполює елементи 60×60-підматриці виділеної частини досліджуваного ЦЗ, на площину ХОУ з визначеними областями B_1, B_2, O_1, O_2 відповідно до (4); б – графік функції, що інтерполює елементи ММБВ, побудованої для O_1; в – графік функції, що інтерполює елементи ММБВ, побудованої для O_2; г – гістограма значень ММБВ для O_1; д – гістограма значень ММБВ для O_2

Висновки

В роботі розроблено метод відокремлення клону від прообразу в умовах ГП клону та його алгоритмічну реалізацію, аналогів якого авторами в відкритих джерелах знайдено не було, що дозволило підвищити інформативність результатів виявлення локальних порушень цілісності ЦЗ. Розроблений метод заснований на забезпеченні незалежності міри відмінності відповідних блоків клону і прообразу від ГП клону шляхом використання в якості цієї міри відмінності сингулярних чисел блоків, враховуючи те, що СНЧ блоку не змінюються при його ГП.

В результаті дослідження властивостей матриць мінімальних блокових відмінностей околів клону/прообразу малого радіуса визначені параметри цих матриць, які дозволяють відокремити клон від прообразу в умовах ГП клону: максимальні значення елементів згаданих матриць та значення, які найчастіше приймаються елементами ММБВ.

При оцінці алгоритмічної реалізації розробленого методу кількість помилок склала 10.8, 11.2, 13% для розміру l , який дорівнював 4, 8, 16 відповідно.

Список література

1. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – 344 с.
2. Ratnam Singh Copy Move Tampering Detection Techniques: A Review / Ratnam Singh, Mandeep Kaur //International Journal of Applied Engineering Research. – 2016. – Vol.11, No 5. – Pp. 3610-3615.
3. Rani, S. A Survey of Copy-Move Forgery Detection Techniques for Digital Images / S. Rani, M. Jayamohan, S. Sruthy // International Journal of Innovations in Engineering and Technology. – 2015. – Vol.5, Iss.2. – Pp.419-426.
4. He, Z. Digital image splicing detection based on approximate run length / Z. He, W. Sun, W. Lu, H. Lu // Pattern Recognition Letters. – 2011. – Vol. 32, No. 12. – Pp. 1591-1597.
5. He, Z. Digital image splicing detection based on markov features in DCT and DWT domain / Z. He, W. Lu, W. Sun, J. Huang // Pattern Recognition Letters. – 2012. – Vol.45, No. 12. – Pp. 4292-4299.
6. Кобозева, А.А. Выявление нарушений целостности цифрового изображения путем использования стеганографических алгоритмов / А.А. Кобозева, И.И. Бобок, Л.М. Дзюбинская // Інформатика та математичні методи в моделюванні. – 2015. – Т.5, №2. – С. 129-134.
7. Бобок, І.І. Підвищення інформативності результатів виявлення клонування в цифровому зображенні / І.І. Бобок // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – No 58. – С.81-89.
8. Лебедева, Е.Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения / Е.Ю. Лебедева // Інформатика та математичні методи в моделюванні. – 2014. – Том 4, №1. – С. 76-84.
9. Кобозєва, А.А. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності постобробки зображення / А.А. Кобозєва, І.І. Бобок // Вісник ЧДТУ. – 2018. – №2. – С. 12-19.
10. Бобок, І.І. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності відмінностей при їх постобробці / І.І. Бобок // Інформатика та математичні методи в моделюванні. – 2017. – Т.7, №4. – С. 276-284.
11. Григоренко, С.М. Розвиток методу виявлення клонування в цифровому зображенні в умовах додаткових збурних дій / С.М. Григоренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1(31). – С. 85-98.
12. Kobozeva, A.A. Method for Detecting of Clone Areas in a Digital Image under Conditions of Additional Attacks / A.A. Kobozeva, I.I. Bobok, S.M. Grygorenko // J. Sign. Process. Syst. Mode of access: https://doi.org/10.1007/s11265-019-01449-6 (Date: 2019).
13. Бобок, І.І. Теоретичні основи вдосконалення методу виявлення результатів клонування в цифровому зображенні в умовах додаткових збурних дій / І.І. Бобок, А.А. Кобозєва // Сучасна спеціальна техніка. – 2018. – №1. – С. 29-39.

14. Хорошко, В.О. Удосконалення методу виявлення результатів клонування в цифровому зображенні / В.О.Хорошко, І.І.Бобок // Вісник УДТУ. – 2019. – №3. – С. 36-44.
15. Кобозєва, А.А. Теоретичні основи методу відокремлення клону від прообразу в цифровому зображенні / А.А. Кобозєва, І.І. Бобок // Безпека інформації. – 2018. – Т.24, №1. – С.49-55.
16. Gloe, T. The 'Dresden Image Database' for benchmarking digital image forensics / T. Gloe, R. Böhme // Proceedings of the 25th Symposium on Applied Computing (ACM SAC 2010). Sierre. – 2010. – Vol. 2. – Pp. 1585–1591.
17. Hsu, Y.F. Detecting image splicing using geometry invariants and camera characteristics consistency / Y.F. Hsu , S.F. Chang // Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'06). – 2006. – Pp. 549-552.

ВЫЯВЛЕНИЕ ЛОКАЛЬНОГО НАРУШЕНИЯ ЦЕЛОСТНОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

В.А. Хорошко[1], И.И. Бобок[2]

[1]Национальный авиационный университет,
пр-т Космонавта Комарова, 1, Киев, 03058, Украина;
[2]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одеса, 65044, Украина; e-mail: onu_metal@ukr.net

На практике нарушение целостности цифрового изображения (ЦИ) часто происходит локально, в пределах некоторой (небольшой) области. Такие локальные изменения происходят, как правило, вследствие клонирования или фотомонтажа, при этом при клонировании нарушения целостности имеет место локально лишь в области клона (при отсутствии какой-нибудь дополнительной обработки ЦИ), поэтому актуальной является задача отделения клона от прообраза, которая не имеет на сегодняшний день удовлетворительного решения. В открытых источниках отсутствует информация о методах, алгоритмах, которые бы позволили выявить область клона в условиях его геометрических преобразований (ГП): отражения относительно вертикальной или/и горизонтальной оси, поворота на угол, кратный 90 градусам, отражения относительно диагонали (главной, побочной) соответствующей матрицы, которым клон часто подвергается на практике. Целью является повышение информативности результатов выявления локальных нарушений целостности ЦИ путем разработки метода отделения области клона от области прообраза малого размера в ЦИ в условиях ГП клона. Разработанный в работе метод основан на обеспечении независимости меры отличия соответствующих блоков клона и прообраза от ГП клона путем использования в качестве этой меры отличие сингулярных чисел блоков, учитывая то, что сингулярные числа блока не меняются при его упомянутых ГП. В результате исследования свойств матриц минимальных блоковых отличий окрестностей клона/прообраза малого радиуса определены параметры этих матриц, которые позволяют отделить клон от прообраза в условиях ГП клона: максимальные значения элементов упомянутых матриц и значения, которые чаще всего принимаются их элементами. При оценке алгоритмической реализации разработанного метода при выявлении клона, линейные размеры которого сравнимы с l=4, 8, 16, количество ошибок составило 10.8, 11.2, 13% соответственно.

Ключевые слова: цифровое изображение, локальное нарушение целостности, клонирование, клон, прообраз, сингулярные числа, матрица минимальных блоковых отличий.

IDENTIFICATION OF A LOCAL VIOLATION OF THE INTEGRITY OF A DIGITAL IMAGE

V.O. Khoroshko[1], I.I. Bobok[2]

[1]National Aviation University,
prosp. Kosmonavta Komarova, 1, Kyiv, 03058, Ukraine;
[2]Odesa National Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: onu_metal@ukr.net

Violation of the integrity of a digital image often occurs locally. These disturbances occur in some (small) area of the image. Such local changes occur, as a rule, due to cloning or photomontage. Integrity violation occurs locally only for the clone if there is no additional processing of the digital image when implementing cloning. Therefore, the urgent task is to determine the area of the clone, which does not currently have a satisfactory solution. Information on methods and algorithms that would identify the clone area under the conditions of its geometric transformations is not available in open sources. The article discusses the following geometric transformations of the clone: reflection relative to the vertical and/or horizontal axis, rotation through an angle multiple of 90 degrees, reflection relative to the diagonal (main, secondary) of the corresponding matrix. A clone often undergoes such transformations in practice. The goal is to increase the information content of the results of detecting local digital image integrity violations. The goal is achieved by developing a method for separating the clone region from the region of the inverse image of the small size in the images under the conditions of geometric transformations of the clone. The method that was developed in the work is based on the fact that singular values of any matrix do not change during its geometric transformations, which are listed above. The difference between image blocks is defined as the difference between their singular spectras. For the matrices of minimal block differences, which are built for small neighborhoods of the clone / prototype, their characteristic parameters are determined: the maximum values, and the values that are most often taken by the elements of these matrices. These parameters allow you to separate the clone from the prototype in the conditions of geometric transformations of the clone. When evaluating the effectiveness of the developed algorithm in identifying a clone whose dimensions are comparable to $l = 4$, 8, 16, the number of errors was 10.8, 11.2, 13%, respectively.

Keywords: digital image, local integrity violation, cloning, clone, prototype, singular values, matrix of minimal block differences.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 38-48

МОДИФІКАЦІЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВИ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В ЗОБРАЖЕННЯ НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Г.В. Ахмаметьєва, Г.А. Баранюк, А.І. Казаков

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: anna-odessitka@mail.ru

В роботі запропоновано модифікацію стеганографічного методу вбудови цифрового водяного знаку в область вейвлет-перетворення цифрового зображення. Запропонований метод здійснює вбудову водяного знаку в високочастотні деталізуючі коефіцієнти трирівневого вейвлет-перетворення з використанням вейвлету Добеші-43, що забезпечує високу якість отриманого стеганоповідомлення, яке зберігається в форматі з втратами, що обумовлено широким розповсюдженням таких зображень у зв'язку з їх малим розміром. До цифрового водяного знаку застосовується дискретне косинусне перетворення, завдяки чому підвищується ефективність виявлення наявності водяного знаку у стеганоповідомленні. В роботі проводиться аналіз ефективності детектування цифрового водяного знаку в залежності від порогових значень, які визначають вибір деталізуючих коефіцієнтів, використовуваних для вбудови, в результаті якого встановлено, що підвищення порогів без застосування до водяного знаку дискретного косинусного перетворення призводить до значного погіршення точності детектування. І навпаки, запропонований метод з пороговими значеннями T_1=80 і T_2=90 вибору деталізуючих коефіцієнтів у поєднанні з дискретним косинусним перетворенням матриці водяного знаку дозволив підвищити відсоток правильно детектованих стеганоповідомлень. Результати проведених обчислювальних експериментів показали стійкість вкладення водяного знаку до атак стиском (навіть при якості зображення QF=5), накладання шуму, підвищення різкості, зсуву, для яких точність детектування становить в середньому 97%. Також метод є стійким до масштабування за умови QF>50. В роботі проводиться порівняння стійкості оригінального методу вбудови цифрового водяного знаку і різних варіацій запропонованої модифікації стеганографічного методу до комплексних атак (стиску у поєднанні з іншими видами обробки цифрових зображень).

Ключові слова: стеганографія, цифровий водяний знак, вейвлет-перетворення, дискретне косинусне перетворення, цифрове зображення.

Вступ

Сучасний розвиток інформаційних технологій та їх широке розповсюдження в соціумі призводять до масштабної миттєвої комунікації між кореспондентами з різних країн світу, обміну документами та мультимедійним даними через електронну пошту, соціальні мережі, месенджери тощо. Такий документообіг значно ускладнює захист авторських прав на інтелектуальну власність, адже будь-хто може скористатися чужим контентом, модифікувати його, видати за власний. Одним із засобів захисту інтелектуальної власності є вбудова в інформаційний контент цифрового водяного знаку (ЦВЗ), за допомогою якого власник може довести своє право на той чи інший контент, з використанням стеганографії, яка приховує сам факт існування у будь-якому цифровому контейнері додаткової інформації. Одними з найбільш розповсюджених об'єктів такого захисту є цифрові зображення (ЦЗ).

Серед стеганографічних методів вбудови ЦВЗ в ЦЗ можна виділити роботи [1-3], які використовують область дискретного косинусного перетворення (ДКП). Однак ці методи, не зважаючи на стійкість до стиску, не забезпечують надість цілісність

сприйняття стеганоповідомлень, отримані значення PSNR не перевищують 40 дБ. Більш якісні стеганоповідомлення можна отримати, вбудовуючи ЦВЗ в область вейвлет-перетворення за допомогою методів [4-5], проте в роботі [4] не проведено дослідження щодо стійкості запропонованого методу до атак, а в роботі [5] спостерігається невисока точність виявлення ЦВЗ.

Таким чином, підвищення стійкості стеганографічної системи ЦВЗ до атак при збереженні надійності сприйняття стеганоповідомлення є надзвичайно важливою і актуальною задачею.

Мета і задачі дослідження

Метою роботи є підвищення стійкості до атак та забезпечення надійного детектування цифрових водяних знаків з стеганоповідомлень, сформованих стеганографічним методом вбудовування ЦВЗ в область вейвлет-перетворення цифрового зображення.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

- проаналізувати вплив параметрів стеганографічного методу вбудовування ЦВЗ в область вейвлет-перетворення на ефективність детектування ЦВЗ;
- з урахуванням проведеного аналізу модифікувати стеганографічний метод вбудови ЦВЗ;
- провести оцінку ефективності запропонованого стеганографічного методу і порівняння його з аналогами.

Основна частина

За основу розроблювальної стеганографічної системи ЦВЗ було взято метод Dugad, Ratakonda і Ahuja [5], який здійснює вбудову водяного знаку в область вейвлет-перетворення. Додаткова інформація, в ролі якої виступає ЦВЗ – зображення в градаціях сірого, вбудовується в деталізовані коефіцієнти трирівневого вейвлет-перетворення на основі вейвлету Добеші-8, значення яких перевищують поріг $T_1 = 40$ за допомогою формули [5]

$$V_i' = V_i + \alpha \cdot |V_i| \cdot x_i, \tag{1}$$

де V_i – значення i-го деталізованого коефіцієнту, який перевищує поріг T_1, V_i' – значення модифікованого i-го деталізованого коефіцієнту стеганоповідомлення, x_i – значення яскравості ЦВЗ в діапазоні від $[0,1]$, α – масштабуючий коефіцієнт, $\alpha = 0.2$.

Детектування наявності в стеганоповідомленні ЦВЗ відбувається за наявності в детекторі водяного знаку наступним чином:

- стеганоповідомлення розкладається на три рівні вейвлет-перетворення, в матриці деталізованих коефіцієнтів обираються такі коефіцієнти, для яких виконується умова $\hat{V}_i > T_2 > T_1$, де $\hat{V}_i$ – стеганоповідомлення з (можливо) спотвореннями каналу зв'язку або навмисними модифікаціями зловмисника, $T_2 = 50$;
- з використанням існуючої в детекторі копії оригінального ЦВЗ обчислюється взаємна кореляція за формулою [5]

$$z = \frac{1}{M} \sum_i \hat{V}_i \cdot x_i, \tag{2}$$

де M – число елементів ЦВЗ;

- обчислене значення z порівнюється з порогом S, який визначається за формулою [5]

$$S = \frac{\alpha}{2M} \sum_i \left| \hat{V}_i \right|. \tag{3}$$

Якщо $z > S$, то детектор визначає наявність ЦВЗ.

Система ЦВЗ, запропонована Dugad, Ratakonda і Ahuja, дозволяє виявляти наявність ЦВЗ в умовах стиску, накладання шуму та деяких афінних перетворень, але, як показав проведений на основі 200 цифрових зображень обчислювальний експеримент, спостерігаються досить низькі значення PSNR: в середньому від 29.35 дБ до 45.78 дБ (для $QF \in [50, 100]$ з кроком 5) в залежності від якості стиску (чим нижче значення QF, тим нижче значення PSNR) та характеристик самого зображення (низька якість та чіткість контейнеру, його невеликий розмір, розмиті контури, тощо).

Одним з шляхів підвищення якості стеганоповідомлень, отриманих в результаті вбудови ЦВЗ, є збільшення порогових значень T_1, T_2, інший – заміна вейвлет-фільтру. Був проведений обчислювальний експеримент, в результаті якого вдалося збільшити значення PSNR в середньому від 31.87 дБ до 47.15 дБ (для $QF \in [50, 100]$ з кроком 5) при використанні вейвлету Добеші-43. Подальша зміна вейвлету не призводила до значного покращення якості стеганоповідомлень. В результаті аналізу матриць деталізованих коефіцієнтів, отриманих трирівневим перетворенням Добеші-43, оптимальними з точки зору якості зображення та забезпечення необхідної пропускної спроможності, значеннями порогів T_1 і T_2 прийнято $T_1 = 80, T_2 = 90$. Однак дослідження, спрямовані на оцінку ефективності детектування ЦВЗ, показали, що одночасна заміна вейвлет-фільтру та підвищення порогових значень T_1 і T_2 призводять до погіршення правильно виявлених стеганоповідомлень, захищених ЦВЗ.

Для забезпечення надійного детектування ЦВЗ в стеганоповідомленні була проведена інтеграція методу Dugad, Ratakonda і Ahuja з методом, запропонованим в [6] Mei Jiansheng, Li Sukang і Tan Xiaomei. На відміну від розглянутого вище методу Dugad, Ratakonda і Ahuja, який представляє собою стеганографічну систему ЦВЗ напівзакритого типу [7], запропонований в роботі [6] метод спрямований на вилучення ЦВЗ за наявності у детектора оригінального контейнеру, тобто система ЦВЗ закритого типу II [7]. Оскільки важливішою задачею для ЦВЗ є правильне детектування наявності вбудованого водяного знаку в стеганоповідомленні, що зазнало випадкових або навмисних спотворень, модифікуємо метод Mei Jiansheng, Li Sukang і Tan Xiaomei як систему ЦВЗ напівзакритого типу.

Згідно з методом [6] перед вбудовою ЦВЗ в контейнер обчислюється ДКП матриці водяного знаку, після чого відбувається його вбудова в контейнер за формулою

$$V_i' = V_i + \alpha \cdot x_i. \tag{4}$$

Таким чином, зазначимо основні кроки модифікованої стеганографічної системи ЦВЗ.

Вбудова ЦВЗ.

Для цифрового зображення в градаціях сірого I (колірної складової кольорового ЦЗ) розміром $m \times n$ і ЦВЗ в градаціях сірого Z розміром $h \times w$:

Крок 1. Побудувати трирівневе вейвлет-перетворення контейнеру I на основі вейвлет-фільтру W. В результаті отримуємо матрицю апроксимуючих коефіцієнтів A і три матриці деталізованих коефіцієнтів H, V, D розміром $m_3 \times n_3$.

Крок 2. Вибір матриці деталізованих коефіцієнтів для вбудови ЦВЗ. Матриця для вбудови ЦВЗ обирається таким чином, щоб кількість коефіцієнтів, більших T_1, перевищувала $k = h \cdot w$. Далі обрану матрицю детальних коефіцієнтів позначаємо як C.

Крок 3. Побудувати ДКП для ЦВЗ Z. Результат – матриця коефіцієнтів ДКП розміром $h \times w$, представлена у виді вектору X розміром k.

Крок 4. *Вбудова ЦВЗ.*

Якщо $C_{i,j} > T_1, i = \overline{1, m_3}, j = \overline{1, n_3},$ то $C_{i,j}{}' = C_{i,j} + \alpha \cdot X_g, g = \overline{1, k}.$

Крок 5. Побудувати обернене трирівневе вейвлет-перетворення на основі вейвлет-фільтру W.

Крок 6. Зберегти стеганоповідомлення.

Детектування наявності ЦВЗ.

Для стеганоповідомлення в градаціях сірого I' (колірної складової кольорового ЦЗ) розміром $m \times n$ і ЦВЗ в градаціях сірого Z розміром $h \times w$:

Крок 1. Побудувати трирівневе вейвлет-перетворення стеганоповідомлення I' на основі вейвлет-фільтру W. В результаті отримуємо матрицю апроксимуючих коефіцієнтів A' і три матриці деталізованих коефіцієнтів H', V', D' розміром $m_3 \times n_3$. Для детектування ЦВЗ використовується одна з матриць H', V', D' – C', яка має містити ЦВЗ Z.

Крок 2. Побудувати ДКП для ЦВЗ Z. Результат – матриця коефіцієнтів ДКП розміром $h \times w$, представлена у виді вектору X розміром k.

Крок 3. Якщо $C'_{i,j} > T_2 > T_1,\ i = \overline{1, m_3},\ j = \overline{1, n_3},$ обчислити взаємну кореляцію

$$z = \frac{1}{k} \sum_{i,j,g} C'_{i,j} \cdot X_g,$$

де $g = \overline{1, k}.$

Крок 4. Обчислити поріг $S = \frac{\alpha}{2k} \sum_{i,j} \left| C'_{i,j} \right|.$

Крок 5. Детектування наявності ЦВЗ.

Якщо $z > S$, *то* стеганоповідомлення I' містить ЦВЗ,

інакше стеганоповідомлення I' не містить ЦВЗ.

В запропонованому стеганографічному методі ЦВЗ стеганоповідомлення зберігаються в форматі з втратами, адже такі зображення найбільш поширені у зв'язку з їх малим розміром і забезпеченням високої якості самого ЦЗ.

Приклад вбудови ЦВЗ в синю колірну складову ЦЗ запропонованим методом та методом [5] наведено на рисунку 1.

В наведеному прикладі стеганоповідомлення (рис.1, в, д) були збережені в форматі з втратами JPG з якістю $QF = 100$. При використанні методу [5] значення PSNR становить 52.036 дБ, а при використанні запропонованого методу – 53.0964 дБ.

Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 кольорових ЦЗ при використанні різних ЦВЗ, які були вбудовані в синю колірну складову контейнерів. В трирівневому вейвлет-перетворенні для вбудови ЦВЗ використовувалися вертикальні деталізовані коефіцієнти. Обчислювальні експерименти проводилися для чотирьох варіацій методів:

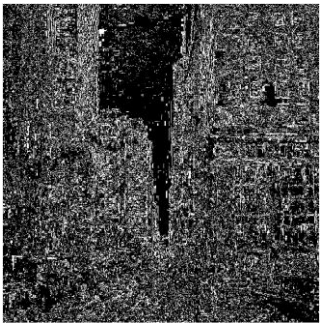
- метод Dugad, Ratakonda і Ahuja з використанням вейвлет-фільтру Добеші-8 та порогами $T_1 = 40, T_2 = 50$ – M1;

- метод Dugad, Ratakonda і Ahuja з використанням вейвлет-фільтру Добеші-43 та порогами $T_1 = 80, T_2 = 90$ – М2;
- запропонований метод з використанням вейвлет-фільтру Добеші-8 та порогами $T_1 = 40, T_2 = 50$ – М3;
- запропонований метод з використанням вейвлет-фільтру Добеші-43 та порогами $T_1 = 80, T_2 = 90$ – М4.

а

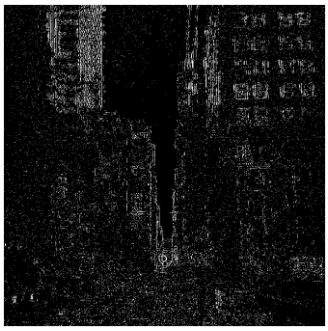
б

в



г

д



є

Рис. 1. Приклад вбудови ЦВЗ в цифрове зображення: а – оригінальний контейнер; б – ЦВЗ; в – стеганоповідомлення, отримане вбудовою ЦВЗ в контейнер методом Dugad, Ratakonda і Ahuja при використанні вейвлет-фільтру Добеші-8 і $T_1 = 40, T_2 = 50$; г – розміщення ЦВЗ в матриці синьої колірної складової стеганоповідомлення в); д – стеганоповідомлення, отримане вбудовою ЦВЗ в контейнер запропонованим методом при використанні вейвлет-фільтру Добеші-43 і $T_1 = 80, T_2 = 90$; є – розміщення ЦВЗ в матриці синьої колірної складової стеганоповідомлення д)

Ефективність методів будемо оцінювати як долю правильно виявлених ЦВЗ в стеганоповідомленні. Результати обчислювального експерименту для зазначених методів з атакою стиску при різних значеннях якості QF наведені в таблиці 1.

Таблиця 1.

Ефективність детектування наявності ЦВЗ в стеганоповідомленні за умови атаки стиском

QF	100	95	90	85	80	75	70	65	60	55
M1	0.765	0.75	0.76	0.75	0.75	0.74	0.74	0.73	0.73	0.73
M2	*0.44*	*0.41*	*0.4*	*0.4*	*0.39*	*0.39*	*0.39*	*0.4*	*0.4*	*0.4*
M3	0.915	0.91	0.94	0.89	0.9	0.91	0.93	0.9	0.94	0.96
M4	**0.995**	**0.99**	**0.98**	**0.98**	**0.96**	**0.95**	**0.97**	**0.95**	**0.96**	**0.95**
QF	50	45	40	35	30	25	20	15	10	5
M1	0.74	0.75	0.73	0.72	0.72	0.73	0.74	0.73	0.71	0.71
M2	*0.39*	*0.4*	*0.38*	*0.39*	*0.38*	*0.39*	*0.38*	*0.39*	*0.39*	*0.4*
M3	0.87	0.88	0.93	0.93	0.94	0.93	0.94	0.94	0.92	0.9
M4	**0.97**	**0.98**	**0.96**	**0.98**	**0.97**	**0.98**	**0.98**	**0.98**	**0.975**	**0.98**

Як видно з таблиці 1, найкращі результати детектування ЦВЗ в умовах стиску характерні для запропонованого методу (варіації M3 і M4), найгірший результат – для варіації методу Dugad, Ratakonda і Ahuja M2, тому в подальших експериментах він не буде розглядатися.

Окрім атаки стиском можуть використовуватися як будь-які навмисні атаки зловмисника, так і випадкові спотворення в процесі передачі стеганоповідомлення по каналу зв'язку. В таблицях 2 і 3 наведено порівняння ефективності детектування ЦВЗ в умовах атак для методів M1, M3 і M4 при різних значеннях параметру QF .

Таблиця 2.

Порівняння ефективності детектування наявності ЦВЗ в стеганоповідомленні за умови атак для методів M1, M3, M4 при $QF \in [55, 100]$

QF		100	95	90	85	80	75	70	65	60	55
Атака	Параметри	**M1**									
Гаусів шум	$m = 0.01$, $d = 0.0005$	0.755	0.75	0.74	0.74	0.74	0.73	0.73	0.73	0.73	0.73
	$m = 0.01$, $d = 0.00005$	0.765	0.76	0.76	0.74	0.75	0.74	0.73	0.74	0.74	0.74
	$m = 0.01$, $d = 0.000005$	0.765	0.76	0.76	0.76	0.74	0.73	0.74	0.74	0.73	0.74
Пуасонівський шум		0.715	0.73	0.73	0.72	0.71	0.7	0.72	0.71	0.71	0.72
Мультиплі-кативний шум	$d = 0.001$	0.755	0.75	0.75	0.75	0.75	0.74	0.74	0.74	0.74	0.73
	$d = 0.0001$	0.765	0.75	0.76	0.75	0.75	0.74	0.73	0.74	0.73	0.74
	$d = 0.00001$	0.765	0.75	0.76	0.75	0.75	0.74	0.73	0.74	0.74	0.73
Імпульсний шум	$d = 0.001$	0.755	0.74	0.75	0.74	0.74	0.73	0.74	0.74	0.74	0.74
Фільтр підвищення різкості «unsharp»		0.77	0.77	0.76	0.77	0.76	0.75	0.76	0.76	0.76	0.76
Зсув	$sh_x = 0.15$, $sh_y = 0.25$	0.79	0.76	0.77	0.76	0.76	0.76	0.75	0.75	0.75	0.75
Масштаб	$s_x = 1.15$, $s_y = 0.85$	0.81	0.81	0.81	0.8	0.75	0.75	0.75	0.75	0.75	0.75

Продовження таблиці 2.

Поворот	30°	0.82	0.81	0.81	0.81	0.81	0.81	0.8	0.75	0.75	0.75
Атака	Параметри	**M3**									
Гаусів шум	$m = 0.01$, $d = 0.0005$	0.915	0.92	0.93	0.91	0.91	0.87	0.94	0.88	0.97	0.95
	$m = 0.01$, $d = 0.00005$	0.955	0.92	0.93	0.91	0.92	0.91	0.95	0.89	0.94	0.95
	$m = 0.01$, $d = 0.000005$	0.91	0.93	0.97	0.93	0.91	0.95	0.96	0.91	0.95	0.92
Пуасонівський шум		0.865	0.89	0.92	0.94	0.96	0.89	0.93	0.94	0.93	0.91
Мультиплі-кативний шум	$d = 0.001$	0.915	0.91	0.9	0.94	0.93	0.9	0.92	0.94	0.95	0.92
	$d = 0.0001$	0.945	0.93	0.93	0.9	0.91	0.93	0.93	0.91	0.96	0.92
	$d = 0.00001$	0.925	0.91	0.94	0.93	0.9	0.92	0.96	0.94	0.96	0.91
Імпульсний шум	$d = 0.001$	0.925	0.95	0.95	0.91	0.93	0.91	0.95	0.92	0.96	0.93
Фільтр підвищення різкості «unsharp»		0.87	0.91	0.89	0.94	0.93	0.91	0.92	0.91	0.9	0.91
Зсув	$sh_x = 0.15$, $sh_y = 0.25$	0.94	0.93	0.95	0.91	0.92	0.93	0.94	0.93	0.95	0.96
Масштаб	$s_x = 1.15$, $s_y = 0.85$	0.51	0.65	0.45	0.41	0.49	0.69	0.69	0.37	0.38	0.34
Поворот	30°	0.5	0.5	0.45	0.45	0.45	0.6	0.65	0.36	0.4	0.6
Атака	Параметри	**M4**									
Гаусів шум	$m = 0.01$, $d = 0.0005$	0.995	0.99	0.98	0.98	0.96	0.95	0.97	0.95	0.96	0.95
	$m = 0.01$, $d = 0.00005$	0.985	0.99	0.99	0.98	0.98	0.99	0.94	0.95	0.95	0.98
	$m = 0.01$, $d = 0.000005$	0.985	1	0.98	0.99	0.97	0.94	0.96	0.98	0.98	1
Пуасонівський шум		0.975	0.95	0.98	1.01	0.96	0.95	0.94	0.97	0.97	0.97
Мультиплі-кативний шум	$d = 0.001$	0.975	0.95	0.98	1.01	0.96	0.95	0.94	0.97	0.97	0.97
	$d = 0.0001$	0.985	0.99	1	0.99	0.99	0.96	0.97	0.99	0.97	0.95
	$d = 0.00001$	0.995	1	0.98	0.97	0.97	0.97	0.95	0.97	0.98	0.97
Імпульсний шум	$d = 0.001$	0.995	1	0.98	0.97	0.96	0.95	0.94	0.99	0.96	0.95
Фільтр підвищення різкості «unsharp»		0.895	0.95	0.92	0.95	0.94	0.97	0.97	0.97	0.97	0.97
Зсув	$sh_x = 0.15$, $sh_y = 0.25$	0.895	0.95	0.92	0.95	0.94	0.97	0.97	0.97	0.97	0.97
Масштаб	$s_x = 1.15$, $s_y = 0.85$	1	1	0.99	0.97	0.98	0.96	0.99	0.97	0.98	0.98
Поворот	30°	0.63	0.57	0.45	0.56	0.47	0.67	0.59	0.58	0.58	0.63

Таблиця 3.

Порівняння ефективності детектування наявності ЦВЗ в стеганоповідомленні за умови атак для методів М1, М3, М4 при $QF \in [5, 50]$

QF		50	45	40	35	30	25	20	15	10	5
Атака	Параметри	**М1**									
Гаусів шум	$m = 0.01$, $d = 0.0005$	0.73	0.72	0.73	0.72	0.71	0.71	0.73	0.73	0.7	0.71
	$m = 0.01$, $d = 0.00005$	0.73	0.74	0.74	0.72	0.71	0.73	0.74	0.73	0.71	0.71
	$m = 0.01$, $d = 0.000005$	0.74	0.74	0.74	0.72	0.71	0.72	0.74	0.74	0.71	0.71
Пуасонівський шум		0.72	0.72	0.69	0.72	0.71	0.7	0.71	0.69	0.7	0.7
Мультиплікативний шум	$d = 0.001$	0.73	0.73	0.72	0.72	0.73	0.73	0.73	0.73	0.71	0.71
	$d = 0.0001$	0.74	0.75	0.74	0.71	0.72	0.74	0.74	0.74	0.71	0.71
	$d = 0.00001$	0.74	0.74	0.74	0.72	0.72	0.73	0.74	0.73	0.71	0.71
Імпульсний шум	$d = 0.001$	0.74	0.74	0.73	0.73	0.72	0.72	0.72	0.72	0.71	0.71
Фільтр підвищення різкості «unsharp»		0.75	0.75	0.74	0.74	0.74	0.74	0.74	0.74	0.74	0.74
Зсув	$sh_x = 0.15$, $sh_y = 0.25$	0.75	0.76	0.74	0.74	0.75	0.74	0.75	0.73	0.71	0.71
Масштаб	$s_x = 1.15$, $s_y = 0.85$	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.7	0.64
Поворот	30°	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.7	0.69
Атака	Параметри	**М3**									
Гаусів шум	$m = 0.01$, $d = 0.0005$	0.9	0.93	0.9	0.89	0.93	0.93	0.94	0.88	0.9	0.9
	$m = 0.01$, $d = 0.00005$	0.92	0.91	0.92	0.93	0.93	0.9	0.92	0.89	0.97	0.9
	$m = 0.01$, $d = 0.000005$	0.92	0.9	0.94	0.89	0.95	0.95	0.94	0.94	0.93	0.9
Пуасонівський шум		0.92	0.96	0.94	0.92	0.95	0.9	0.88	0.93	0.89	0.9
Мультиплікативний шум	$d = 0.001$	0.93	0.9	0.94	0.97	0.95	0.91	0.95	0.92	0.92	0.9
	$d = 0.0001$	0.92	0.94	0.92	0.89	0.93	0.95	0.9	0.92	0.94	0.9
	$d = 0.00001$	0.87	0.94	0.92	0.91	0.95	0.95	0.9	0.91	0.94	0.9
Імпульсний шум	$d = 0.001$	0.91	0.92	0.9	0.92	0.95	0.93	0.94	0.89	0.89	0.9
Фільтр підвищення різкості «unsharp»		0.94	0.93	0.88	0.92	0.92	0.94	0.97	0.9	0.92	0.9
Зсув	$sh_x = 0.15$, $sh_y = 0.25$	0.9	0.91	0.95	0.94	0.96	0.93	0.96	0.95	0.94	0.9
Масштаб	$s_x = 1.15$, $s_y = 0.85$	0.37	0.37	0.69	0.69	0.37	0.41	0.37	0.41	0.39	0.5

Продовження таблиці 3.

Поворот	30°	0.64	0.4	0.65	0.37	0.44	0.4	0.36	0.37	0.34	0.4
Атака	Параметри	**M4**									
Гаусів шум	$m=0.01,$ $d=0.0005$	0.95	0.94	0.97	0.98	0.97	0.95	0.97	0.97	0.935	0.945
	$m=0.01,$ $d=0.00005$	0.95	0.98	1	0.99	0.95	0.95	0.98	0.94	0.955	0.945
	$m=0.01,$ $d=0.000005$	0.96	0.99	0.99	0.94	0.97	0.97	0.99	0.97	0.935	0.955
Пуасонівський шум		0.98	0.96	0.96	0.96	0.97	0.95	0.97	0.98	0.965	0.975
Мультиплі-кативний шум	$d=0.001$	0.95	0.98	0.98	0.96	0.98	0.98	0.95	0.97	0.975	0.955
	$d=0.0001$	0.98	0.98	0.99	0.97	0.98	0.95	0.98	0.98	0.965	0.955
	$d=0.00001$	0.97	0.99	0.97	0.97	1	0.96	1	0.95	0.955	0.975
Імпульсний шум	$d=0.001$	0.96	0.98	0.95	0.98	0.98	0.97	0.97	0.98	0.945	0.955
Фільтр підвищення різкості «unsharp»		0.96	0.93	0.93	0.96	0.96	0.93	0.94	0.96	0.965	0.985
Зсув	$sh_x=0.15,$ $sh_y=0.25$	1	0.99	0.98	0.98	1	0.98	0.98	0.99	0.98	0.99
Масштаб	$s_x=1.15,$ $s_y=0.85$	0.63	0.7	0.48	0.54	0.54	0.51	0.47	0.58	0.68	0.61
Поворот	30°	0.54	0.59	0.63	0.48	0.59	0.53	0.49	0.53	0.46	0.47

Порівнюючи варіації запропонованого методу вбудови ЦВЗ М3 і М4 можна зробити висновок, що використання вейвлет-фільтру Добеші-43 разом з порогами $T_1=80, T_2=90$ дає кращі результати детектування наявності ЦВЗ в цифровому контенті при забезпеченні високої якості стеганоповідомлень.

Висновки

В роботі запропоновано модифікацію стеганографічного методу вбудови ЦВЗ в область вейвлет-перетворення ЦЗ. В ході дослідження впливу порогових значень T_1, T_2 і обраного вейвлет-фільтру було встановлено, що використання вейвлету Добеші-43 у порівнянні з Добеші-8 дає кращі показники цілісності сприйняття стеганоповідомлення (значення PSNR вище при використанні Добеші-43), однак одночасне збільшення порогових значень T_1, T_2 призводить до погіршення результатів детектування ЦВЗ.

З метою покращення виявлення наявності ЦВЗ в стеганоповідомленні до ЦВЗ перед вбудовою в контейнер було застосовано ДКП. Це дозволило забезпечити високу точність детектування ЦВЗ не тільки в умовах стиску, а й під впливом додаткових атак, таких як шум, підвищення різкості, деякі афінні перетворення, зберігаючи при цьому високу якість сформованого стеганоповідомлення.

Проведені обчислювальні експерименти, спрямовані на визначення ефективності запропонованого стеганографічного методу, показали, що метод є стійким до стиску,

накладання шуму, підвищення різкості та деяких афінних перетворень (зсуву та масштабування при $QF > 50$).

Список літератури

1. Podilchuk, I. Image-Adaptive Watermarking Using Visual Models / I. Podilchuk, W. Zeng. // IEEE Journal on selected areas in communications. – 1998. – №4. – Pp. 525-539.
2. Chiou-Ting, Hsu. Multiresolution Watermarking for Digital Images / Hsu. Chiou-Ting, Ja-Ling Wu // IEEE Transactions on circuits and systems—II: Analog and digital signal processing. – 1998. – №8. – Pp. 1097-1101.
3. Pal, A. A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity / A. Pal, K. Naik, R. Agarwal. // The International Arab Journal of Information Technology. – 2019. – №1. – С. 116-124.
4. Baby, D. A Novel DWT based Image Securing Method using Steganography / D. Baby, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela // International Conference on Information and Communication Technologies (ICICT 2014). – 2015. – С. 612-618.
5. Dugat, R. A new wavelet-based scheme for watermarking images / R. Dugat, K. Ratakonda, N. Ahuja // Proceedings of the IEEE International Conference Image Processing. – 1998. – Pp. 357-372.
6. Jiansheng, M. A Digital Watermarking Algorithm Based On DCT and DWT / M. Jiansheng, Li Sukang and Tan Xiaomei // Proceedings of the 2009 International Symposium on Web Information Systems and Applications. – 2009. – Pp. 104-107.
7. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2017. – 262 с.

МОДИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ВСТРАИВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ИЗОБРАЖЕНИЕ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

А.В. Ахмаметьева, А.А. Баранюк, А.И. Казаков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: anna-odessitka@mail.ru

В работе предложена модификация стеганографического метода встраивания цифрового водяного знака в область вейвлет-преобразования цифрового изображения. Предложенный метод осуществляет встраивание водяного знака в высокочастотные детализирующие коэффициенты трехуровневого вейвлет-преобразования с использованием вейвлета Добеши-43, который обеспечивает высокое качество полученного стеганосообщения, сохраняемого в формате с потерями, что обусловлено широким распространением таких изображений в связи с их малым размером. К цифровому водяному знаку применяется Дискретное косинусное преобразование, благодаря чему повышается эффективность выявления наличия водяного знака в стеганосообщении. В работе проводится анализ эффективности детектирования цифрового водяного знака в зависимости от пороговых значений, определяющих выбор детализирующих коэффициентов, используемых для погружения, в результате которого установлено, что повышение порогов без применения к водяному знаку Дискретного косинусного преобразования приводит к значительному ухудшению точности детектирования. И наоборот, предложенный метод с пороговыми значениями T_1=80 и T_2=90 выбора детализирующих коэффициентов в соединении с Дискретным косинусным преобразованием матрицы водяного знака позволил повысить процент правильно выявленных стеганосообщений. Результаты проведенных экспериментов показали стойкость вложения цифрового водяного знака к атакам сжатия (даже при качестве изображения QF=5), наложению шума, повышения резкости, сдвига, для которых точность детектирования составляет в среднем 97%. Также метод является стойким к масштабированию при условии QF>50. В работе проводится сравнение стойкости оригинального метода встраивания цифрового водяного знака и разных вариаций предложенной модификации стеганографического метода к комплексным атакам (сжатию в соединении с другими видами обработки цифровых изображений).

Ключевые слова: стеганография, цифровой водяной знак, вейвлет-преобразование, Дискретное косинусное преобразование, цифровое изображение.

MODIFICATION OF THE STEGANOGRAPHIC METHOD OF EMBEDDING A DIGITAL WATERMARK INTO IMAGE BASED ON A WAVELET TRANSFORM

A.V. Akhmametieva, A.A. Baranuk, A.I. Kazakov

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: anna-odessitka@mail.ru

The paper proposes a modification of the steganographic method of embedding a digital watermark into Wavelet transform domain of a digital image. The proposed method embeds a watermark in the high-frequency detail coefficients of a three-level Wavelet transform using the Dobeshi-43 wavelet, which ensures the high quality of the resulting stego. Stego is a result of embedding of digital watermark into container and is saved in a losses format that is caused by wide dissemination of such images due to their small size. Discrete cosine transform is applied to a digital watermark, thereby increasing the efficiency of detecting the presence of a watermark in a stego. In work the analysis of efficiency of detecting of the digital watermark depending on the threshold values defining the choice of the detailing coefficients used for embedding is carried out. A result of this analysis is establishment the fact that increase in thresholds without application of Discrete cosine transformation to the watermark leads to considerable deterioration in accuracy of detecting. Conversely, the proposed method with the threshold values T_1=80 and T_2=90 of the choice of detailing coefficients in conjunction with the Discrete Cosine Transformation of the watermark matrix increased the percentage of correctly identified stegos. The results of the experiments showed the resistance of embedding a digital watermark to compression attacks (even with image quality QF=5), imposing noise, sharpening, shifting, for which the detection accuracy averages 97%. Also, the method is resistant to scaling provided QF>50. This paper compares the resistance of the original method of embedding a digital watermark and different variations of the proposed modification of the steganographic method to complex attacks (compression in combination with other types of digital image processing).

Keywords: steganography, digital watermark, Wavelet-transform, Discrete cosine transformation, digital image

УДК 681

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 49-58

АЛГОРИТМ ВИЯВЛЕННЯ ОБРОБКИ ЦИФРОВОГО ЗОБРАЖЕННЯ ФІЛЬТРОМ «MOTION BLUR»

В.В. Зоріло, О.А. Карпова

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: vikazorilo@gmail.com, kaaarpova@gmail.com

Цифрові зображення відіграють велику роль у житті сучасних людей, адже постійно використовуються у повсякденній діяльності, а також у засобах масової інформації, юриспруденції, політиці, мистецтві, медицині, науці. Простота та доступність програмного забезпечення для зміни цифрових зображень є однією з головних причин виникнення великої кількості фальсифікованих фото. Існуючі методи виявлення порушень цілісності цифрових зображень не є універсальними. Через це актуальним є пошук нових рішень цієї проблеми. Як показує практика та факти, відомі з відкритих джерел, розмиття є одним з програмних інструментів, який часто використовують для обробки цифрового зображення. Для розгляду у даній роботі обрано розмиття при відтворенні ефекту руху фільтром графічного редактора Adobe Photoshop «Motion blur». У відкритому друці не знайдено алгоритмів, які виявляють розмиття даного виду. Метою даної роботи є виявлення розмиття цифрового зображення фільтром «Motion blur» шляхом розробки алгоритму, заснованого на аналізі сингулярних чисел блоків матриці цифрового зображення. В роботі проведено огляд існуючих методів виявлення розмиття зображення; виявлено характерні особливості матриці цифрового зображення, які дозволять встановити наявність розмиття зазначеним фільтром. Розроблено алгоритм, який засновано на аналізі шести найменших сингулярних чисел блоків матриці цифрового зображення за червоним колірним каналом. Кількість сингулярних чисел для перевірки та вибір колірного каналу цифрового зображення обґрунтовано обчислювальним експериментом з використанням 600 зображень. Кількість помилок 1 роду розробленого алгоритму складає 1%, кількість помилок 2 роду – 2%. За допомогою розробленого алгоритму також за необхідності можна встановити кут розмиття з вірогідністю помилки 7,68%. Подальший напрямок досліджень націлено на вдосконалення виявлення обробки цифрового зображення різними фільтрами сучасних графічних редакторів.

Ключові слова: виявлення розмиття зображення, цифрове зображення, ефект руху, порушення цілісності, сингулярні числа, коефіцієнт швидкості росту.

Вступ

Безпека та автентичність – головні проблеми з початку використання цифрових зображень у багатьох сферах діяльності людини. Процес їхньої зміни став настільки популярним та простим, що користувачі без особливих зусиль можуть втручатися у зображення. Доступність та потужність програм для обробки цифрових зображень, таких як Adobe Photoshop чи GIMP, дає змогу змінювати цифрове зображення, не залишаючи помітних візуальних слідів. Через це треба володіти інструментами для виявлення порушень цілісності зображень, щоб мати змогу довести їх оригінальність.

Відомо багато способів зміни цифрового зображення, які є різними за своєю дією та складністю. Одним з популярних інструментів обробки є розмиття. Необхідно зауважити, що розмиття нерідко використовується в фотоіндустрії для акцентування уваги на деякому об’єкті за рахунок розмиття області навколо нього; надання об’єкту ефекту руху; усунення дефектів зображення, що можуть з’явитися під час сканування; усунення дефектів шкіри людини тощо. На жаль відомі сьогодні методи не дають можливості вирішити проблему виявлення програмного розмиття повністю.

Існують деякі види розмиття, які використовують для надання зображенню художнього ефекту, наприклад, для створення ефекту руху певного об’єкта на зображенні. Цього можна досягти за допомогою налаштувань фотокамери та прийомів фотографа, тобто, не використовуючи обробку зображення графічними редакторами, тоді таке зображення буде оригінальним. Також цей ефект можна підробити і у графічному редакторі, наприклад, фільтром «Motion blur» редактора Adobe Photoshop. Тоді такі дії можна вважати втручанням у цілісність початкового зображення.

Мета і задачі

Метою даної роботи є забезпечення виявлення розмиття цифрового зображення фільтром «Motion blur» шляхом розробки алгоритму, заснованого на аналізі сингулярних чисел блоків матриці цифрового зображення.

Для досягнення цієї мети необхідно вирішити наступні *задачі*:

- провести аналіз існуючих методів виявлення розмиття зображення;
- виявити характерні особливості матриці цифрового зображення, які дозволять встановити наявність розмиття;
- розробити алгоритм виявлення розмиття цифрового зображення фільтром «Motion blur» та провести аналіз його ефективності.

Основна частина

Розроблений у [1] метод виявлення розмиття (МВР), який засновано на загальному підході до аналізу інформаційної системи [2], відрізняється від інших відомих методів виявлення розмиття [3, 4] своєю ефективністю, але має суттєві недоліки. Першим недоліком є різні порогові значення для знімків, отриманих непрофесійною та професійною фототехнікою, щоб мати змогу відокремити розмите зображення від нерозмитого. Другим недоліком є те, що цей метод було перевірено для малої кількості видів розмиття, хоча сучасні графічні редактори надають можливість виконувати розмиття зображення більш ніж десятьма різними способами.

Один з основних параметрів розмиття – радіус. Чим більший радіус, тим сильніше і помітніше розмиття. Розмиття з великим радіусом у більшості випадків викликає підозри до ЦЗ, що є небажаним, якщо метою цього розмиття було приховання результатів стеганографічної атаки чи фальсифікації. Проте для розмиття для передачі ефекту руху великий радіус розмиття не є таким неприроднім та підозрілим. Наприклад, для передачі швидкого руху автівки є цілком логічним значне розмиття навколишніх об’єктів (рис. 1). У фільтрі «Motion blur» аналогом радіусу є параметр – довжина розмиття.

Рис. 1. Приклад застосування фільтру «Motion blur»

У зв'язку із вказаним вище, для проведення досліджень в якості мінімуму для довжини розмиття L було обрано значення у 50 пікселів. Для сучасних цифрових фотографій, які мають зазвичай досить великі розміри, ефект розмиття у 50 пікселів за допомогою фільтру «Motion blur» не є сильним при перегляді повного зображення. Другий параметр даного фільтру – кут розмиття. Даний параметр визначає, під яким кутом будуть «розтягнуті» об'єкти зображення.

Як відомо, розмиття зображення призводить до зменшення його високочастотної складової. Візуально результатом роботи даного інструменту обробки є згладжування контурів. Головну роль при аналізі стану й властивостей цифрового зображення грають сингулярні числа (СНЧ) матриці, що відповідають даному цифровому зображенню (ЦЗ). Із [1] відомо, що при застосуванні розмиття СНЧ зменшуються наступним чином: СНЧ, які відповідають високим частотам ЦЗ, тобто найменші, а також середні за значенням СНЧ будуть змінені найбільше, на відміну від швидкості росту найменших СНЧ нерозмитого зображення. Можна зробити припущення, що такий фільтр як «Motion blur» також буде зменшувати високочастотну та середньочастотну складову цифрового зображення. Перевіримо, чи можна модифікувати МВР чи адаптувати його порогове значення до виявлення зазначеного фільтру.

Для аналізу оригінальних ЦЗ будемо використовувати матриці усіх трьох колірних каналів. Кожну матрицю розіб'ємо стандартним чином на блоки 8×8 та знайдемо множину СНЧ для кожного блоку. У результаті отримаємо матриці сингулярних чисел (МСНЧ) блоків ЦЗ. Будемо перевіряти від 3 до 6 найменших сингулярних чисел. Побудуємо для обраних СНЧ лінійні апроксимації по кожній колірній матриці та визначимо похідні, значення яких являє собою коефіцієнти швидкості росту (КШР) обраних СНЧ згідно МВР. Після цього знайдемо середні та максимальні значення цих коефіцієнтів. Аналогічним чином проводимо аналіз розмитих ЦЗ за допомогою фільтру «Motion blur».

Проведемо аналіз середніх та максимальних значень КШР. Типові результати обчислення надано у таблицях 1-8.

Таблиця 1.

Середні значення КШР трьох найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,13	0,13	0,13	0,19	0,19	0,19	0,28	0,29	0,28
2	0,29	0,33	0,34	0,18	0,18	0,18	0,27	0,27	0,27
3	0,34	0,34	0,33	0,14	0,13	0,12	0,23	0,23	0,22
4	0,34	0,35	0,33	0,08	0,08	0,09	0,17	0,17	0,18

Таблиця 2.

Максимальні значення КШР трьох найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,34	0,34	0,33	0,24	0,24	0,23	0,34	0,34	0,37
2	0,38	0,37	0,39	0,21	0,20	0,2	0,31	0,3	0,30
3	0,38	0,37	0,37	0,18	0,17	0,17	0,27	0,3	0,26
4	0,39	0,38	0,37	0,13	0,14	0,14	0,24	0,24	0,24

Таблиця 3.

Середні значення КШР чотирьох найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,15	0,15	0,15	0,14	0,14	0,14	0,26	0,26	0,26
2	0,33	0,38	0,39	0,17	0,16	0,16	0,26	0,26	0,26
3	0,40	0,39	0,39	0,18	0,17	0,16	0,26	0,26	0,26
4	0,40	0,41	0,38	0,16	0,14	0,11	0,28	0,27	0,24

Таблиця 4.

Максимальні значення КШР чотирьох найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,39	0,38	0,39	0,23	0,23	0,23	0,31	0,30	0,30
2	0,44	0,42	0,43	0,22	0,22	0,22	0,30	0,30	0,31
3	0,44	0,43	0,44	0,25	0,23	0,23	0,32	0,30	0,31
4	0,44	0,44	0,42	0,20	0,18	0,16	0,30	0,30	0,29

Таблиця 5.

Середні значення КШР п’яти найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,19	0,18	0,18	0,17	0,18	0,18	0,31	0,31	0,30
2	0,41	0,47	0,48	0,20	0,20	0,19	0,30	0,30	0,30
3	0,50	0,48	0,48	0,21	0,20	0,19	0,30	0,30	0,30
4	0,51	0,50	0,48	0,19	0,18	0,15	0,33	0,32	0,28

Таблиця 6.

Максимальні значення КШР п’яти найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,47	0,47	0,47	0,24	0,24	0,23	0,36	0,35	0,35
2	0,56	0,53	0,53	0,23	0,23	0,24	0,35	0,34	0,35
3	0,56	0,55	0,55	0,25	0,24	0,24	0,37	0,36	0,35
4	0,57	0,55	0,53	0,23	0,21	0,20	0,37	0,35	0,34

Таблиця 7.

Середні значення КШР шести найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,24	0,24	0,24	0,21	0,22	0,21	0,98	0,98	0,95
2	0,53	0,60	0,62	0,22	0,23	0,22	0,63	0,64	0,64
3	0,65	0,63	0,62	0,23	0,23	0,22	0,33	0,33	0,33
4	0,69	0,65	0,62	0,23	0,22	0,19	0,44	0,47	0,46

Таблиця 8.

Максимальні значення КШР шести найменших СНЧ

№ ЦЗ	Оригінальні ЦЗ			Розмиті ЦЗ під кутом 0°			Розмиті ЦЗ під кутом 20°		
	R	G	B	R	G	B	R	G	B
1	0,61	0,61	0,61	0,26	0,26	0,25	1,33	1,35	1,30
2	0,74	0,70	0,69	0,25	0,25	0,25	0,97	0,99	0,99
3	0,75	0,71	0,71	0,25	0,25	0,26	0,36	0,36	0,37
4	0,76	0,72	0,69	0,25	0,24	0,23	0,64	0,67	0,66

Аналізуючи результати досліджень, було встановлено, що виділити певне порогове значення для відокремлення оригінальних ЦЗ від фальсифікованих неможливо. Помічено й те, що СНЧ змінюються по різному в залежності від кута розмиття, та найбільш «сильним» в плані зменшення значень СНЧ є розмиття під кутами 0° та 90° по множині {0°; 10, …, 90°}. У МВР в якості інструменту додаткової перевірки зображення використовувалося експертне розмиття – проведення експертом навмисного розмиття досліджуваного зображення для подальшого аналізу відмінностей отриманого та початкового ЦЗ. Доцільність даного інструменту обґрунтовано тим, що суттєво впливає на СНЧ тільки первинне розмиття. Повторне розмиття також зменшує СНЧ, проте порівняно з первинним ці зміни якісно відрізняються. Для перевірки, чи виконується це при обробці фільтром «Motion blur», протестовано 100 різних оригінальних ЦЗ. Для проведення експертного розмиття використано наступні параметри: довжина розмиття $L = 50$ пікселів та кут розмиття $\varphi \in \{0°;10,...,90°\}$. Кількісні зміни середніх значень коефіцієнтів швидкості росту СНЧ для одного зображень наведено у таблиці 9. Коефіцієнти у таблиці визначають, у скільки разів зменшується середня швидкість росту СНЧ після першого розмиття зображення.

Таблиця 9.

Зміна СНЧ при першому розмитті оригінального ЦЗ

Кут розмиття	Для трьох найменших СНЧ	Для чотирьох найменших СНЧ	Для п’яти найменших СНЧ	Для шести найменших СНЧ
0°	6,04053	4,45909	4,12397	4,06317
10°	5,07240	3,84393	3,57696	3,61012
20°	3,71371	3,11919	3,06719	3,18236
30°	3,11153	2,72332	2,78027	2,97580
40°	2,79765	2,57166	2,65954	2,88801
50°	2,76453	2,54792	2,65272	2,89159
60°	2,98194	2,60114	2,67007	2,91890
70°	3,45075	2,83305	2,83051	3,08270
80°	4,70739	3,42173	3,16499	3,33101
90°	6,50217	4,14563	3,61760	3,56480

В результаті перевірки зроблено висновок, що при розмитті під будь-яким кутом середні значення коефіцієнтів швидкості росту сингулярних чисел оригінального зображення зменшуються більш ніж у 2 рази.

У таблиці 10 наведено, у скільки разів при повторному розмитті під усіма кутами зменшуються середні значення коефіцієнтів швидкості росту СНЧ попередньо розмитого ЦЗ під кутом 0°.

Таблиця 10.

Результат перевірки зменшення СНЧ при повторному розмитті

Кут розмиття	Для трьох найменших СНЧ	Для чотирьох найменших СНЧ	Для п’яти найменших СНЧ	Для шести найменших СНЧ
0^o	1,75200	1,41451	1,24876	1,18078
10^o	1,75719	1,43252	1,27116	1,19764
20^o	1,76199	1,43762	1,29177	1,21337
30^o	1,76525	1,48178	1,33080	1,23575
40^o	1,83247	1,54906	1,38377	1,26618
50^o	1,84373	1,57676	1,41566	1,28615
60^o	1,93130	1,61706	1,44255	1,29563
70^o	2,04442	1,67395	1,45522	1,29821
80^o	2,19569	1,74285	1,51545	1,33069
90^o	2,38344	1,81017	1,53413	1,33157

Як можна побачити у таблиці 10, найменше змінилися СНЧ цифрового зображення після повторного розмиття під кутом 0^o, а саме від 1,18 до 1,75 разів, що менше за 2. Аналогічних результатів досягнуто й при перевірці інших ЦЗ, які попередньо було розмито під іншими кутами.

Отже, для виявлення штучного ефекту руху необхідно розмити ЦЗ під тим кутом, який було використано при обробці. Для визначення кута будемо використовувати експертне розмиття під різними кутами (у роботі використано кути розмиття з множини $\{0^o; 10, \ldots, 90^o\}$). Далі знайдемо мінімум від ділення середнього значення коефіцієнту швидкості росту СНЧ цифрового зображення до та після експертного розмиття. Якщо це значення буде меншим за 2, то можна зробити висновок, що початкове ЦЗ було розмите до перевірки.

При дослідженні ефективності алгоритму виявлення розмиття у русі було проведено обчислювальний експеримент з використанням 600 цифрових зображень, що були отримані сучасними цифровими фотокамерами. Використовувались зображення як у форматі без втрат, так і з втратами, після розмиття усі ЦЗ було збережено у форматі без втрат. Оцінку ефективності розробленого алгоритму виконано у термінах помилок першого і другого роду, де пропуск небезпечної ситуації є помилкою першого роду, хибна тривога – помилка другого роду. На початковому етапі для досліджень обрано від трьох до шести найменших сингулярних чисел. Це зумовлено тим, що є необхідність у встановленні кількості найменших СНЧ, при роботі з якими алгоритм буде найефективнішим.

Перевірку було проведено для червоної колірної компоненти цифрових зображень. Результати підрахунку ефективності роботи алгоритму за обраних умов надано у таблиці 11.

Таблиця 11.

Ефективність роботи алгоритму за червоним колірним каналом для різної кількості найменших СНЧ

Кількість СНЧ	Помилки першого роду	Помилки другого роду
3	4%	14%
4	2.8%	9%
5	1.4%	6%
6	1%	2%

Як бачимо, найефективнішим є використання 6 найменших СНЧ, тому для подальших досліджень було використано саме таку кількість.

Далі усі ЦЗ було перевірено за трьома колірними компонентами та підраховано кількість помилок. У таблиці 12 надано результати проведеного дослідження.

Таблиця 12.

Ефективність роботи алгоритму для шести найменших СНЧ за різними колірними каналами

Колірний канал ЦЗ	Помилки першого роду	Помилки другого роду
R	1%	2%
G	1.2%	4%
B	1.4%	4%

Для кінцевого алгоритму було вирішено обрати лише одну колірну компоненту ЦЗ, адже перевірка за усіма каналами подовжить час роботи алгоритму та не поліпшить значення помилок першого та другого роду.

З таблиці 12 бачимо, що для виявлення розмиття у русі краще використовувати червоний колірний канал ЦЗ.

Також проведено експеримент на встановлення кута розмиття цифрового зображення. Результат оцінки помилки при встановленні кута розмиття для кожної колірної компоненти наведено у таблиці 13.

Таблиця 13.

Оцінка помилки встановлення кута розмиття

Колірний канал ЦЗ	Неправильне встановлення кута, %
R	7,68%
G	6,48%
B	6,9%

Аналізуючи значення таблиці 13, було зроблено висновок, що найефективнішим у визначенні кута розмиття алгоритм виявився при роботі із зеленим каналом ЦЗ. Для червоного каналу ЦЗ кількість неправильно встановлених кутів розмиття виявилася найбільшою. Проте пріоритетним все ж є встановлення самого факту розмиття.

Підсумовуючи усе, для кінцевого алгоритму було обрано шість найменших сингулярних чисел та червону колірну компоненту цифрового зображення. Кроки кінцевого алгоритму наведено нижче.

Нехай $I - N \times M$ – матриця цифрового зображення, обраного для перевірки.

Крок 1. Виділити із матриці I підматрицю C довільного $k \times l$-розміру за червоним колірним каналом.

Крок 2. Розбити матрицю C стандартним чином на блоки 8×8:

$$C_{ij},\ i = 1,2,...,\left[k/8\right],\ j = 1,2,...,\left[l/8\right],$$

де $\left[.\right]$ – ціла частина аргумету.

Крок 3. Скласти матрицю сингулярних чисел: побудувати сингулярне розкладання для кожного блоку C_{ij}:

$$C_{ij} = U_{ij}\Sigma_{ij}V_{ij}^{T},$$

де U_{ij}, V_{ij} – ортогональні матриці лівих та правих сингулярних векторів C_{ij} відповідно розміром 8×8; $\sum_{ij} = diag(\sigma_1,...,\sigma_8)$ – матриця сингулярних чисел $\sigma_1 \geq ... \geq \sigma_8 \geq 0$.

Крок 4. Для $\sigma_k, k = 3,..,8$ блоків C_{ij} побудувати лінійну апроксимуючу функцію:

$$y = ax + b\,.$$

Крок 5. Побудувати матрицю швидкості росту W, елементи якої $W_{ij} = a$.

Крок 6. Побудувати вектори середніх значень VMV_c для W та знайти їхнє середнє значення $avgC$.

Крок 7. Провести експертні розмиття матриці C під кутами $angle$, які належать множині {0°, 10°, …, 90°}. В результаті чого буде отримано 10 матриць.

Крок 8. Нехай R_{angle}, $angle \in \{0°, 10°, …, 90°\}$ – матриці отримані на кроці 7. Виконати для цих матриць кроки 2-6, результатом чого будуть середні значення $avgR_{angle}$.

Крок 9. Знайти найменше значення відношення $avgC / avgR_{angle}$ та виконати порівняння:

якщо $\min\limits_{angle[0°;90°]} \dfrac{avgC}{avgR_{angle}} < 2$, то зображення розмите;

інакше – розмиття не виявлено.

Висновки

У даній статті проведено аналіз поведінки сингулярних чисел цифрового зображення при розмитті фільтром «Motion blur» у графічному редакторі Adobe Photoshop. В ході обчислювального експерименту встановлено, що при повторному розмитті ЦЗ швидкість росту сингулярних чисел його матриці зменшується менш ніж у 2 рази за умови того, що повторне розмиття проводиться під тим самим кутом, що і первинне. На основі проведених досліджень розроблено алгоритм виявлення розмиття зображення фільтром «Motion blur».

Аналіз ефективності алгоритму показав, що кількість помилок 1 роду складає 1%, кількість помилок 2 роду – 2%.

Предметом подальшого розвитку розробленого алгоритму є проведення робіт для вдосконалення точності відділення оригінальних зображень від фальсифікованих, а також розширення спектру досліджуваних кутів розмиття.

Список літератури

1. Зорило В.В. Метод выявления результатов размытия цифрового изображения / В.В. Зорило, А.А. Кобозева // Сучасна спеціальна техніка. – 2010. – №3(22). – С.72-82.
2. Кобозева, А.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. В. Даля. – 2008. – №8(126), Ч.1. – С. 62-72.
3. Кольцов, П.П. Оценка размытия изображения / П.П. Кольцов // Компьютерная оптика. – 2011. – Т.35, №1. – С. 95–102.
4. Бобок, И.И. Адаптация стеганоаналитического метода, основанного на теории возмущений, для задачи выявления нарушения целостности цифрового изображения / И.И. Бобок, Е.В. Малахов // Інформатика та математичні методи в моделюванні. – 2012. – Том 2, №4. – С. 297–303.

АЛГОРИТМ ОБНАРУЖЕНИЯ ОБРАБОТКИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ФИЛЬТРОМ «MOTION BLUR»

В.В. Зорило, А.А. Карпова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vikazorilo@gmail.com,
kaaarpova@gmail.com

Цифровые изображения играют большую роль в жизни современных людей, ведь постоянно используются в повседневной деятельности, а также в средствах массовой информации, юриспруденции, политике, искусстве, медицине, науке. Простота и доступность программного обеспечения для изменения цифровых изображений является одной из главных причин возникновения большого количества фальсифицированных фото. Существующие методы выявления нарушений целостности цифровых изображений не являются универсальными. Поэтому поиск новых решений этой проблемы является актуальным. Как показывает практика и факты, известные из открытых источников, размытие является одним из программных инструментов, который часто используют для обработки цифрового изображения. Для рассмотрения в данной работе выбрано размытие при создании эффекта движения фильтром графического редактора Adobe Photoshop «Motion blur». В открытой печати не найдено алгоритмов, которые выявляют размытие данного вида. Целью данной работы является выявление размытия цифрового изображения фильтром «Motion blur» путём разработки алгоритма, основанного на анализе сингулярных чисел блоков матрицы цифрового изображения. В работе проведен обзор существующих методов обнаружения размытия изображения; выявлены характерные особенности матрицы цифрового изображения, которые позволят установить наличие размытия указанным фильтром. Разработан алгоритм, который основан на анализе шести наименьших сингулярных чисел блоков матрицы цифрового изображения по красному цветовому каналу. Количество сингулярных чисел для проверки и выбор цветового канала цифрового изображения обосновано вычислительным экспериментом с использованием 600 изображений. Количество ошибок 1 рода разработанного алгоритма составляет 1%, количество ошибок 2 рода - 2%. С помощью разработанного алгоритма также при необходимости можно установить угол размытия с вероятностью ошибки 7,68%. Дальнейшее направление исследований нацелено на совершенствование обнаружения обработки цифрового изображения различными фильтрами современных графических редакторов.

Ключевые слова: выявление размытия изображения, цифровое изображение, эффект движения, нарушение целостности, сингулярные числа, коэффициент скорости роста.

ALGORITHM OF DETECTION OF DIGITAL IMAGE PROCESSING BY MOTION BLUR FILTER

V.V. Zorilo, A.A. Karpova

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: vikazorilo@gmail.com,
kaaarpova@gmail.com

Digital images play a big role in the lives of modern people, because they are constantly used in daily activities, as well as in mass media, jurisprudence, politics, art, medicine, science. Simplicity and accessibility of software for changing digital images is one of the main reasons for the appearance of a large number of falsified photos. Existing methods for detecting violations of the integrity of digital images are not universal. Therefore, the search for new solutions to this problem is urgent. As practice and facts from open source sources show, blur is one of the software tools that are often used to handle a digital image. For consideration in this work blur was chosen when creating the motion effect by the filter of the Adobe Photoshop graphic editor "Motion blur". In an open print, no algorithms are found that will detect blurring of this kind. The purpose of this work is to detect the blurring of the digital image with the Motion Blur filter by developing an algorithm based on the analysis of the singular numbers of the blocks of the digital image matrix. A review of existing methods for detecting blurred images is presented in the work; characteristic features of a digital image matrix are revealed which will allow to establish the presence of blur with the specified filter. The algorithm is developed, which is based on the analysis of the six smallest singular numbers of blocks of the matrix of a digital image on a red color channel. The number of singular numbers for verification and the choice of the color channel of a digital image is based on a computational experiment using 600 images. The number of errors of the first kind of the developed algorithm is 1%, the number of errors of the 2nd kind - 2%. With the help of the developed algorithm, you can also set the blur angle with a probability of error of 7.68%, if necessary. The further direction of research is aimed at improving the detection of digital image processing by various filters of modern graphic editors.

Keywords: detection of image blur, digital image, motion effect, violation of integrity, singular numbers, coefficient of growth rate.

УДК 004.051

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 59-68

РОЗРОБКА АЛГОРИТМУ ПОШУКУ ТА ВІДСТЕЖЕННЯ ОБ'ЄКТІВ НА ВІДЕО

О.Ю. Лебедєва, Т.О. Бирченко, В.М. Лебіга

Одеський національний політехнічний університет,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@opu.ua, tane4ka2404@gmail.com

Сьогодні відеоспостереження – це найбільш затребувана система для охоронних та моніторингових цілей. Розвиток систем відеоспостереження відкриває нові можливості не тільки для фіксації правопорушень, а й для їх попередження. Щодо відстеження об'єктів на відео, можна зазначити, що така необхідність виникає у багатьох сферах життя, наприклад, у системах безпеки, при створенні систем автоматизованого аналізу спортивних змагань, в системах контролю якості процесів, при створенні людино-машинного інтерфейсу. Край важливо, щоб користувачі системи відеоспостереження не тільки могли використовувати систему, зберігати та обробляти дані, а також отримувати необхідну інформацію про той чи інший об'єкт, який відображений на відео за допомогою такого інструменту, як відстеження об'єктів. У роботі розглядається розроблений алгоритм пошуку та відстеження об'єктів на відео. Розроблений алгоритм складається з двох етапів: пошук, або виявлення об'єктів, та відстеження об'єктів на відео. Розглянуто метрики, які буде використано для оцінки подібності двох блоків в кадрі. Більшість метрик якості відеозображень засновано на метриках якості статичних зображень, і тому відеозображення порівнюють покадрово. У зв'язку з цим метрики застосовні тільки для порівняння відеозображень, що мають однакову кількість пікселів. В роботі проведено аналіз існуючих методів виявлення об'єктів, а саме облич людини. Обрано метод Віоли-Джонса, який дозволяє виявляти об'єкти на відео. Цей метод складається з декількох кроків, одним з котрих є використання ознак Хаара, за допомогою яких відбувається пошук потрібного об'єкта. В роботі розглядались як стандартні так і додаткові ознаки Хаара. Було програмно реалізовано метод Віоли-Джонса та проведено експеримент. Розглянуто метрики, які буде використано для оцінки подібності двох блоків в кадрі.

Ключові слова: відеоспостереження, метод Віоли-Джонса, ознаки Хаара, відстеження об'єктів, метрика.

Вступ

На сьогодні відеоспостереження відіграє важливу роль чи не в усіх галузях діяльності суспільства та стає невід'ємною та незамінною частиною комплексної системи безпеки об'єкту, оскільки сучасні системи відеоспостереження дозволяють не тільки спостерігати і записувати відео, але і програмувати реакцію всієї системи безпеки при виникненні тривожних подій або ситуацій. Сучасний етап розвитку систем охоронного телебачення характеризується зростанням обсягу реєстрування відеоінформації та швидкості її обробки в аналогових і цифрових формах. Це висуває підвищені вимоги до якості представлення, передачі по системам зв'язку, зберігання і відновлення зображень об'єктів спостереження. При цьому виявлення та відстеження об'єктів стає все більш актуальною і важливою задачею особливо для вирішення завдань моніторингу – виявлення осіб, номерних знаків автотранспорту, спостереження за об'єктами, виявлення появи нових і зникнення встановлених об'єктів на територіях, що охороняються, та інше. Тому існує потреба в розробці надійного і невибагливого до обчислювальних ресурсів алгоритму для можливості пошуку осіб на відео та їх відстеження, що робить дану роботу актуальною в житті суспільства.

Мета роботи

Метою даної роботи є створення програмного продукту для системи відеоспостереження шляхом розробки алгоритму пошуку та відстеження об’єктів на відео.

Для досягнення мети в роботі були вирішені наступні *задачі*:

- аналіз існуючих методів виявлення об’єктів;
- аналіз метрик для оцінки схожості двох блоків зображення;
- розробка алгоритму пошуку та відстеження об’єктів на відео.

Основна частина

В реальному світі існує величезна кількість різних об'єктів, але значний інтерес представляє розробка алгоритмів виявлення більш вузького класу об'єктів – облич людини.

Виявлення осіб – це визначення кількості облич, присутніх на зображенні, і виявлення їх положення. Загалом, процес виявлення осіб складається з двох етапів, на першому з яких зображення сканується цілком для виявлення області (функцій), які можуть бути ідентифіковані як обличчя; найбільш поширеною ознакою є колір шкіри. Далі йде локалізація, яка дає більш точну оцінку розмірів і положення облич.

Існують чотири технології локалізації обличчя людини [1]:

- детектування особи на зображеннях з контрольованим фоном;
- детектування особи за кольором;
- детектування особи за методом Віоли-Джонса;
- детектування особи з використанням нейронних мереж.

Детектування особи на зображеннях з контрольованим фоном ґрунтується на локалізації особи на монохромному фоні, де особу знято фронтально. Видаляючи однорідний фон, виділити контур особи не становить жодних проблем. Один з головних плюсів цієї технології – даний алгоритм є найпростішим з існуючих. Великий мінус даного методу – фон повинен бути монохромним.

Детектування особи за кольором визначає обличчя за кольором шкіри в певній колірній моделі. Скануючи картинку і визначаючи зони, типові для кольору шкіри людини, шукає характерні ключові точки. Мінус цієї технології в залежності від умов освітлення, що може спотворити результати. Головний плюс в тому, що вона широко поширена і досить проста.

Третя технологія добре розпізнає риси обличчя під невеликим кутом. Метод Віоли-Джонса використовує прямокутні ознаки, вони називаються хаароподібними вейвлетами, інакше ознаками Хаара.

Детектування особи з використанням нейронних мереж використовує каскадну архітектуру, побудовану на загортальній нейронній мережі. Дана технологія працює з різними масштабами, але її мінус в значних вимогах до обчислювальних потужностей, крім цього, навчання доведеться проводити для кожної моделі.

Метод Віоли-Джонса є одним з кращих по співвідношенню показників «ефективність розпізнавання» / «швидкість роботи». Він складається з таких основних етапів:

- обчислення інтегрального перетворення;
- використання ознак Хаара;
- використання бустінга (Ada Boost);
- використання каскади ознак.

Інтегральне перетворення зображення – це матриця, що збігається за розмірами з вихідним зображенням [2]. У кожному її елементі зберігається сума інтенсивностей

усіх пікселів, що знаходяться лівіше і вище даного елемента. Інтегральне уявлення дозволяє швидко розраховувати сумарну яскравість довільного прямокутника на даному зображенні.

На етапі виявлення в методі Віоли-Джонса вікно встановленого розміру рухається по зображенню, і для кожної області зображення, над якою проходить вікно, розраховується ознака Хаара (рис. 1) [2].

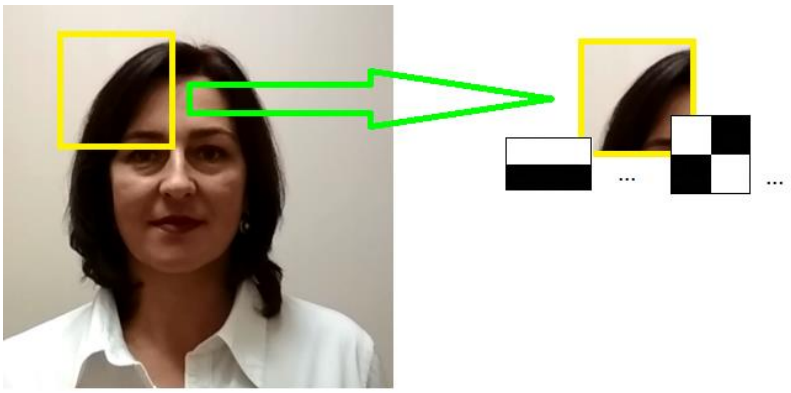


Рис. 1. Принцип скануючого вікна

Наявність або відсутність предмета в вікні визначається різницею між значенням ознаки і порогом. Оскільки ознаки Хаара мало підходять для навчання або класифікації, для опису об'єкта з достатньою точністю необхідна більша кількість ознак. Тому в методі Віоли-Джонса ознаки Хаара організовані в каскадний класифікатор.

У стандартному методі Віоли - Джонса використовуються прямокутні ознаки, вони називаються примітивами Хаара (рис. 2). Обчислення ознак Хаара є одним з основних алгоритмів, без якого немає можливості проводити подальші етапи алгоритму Віоли-Джонса.

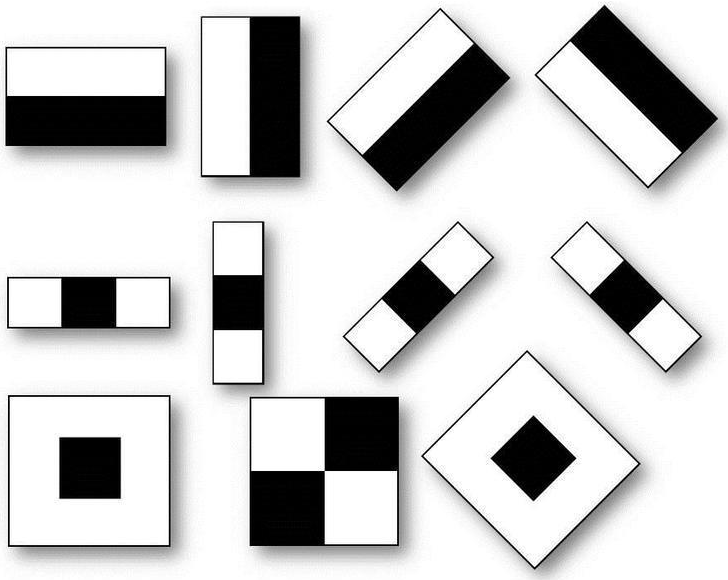


Рис. 2. Стандартні ознаки Хаара

Обчислювані значення ознаки буде значення $F = A - B$, де A – сума яскравостей точок, що закриваються світлою частиною ознаки, а B – сума яскравостей точок, що закриваються темною частиною. Для їх обчислення використовується поняття інтегрального перетворення.

У розширеному методі Віоли-Джонса використовуються додаткові ознаки (рис. 3) [2].

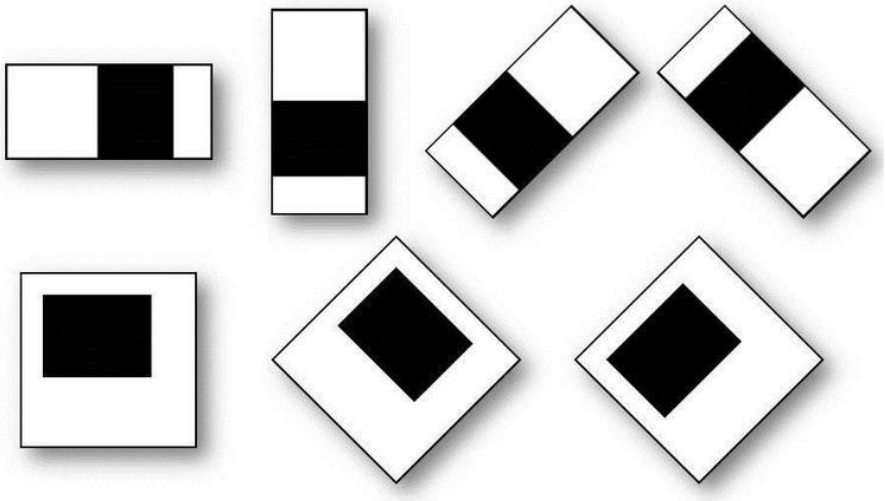


Рис. 3. Додаткові ознаки Хаара

Бустінг – комплекс методів, що сприяють підвищенню точності аналітичних моделей. Бустінг є жадібним алгоритмом побудови композиції алгоритмів (greedy algorithm) – це алгоритм, який на кожному кроці робить локально найкращий вибір в надії, що підсумкове рішення буде оптимальним [2].

Розвитком даного підходу є розробка більш досконалого сімейства алгоритмів бустінга AdaBoost (adaptive boosting – адаптоване поліпшення), запропонована Йоав Фройнд (Freund) і Робертом Шапіро (Schapire) в 1999 році [3], яка може використовувати довільне число класифікаторів і виробляти навчання на одному наборі прикладів, по черзі застосовуючи їх на різних етапах.

Дерево прийняття рішень – це дерево, в листі якого стоять значення цільової функції, а в інших вузлах – умови переходу, що визначають, по якому з ребер йти. Каскадна модель сильних класифікаторів – це, по суті, дерево прийняття рішень, де кожен вузол дерева побудований таким чином, щоб детектувати всі образи, що цікавлять, і відхиляти області, які не є образами. Крім цього, вузли дерева розміщені таким чином, що чим ближче вузол знаходиться до кореня дерева, тим з меншої кількості примітивів він складається і тим самим вимагає меншого часу на прийняття рішення. Даний вид каскадної моделі добре підходить для обробки зображень, на яких загальна кількість детектованих образів мала [2].

Програмно реалізовно алгоритм методу Віоли-Джонса з стандартними та додатковими ознаками Хаара. Було проведено експеримент для виявлення облич на зображеннях, які містять в собі:

- обличчя людей різного віку;
- різного кольору шкіри;
- наявності волосся, бороди, татуювань, веснянок, окулярів, макіяжу;
- зображення з різною яскравістю;
- наявністю різних емоцій на обличчі;
- кадри з кіно в градаціях сірого;
- обличчя з картин;
- наявністю декількох облич на зображенні.

Як можна побачити з результатів, метод добре відпрацював як на чітких так і на розмитих зображеннях. Метод спрацював позитивно, незалежно від типу окулярів, виявив обличчя на фото, не зважаючи на стать, вік, колір обличчя, волосся, емоції.

Також експеримент виявив зображення, де є обличчя людини, але метод їх не знаходить. До них відносяться обличчя людей, які не присутні повністю. Також є зображення, де метод знаходить та виділяє квадратом область, де нема обличчя людини. Деякі результати роботи методу Віоли-Джонса продемонстровані на рисунку 4.

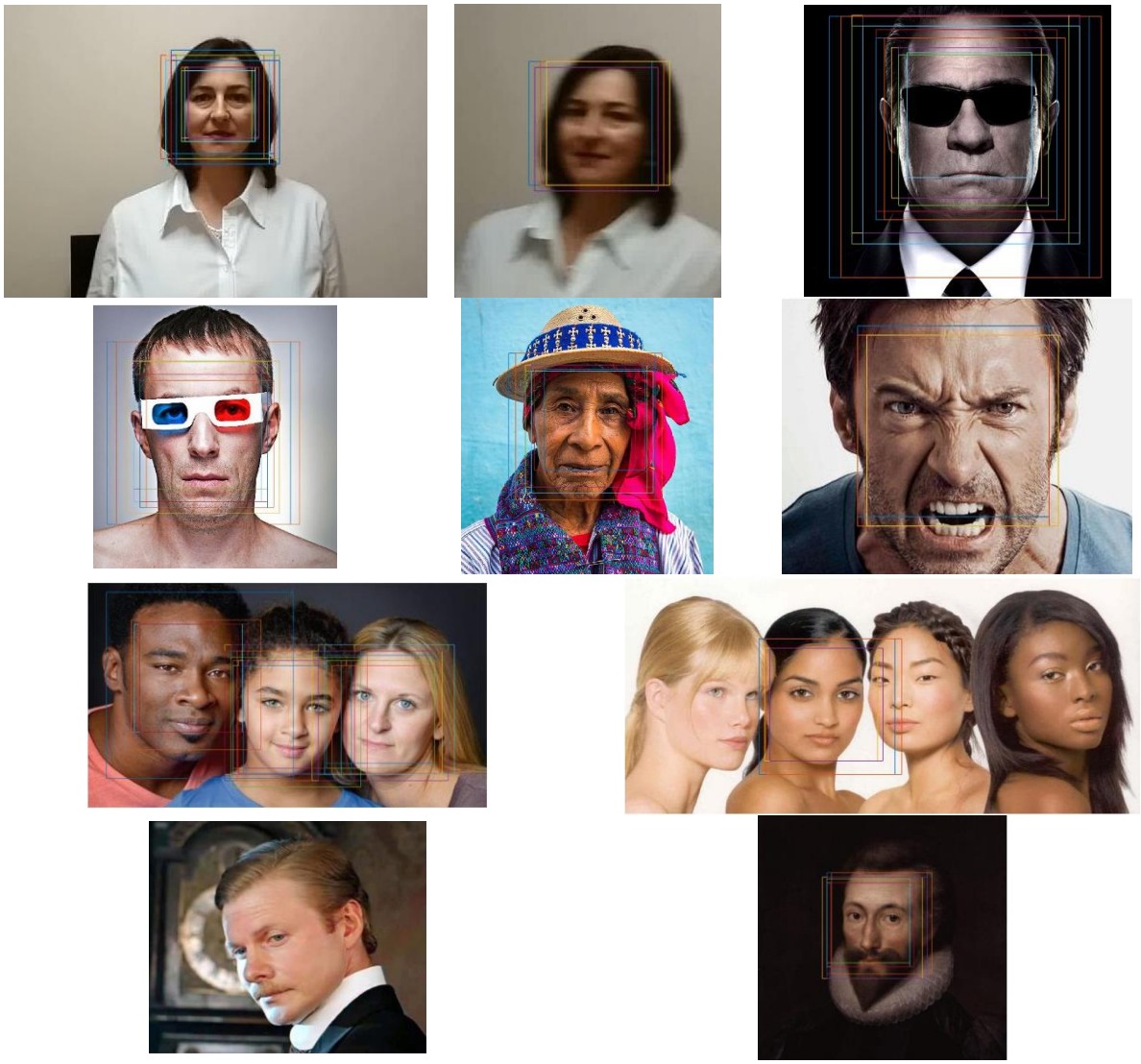


Рис. 4. Результати роботи методу Віоли-Джонса

Відеофайл – це набір стаціонарних картинок, які змінюють одна одну з певною частотою.

Алгоритми відстеження об’єктів на відео розділені на чотири основні категорії: відстеження областей, відстеження по активному контуру, відстеження за характерними признаками, відстеження по моделі [4].

Алгоритми відстеження областей застосовуються для відстеження об'єктів в відповідно до змін областей зображення, відповідних рухомих об'єктів.

Алгоритми відстеження по активному контуру відстежують об'єкти шляхом подання їх обрисів у вигляді обмежуючих контурів і динамічного оновлення цих контурів на наступних кадрах. Ці алгоритми мають своєю метою пряме вилучення форми об'єктів і дають більш повний опис об'єктів в порівнянні з алгоритмами відстеження областей.

Алгоритми відстеження за характерними ознаками виконують розпізнавання і відстеження об'єктів шляхом вилучення елементів зображення, їх об'єднання в

характерні ознаки більш високого рівня і наступного порівняння з характерними ознаками інших зображень.

Алгоритм, що розробляється відноситься до категорії відстеження областей.

Розроблений алгоритм пошуку та відстеження об'єктів на відео складається з двох глобальних кроків:

- пошук об'єкту на якомусь кадрі на відео;
- відстеження знайденого об'єкту на наступних кадрах на відео.

Пошук об'єкту відбувається за допомогою методу Віоли-Джонса. В результаті цього етапу маємо блок для пошуку на наступних кадрах на відео.

Ідея порівняння обраного блоку на кадрі з блоками на наступному кадрі випливає з того, що об'єкт, який рухається на сусідніх кадрах, не рухається з великою відстанню. Тобто, практично у всіх випадках об'єкт буде переміщуватися на декілька пікселів.

Отже, маємо відео V, яке складається з кадрів $F_1, F_2, ..., F_t$. Нехай F_i – це i-ий – кадр, цифрового зображення розміром $n \times m$.

Основні кроки методу відстеження об'єкту.

Крок 1. На кадрі F_1 виділяється блок p_1, який відстежується. Нехай (x_1, y_1) – координати лівої верхньої вершини блоку та $k \times l$ – розмір блоку; f – зміщення для пошуку; δ – порогове значення коефіцієнту метрики подібності.

Крок 2. Для кожної пари кадрів F_i та F_{i+1}:

Розбити кадр F_{i+1} на множину пересічних $k \times l$ – блоків, починаючи з координати $(x_i - f, y_i - f)$ до координати $(x_i + f, y_i + f)$: $C = \{c_1, ..., c_s\}$. Нехай p_i – блок за координатами (x_i, y_i) та розміром $k \times l$ з кадру F_i.

Для кожної пари блоків p_i та c_j обчислити коефіцієнт метрики між ними. Нехай cor_j – значення коефіцієнту метрики подібності.

Знайти максимальне значення $cor^j_{\max}$ серед cor_j. Нехай (x_j, y_j) – координати лівої верхньої вершини блоку з максимальним значенням коефіцієнту метрики подібності.

Якщо $cor^j_{\max} \geq \delta$, то для блоку p_j за координатами (x_j, y_j) накладається рамка навколо блоку, інакше рамка не додається та $f = 2f$; блок, який відстежується, та його координати не змінюються.

Експерименти показали, що об'єкт, який відстежується, може наближатися або віддалятися від камери, тим самим змінюється його розмір.

Модифікуємо цей алгоритм для використання блоків з різним масштабом. Маємо наступні основні кроки алгоритму:

Крок 1. На кадрі F_i виділяється блок p_1, який відстежується. Нехай (x_j, y_j) – координати лівої верхньої вершини блоку та $k \times l$ – розмір блоку; f – зміщення для пошуку; δ – порогове значення коефіцієнту метрики; *scale* – масштаб в пікселях для збільшення та зменшення блоку.

Крок 2. Для кожної пари кадрів F_i та F_{i+1}:

Розбити кадр F_{i+1} на множину пересічних $k \times l$ – блоків, починаючи с координати $(x_i - f, y_i - f)$ до координати $(x_i + f, y_i + f)$: $C = \{c_1, ..., c_r\}$. Нехай p_i – блок за координатами (x_i, y_i) та розміром $k \times l$ з кадру F_i; p_i^{+scale} та p_i^{-scale} – збільшений та зменшений блок за координатами (x_i, y_i) та розміром $(k + scale) \times (l + scale)$ та $(k - scale) \times (l - scale)$ з кадру F_i.

Для кожної пари блоків p_i, p_i^{+scale}, p_i^{-scale} та c_j, c_j^{+scale}, c_j^{-scale} обчислити коефіцієнт метрики між двома блоками парами відповідних блоків. Нехай cor_j, cor_j^{+scale}, cor_j^{-scale} – значення коефіцієнту метрики подібності відповідних блоків.

Знайти максимальне значення $cor_{\max}^j$ серед cor_j, cor_j^{+scale}, cor_j^{-scale}. Нехай (x_i, y_i) – координати лівої верхньої вершини блоку з максимальним значенням коефіцієнту метрики. Нехай $(k_{\max})\times(l_{\max})$ – розміри блоку з максимальним значенням коефіцієнту метрики подібності.

Якщо $cor_{\max}^j \geq \delta$, то для блоку p_j за координатами (x_j, y_j) та розміром $(k_{\max})\times(l_{\max})$, який стає поточним розміром блоку пошуку, накладається рамка навколо блоку, інакше рамка не додається, збільшується зміщення для пошуку: $f = 2f$; блок, який відстежується, його координати та розмір не змінюються.

Збільшення області пошуку залежить від того, що об'єкти в кадрі можуть переміщатися по-різному: їх траєкторії можуть перетинатися, вони можуть зникати і з'являтися знову (наприклад, якщо камера стежить за автомагістраллю, то автомобіль в кадрі може перекриватися іншим, а потім знову виїжджати), кілька об'єктів можуть об'єднуватися або різко міняти напрям руху. Тому в даному алгоритмі враховується такий випадок.

Результати роботи алгоритма пошуку та відстеження об'єктів на відео наведено на рисунку 5 у вигляді випадково вибраних кадрів з відео.

Рис. 5. Результати роботи алгоритм пошуку та відстеження об'єктів на відео

В якості метрики в розробленому алгоритмі, що розробляється можна використовувати наступні:

- евклідова відстань;
- кореляція;
- MSE.

Для двох блоків X та Y розміром $M \times N$ пікселів значення метрики MSE задається формулою:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[X(m,n)-Y(m,n)]^2,$$

де $X(i, j)$ та $Y(i, j)$ – це значення компоненти яскравості пікселя (i, j) блока X та Y відповідно.

Коефіцієнт кореляції задається формулою:

$$cor = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{\left[\sum x^2 - \frac{\left(\sum x\right)^2}{n}\right] \times \left[\sum y^2 - \frac{\left(\sum y\right)^2}{n}\right]}}$$

Було проведено експеримент для визначення того, яка з метрик, що розглядається найбільш підходить для розробленого алгоритму. Оцінювався час роботи програми з метриками, що розглядаються, для 20 кадрів різних відеофайлів. Результати дослідження наведено в таблиці 1.

Таблиця 1.

Час роботи програми з певними метриками

Відеофайл	Кореляція (год./хв./с./мс.)	MSE (год./хв./с./мс.)	Евклідова відстань (год./хв./с./мс.)
1	00:00:05:38	00:00:05:32	00:00:05:18
2	00:00:04:51	00:00:04:69	00:00:04:59
3	00:00:04:74	00:00:04:87	00:00:04:77
4	00:00:04:51	00:00:04:75	00:00:04:69
5	00:00:05:37	00:00:05:91	00:00:05:80

Для таблиці було обрано п’ять відеофайлів з множини відео, над якими було проведено дослідження. Для коефіцієнта кореляції було обрано значення від 0,85 до 0,9, бо якщо коефіцієнт кореляції наближається до одиниці, це означає що блоки ідентичні. Експериментальним шляхом для коефіцієнта MSE було обрано значення 3000, а для евклідової відстані – 2000.

По даним таблиці зрозуміло, що вибір метрики незначно впливає на час роботи програми, але обирати коефіцієнт метрики MSE та евклідової відстані для оцінки подібності блоків значно складніше, ніж обрати коефіцієнт метрики кореляції. Тому висновком можна зазначити, що метрика кореляції краща і простіша в використанні користувачем даного програмного продукту.

Висновки

Було проведено аналіз існуючих методів виявлення об’єктів. Для розробки алгоритму пошуку та відстеження об’єктів на відео на першому кроку використовується метод Віоли-Джонса виявлення облич на відео. Було розроблено алгоритм пошуку та відстеження об’єктів на відео. Було проведено аналіз метрик для оцінки схожості двох блоків зображення. У якості метрики для алгоритм пошуку та відстеження об’єктів на відео рекомендується використовувати коефіцієнт кореляції.

Література

1. Тынченко, С.В. Сравнение алгоритмов обнаружения и локализации лица на изображении / С.В. Тынченко, В.О. Путилин, А.К. Овсянников // Проблемы Науки. – 2018. – №3. – 123 с.

2. Метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц [Електроний ресурс] // Режим доступу: https://habr.com/ru/post/133826/.
3. Freund, Y A Short Introduction to Boosting / Y. Freund, R.E. Schapire // Shannon Laboratory, USA, – 1999. – 771 – 780 p.
4. Лавелина, Е.С. Отслеживание объектов в видеопотоке / Е.С. Лавелина, М.Р. Закуанова, М.А. Масловская // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. LIV междунар. студ. науч.-практ. конф, 2017. – № 6(53).

РАЗРАБОТКА АЛГОРИТМА ПОИСКА И ОТСЛЕЖИВАНИЯ ОБЪЕКТОВ НА ВИДЕО

Е.Ю. Лебедева, Т.А. Бырченко, В.М. Лебига

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: o.y.lebedieva@opu.ua,
tane4ka2404@gmail.com

Сегодня видеонаблюдение – это наиболее востребованная система для охранных и мониторинговых целей. Развитие систем видеонаблюдения открывает новые возможности не только для фиксации правонарушений, но и для их предупреждения. По отслеживанию объектов на видео, можно отметить, что такая необходимость возникает во многих сферах жизни, например, в системах безопасности, при создании систем автоматизированного анализа спортивных соревнований, в системах контроля качества процессов, при создании человеко-машинного интерфейса. Край важно чтобы пользователи системы видеонаблюдения не только могли использовать систему, хранить и обрабатывать данные, а также получать необходимую информацию о том или ином объекте, который запечатлен на видео с помощью такого инструмента, как отслеживание объектов. В работе рассматривается разработанный алгоритм поиска и отслеживания объектов на видео. Разработанный алгоритм состоит из следующих этапов: поиск, или обнаружения объектов, и отслеживания объектов на видео. Рассмотрено метрики, которые будут использованы для оценки сходства двух блоков в кадре. Большинство метрик качества видеоизображений основано на метриках качества статических изображений, и поэтому видеоизображения сравнивают покадрово. В связи с этим метрики применимы только для сравнения видеоизображений, имеющих одинаковое количество пикселей. В работе проведен анализ существующих методов обнаружения объектов, а именно лиц человека. Выбран метод Виолы-Джонса, который позволяет обнаруживать объекты на видео. Этот метод состоит из нескольких шагов, одним из которых является использование признаков Хаара, с помощью которых происходит поиск нужного объекта. В работе рассматривались как стандартные, так и дополнительные признаки Хаара. Было программно реализован метод Виолы-Джонса и проведен эксперимент. Рассмотрено метрики, которые будут использованы для оценки сходства двух блоков в кадре.

Ключевые слова: видеонаблюдение, метод Виолы-Джонса, признаки Хаара, отслеживание объектов, метрика.

DEVELOPING THE SEARCH ALGORITHM AND MOVING OBJECTS

O.Y. Lebedieva, T.A. Byrchenko, V.M. Lebiga

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: o.y.lebedieva@opu.ua,
tane4ka2404@gmail.com

Today, video surveillance is the most sought after system for security and monitoring purposes. The development of video surveillance systems opens up new opportunities not only for fixing offenses but also for preventing them. With regard to object tracking on video, it can be noted that this need arises in many areas of life, such as security systems, the creation of systems for the automated analysis of sports competitions, the quality control of processes, the creation of human-machine interface. It is essential that CCTV users not only be able to use the system, store and process data, but also obtain the necessary information about a particular object that is displayed on video using a tool such as object tracking. This paper describes a developed algorithm for searching and tracking objects on video. The algorithm developed consists of the following steps: finding or detecting objects and tracking objects on video. You should also consider the metrics that will be used to evaluate the similarity of the two blocks in the frame. Most video quality metrics are based on still image quality metrics, which is why video images are compared frame by frame. In this regard, the metrics are only applicable to compare videos that have the same number of pixels. The paper analyzes the existing methods of object detection, namely human faces. The Viola-Jones method was chosen to detect objects on video. This method consists of several steps, one of which is to use the Haar traits to find the desired object. Both standard and additional features of Haar were considered in the paper. The Viola-Jones method was programmatically implemented and an experiment was conducted. You should also consider the metrics that will be used to evaluate the similarity of the two blocks in the frame.

Keywords: CCTV, Viola-Jones method, Haar signs, object tracking, metric.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 69-76

МОДИФІКАЦІЯ АЛГОРИТМУ ХЕШ-СТЕГАНОГРАФІЇ

В.В. Зоріло, М.В. Бохонько, А.І. Казаков

Одеський національний політехнічний університет
просп. Шевченко, 1, Одесса, 65044, Україна; e-mail: mishabahus28@gmail.com

Інформація, яка передається каналами зв'язку, піддається різноманітним загрозам, таким, як викриття, спотворення та знищення. Одним із можливих рішень проблеми загрози викриття є використання стеганографічних методів, які, в свою чергу, мають свої обмеження за областю застосування. Стеганографія передбачає вбудовування секретного повідомлення у стеганографічний контейнер (наприклад, цифрове зображення) так, щоб не порушувати стійкість візуального сприйняття контейнера. Одною з основних вимог стеганографічного методу є його стійкість до різноманітних видів атак. Сучасний напрям стеганографії, хеш-стеганографія, базується на обчисленні хеш-коду цифрових зображень та повідомлення, що передається, та подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення. Зазвичай більшість атак на цифрові зображення складають небезпеку переважно для високих частот сигналу, в результаті чого хеш-код цифрового зображення також зазнаватиме змін, що може призвести до часткової або повної втрати стеганографічного повідомлення. Більшість сучасних методів отримання хеш-коду цифрового зображення засновані на використані високих частот, що робить методи хеш-стеганографії вразливими до атак. Метою роботи є підвищення ефективності алгоритму хеш-стеганографії шляхом його модифікації за допомогою перцептивних хеш-алгоритмів. Проведено аналіз існуючих перцептивних хеш-алгоритмів для обчислення хеш-коду зображення. Виконано модифікацію алгоритму хеш-стеганографії. Модифікований алгоритм заснований на використанні перцептивного хеш-алгоритму Simple Hash. Проведено аналіз ефективності модифікованого алгоритму, який показав, що модифікація забезпечує підвищення стійкості стеганоповідомлення до різних атак в порівнянні з оригіналом.

Ключові слова: стеганографія, хеш-стеганографія, перцептивний хеш-алгоритм, вбудовування додаткової інформації.

Вступ

Як відомо, для захисту даних найчастіше використовують криптографію, але наявність зашифрованого повідомлення привертає до себе увагу і створює інтерес до злому переданого повідомлення. Для того, щоб цього уникнути, використовують криптографію спільно зі стеганографією. Стеганографія представляє собою вбудовування секретного повідомлення із подальшим його відновленням у стеганографічний контейнер (наприклад, цифрове зображення) так, щоб не порушувати стійкість візуального сприйняття контейнера. Стеганографія приховує сам факт передачі інформації. Наприклад, передача повідомлення відбувається під виглядом передачі зображення у форматі JPEG. Одною з основних вимог до стеганографічного методу є його стійкість до різноманітних видів атак. Сучасний напрям стеганографії – хеш-стеганографія, базується на обчисленні хеш-коду цифрових зображень та повідомлення, що передається, і в подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення. Зазвичай більшість атак на цифрові зображення складають «небезпеку» переважно для високих частот, в результаті чого хеш-код цифрового зображення також зазнаватиме змін, що може призвести до часткової або повної втрати стеганографічного повідомлення. Більшість сучасних методів отримання

хеш-коду цифрового зображення засновані на використанні високих частот, що робить методи хеш-стеганографії вразливими до атак.

Мета роботи

Метою роботи є підвищення ефективності алгоритму хеш-стеганографії шляхом його модифікації за допомогою перцептивних хеш-алгоритмів.

Основна частина

Нині часто при шифруванні та приховуванні секретних повідомлень стеганографія та криптографія використовуються разом: інформацію, яку передають, шифрують спочатку стійким криптографічним методом; далі отримане повідомлення вбудовують в контейнер (зображення) [1]. Як правило, при цьому в зображені з'являються зміни, непомітні для людського ока. І для шифрування, і для дешифрування використовують секретний ключ, який передають захищеним каналом зв'язку.

Проте, хеш-стеганографія використовує інший принцип. Щоб уникнути зайвої уваги зі сторони зловмисника, не обов'язково вбудовувати повідомлення у зображення, змінюючи його. Головний принцип хеш-стеганографії полягає у тому, що послідовність зображень, що передаються, і є повідомленням [2].

Для того, щоб передати секретне повідомлення, необхідно обчислити його хеш-код і передавати дане повідомлення у вигляді послідовності зображень, хеш-коди яких певним чином частково співпадають з хеш-кодом повідомлення. Розглянемо детальніше основні кроки такого виду шифрування.

Для ефективного шифрування повідомлення для початку необхідно створити велику базу цифрових зображень. Далі за допомогою криптографічної хеш-функції, яка задовольняє властивості рівноймовірності (наприклад, MD5), розраховуємо хеш-код усіх зображень, дані заносимо в таблицю. Припустимо, що необхідно передати повідомлення «morior» в шістнадцятирічному вигляді: 56585B52585B. Тоді основні кроки алгоритму хеш-стеганографічного шифрування будуть наступні. Дане повідомлення розділяємо на біграми: 56 58 5B 52 58 5B. Отримані біграми будемо називати словами (у загальному випадку слова можуть мати більшу довжину). В прикладі, що розглядається, є шість слів. Кожному слову ставиться у відповідність зображення, перші n символів якого співпадають зі словом (n дорівнює довжині слова). В результаті отримаємо послідовність зображень, які представляють собою повідомлення, що передається.

Такий спосіб передачі повідомлень досить простий, але він не є надійним з наступних причин. Якщо при передачі буде проведено атаку на цифрові зображення (які, нагадаємо, в певній послідовності і є повідомленням), то хеш-код зображень буде змінено, і повідомлення буде втрачено.

Для вирішення цієї проблеми в даній роботі запропоновано наступний підхід. Підвищити надійність шифрування та стійкість до атак можна за допомогою використання перцептивного хеш-алгоритму. Особливість усіх перцептивних хеш-алгоритмів полягає у тому, що при різних перетвореннях зображення, наприклад, при зміні розміру, зміні співвідношення сторін, незначних змінах яскравості, контрастності тощо, хеш-код зображення не змінюється. Розглянемо деякі перцептивні хеш-алгоритми.

Ідея перцептивного хеш-алгоритму Simple Hash полягає у відображенні середнього значення низьких частот [3]. У зображеннях високі частоти забезпечують деталізацію, а низькі – показують структуру. Тому для побудови такої хеш-функції, яка

для схожих збережень видаватиме близький хеш-код, доцільно «позбутися» високих частот.

В роботі [4] описано алгоритм Discrete Cosine Transform Based Hash, ідея якого полягає у розрахунку середнього значення за допомогою дискретного косинусного перетворення для невраховування високих частот з сигналу-зображення.

Суть алгоритму Radial Variance Based Hash полягає в побудові променевого вектору дисперсії на основі перетворення Радону [5]. Потім до променевого вектора дисперсії застосовують дискретне косинусне перетворення і обчислюють хеш-код. Перетворення Радону стійке до обробки зображень за допомогою різних маніпуляцій (наприклад, стиснення) і геометричних перетворень (наприклад, поворотів).

Алгоритм MarrHildreth Operator Based Hash також зарекомендував себе як стійкий до атак [6]. Оператор Марра-Хілдрет дозволяє визначати границі на зображенні. Взагалі кажучи, границю на зображенні можна визначити як край або контур, що відокремлює сусідні частини зображення, які мають порівняно відмінні характеристики відповідно до деяких особливостей.

Цими особливостями можуть бути колір або текстура, але частіше за все використовують сіру градацію кольору зображення (яскравість). Результатом визначення меж є карта кордонів. Карта кордонів описує класифікацію меж для кожного пікселя зображення. Якщо границю визначати як різку зміну яскравості, то для їх знаходження можна використовувати похідні або градієнт.

Для досягнення поставленої в роботі мети було обрано перцептивний хеш-алгоритм Simple Hash – він легкий в реалізації та відносно швидкий у роботі. Основні кроки перцептивного алгоритму Simple Hash наведені нижче.

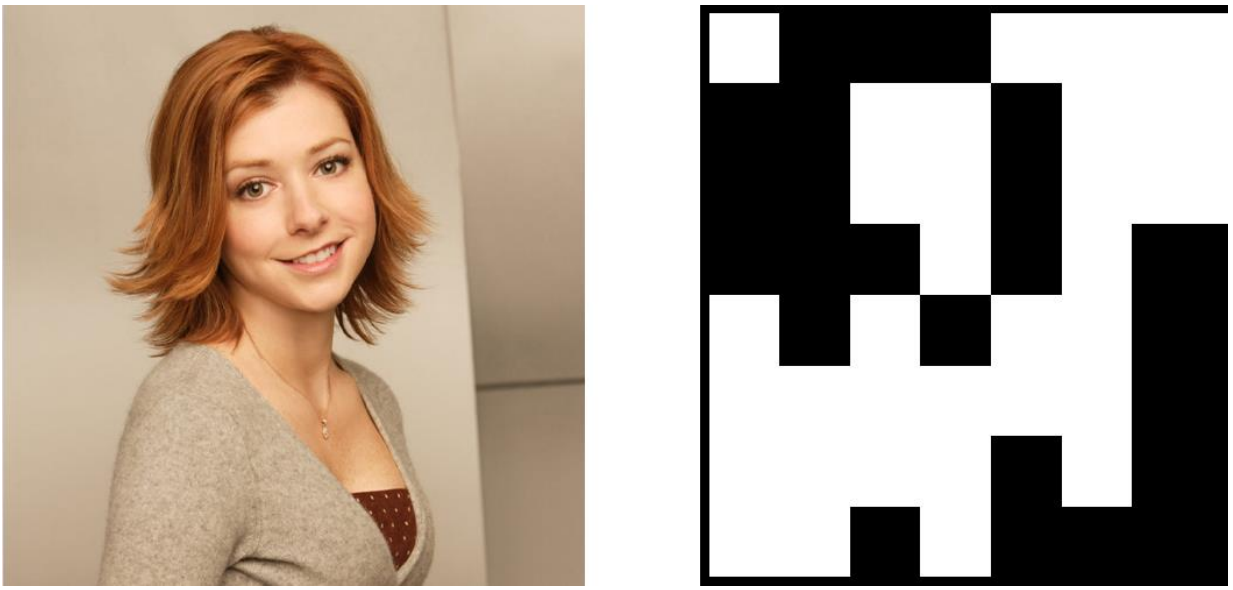
Перший крок – зменшення розміру цифрового зображення шляхом масштабування його до розміру 8×8 пікселів незалежно від початкового розміру. Найшвидший спосіб позбутися від високих частот – зменшити зображення шляхом масштабування. Завдяки цьому ще більше спрощуємо наступні етапи, не втрачаючи занадто багато структурної інформації зображення, а також отримуємо деяку міру інваріантності масштабу. На другому кроці необхідно прибрати колір, тобто перевести вхідне зображення у відтінки сірого (рис. 1).

а б в

Рис. 1. Зменшення розмірів та зміна кольорового режиму зображення: а – оригінальне зображення; б – зменшене зображення; в – зображення у градаціях сірого

Цей крок значно підвищує швидкість роботи алгоритму за рахунок скорочення обсягу інформації, яку потрібно обробляти на більш пізніх етапах. Після цього необхідно знайти середнє значення пікселів. Робимо це шляхом підсумовування всіх значень нашого зображення і ділення результату на 64.

На наступному етапі необхідно побудувати ланцюжок бітів. Для кожного пікселя зображення робиться наступна заміна. Якщо значення пікселю більше середнього, то замість значення кольору ставимо 1. Аналогічно, якщо значення пікселю менше середнього – ставимо 0 (рис. 2).



а б

Рис. 2. Приклад кінцевого результату масштабування та представлення в бінарному вигляді сірого початкового зображення: а – початкове зображення; б – отриманий «відбиток»

Записуємо значення отриманого бітового зображення у певній послідовності, в результаті чого отримаємо значення довжиною 64 біт. Послідовність зчитування не має значення, але зазвичай біти записуються зліва направо, зверху вниз. Після виконання усіх кроків останнім етапом є побудова хеш-коду. За допомогою хеш-функції (наприклад, SHA-3 [7]) розрахуємо хеш-код бітової послідовності, отриманої на попередньому кроці.

Етапи модифікованого алгоритму хеш-стеганографії полягають в наступному.

Для кожного зображення обчислюємо значення хеш-коду за допомогою перцептивного алгоритму Simple Hash (рис. 3). Отримані значення хеш-коду запишемо в текстовий файл, який будемо зберігати для подальшого використання при кожному шифруванні повідомлення.

Кожен окремо взятий символ повідомлення переводимо в систему ASCII і порівнюємо кожну пару значень з першими двома символами хеш-кодів зображень. В результаті отримаємо набір зображень. Виконавши перераховані кроки з усіма символами повідомлення, отримаємо набір зображень (відповідно до кількості символів повідомлення), які слід відправляти одержувачу в певно визначеному порядку, інакше сенс повідомлення загубиться.

Приклад зашифрованого таким чином повідомлення (рис. 4).

Одержувач, отримавши зображення, записує у рядок перші два символи хеш-кодів, в результаті чого отримує ASCII-код. Далі необхідно перевести ASCII-код в текст, який і буде повідомленням.

Описаний спосіб шифрування не позбавлений недоліків, проте має і певні переваги. До недоліків можна віднести наступні фактори. Створення нової або оновлення існуючої бібліотеки зображень займає великий проміжок часу.

Масштабування зображень, перехід до градацій сірого, обчислення середнього арифметичного значення яскравості пікселів у градаціях сірого та побудова бітової

послідовності для зображення – доволі громіздкий процес для середніх обчислювальних машин.

```
e84014ff8666378de4f997e4536950f3
aed21eb87010e8dcd8f77d5ef2b3b64b
388bb38e38db9d3474d076e92154e178
bf0c959a017a46abe942dc47a2f96843
e0a952358b03def495fe558da26f208b
a76b210b02bc63050a0943cd25edc2ed
ec1ad6716c85a93c3164223ba978f2e1
cf097b964ab7ca0b3d48b19f64e1eb94
0f8c3ecb62a71ee6a4f3ac862acb180a
2eb87b2767e836e9792c0dfcac762212
6ebec9533947729d4fd61d8954df2c9c
65d7d095eecca3ab197792c07dbfd481
3198feb4dbd2fa68ae318f9b7df41def
041056ba10bfc48a3119716b1e63417c
d1b3346e2d5cee3df607a6c40fe59c7a
50efb5183b6cfa2c75f63e17a0ac936d
804e46f6d91716e1253e3aa679b0d630
de5e9e8f27e96e8bbd2e1ceed06c29b4
```

Рис. 3. Хеш-коди декількох зображень

Рис. 4. Відібрані зображення, які шифрують повідомлення «Bad company»

Проте, незручності це викликатиме лише при першому запуску самого програмного продукту. Усі наступні звернення до даного методу шифрування проходитимуть значно швидше саме через те, що буде сформовано файл для зберігання отриманих хеш-кодів для усіх зображень, що їх використовують при передачі секретного повідомлення. Другим недоліком є те, що, як було зазначено вище, необхідна велика бібліотека зображень. Для експериментів, описаних у даній роботі, було використано 1500 унікальних зображень, чого виявилося достатньо при розбитті повідомлення на біграми.

До переваг даного алгоритму можна віднести наступне. Хеш-коди зображень мають високу стійкість до різноманітних видів атак на зображення – масштабування, стиснення, корекція яскравості та контрастності зображення. Зазвичай повідомлення вбудовується в цифрове зображення, тим саме пошкоджуючи високі частоти зображення. Якщо при передачі на зображення буде проведена атака, то стегано-повідомлення буде пошкоджене або взагалі втрачене. Схему кодування представлено на рисунку 5.

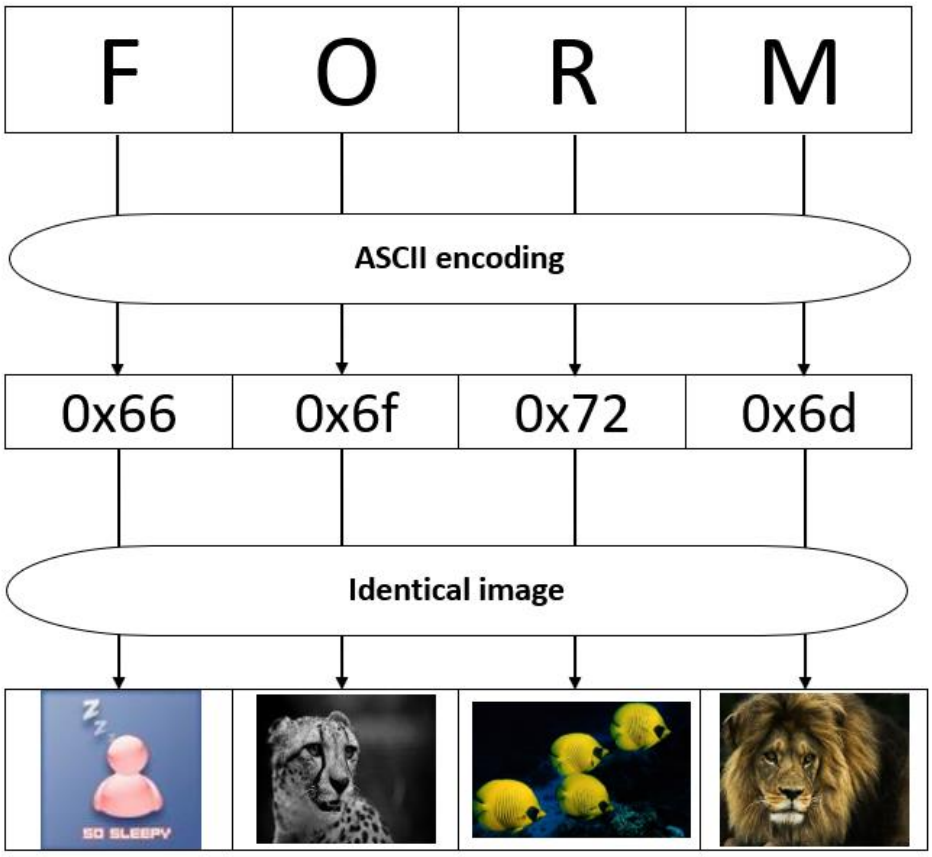


Рис. 5. Схема кодування повідомлення

Декодування відбувається у зворотньому порядку. Проведено також аналіз ефективності даного алгоритму кодування при застосуванні стеганографічних атак на послідовність цифрових зображень. Види атак та результати аналізу представлено у таблиці 1. До повідомлень у вигляді зображень було застосовано масштабування, корекцію яскравості та стиснення.

Таблиця 1.

Аналіз ефективності алгоритму при застосуванні стеганографічних атак

Стеганографічна атака	Масштабування	Зміна яскравості	Стиснення
Відсоток відновлених повідомлень	98%	95%	97%

Як бачимо з даної таблиці, відновлення повідомлень виконано у більшості випадків.

Висновок

Стеганографія – один з найперспективніших сучасних напрямів захисту інформації, наука, яка розвивається дуже швидко. Одним з основних критеріїв оцінки надійності стеганографічного методу є його стійкість до різноманітних видів атак. Останнім часом виділився такий напрям стеганографії як хеш-стеганографія, який базується на обчислювані хеш-коду цифрових зображень та повідомлення, що передається, та подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення.

В роботі виконано модифікацію алгоритму хеш-стеганографії. Модифікований алгоритм засновано на використанні перцептивного хеш-алгоритму Simple Hash замість використання криптографічних хеш-функцій. Проведено аналіз ефективності модифікованого алгоритму, який показав, що модифікація забезпечує стійкість стеганоповідомлення до різних атак на відміну від оригіналу.

Список літератури

1. Carlo Blundo, Clemente Galdi - Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics, International Conference IFIP TCS 2000 – Pp.140-151.
2. Shin N. One-Time Hash Steganography / N. Shin // Springer-Verlag Berlin Heidelberg. – 2000 – Pp.17-28.
3. Testing Different Image Hash Functions [Електронний ресурс] // Режим доступу: https://content-blockchain.org/research/testing-different-image-hash-functions/.
4. Jie, Z. A Novel Block-DCT and PCA Based Image Perceptual Hashing Algorithm / Z. Jie // IJCSI International Journal of Computer Science Issues. – 2013. – V.10. – Pp. 399-403.
5. Standaert, F.X. Practical evaluation of a radial soft hash algorithm / F.X. Standaert, F. Lefebvre, G. Rouvroy, B.M. Macq, J.J. Quisquater, J.D. Legat // In Proceedings of the International Symposium on Information Technology: Coding and Computing (ITCC). – 2005. – V.2. – Pp. 89-94.
6. Marrand, D. Theory of edge detection / D. Marrand, E. Hildret // Proc. R. Soc. Lond. – 1980. – V.207. – Pp. 187-215.
7. Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms Read more at [Електроний ресурс] // Режим доступу : https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

МОДИФИКАЦИЯ АЛГОРИТМА ХЕШ-СТЕГАНОГРАФИИ

В.В. Зорило, М.В. Бохонько, А.И. Казаков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: mishabahus28@gmail.com

Информация, которая передается по каналам связи, подвергается разнообразным угрозам, таким, как разоблачение, искажение и уничтожение. Одним из возможных решений проблемы угрозы разоблачения является использование стеганографических методов, которые в свою, очередь имеют свои ограничения по области применения. Стеганография предусматривает встраивание секретного сообщения в стеганографический контейнер (например, цифровое изображение) так, чтобы не нарушать устойчивость визуального восприятия контейнера. Одним из основных условий стеганографического метода является его устойчивость к различным видам атак. Современное направление стеганографии, хэш-стеганография, базируется на вычислении хэш-кода цифровых изображений и передаваемого сообщения, и дальнейшем использовании полученных хэш-кодов для шифрования секретного сообщения. Обычно большинство атак на цифровые изображения составляют опасность преимущественно для высоких частот, в

результате чего хэш-код цифрового изображения также будет претерпевать изменения, что может привести к частичной или полной потере стеганографического сообщения. Большинство современных методов получения хэш-кода цифрового изображения основаны на использовании высоких частот, что делает методы хэш-стеганографии уязвимыми к атакам по сравнению с оригиналом. Целью работы является повышение эффективности алгоритма хеш-стеганографии путем его модификации с помощью перцептивных хэш-алгоритмов. Проведен анализ существующих перцептивных хэш-алгоритмов для вычисления хэш-кода изображения. Выполнена модификация алгоритма хеш-стеганографии. Модифицированный алгоритм основан на использовании перцептивного хэш-алгоритма Simple Hash. Проведен анализ эффективности модифицированного алгоритма, который показал, что модификация обеспечивает повышение устойчивости стеганосообщения к различным атакам.
Ключевые слова: стеганография, хэш-стеганография, перцептивный хэш-алгоритм, встраивание дополнительной информации.

MODIFICATION OF THE HESH-STEGANOGRAPHY ALGORITHM

V.V. Zorilo, M.V. Bokhonko, A.I. Kazakov

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: mishabahus28@gmail.com

Abstract. Information transmitted through communication channels is subject to a variety of threats, such as exposure, distortion and destruction. One possible solution to the threat of autopsy is to use steganographic techniques, which in turn have limitations in scope. Steganography involves embedding a secret message in a steganographic container (for example, a digital image) so as not to violate the stability of the visual perception of the container. One of the main conditions of the steganographic method is its resistance to various types of attacks. The modern direction of steganography, hash steganography, is based on the calculation of the hash code of digital images and the transmitted message, and the further use of the received hash codes to encrypt the secret message. Typically, most digital image attacks are a high-frequency threat, causing the digital image hash code to be modified, which may result in partial or complete loss of the steganographic message. Most current digital imaging hash codes are based on high frequencies, making hash steganography vulnerable to attack. The purpose of this work is to increase the efficiency of the hash steganography algorithm by modifying it using perceptual hash algorithms. The analysis of existing perceptual hash algorithms for calculating the hash code of the image is performed. The hash algorithm has been modified. The modified algorithm is based on the use of the perceptual hash algorithm Simple Hash. The analysis of the effectiveness of the modified algorithm is carried out, which showed that the modification provides increased stability of the steganostation to various attacks.
Keywords: steganography, hash-steganography, perceptual hash algorithm, embedding additional information.

УДК 004.93'14

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 77-87

РОЗРОБКА СИСТЕМИ РОЗПІЗНАВАННЯ ОСІБ НА ОСНОВІ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ

О.О. Яковенко, Н.І. Кушніренко, І.С. Дорофєєва, А.Р. Євтушенко

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: dorofeeva283@gmail.com

Захищеність і цілісність особистих даних є актуальною проблемою в сучасному світі, так як останнім часом стало більш випадків зломів паролів, банківських аккаунтів і рахунків, невірної ідентифікації особистостей, підробки особистих даних. Такі способи автентифікації, як доступ за паролем, використання електронних перепусток, одноразові повідомлення з кодом є ненадійними на відміну від біометричних методів. Пароль можна забути, втратити, підібрати або вкрасти, а біометричні системи контролю доступу зручні для користувачів тим, що носії інформації знаходяться завжди при них, не можуть бути загублені або вкрадені. Біометричний контроль доступу вважається більш надійним, так як ідентифікатори не можуть бути передані третім особам, скопійовані. З усіх видів біометрії (ідентифікація за відбитками пальців, по райдужній оболонці ока, по голосу, по геометрії руки) ми вирішили зупинитися на розпізнаванні облич. Проаналізувавши існуючі методи класифікації зображень, був вибраний оптимальний варіант – згортальна нейронна мережа, успіх якої обумовлений можливістю обліку двовимірної топології зображення, на відміну від багатошарового персептрона. Технології розпізнавання осіб застосовуються в найрізноманітніших сферах: забезпечення безпеки в місцях великого скупчення людей; системах охорони; фейс-контроль в сегменті громадського харчування та розваг, пошук підозрілих і потенційно небезпечних відвідувачів; верифікація банківських карт; онлайн-платежі. В роботі розроблена система класифікації облич на основі згорткової нейронної мережі та система інтерпретації результатів класифікації, що дозволяє задавати співвідношення помилок 1-го та 2-го роду та обирати поріг детектування на основі цього співвідношення. На відміну від стандартного рішення, система не використовує критерій максимальної правдоподібності, що дозволяє отримувати більше інформації від класифікатора та зменшити рівень помилок системи. Вихідними даними для нашого дослідження є 840 фотографій, на яких зображені автори статті. Розроблений нами метод є інноваційним і дозволяє поліпшити комплексні захисні системи.

Ключові слова: згорткова нейронна мережа, розпізнавання обличчя, машинне навчання, класифікація зображень, управління помилками.

Вступ

Захищеність і цілісність особистих даних є актуальною проблемою в сучасному світі, так як останнім часом стало більш випадків зломів паролів, банківських аккаунтів і рахунків, невірної ідентифікації особистостей, підробки особистих даних. Такі способи автентифікації, як доступ за паролем, використання електронних перепусток, одноразові повідомлення з кодом є ненадійними на відміну від біометричних методів. Пароль можна забути, втратити, підібрати або вкрасти, а біометричні системи контролю доступу зручні для користувачів тим, що носії інформації знаходяться завжди при них, не можуть бути загублені або вкрадені. Біометричний контроль доступу вважається більш надійним, так як ідентифікатори не можуть бути передані третім особам, скопійовані. З усіх видів біометрії (ідентифікація за відбитками пальців, по райдужній оболонці ока, по голосу, по геометрії руки) було прийнято рішення зупинитися на розпізнаванні облич. Проаналізувавши існуючі методи класифікації зображень, було обрано оптимальний варіант – згорткова нейронна мережа, успіх якої обумовлений

можливістю обліку двовимірної топології зображення, на відміну від багатошарового персептрона. Технології розпізнавання осіб застосовуються в найрізноманітніших сферах: забезпечення безпеки в місцях великого скупчення людей; системах охорони; фейс-контроль в сегменті громадського харчування та розваг, пошук підозрілих і потенційно небезпечних відвідувачів; верифікація банківських карт; онлайн-платежі. Було розроблено згорткову нейронну мережу, та метод інтерпретації її результатів з подальшою можливістю вибору порога детектування, що надає можливість управляти помилками 1-го і 2-го роду. Математична модель згорткової нейронної мережі була побудована в системі Matlab. Вихідними даними для дослідження є 840 фотографій, на яких зображені автори статті. Розроблений метод базується на сучасних технологіях, та поєднує переваги загортальних нейронних мереж та розповсюджені методи управління помилками.

Актуальність дослідження полягає в тому, що багато напрямків науки, техніки і виробництва в значній мірі орієнтуються на розвиток систем, в яких інформація несе характер поля (зображення). При обробці такої інформації виникає ряд складних наукових, технічних і технологічних проблем. Однією з найскладніших на сьогоднішній момент з них є обробка і розпізнавання зображень. Про важливість цієї проблеми свідчить той факт, що дослідження з розпізнавання образів, аналізу зображень та мови включені в перелік пріоритетних напрямів розвитку науки і техніки.

Розпізнавання зображень знаходить широке застосування в різних сферах діяльності людини – це може бути контроль топології друкованих плат, текстури тканини, робототехніка (інтелектуальні системи). В інформатиці – контроль доступу до інформації щодо ідентифікації особи (біометрична ідентифікація). Спеціальне застосування – це контроль доступу до об'єктів обмеженого доступу, оперативний пошук в картотеці зображень, дактилоскопія та ін. Широко використовуються ці методи для класифікації історичних джерел на папері, а також у фізиці, хімії, біології та ін. галузях науки [1].

В даний час все більш широке поширення набувають біометричні системи ідентифікації людини. Цей напрямок знайшов відображення у роботах В.В. Моліцького, І.І. Данилюка, В.В. Карпінецького, А.В. Приймака, Ю.Є. Яремчука, О.І. Костюченка, М.О. Войтка, І.А. Терейковського. Традиційні системи ідентифікації вимагають знання пароля, наявності ключа, ідентифікаційної картки, або іншого ідентифікуючого предмету, який можна забути або втратити. На відміну від них біометричні системи ґрунтуються на унікальних біологічних характеристиках людини, які важко підробити і які однозначно визначають конкретну людину. До таких характеристик відносяться відбитки пальців, форма долоні, візерунок райдужної оболонки, зображення сітківки ока. Особа, голос і запах кожної людини так само індивідуальні [2].

Мета роботи

Метою дослідження є розробка згорткової нейронної мережі з постобробкою результатів, що полягає в встановлені порога. Це дає можливість краще розпізнавати зображення і керувати помилками 1-ого та 2-ого роду.

Основна частина

Штучну нейронну мережу (ШНМ) також називають просто «нейронна мережа» (НМ) – це математична модель, побудована за принципом роботи біологічних нейронних мереж – мереж нервових клітин живого організму. ШНМ складається з пов'язаної групи штучних нейронів і обробляє інформацію, використовуючи коннективізм. У більшості випадків – це адаптивна система, яка змінює свою структуру,

ґрунтуючись на обробці вхідної або вихідної інформації, яка тече через мережу під час фази навчання.

Машинне навчання – великий підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, здатних навчатися.

Згорткова нейронна мережа – спеціальна архітектура ШНМ, запропонована Яном Лекуном [3] і націлена на ефективне розпізнавання зображень, входить до складу технологій глибокого навчання. Використовує деякі особливості зорової кори, в якій були відкриті так звані прості клітини, що реагують на прямі лінії під різними кутами, і складні клітини, реакція яких пов'язана з активацією певного набору простих клітин. Таким чином, ідея згорткових нейронних мереж полягає в чергуванні згорткових шарів і субдискретизуючих шарів.

Переваги згорткової нейронної мережі перед звичайною ШНМ:

- в порівнянні з повнозв’язною нейронною мережею – набагато менша кількість налаштованих ваг, так як одне ядро ваг використовується цілком для всього зображення, замість того, щоб робити для кожного пікселя вхідного зображення свій персональний ваговий коефіцієнт. Це підштовхує ШНМ при навчанні до узагальнення демонстрованої інформації, а не до попіксельного запам'ятовування кожної показаної картинки у великій кількості вагових коефіцієнтів, як це робить перцептрон [4];
- зручне розпаралелювання обчислень, а також можливість реалізації алгоритмів роботи і навчання мережі на графічних процесорах;
- відносна стійкість до повороту і зсуву зображення, яке розпізнається;
- навчання за допомогою класичного методу зворотного поширення помилки.

Метод гнучкого порівняння на графах [5]. Суть методу зводиться до еластичного порівняння графів, що описують зображення осіб. Особи представлені у вигляді графів зі зваженими вершинами і ребрами. На етапі розпізнавання один з графів – еталонний, залишається незмінним, в той час як інший деформується з метою найкращої підгонки до першого. У подібних системах розпізнавання графи можуть являти собою як прямокутну решітку, так і структуру, утворену характерними точками особи. Недоліки: висока обчислювальна складність процедури розпізнавання, низька технологічність при запам'ятовуванні нових еталонів, лінійна залежність часу роботи від розміру бази даних осіб.

Нейронні мережі [6]. В даний час існує безліч різновидів нейронних мереж. Одним з найбільш широко використовуваних варіантів є мережа, побудована на багатошаровому перцептроні, яка дозволяє класифікувати подане на вхід зображення/сигнал відповідно до попереднього навчання мережі. Недоліки: додавання нової еталонної особи в базу даних вимагає повного перенавчання мережі на всьому наявному наборі (досить тривала процедура, в залежності від розміру вибірки від 1 години до декількох днів). Проблеми математичного характеру, пов'язані з навчанням: потрапляння в локальний оптимум, вибір оптимального кроку оптимізації, перенавчання і тому подібне. Важко формалізується етап вибору архітектури мережі (кількість нейронів, шарів, характер зв'язків).

Приховані Марковські моделі (ПММ) [7]. Одним з статистичних методів розпізнавання осіб є приховані Марковські моделі з дискретним часом. ПММ використовують статистичні властивості сигналів і враховують безпосередньо їх просторові характеристики. Елементами моделі є: безліч прихованих станів, безліч спостережуваних станів, матриця перехідних ймовірностей, початкова ймовірність станів. Кожному відповідає своя Марковська модель. При розпізнаванні об'єкта перевіряються згенеровані для заданої бази об'єктів Марковської моделі і шукається максимальна із спостережуваних ймовірність того, що послідовність спостережень для даного об'єкта згенерована відповідною моделлю. На сьогоднішній день не вдалося знайти приклад комерційного застосування ПММ для розпізнавання осіб. Недоліки: необхідно підбирати параметри моделі для кожної бази даних.

Метод головних компонент (Principal Component Analysis, PCA) [8]. Одним з найбільш відомих і опрацьованих є метод головних компонент, заснований на перетворенні Карунена-Лоєва. Спочатку метод головних компонент почав застосовуватися в статистиці для зниження вимірності простору ознак без істотної втрати інформації. У задачі розпізнавання осіб його застосовують головним чином для представлення зображення особи вектором малої розмірності (головних компонент), який порівнюється потім з еталонними векторами, закладеними в базу даних. Недоліки: метод головних компонент добре зарекомендував себе в практичних додатках. Однак в тих випадках, коли на зображенні особи присутні значні зміни в освітленості або виразі обличчя, ефективність методу значно падає. Вся справа в тому, що PCA вибирає підпростір з такою метою, щоб максимально апроксимувати вхідний набір даних, а не виконати дискримінацію між класами осіб.

Активні моделі зовнішнього вигляду (Active Appearance Models, AAM) і активні моделі форм (Active Shape Models, ASM) [9].

Активні моделі зовнішнього вигляду (AAM) – це статистичні моделі зображень, які шляхом різного роду деформацій можуть бути підігнані під реальне зображення. Даний тип моделей в двовимірному варіанті було запропоновано Тімом Кутсом і Крісом Тейлором в 1998 році. Спочатку активні моделі зовнішнього вигляду застосовувалися для оцінки параметрів зображень облич. Активна модель зовнішнього вигляду містить два типи параметрів: параметри, пов'язані з формою, і параметри, пов'язані зі статистичною моделлю пікселів зображення або текстурою. Суть методу ASM полягає в обліку статистичних зв'язків між розташуванням антропометричних точок на наявній вибірці зображень осіб, знятих в анфас. На зображенні експерт розмічає розташування антропометричних точок. На кожному зображенні точки пронумеровані в однаковому порядку. Недоліки: моделі AAM і ASM призначені для того, щоб точно локалізувати ці антропометричні точки на зображенні особи, а не класифікувати його.

Згорткові нейронні мережі [10]. Найкращі результати в області розпізнавання осіб (за результатами аналізу публікацій) показала Convolutional Neural Network або згорткова нейронна мережа (далі – ЗНМ). Успіх обумовлений можливістю обліку двовимірної топології зображення, на відміну від багатошарового перцептрона.

Саме тому для вирішення нашої задачі ми будемо використовувати ЗНМ.

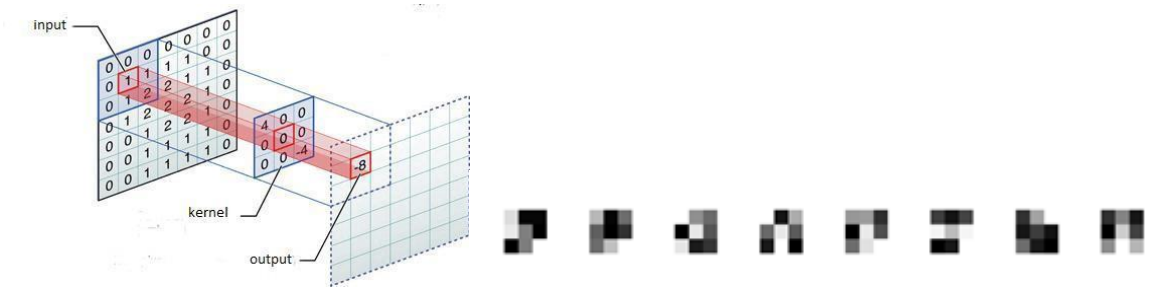
Відмінними рисами ЗНМ є локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів), загальні ваги (забезпечують детектування деяких рис в будь-якому місці зображення) і ієрархічна організація з просторовими семплінгом. Завдяки цим нововведенням ЗНМ забезпечує часткову стійкість до змін масштабу, зсувів, поворотів, змін ракурсу і інших спотворень.

Особливістю згорткової нейронної мережі є операція згортки. Згортка – це операція над парою матриць A (розміром $n_x \times n_y$) та B (розміром $m_x \times m_y$), результатом якої є матриця $C = A \times B$ розміру $(n_x - m_x + 1) \times (n_y - m_y + 1)$. Кожен елемент результату обчислюється як множення матриці B і деякої підматриці A такого ж розміру (підматриця визначається положенням елемента в результаті).

Логічний сенс згортки полягає в наступному: чим більше величина елемента згортки, тим більше ця частина матриці A буде схожа на матрицю B (схожа в контексті скалярного множення). Тому матрицю A називають зображенням, а матрицю B – фільтром або зразком (kernel).

У згортковій нейронній мережі виходи проміжних шарів утворюють матрицю (зображення) або набір матриць (кілька шарів зображення). Так, наприклад, на вхід згорткової нейронної мережі можна подавати три шари зображення (R-, G-, B-канали зображення). Основними видами шарів в згортковій нейронній мережі є згорткові шари, пулінгові шари і повнозв'язні шари.

Згорткові нейронні мережі працюють на основі фільтрів, які займаються розпізнаванням певних характеристик зображення (наприклад, прямих ліній). Фільтр – це колекція кернелів; іноді в фільтрі використовується один кернел (рис. 1). Кернел – це звичайна матриця чисел, що називаються вагами, які навчаються з метою пошуку на зображеннях певних характеристик. Фільтр зміщується уздовж зображення і визначає, чи присутня деяка шукана характеристика в конкретній його частині [11]. Для отримання відповіді такого роду здійснюється операція згортки, яка є сумою добутків елементів фільтра і матриці вхідних сигналів.



а б

Рис. 1. Приклад роботи фільтра: а – візуалізація процесу згортки; б – приклад кернелів, отриманих у результаті експерименту

Архітектура згорткової нейронної мережі

Згорткова нейронна мережа складається з декількох типів шарів (рис. 2).

Вхідні дані (Image Input) – це шар, у якому зображення подається на ЗНМ.

Двовимірна згортка (Convolution 2D) – двовимірний згортковий шар застосовує ковзаючи згорткові фільтри до вхідних даних. Шар згортає вхідні дані, переміщаючи фільтри уздовж вхідних даних по вертикалі і горизонталі і обчислюючи точкове множення ваг і вхідних даних, а потім додаючи член зміщення.

Пакетна нормалізація (Batch Normalization) – шар нормалізації партії, нормалізує кожен вхідний канал в міні-партії. Щоб прискорити навчання згорткових нейронних мереж і знизити чутливість до ініціалізації мережі, шари пакетної нормалізації використовуються між згортковими шарами та лінійними шарами, такими як *ReLU*. Шар спочатку нормалізує активації кожного каналу, віднімаючи середнє значення міні-партії і ділячи його на стандартне відхилення міні-партії. Потім шар зрушує вхідний сигнал на навчене зміщення β і масштабує його на той, який навчає масштабний коефіцієнт γ.

Шар-випрямляч (*ReLU*) – виконує порогову операцію для кожного елемента вводу, де будь-яке значення менше нуля встановлюється в нуль.

Шар вибору максимального елемента (*Max Pooling 2D*) виконує знижувальну дискретизацію шляхом ділення вхідних даних на прямокутні області пулу і обчислення максимуму кожної області.

Повнозв’язний шар (*Fully Connected*) – повністю пов'язаний шар примножує вхідні дані на матрицю ваг, а потім додає вектор зміщення.

Softmax – застосовує функцію *softmax* до входу.

Результат класифікації (*Classification Output*) – шар класифікації, обчислює крос-ентропійну втрату для задач мультикласової класифікації з взаємовиключними класами. Шар виводить кількість класів з вихідного розміру попереднього шару.

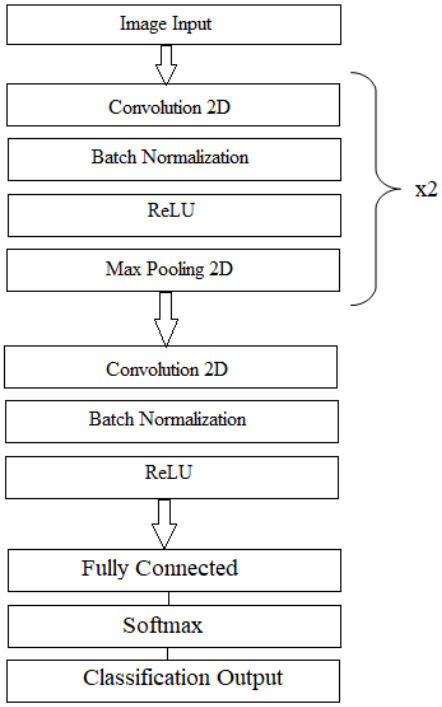


Рис. 2. Структурна схема ЗНМ

Метод постобробки при класифікації зображень.

На рисунку 3 зображено: 2 класа зображень (*A* і *B*), зображення *X* і визначається близькість зображення до одного з класів. У такому виді дані отримуються зі загорткової мережі.

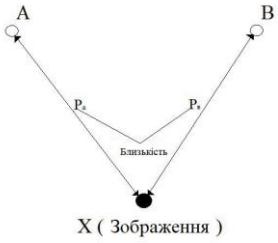


Рис. 3. Графічне зображення поняття близькості до класу, *A* та *B* – класи зображень, P_A та P_B – близькість зображення до класів *A* та *B* відповідно

У таблиці 1 показані дані, в яких відображені значення параметра *P* (близькість, *proximity*).

Таблиця 1.

Значення параметра близькості зображень до класів *A* та *B* для перших трьох зображень

	P_A	P_B
1	0.9862	0.0138
2	0.9964	0.0036
3	0.9932	0.0068

Використовувались два класа зображень *A* і *B*, які в реальності являли собою фотографії двох людей, а саме авторів статті. Використання стандартного класифікатора Matlab визначає найближчий клас *A* або *B*.

За замовчуванням при класифікації зображень Matlab використовує принцип максимальної правдоподібності. Цей принцип не досконалий, так як не дозволяє гнучко налаштовувати помилки першого і другого роду.

Для того, щоб керувати помилками 1-го і 2-го роду потрібно використовувати близькість до класу. Наприклад, якщо $P_A = 0.9$, а $P_B = 0.89$, то система фактично не впевнена, але проста класифікація повертає клас *A*. В роботі розроблена система, яка враховує цей недолік. Пропонується використовувати параметр вірогідності класу A – L_A (*likelihood of A*), який дозволяє вирішити цей недолік (1). Цей параметр базується на різності параметрів близькості до класів *A* та *B*:

$$P_A - P_B .$$

Якщо зображення ближче до класу *A*, то його індекс $P_A - P_B$ більше нуля. Для наочності приведемо графік (рис. 4), де по горизонталі номера зображень, а по вертикалі індекс поточного зображення. Перші 320 зображень – реальний клас *A*, а другі – реальний клас *B*.

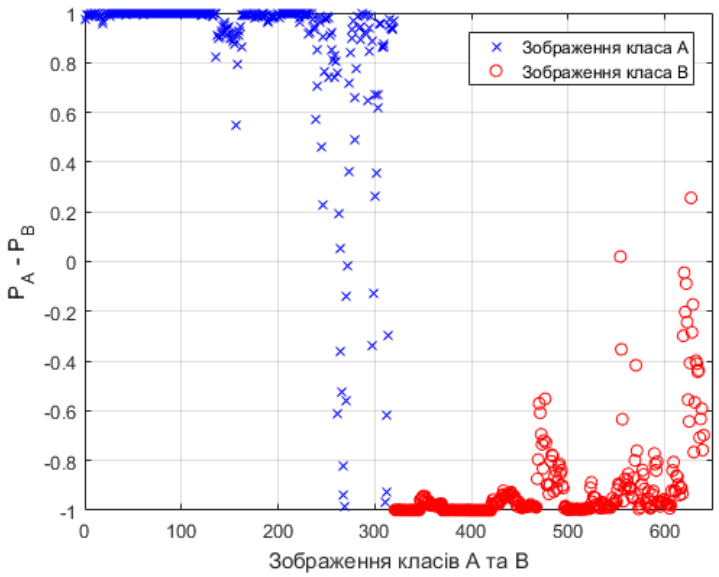


Рис. 4. Графік $P_A - P_B$

Для того, щоб перетворити індекс в діапазон [0,1] перетворимо вище наведену формулу таким чином:

$$L_A = (P_A - P_B + 1)/2 \qquad (1)$$

Тепер значення близькості до класу розподіляються від 0 до 1. 1 – клас *A*, 0 – клас *B*. На графіку видно (рис. 5), що в останніх 80 зображеннях програмі важко визначити належність до класу *A* або класу *B*.

Параметр L_A знаходиться в діапазоні [0,1]. Виникає питання встановлення значення порога t таким чином, щоб отримати контрольовані значення ймовірності помилок першого (P_{FP}) і другого (P_{FN}) роду.

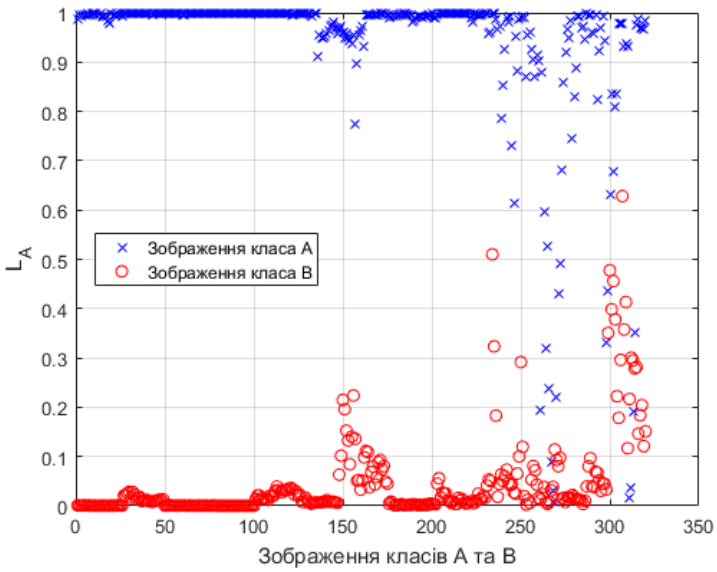


Рис. 5. Значення індексу L_A для зображень обох класів

Для цього використовуються отримані значення L_A для зображень обох класів, графіки помилок отримаємо наступним чином:

- перебираються значення порога t від 0 до 1 з деяким кроком (наприклад, 0.001);
- для кожного значення t знаходиться відсоток зображень класу A, для яких $L_A < t$, цей відсоток є P_{FN} для цього значення порога;
- аналогічно, відсоток значень класу B, для яких $L_A > t$ є P_{FP} для цього значення порога.

Таким чином, на графіку можна бачити залежність помилок від порога, і вибирати поріг відповідно з необхідним рівнем обох помилок. Перетин графіків помилок першого і другого роду відповідає рівності помилок ($P_{FP} = P_{FN}$). Клас A на графіку позначається x-подібними символами, клас B – кружками.

На графіку (рис. 6) зображені помилки 1-го і 2-го роду в залежності від значення порога детектування t. Помилка першого роду (також *false positive, FP*) – це помилка, при якої реальний елемент класу B детектується як клас A. Помилка другого роду (також *false negative, FN*) – це помилка, при якої реальний елемент класу A детектується як клас B.

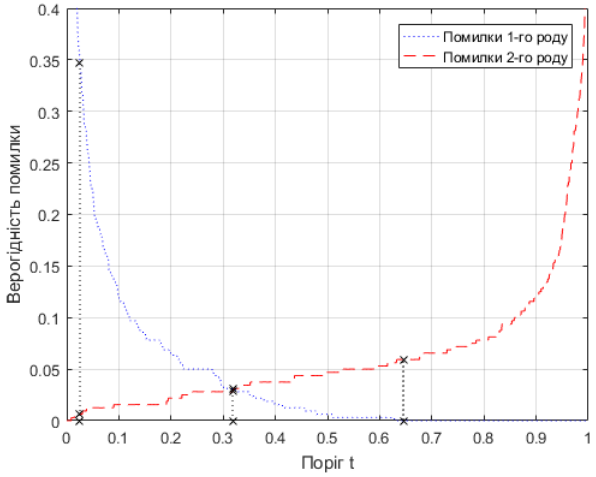


Рис. 6. Помилки 1-го і 2-го роду в залежності від порога детектування

Наприклад, є пропускний пункт. Клас *A* – співробітники організації, клас *B* – сторонні. При виборі порога $t = 0.318$, система буде в рівному ступені помилятися при визначенні близькості і до класу *A*, і до класу *B*, то ймовірність пропустити не співробітника дорівнює ймовірності не пропустити співробітника, і дорівнює p = 0.04.

Якщо вибрати поріг $t = 0.6452$, то система буде схильна до того, щоб детектувати елементи класа *A* як клас *B*. Іншими словами, ніколи не буде пускати сторонніх, але іноді, буде ймовірність не пустити співробітника $P_{FN} = 0.06$.

При виборі порога $t = 0.025$ система буде схильна до того, щоб детектувати елементи класа *B* як клас *A*. Тобто, система пропустить співробітників в 99% випадках, але з імовірністю 35 % пропустить сторонніх.

Таким чином, розроблена система дозволяє адміністратору вибрати оптимальний варіант пропускної системи відповідно до потреби.

Особливості тренування ЗНМ.

Для дослідження було використано по 420 зображень кожного класу, на тренування довільного вибиралися по 100 зображень з кожного класу. Для тренування і аналізу зображення проходили попередню обробку, а саме знебарвлення і зменшення до розміру 25×25 пікселів (рис. 7). Зменшення зображень обумовлено продуктивністю.

Для тренування були використані наступні параметри:

- *sgdm* – оптимізатор стохастичного градієнтного спуску з імпульсом (*Stochastic Gradient Descent with Momentum,* SGDM [12]), можна вказати значення імпульсу, використовуючи аргумент пари ім'я-значення 'Momentum';
- *InitialLearnRate* – початкова швидкість навчання, яка використовується для навчання, вказується у вигляді розділеної запитом пари, що складається з *InitialLearnRate* і позитивного скаляра; значення за замовчуванням становить 0,01 для оптимізатора *sgdm* і 0,001 для вирішувачей *rmsprop* і *adam*, якщо швидкість навчання занадто низька, то навчання займає багато часу, якщо висока, то навчання може досягти неоптимального результату або розходитися;
- *Shuffle, every-epoch* – заново перемішувати тренувальні дані в кожній епохі;
- *ValidationFrequency* – валідація проводиться кожні 30 епох.

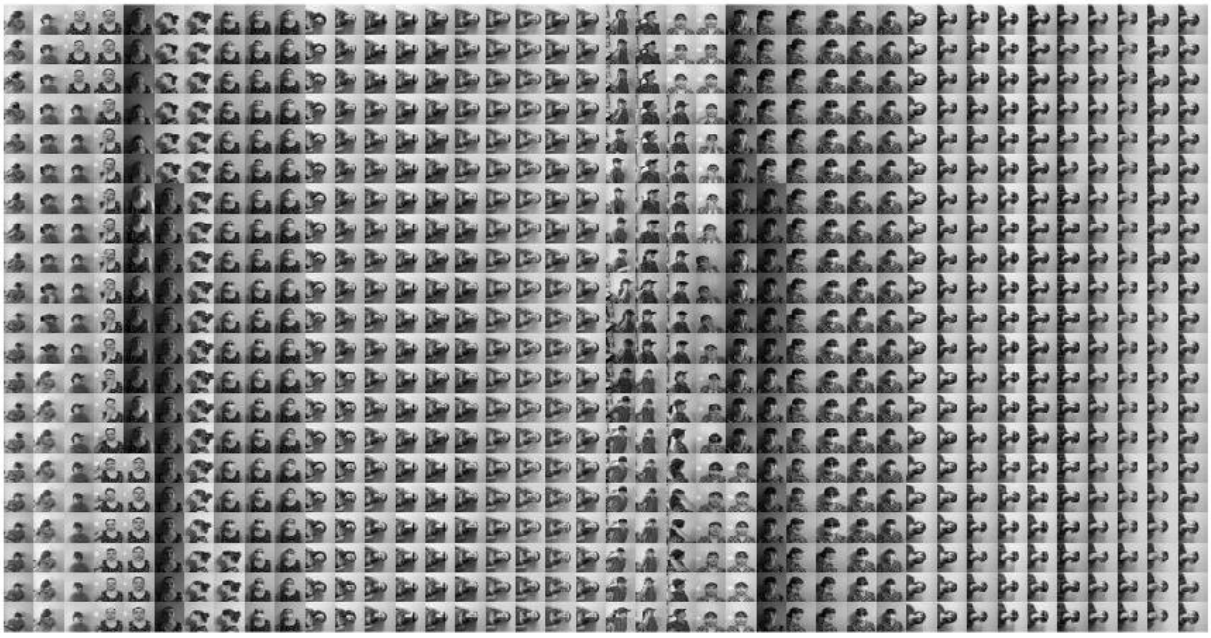


Рис. 7. Всі зображення (тренувальні та перевірочні)

Висновки

У даній роботі були проаналізовані існуючі рішення в області класифікації зображень. В результаті проведення експерименту була створена згортальна нейронна мережа з постобробкою результатів, були проаналізовані різні значення порога класифікації, в залежності від якого можуть завдання реалізовуватися різні політики безпеки. Розроблений метод є інноваційним і дозволяє покращити комплексні захисні системи. Даний напрямок буде об'єктом подальших досліджень.

Список літератури

1. Галушкин, А.И. Нейронные сети. Основы теории / А.И. Галушкин. – М.: Горячая линия – Телеком, 2010. – 480 с.
2. Панканти, Ш. Биометрия: будущее идентификации / Ш. Панканти, Р.М. Болле, Э. Джейн // Открытые Системы. – 2000.– № 3. – С. 51-63.
3. Santaji, G. Neural networks for facerecognition using SOM / G. Santaji, G. Jayshree, M. Shamla, G. Dhanaji // IJCST. – 2010. – 287c.
4. Субботін, С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень / С.О. Субботін. – Запоріжжя: ЗНТУ, 2008. – 341 с.
5. Степанов, В.Н. Дискретная математика: графы и алгоритмы на графах / В.Н. Степанов. – ОмГТУ, 2010. – 120 с.
6. Савельев, А.В. На пути к общей теории нейросетей. К вопросу о сложности / А.В. Савельев // Нейрокомпьютеры: разработка, применение. – 2006. – С. 4-14.
7. Yu, S. Hidden semi-Markov models / S. Yu // Artificial Intelligence. – 2010. – Vol.174, No 2. – Pp. 215-243.
8. Jolliffe, I.T. Principal component analysis, series: springer series in statistics / I.T. Jolliffe. – 2nd ed. Springer, 2002. – 487 p.
9. Русай, А.Н. Биометрическая аутентификация диктора в MATLAB / А.Н. Русай. – Учебное пособие. – М.: Русайнс, 2017. – 512 с.
10. Барский, А.Б. Логические нейронные сети / А.Б. Барский. – М.: Интернет-университет информационных технологий, бином. Лаборатория знаний, 2007. – 352 с.
11. Fukushima, K. Artificial Vision by Multi-Layered Neural Networks: Neocognitron and its Advances / K. Fukushima // Neural Networks. – 2013. – Pp. 103-119.
12. Qian, N. On the momentum term in gradient descent learning algorithms. Neural Networks / N. Qian // The Official Journal of the International Neural Network Society. – 1999. – 12(1). – Pp. 145–151.

РАЗРАБОТКА СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ НА ОСНОВЕ СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ

А.А. Яковенко, Н.И. Кушниренко, И.С. Дорофеева, А.Р. Евтушенко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: dorofeeva283@gmail.com

Защищенность и целостность личных данных является актуальной проблемой в современном мире, так как в последнее время участились случаи взломов паролей, банковских аккаунтов и счетов, неверной идентификации личностей, подделки личных данных. Такие способы аутентификации, как доступ по паролю, использование электронных пропусков, одноразовые сообщения с кодом являются ненадежными в отличие от биометрических методов. Пароль можно забыть, потерять, подобрать или украсть, а биометрические системы контроля доступа удобны для пользователей тем, что носители информации находятся всегда при них, не могут быть утеряны либо украдены. Биометрический контроль доступа считается более надежным, т. к. идентификаторы не могут быть переданы третьим лицам, скопированы. Из всех видов биометрии (идентификация по отпечатку пальца, по радужной оболочке глаза, по голосу, по геометрии руки) мы решили остановиться на распознавании лиц. Проанализировав существующие методы классификации изображений, был выбран оптимальный вариант – сверточная нейронная сеть, успех

которой обусловлен возможностью учета двумерной топологии изображения, в отличие от многослойного персептрона. Технологии распознавания лиц применяются в самых разнообразных сферах: обеспечение безопасности в местах большого скопления людей; системы охраны, избежание незаконного проникновения на территорию объекта, поиск злоумышленников; фейс-контроль в сегменте общепита и развлечений, поиск подозрительных и потенциально опасных посетителей; верификация банковских карт; онлайн-платежи. В работе разработана система классификации лиц на основе сверточной нейронной сети и система интерпретации результатов классификации, что позволяет задавать соотношение ошибок 1-го и 2-го рода и выбирать порог детектирования на основе этого соотношения. В отличие от стандартного решения, система не использует критерий максимального правдоподобия, что позволяет получать больше информации от классификатора и уменьшить уровень ошибок системы. Исходными данными для нашего исследования являются 840 фотографий, на которых изображены авторы статьи. Разработанный нами метод является инновационным и позволяет улучшить комплексные защитные системы.

Ключевые слова: сверточная нейронная сеть, распознавание лица, машинное обучение, классификация изображений, управление ошибками.

DEVELOPING OF THE FACE RECOGNITION SYSTEM ON THE BASIS OF CONVOLUTIONAL NEURAL NETWORK

O.O. Iakovenko, N.I. Kushnirenko, I.S. Dorofieieva, A.R. Yevtushenko

Odessa National Polytechnic University,
1, Shevchenko Avenue, Odessa, 65044, Ukraine; e-mail: dorofeeva283@gmail.com

Security and integrity of personal data is an important issue in the modern world, as cases of password cracks, bank accounts and accounts, incorrect identification of individuals, falsification of personal data have recently become more frequent. Such methods of authentication as password access, use of electronic passes, one-time messages with a code are unreliable in contrast to the biometric methods. The password can be forgotten, lost, cracked or stolen, thus biometric access control systems are convenient for users because data storage devices are always with them, cannot be lost or stolen. Biometric access control is considered more reliable, because identifiers cannot be transferred to third parties or be copied. Among all the types of biometrics (identification by fingerprint, by iris, by voice, by hand geometry) we decided to choose the face recognition. After analyzing the existing methods of image classification, we have chosen the best option - a convolutional neural network, the success of which is due to the possibility of taking into account the two-dimensional image topology, in contrast to the multilayer perceptron. Face recognition technologies are used in a wide variety of areas: security in places with large concentrations of people; security systems; face control in the catering and entertainment segment, searching for suspicious and potentially dangerous visitors; verification of bank cards; online payments. We have developed a convolutional neural network, on the basis of which a post-processing method was created with the subsequent possibility of choosing a threshold, which makes it possible to manage type I and type II errors. The mathematical model of our convolutional neural network was built on the Matlab system. The initial data for our study are 840 photos, on which are depicted the authors of the article. The method developed by us is innovative and allows for improving protective complex systems.

Keywords: convolutional neural network, face recognition, machine learning, image classification, error management.

УДК 681

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 88-95

ANALYSIS AND MODIFICATION OF THE ALGORITHM FOR THE BLUR DETECTION IN A DIGITAL IMAGE

V.V. Zorilo, O.Yu. Lebedieva, P.S. Safronov

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: vikazorilo@gmail.com, o.y.lebedieva@opu.ua

The use of the digital images in modern society is very common, making it difficult to name an industry where digital images are not used. However, in certain situations, the digital images may be direct or indirect digital evidence, such as in court cases. Tampering or violating the integrity of the digital images is one of the important issues in the information protection. The issue of the digital signal authentication by cybersecurity experts is a pressing issue in the present days. Therefore, the development of methods and algorithms for detecting the integrity of digital signals in general, and digital images in particular, is a very crucial task. Among all the possible variations in the integrity violation of digital images can be distinguished a separate group, in which the digital images are processed by various filters editors, such as blurring, sharpening, etc. The blurring is often applied to images not only when they are tampered, but also as a steganographic attack. Blur detection indicates the inability to use a digital image as the evidence of anything. One of the most effective blur detection methods known from the open sources is a method based on the analysis of singular values of blocks of a digital image matrix. The aim of this paper is to increase the efficiency of the blur detection in a digital image by modifying an algorithm based on the analysis of singular values. Computational experiments are performed to determine the number of parameters to be verified. The results obtained allow modifying the algorithm of the method of the blur detection in a digital image. The modification makes it possible to detect tampered access to a digital image. The modified algorithm is no less effective than the original algorithm, and allows analyzing fewer parameters in a shorter time. The computational complexity of the algorithm is determined by the second order polynomial that is acceptable in terms of the practical application.

Keywords: digital image, blurring, integrity violations, singular values, digital evidences, digital forensics.

Introduction

At present, the digital content expertise is actively developing, the software methods for detecting the integrity violations of a digital image (DI), such as cloning, collage, scaling, brightness correction, blurring, are being created and improved. As practice shows, blurring is a very popular tool among graphic designers. The presence of blurring indicates the possible tampering with DI, or the use of a steganographic attack.

In [1], the blur detection method (BDM) based on a general approach, to the analysis of the state and technology of the functioning of the information system, is developed. Among the methods well-known from the open sources, the BDM is the most effective. It is capable of detecting a Gaussian blur of 1 pixel radius that is the most difficult case to detect (figure 1).

One of the advantages of this method is the ability to separate DIs blurred by graphic editors from those which are stored in low-quality lossy format and (or) have a shallow depth of field in the image space (figure 2).

To date, BDM has many modifications and adaptations to detect different types of blurring [2, 3]. The method is based on the analysis of the growth rate of singular values (SVs) of n×n-blocks of a digital image matrix (figure 3).

a

b

Fig. 1. Image processing: a – before blur; b – after blur

Fig. 2. Shallow depth of field in the image space

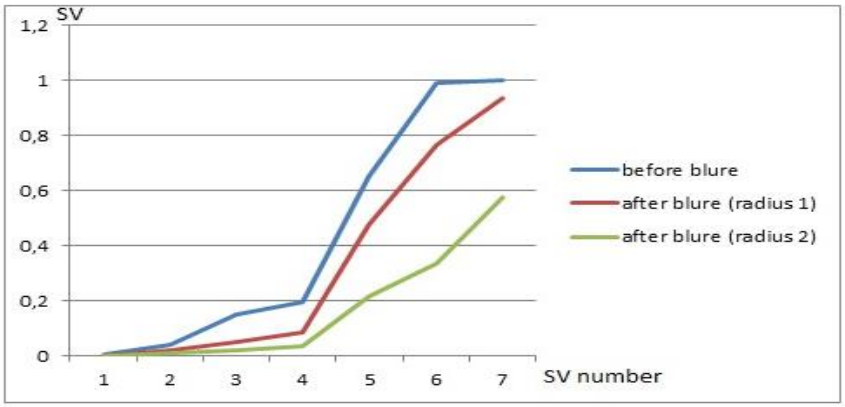


Fig. 3. Interpolating spline powers of one for SV set

According to [4], there is a correspondence between the singular spectrum and frequency spectrum of the digital signal, i.e. the largest singular values correspond mostly to low frequencies, the smallest ones correspond to high ones, with the decrease of the singular value, the contribution of low frequencies becomes smaller and the contribution of high frequencies becomes greater. Because blurring affects mainly the contour of a digital image, it reduces the growth rate of the smallest singular values. The authors of the method found that the analysis of at least five of the eight singular values makes it possible to detect the application of the specified filter. However, the question arises as to why only the five SVs/ are analyzed, since the higher the contribution of the higher frequencies, the smaller the singular value.

The basis of the modification performed is to verification the effect of the number of analyzed singular values on the effectiveness of the blur detection method in a digital image.

The aim of the paper

Is to improve the efficiency of the blur detection in the digital image by modifying an algorithm based on the analysis of singular values.

Main part

The visual result of the blurring is the contour smoothing, which will lead to a decrease in the high-frequency component of the signal. The basic steps of the blur detection method are as follows. The digital image matrix is divided into 8×8-blocks in standard manner. For each block, the set of singular values is found. For the five smallest singular values in each block, the linear approximation is obtained, and for the approximating function, the derivative, whose value (constant) is the coefficient of the growth rate of the said singular values, is determined. If the maximum value of the coefficient of the growth rate (Vmax) among all 8×8-blocks does not exceed the threshold value, then the image is considered blurred.

If the average value of the coefficient of the growth rate (Vav) among all 8×8-blocks exceeds the threshold value, then the image is not considered blurred. In other cases, the method requires additional verification. An additional verification is to have a deliberate blurring of the digital image by an expert, followed by a comparison of the analyzed parameters. If the expert blurring for the image is the first, the analyzed parameters are decreased more than twice (table 4).

With repeated blurring, the required parameters are decreased twice or less. This feature makes it possible to conclude whether the blurring by the expert is repeated for the image, or

it is applied for the first time. Increasing the blur radius only facilitates the blur detection in a digital image. However, the larger the blur radius, the lower the stability of visual perception. That is, an image blurred with a radius greater than one-pixel radius should be alarming, since it is most likely not original.

Table 1.

Influence of the expert blurring on the image analyzed parameters

	Digital image	Vav	Vmax
Original image		2,51	3,54
First blur		0,53	0,7
First blur		0,44	0,52

An experiment is conducted in which three, four, and six smallest singular values of eight ones in the blocks of a digital image matrix are analyzed for the blur detection. The images from the NRSC database recommended for the experimental DI is used for the experiment [6]. One-pixel radius Gaussian blur is performed using Adobe Photoshop. The experiments gave the following results.

In this case, the use of the three smallest singular values has led to a situation where it is almost impossible to distinguish a threshold value when it comes to a Gaussian blur with a radius of 1 pixel. Therefore, the given number of singular values for analysis is not successful in achieving the aim and solving the tasks of the paper. This fact indicates that it is inappropriate to use three SVs instead of the five SVs as in the original algorithm.

The use of the six SVs is resulted in a large number of type I errors, i.e. it led to a situation where the blur is applied, but it could not be detected. The results of the experiment are shown in table 2.

Table 2.

The effectiveness of blur detection with the analysis of the six SVs

	Analysis of the six SVs	
Image format	TIFF	JPEG
Type I errors	48	48
Type II errors	0,0	0,0

Instead, the use of the four singular values is comparable to the results obtained by the use of the five singular values.

The experimental data is partially presented in Table 3. To establish the fact of blurring, the coefficients is calculated using the ten blurred images as an example.

Table 3.

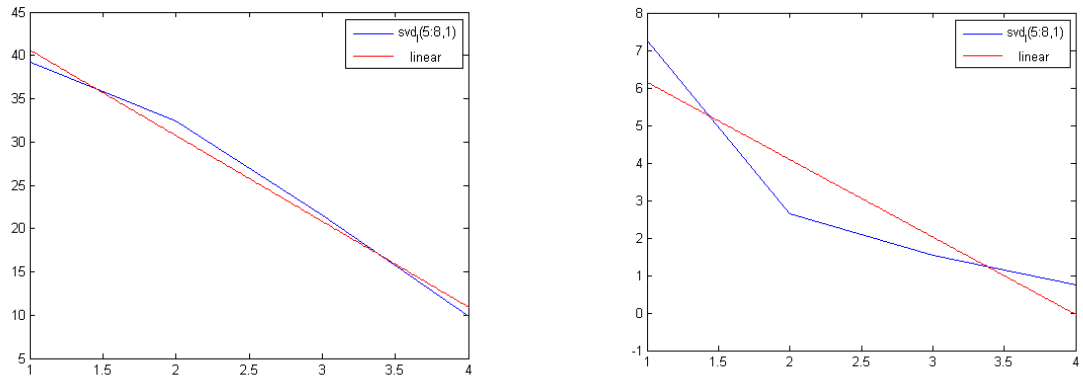
The coefficients of the average growth rate of the four SVs in the images before and after blurring

No	Coefficient of the average growth rate of SVs in the images before blurring	Coefficient of the average growth rate of SVs in the images after blurring
1.	5.3135	0.34524
2.	7.0841	0.73518
3.	5.3754	0.60165
4.	2.5972	0.2591
5.	2.2639	0.5707
6.	3.0558	0.43457
7.	1.9286	0.32922
8.	1.509	0.31949
9.	2.1537	1.439
10.	4.0608	0.6345

As we can see, including in Figure 5, the analyzed indices before blurring are significantly different from those after blurring. This allows to set a threshold value and indicates the possibility of using four singular values for analysis instead of five singular values.

The threshold value is set experimentally and equals to 1.75 when using the four smallest singular values of blocks of a digital image matrix.

Compare the efficiency of the said algorithm to the efficiency of the original algorithm (table 3).



a b

Fig. 5. First order interpolating spline for the 4 SVs (blue graph) and a linear approximation (red graph): a – before blurring; b – after blurring

As we can see, the number of type I errors when using four SVs for analysis is 0.5% higher than when using five SVs. However, the amount of time for the image verification by the software with analysis of the four singular values is 3.6% less than with using five SVs.

Based on the findings obtained, an algorithm of modified method for the blur detection in a digital image is developed.

Table 3.

Comparative analysis of the algorithm with the analysis of four SVs and five SVs

	Analysis of the five SVs		Analysis of the four SVs	
Image format	TIFF	JPEG	TIFF	JPEG
Type I errors	0.0	0.5	0.0	1
Type II errors	0.0	0.0	0.0	0.0

Let F is the $n \times m$-matrix of the experimental DI.

Step 1. The matrix of the experimental digital image is divided into 8×8 blocks in standard manner:

$$F_{ij,}\ i = 1,2,...,[n/8],\ j = 1,2,...,[m/8].$$

Step 2. The matrix of singular values is composed: singular value decomposition is performed for each block F_{ij}

$$F_{ij} = U_{ij} \sum_{ij} V_{ij}^{T},$$

where U_{ij}, V_{ij} are the orthogonal 8×8-matrices of the left and right singular vectors F_{ij} respectively,

$$\sum_{ij} = diag(\sigma_1,...,\sigma_8)$$

is a matrix of singular values, $\sigma_1 \geq ... \geq \sigma_8 \geq 0$.

Step 3. For $\sigma_l, l = 5,...,8$ blocks F_{ij} a linear approximating function is obtained

$$y = ax + b\ (w_{ij} = a).$$

Step 4. The matrix of the growth rate W is composed.

Step 5. The average value of the matrix of the growth rate M_F is calculated. If M_F>1.75, the image is not blurred, otherwise the image is blurred.

When obtaining a conclusion about the presence of a blurring, it is recommended to perform an additional verification with the blurring by expert.

Conclusion

The performed modification of the algorithm makes it possible to detect tampered access to the digital image. The modified algorithm is no less effective than the original one and allows fewer parameters to be analyzed in a shorter time. The computational complexity of the algorithm is determined by a second order polynomial that is acceptable in terms of the practical application.

References

1. Зорило, В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения. / В.В. Зорило // Інформаційна безпека. – 2013. – №1(7). – С. 34-41.
2. Зорило, В.В. Вплив розмиття різного радіусу на властивості матриці цифрового зображення / В.В. Зорило, Ю.С. Колісніченко // Матеріали міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології». – Одеса, 2013. – С.7-9.
3. Зоріло, В.В. Аналіз параметрів цифрового зображення в умовах різних видів розмиття засобами графічного редактору Adobe Photoshop / В.В. Зоріло, К. Кейта // «Захист інформації і безпека інформаційних систем»: Матеріали V міжнародної науково-технічної конференції 02-03 червня 2016 р. – Львів: 2016 – С. 56-57.
4. Кобозева, А.А. Использование особенностей возмущения сингулярних чисел матрицы цифрового изображения для обнаружения его фальсификации / А.А. Кобозева // Искусственный интеллект. – 2008. – №1. – С.145-153.

АНАЛІЗ ТА МОДИФІКАЦІЯ АЛГОРИТМУ ВИЯВЛЕННЯ РОЗМИТТЯ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, О.Ю. Лебедєва, П.С. Сафронов

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: vikazorilo@gmail.com, o.y.lebedieva@opu.ua

Використання цифрових зображень в сучасному суспільстві настільки поширене, що важко назвати галузь, де б їх не застосовували. Однак у певних ситуаціях цифрові зображення можуть бути прямими або непрямими цифровими доказами, наприклад, у судових справах. Підробка або порушення цілісності цифрових зображень – одна з важливих проблем захисту інформації. Перед фахівцями з кібербезпеки сьогодні гостро стоїть питання перевірки автентичності цифрових сигналів. Отже, розробка методів та алгоритмів виявлення порушень цілісності цифрових сигналів взагалі та цифрових зображень зокрема є дуже актуальною темою. Серед усіх можливих варіантів порушення цілісності цифрових зображень можна виділити окрему групу – застосування обробки різними фільтрами графічних редакторів, таких як розмиття, підвищення різкості тощо. Розмиття доволі часто застосовують до зображень не лише при їх фальсифікації, а й як стеганографічну атаку. Виявлення розмиття вказує на неможливість використання цифрового зображення в якості доказу будь-чого. Один з найефективніших методів виявлення розмиття, відомих з відкритого друку,це метод, заснований на аналізі сингулярних чисел блоків матриці цифрового зображення. Метою даної роботи є підвищення ефективності виявлення розмиття цифрового зображення шляхом модифікації алгоритму, заснованого на аналізі сингулярних чисел. В роботі проведено обчислювальні експерименти щодо встановлення кількості параметрів, що перевіряються. Отримані результати дозволяють модифікувати алгоритм методу виявлення розмиття цифрового зображення. Виконана модифікація дозволяє виявити наявність несанкціонованого доступу до цифрового зображення. Модифікований алгоритм є не менш ефективним в порівнянні з оригіналом і при цьому дозволяє аналізувати меншу кількість параметрів за коротший час. Обчислювальна складність алгоритму визначається поліномом другого степеня, що є прийнятним з точки зору його практичного застосування.

Ключові слова: цифрове зображення, розмиття, порушення цілісності, сингулярні числа, цифрові докази, цифрова криміналістика.

АНАЛИЗ И МОДИФИКАЦИЯ АЛГОРИТМА ВЫЯВЛЕНИЯ РАЗМЫТИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

В.В. Зорило, Е.Ю. Лебедева, П.С. Сафронов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vikazorilo@gmail.com,
o.y.lebedieva@opu.ua

Использование цифровых изображений в современном обществе настолько распространено, что трудно назвать отрасль, где бы их не применяли. Однако в определенных ситуациях цифровые изображения могут быть прямыми или косвенными цифровыми доказательствами, например, в судебных делах. Подделка или нарушение целостности цифровых изображений - одна из важных проблем защиты информации. Перед специалистами по кибербезопасности сегодня остро стоит вопрос проверки подлинности цифровых сигналов. Таким образом, разработка методов и алгоритмов выявления нарушений целостности цифровых сигналов вообще и цифровых изображений в частности является очень актуальной темой. Среди всех возможных вариантов нарушения целостности цифровых изображений можно выделить отдельную группу - применение обработки различными фильтрами графических редакторов, таких как размытие, повышение резкости и тому подобное. Размытие довольно часто применяют к изображениям не только при их фальсификации, но и как стеганографической атаку. Выявление размытия указывает на невозможность использования цифрового изображения в качестве доказательства чего-либо. Один из самых эффективных методов выявления размытие, известных из открытого печати, это метод, основанный на анализе сингулярных чисел блоков матрицы цифрового изображения. Целью данной работы является повышение эффективности выявления размытия цифрового изображения путем модификации алгоритма, основанного на анализе сингулярных чисел. В работе проведен вычислительные эксперименты по установлению количества параметров, проверяемых. Полученные результаты позволяют модифицировать алгоритм метода выявления размытия цифрового изображения. Выполненная модификация позволяет выявить наличие несанкционированного доступа к цифрового изображения. Модифицированный алгоритм не менее эффективным по сравнению с оригиналом и при этом позволяет анализировать меньшее количество параметров за более короткое время. Вычислительная сложность алгоритма определяется полиномом второй степени, что является приемлемым с точки зрения его практического применения.

Ключевые слова: цифровое изображение, размытие, нарушения целостности, сингулярные числа, цифровые доказательства, цифровая криминалистика.

УДК 004.942:615.82

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 96-105

РОЗРОБКА ІНФОРМАЦІЙНОЇ МОДЕЛІ ОПОРИ ДЛЯ ХОДЬБИ ДІТЕЙ ХВОРИХ НА ДЦП

В.М. Тігарєв, В.І. Салій, Ю.І. Бабич, К.В. Кіценко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044,Україна; e-mail: volodymyr_t@ukr.net, svi099svi@gmail.com

Інформаційне проектування інженерних об'єктів базується на використанні інформаційних моделей об'єктів. Інформаційна модель спрощує розробку алгоритму проектування та прискорює процес виготовлення об'єкта. Метою роботи є розробка інформаційної моделі та її застосування для створення адаптивно-параметричної моделі об'єкта. Проведено аналіз існуючих моделей опори та виявлено їх переваги та недоліки. Запропоновано прототип конструкції, який відповідає вимогам успішної соціально-побутової адаптації дитини. У статті запропоновано технологію створення інформаційної моделі опори для ходьби дітей, хворих на ДЦП, та докладно розглянуто вісім рівнів проектування опори з використанням інформаційної моделі. Розроблено адаптивно-параметричну модель опори в сучасній САПР Autodesk Inventor Professional, яка розраховує та модифікує конструкцію залежно від вхідних антропометричних даних дитини (вага та зріст). Виявлено залежності розмірів конструктивних елементів опори від антропометричних даних дитини, які були наведені в табличній формі. В роботі було проведено моделювання статичних і динамічних навантажень на створену конструкцію та досліджено вплив механічних навантажень на її елементи. Результати моделювання навантажень дозволяють оптимізувати та удосконалити конструкцію шляхом зміни кількості стійок та вибору матеріалу, з якого буде виготовлено об'єкт. Запропонована інформаційна модель може бути використана для різних інженерних об'єктів. Використання інформаційної моделі скорочує час і підвищує надійність проектування об'єкта. Подальшим розвитком роботи є створення програмного додатку для автоматизації проектування в середовищі iLogic САПР Autodesk Inventor Professional на основі отриманої інформаційної моделі.

Ключові слова: інформаційна модель, параметризація, адаптивно-параметрична модель, статичні навантаження, динамічні навантаження.

Вступ

В сучасному світі проектування об'єкту починається з інформаційної моделі об'єкту, яка уточнюється і доповнюється в процесі проектування. При створенні інформаційної моделі обов'язково використовується комп'ютерна математична модель, яка описує сам об'єкт та етапи його проектування, аналізу та виготовлення. Інформаційна модель повинна містити методологію і технологію створення об'єкта. Розроблено інформаційну модель опори для ходьби дитини хворої на дитячий церебральний параліч. Дана модель дозволить розробити алгоритм проектування об'єктів аналогічного дизайну. Опору для ходьби спроектовано так, щоб вона витримувала вагу дитини, а також всі необхідні для цього навантаження без надмірних відхилень. Проектування опори для ходьби дитини хворої на ДЦП з використанням сучасних комп'ютерних технологій дозволяє скоротити час, підвищити точність, створити комп'ютерну модель для аналізу механічних навантажень. Комп'ютерну модель опори ходьби зручніше реалізовувати за допомогою САПР Autodesk Inventor Professional, яка дозволяє створити тривимірну модель опори для ходьби та виконати її параметризацію, а також дозволяє аналізувати створену модель на необхідні статичні та динамічні навантаження.

Формування ефективної ходи є пріоритетним завданням реабілітації пацієнтів, адже хода є важливою передумовою успішної соціально-побутової адаптації дитини [1] Розглядаючи це питання з точки зору освоєння технічних засобів реабілітації в лікувальну фізіотерапію слід включати максимально різноманітні рухи з самого раннього віку. Одним із засобів формування ходи є тренування на ходунках з підтримкою ваги тіла [1-3], які розроблені спеціально для полегшення пересування хворих з порушенням функцій опорно-рухового апарату і сконструйовані з урахуванням усіх вимог.

Мета роботи

Метою роботи є розробка адаптивно-параметричної моделі опори для ходьби дитини хворої на дитячий церебральний параліч на основі інформаційної моделі інженерного об'єкту.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

- розробка інформаційної моделі опори для ходьби дитини хворої на ДЦП
- вибір моделі опори для ходьби та її реалізація в середовищі сучасної САПР;
- виявити та усунути недоліки моделі, пов’язані зі зручністю та безпекою для хворої дитини;
- розробити адаптивно-параметричну модель опори для ходьби;
- провести аналіз розробленої моделі на статичні та динамічні навантаження.

Основна частина

Запропоновано інформаційну модель опори для ходьби дитини хворої на ДЦП, яка включає в себе всі необхідні рівні і взаємозв'язки між ними. Блок-схема інформаційної моделі наведена на рисунку 1. Розглянемо докладно все рівні інформаційної моделі та їх взаємозв’язки.

Рівень аналізу існуючих аналогів. На цьому рівні виконується аналіз існуючих моделей опори для ходьби та обирається прототип конструкції.

Рівень моделювання деталей. Всі деталі опори для ходьби створюються за допомогою команд просторового моделювання сучасної САПР. Моделі деталей є параметричними, оскільки всі розміри пов'язані та розміщені в таблицю параметрів моделі.

Рівень створення складального вузла. Створення тривимірної моделі складального вузла опори для ходьби шляхом накладення зв'язків та залежностей.

Рівень параметризації. Накладення параметричних залежностей.

Рівень симуляції навантажень. Проведення моделювання статичних та динамічних навантажень на опору для ходьби із зусиллями близькими до максимального значення сили дитини, враховуючи її вагу.

Рівень оптимізації. На основі результатів, які отримали шляхом симуляції навантажень на опору, оптимізуємо створену модель та обираємо матеріал, з якого буде реалізована модель.

Рівень підготовки до виготовлення. Створення комплекту конструкторської документації опори для ходьби необхідного для його виготовлення.

Рівень тестування та експлуатації. Виготовлення дослідного зразка.

Докладно розглянемо всі рівні інформаційної моделі при створенні адаптивно-параметричної тривимірної моделі опори для ходьби дитини хворої на ДЦП.

На першому рівні було проведено докладний аналіз конструкції обраної моделі опори для ходьби та порівняно її з більш дорогими аналогами.

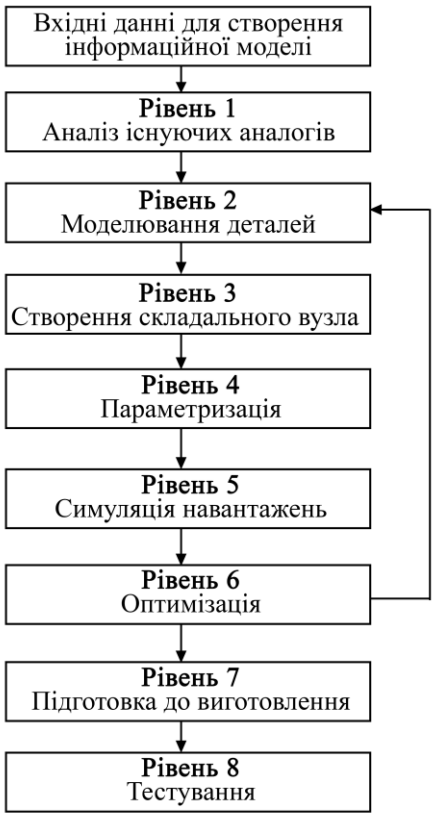


Рис. 1. Блок-схема інформаційної моделі

Проблема дитячого церебрального паралічу (ДЦП) хвилює весь цивілізований світ і цього неможливо не помічати. Адже правильно проведена реабілітація допоможе уникнути сильних відхилень у розвитку дитини та допоможе повернути його в середовище однолітків [3] Процес реабілітації не тільки складний та довгостроковий, а й достатньо дорогий. Всі технічні засоби, які при цьому використовують, мають дуже високу вартість, тому було розглянуто найпростіші ходунки (рис. 2), які не тільки допомагають дитині розвинути правильну ходу та поставу, а також допомагають бути більш самостійним у повсякденному житті [3].

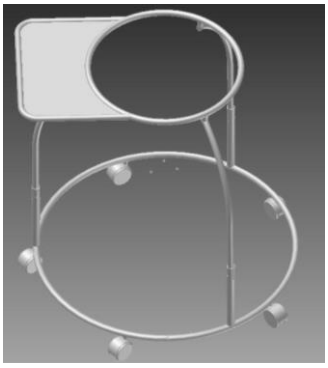


Рис. 2. Найпростіший вид опори для ходьби дитини хворою на ДЦП

В результаті якого було виявлено значні недоліки:

- при наїзді навіть на незначну перешкоду (наприклад, шви на підлозі) ходунки різко зупиняються та перегортаються через конструкцію коліс (рис. 2);
- ходунки з колесами даного типу важче зрушити з місця;
- невдале розташування коліс призводило до того, що при русі назад ноги дитини потрапляють під переднє колесо;

- наявність тільки трьох стійок збільшують вірогідність перегортання опори при різких рухах та зупинці;
- не реалізована можливість зміни висоти конструкції.

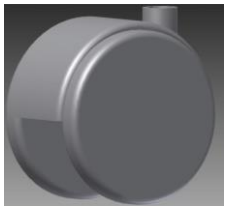


Рис. 3. Колесо опори для ходьби, конструкція якого виявилась невдалою

Для ліквідації недоліків було запропоновано:

- повна зміна конструкції колеса (рис. 4г);
- скорочення кількості коліс до чотирьох та зміна їх розташування;
- збільшення кількості стійок до чотирьох, що допомагає краще тримати рівновагу та збільшує міцність конструкції;
- висота конструкції регулюється за допомогою системи кріплень.

На другому рівні виконуємо моделювання всіх деталей опори для ходьби. При створенні моделей використовуються параметричні 2D ескізи, всі розміри пов'язані та розміщені в таблиці параметрів моделі.

Технологія створення опори для ходьби дітей страждаючих на ДЦП з урахуванням зазначених вище недоліків в середовищі сучасної САПР Autodesk Inventor Professional наступна:

Крок 1. Побудова деталі «Столик» відбувається в середовищі «Проектування рам», в процесі чого необхідно врахувати де будуть місця стиків із стійками (рис. 4а).

Крок 2. Побудова деталі «Основа» відбувається в середовищі «Проектування рам», в процесі чого необхідно врахувати де будуть місця стиків із стійками та колесами для зручності формування майбутнього складального вузла (рис. 4б).

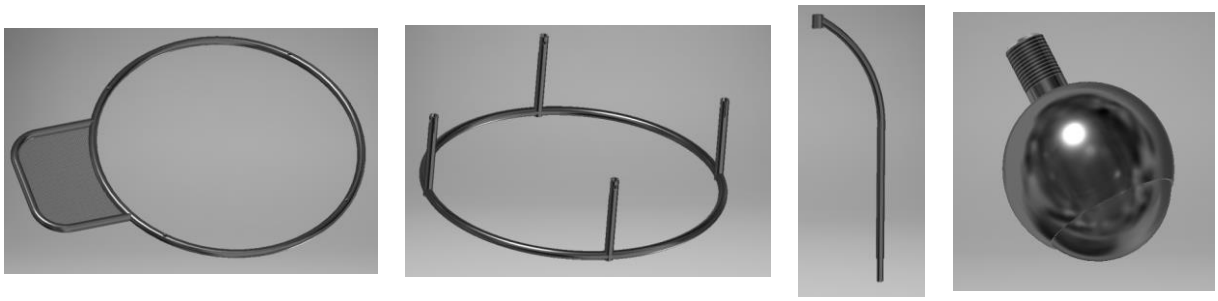
Крок 3. Побудова деталі «Стійка», яка з'єднує деталі «Столик» та «Основу», відбувається в середовищі «Проектування рам» (рис. 4в, 5).

Крок 4. Створення деталі «Колесо» (рис. 4г).

Крок 5. Наступним етапом буде об'єднання усіх складових частин опори для ходьби в єдиний складальний вузол (рис. 6).

Крок 6. Розробка адаптивно-параметричної моделі (рис. 7).

Крок 7. Симуляція статичних та динамічних навантажень на створену модель.



а б в г

Рис. 4. Комп'ютерні моделі складових частин опори для ходьби, які були створені в середовищі сучасної САПР Autodesk Inventor Professional: а – деталь «Столик»; б – деталь «Основа»; в – деталь «Стійка»; г – деталь «Колесо»

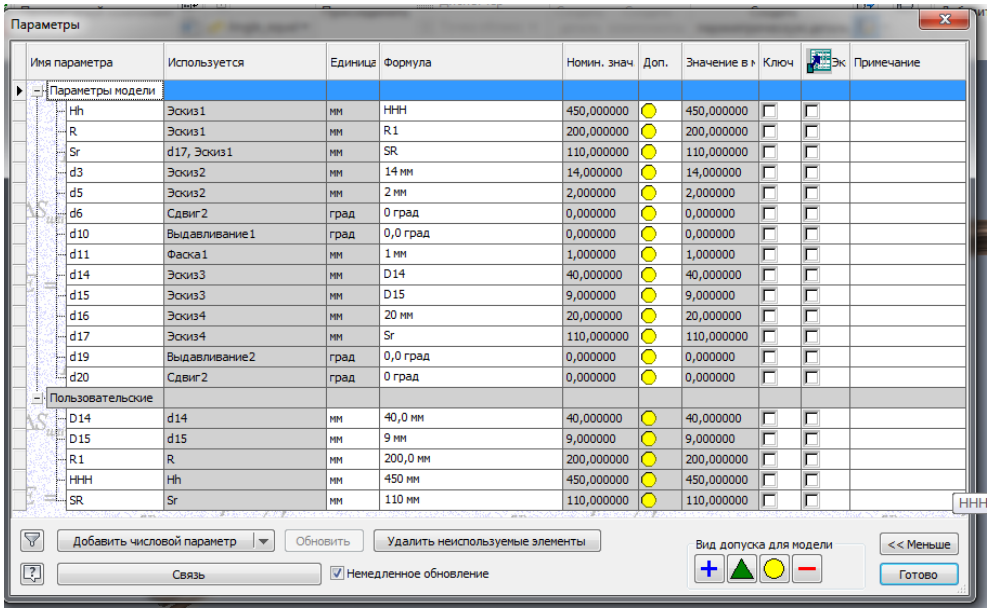


Рис. 5. Вікно таблиці параметрів моделі деталі «Стійка»

Четвертим рівнем буде розробка адаптивно-параметричної моделі опори для ходьби дитини з ДЦП в середовищі програми Autodesk Inventor Professional. Модель ходунків змінюється залежно від антропометричних даних дитини, які приведені в таблиці 1, [4] що дає можливість розробки оптимальної конструкції для кожної дитини.

Перерахунок здійснюється таким чином:

Крок 1. Завдання ваги дитини змінює діаметри труб «Основи», «Столика» та «Стійки», а також кількість стійок (табл. 2).

Рис. 6. Удосконалена модель опори для ходьби дитини хворою на ДЦП порівняно з аналогічними моделями представленими на ринку

Таблиця 1.

Антропометричні данні дітей віком від 1 до 10 років

Вік	Вага	Зріст
1 – 3	10 – 15	75 – 95
3 – 5	15 – 20	95 – 110
5 – 7	20 – 25	110 – 125
7 – 10	25 – 30	125 – 140

Таблиця 2.

Параметри опори, які залежать від ваги дитини

Вага	$D_{труб}$	$I_{стійок}$
10 – 15	10	4
15 – 20	12	4
20 – 25	14	4
25 – 30	14	6

Крок 2. Завдання зросту дитини змінює довжину стійок (табл. 3).

Таблиця 3.

Параметри довжини стійки, які залежать від зросту дитини

Зріст	$L_{стійки}$
75 – 95	30
95 – 110	45
110 – 125	60
125 – 140	85

Крок 3. Залежно від обох параметрів (вага та зріст) змінюються діаметри кіл «Основи» та «Столика» (табл. 4).

Таблиця 4.

Параметри конструкції опори, які одночасно залежать від ваги та зросту дитини

Вага	Зріст	$D_{столика}$	$D_{основи}$
10 – 15	75 – 95	30	60
15 – 20	95 – 110	40	70
20 – 25	110 – 125	45	85
25 – 30	125 – 140	50	95

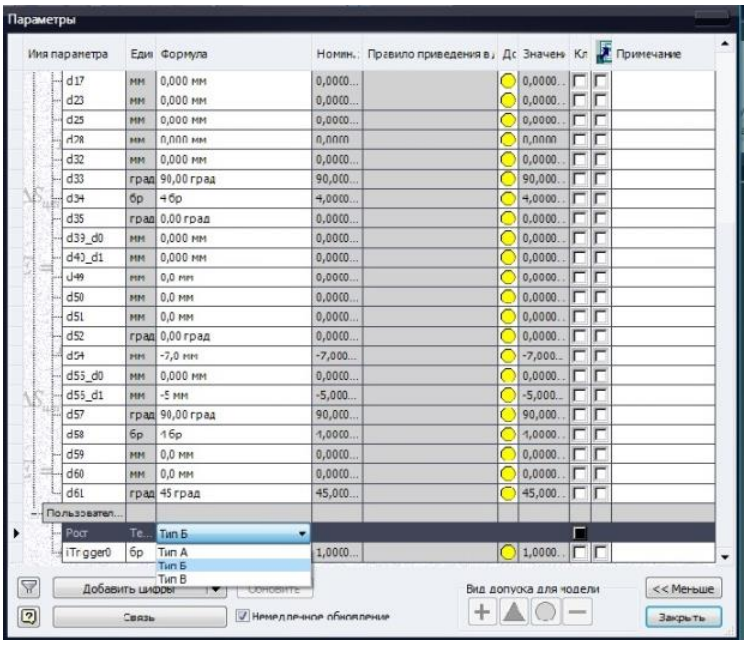


Рис. 7. Вікно таблиці параметрів моделі опори для ходьби дитини хворої на ДЦП

На п'ятому рівні інформаційної моделі виконуємо дослідження створеної опори на деформацію та стійкість під впливом навантажень відбувається в середовищі програми Autodesk Inventor Professional. Дане дослідження моделює стан моделі в певних умовах, що дозволяє виявити та виправити недоліки ще на стадії проектування [5] При проектуванні опори для ходьби важливо врахувати всі можливі навантаження для гарантування безпеки [5] в процесі реабілітації дитини, а також зробити цей процес максимально зручним. Щоб конструкція опори була безпечною та зручною під час використання, вона має бути достатньо міцною та легкою одночасно. Тому було проведено моделювання статичних (рис. 8) та динамічних (рис. 9) навантажень на опору із зусиллям близьким до максимального значення сили дитини, враховуючи її вагу.

Моделювання навантажень на конструкцію опори дозволяє проаналізувати велику кількість параметрів, за допомогою яких можливо зробити правильні висновки і вибрати оптимальні параметри моделі.

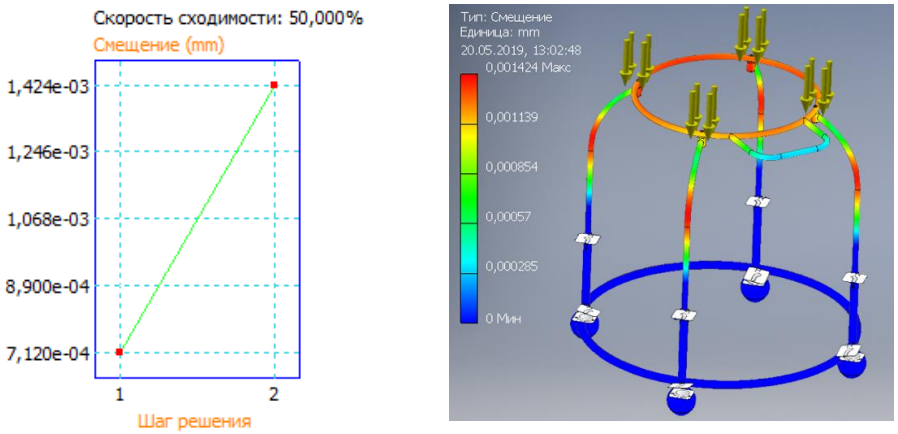


Рис. 8. Результат симуляції статичних навантажень на математичну комп'ютерну модель опори для ходьби дитини хворої на ДЦП

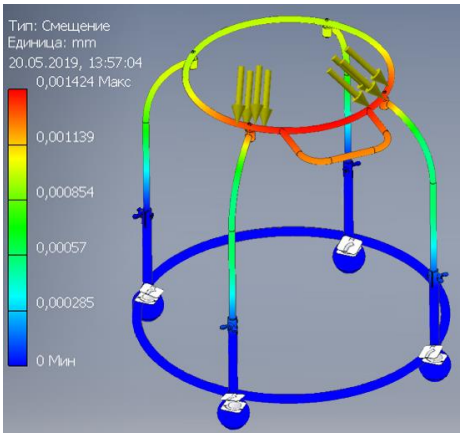


Рис. 9. Результат симуляції динамічних навантажень на математичну комп'ютерну модель опори для ходьби дитини хворої на ДЦП

Шостим рівнем інформаційної моделі є оптимізація. В процесі дослідження для несучої конструкції моделі були призначені різні матеріали (алюміній, сталь). В результаті чого було визначено, що оптимальними матеріалами для конструкції є алюміній або його сплави, за рахунок своєї легкості та достатньої міцності. Аналізуючи результати симуляції на міцність із зусиллям близьким до максимального значення сили дитини, враховуючи її вагу, робимо висновок, що наша конструкція достатньо міцна для використання (рис. 10).

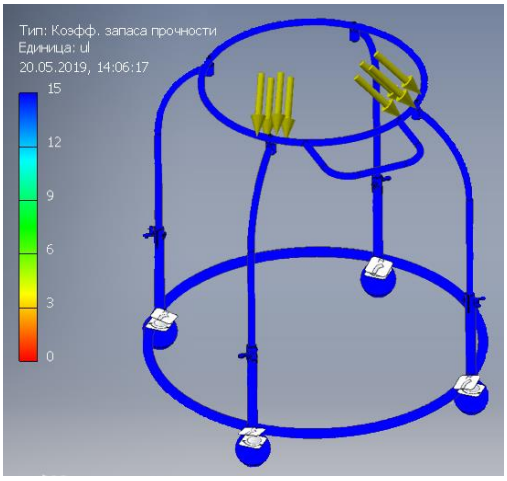


Рис. 10. Аналіз на міцність математичної комп'ютерної моделі опори для ходьби дитини хворої на ДЦП

На сьомому рівні виконуємо підготовку об'єкта до виготовлення, для чого створюємо необхідний комплект конструкторської документації моделі [6]. Восьмим рівнем інформаційної моделі є виготовлення дослідного зразка та введення в експлуатацію об'єкта.

Розроблена адаптивно-параметрична модель дозволяє мінімізувати витрати часу та матеріалів на конструювання та виготовлення опори для ходьби дитини хворої на ДЦП та в режимі реального часу вносити зміни в конструкцію, залежно від антропометричних даних. При моделюванні статичних та динамічних навантажень на опору для ходьби із зусиллям близьким до максимального значення сили дитини, враховуючи її вагу, були отримані результати (рис. 8, рис. 9). Докладний аналіз результатів показує, що запропонована конструкція виявилась достатньо стійкою та міцною, щоб витримати необхідні навантаження. Порівняно з найдешевшим зразком опори для ходьби (рис. 2) розроблена конструкція є більш зручною, практичною та безпечною.

Висновки

У статті розглянуто загальний підхід до створення та аналізу інформаційної моделі опори для ходьби. Докладно викладена методика та технологія створення тривимірної адаптивно-параметричної моделі опори для ходьби в САПР Autodesk Inventor Professional на основі запропонованої інформаційної моделі. Проведено аналіз та виявлені недоліки існуючої конструкції ходунків, у результаті було удосконалено конструкцію шляхом зміни типу коліс, їх кількості та розташування, а також модифікація стійок, їх кількості. З урахуванням внесених змін розроблено адаптивно-параметричну модель ходунків та проведено моделювання статичних та динамічних навантажень на неї. На основі проведених досліджень запропоновано оптимальний варіант матеріалу, з якого в подальшому буде виготовлятися конструкція. Створена адаптивно-параметрична модель дозволяє інтерактивно модифікувати параметри таким чином, щоб ходунки змінювалися залежно від ваги та зросту дитини. Інформаційна модель дає можливість скоротити час і підвищити надійність проектування об'єкту. Подальшим розвитком роботи є створення програмного додатку для автоматизації проектування ходунків в середовищі iLogic САПР Autodesk Inventor Professional. Для чого буде використана адаптивно-параметрична модель, яка створена на базі інформаційної моделі. На підставі проведеної розробки конструкції та досліджень моделі на навантаження буде створено дослідний зразок.

Список літератури:

1. Бадалян, Л.О. Детская неврология / Л.О. Бадалян. – М.: МЕДПРЕСС-Информ, 2002. – 608 с.
2. Лайшева, О.А. Ремоделирование двигательного акта в реабилитации детей с детским церебральным параличом: Дис. докт. мед. наук. – 2007.
3. Детский церебральный паралич [Электронный ресурс] // Режим доступа: http://neuroreha.ru/detskij-cerebralnyj-paralich.
4. The WHO Child Growth Standards. Mode of access: https://www.who.int/ childgrowth/standards/en/.
5. Analysis and Simulation. Mode of access: https://knowledge.autodesk.com/support/ inventor-products/learn-explore/caas/CloudHelp/ cloudhelp/2018/ENU/Inventor-Help/ files/GUID-B6101620-E1A5-467B-AF45-011E2BEDAA9F-htm.html (Date:18.04.2018).
6. Inventor Help. Mode of access: http://help.autodesk.com/view/INVNTOR/2019/ENU.

DEVELOPMENT OF THE INFORMATION MODEL SUPPORT FOR CHILDREN OF PATIENTS WITH CALCULATIONS

V.M. Tigariev, V.I. Salii, Y.I. Babych, K.V. Kitsenko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: volodymyr_t@ukr.net

Information design of engineering objects is based on the use of information models of objects. The information model simplifies the design of the algorithm and accelerates the process of manufacturing the object. The aim of the work is to develop an information model and its application for creating an adaptive-parametric model of an object. The analysis of existing models of support was carried out and their advantages and disadvantages were revealed. The prototype of the design, which meets the requirements of successful social and everyday adaptation of the child, is proposed. In the article the technology of creation of the information model of support for walking of children with cerebrovascular disease is offered and in detail the eight levels of designing the support using the information model are considered. The adaptive-parametric model of support in the modern CAD Autodesk Inventor Professional is developed, which calculates and modifies the structure depending on the incoming anthropometric data of the child (weight and height). Dependences of sizes of structural elements of support from anthropometric data of the child, which were given in tabular form, were revealed. In the work modeling of static and dynamic loads on the created construction was conducted, and the influence of mechanical loads on its elements was investigated. The results of load simulation allow optimizing and improving the design by changing the number of racks and selecting the material from which the object will be made. The proposed information model can be used for various engineering objects. Using the information model reduces the time and increases the reliability of the design of the object. Further development of work is the creation of a software application for automation of designing in the iLogic environment of CAD Autodesk Inventor Professional on the basis of the received information model.

Keywords: information model, parameterization, adaptive-parametric model, static load, dynamic load.

РАЗРАБОТКА ИНФОРМАЦИОННОЙ МОДЕЛИ ОПОРЫ ДЛЯ ХОДЬБЫ ДЕТЕЙ БОЛЬНЫХ ДЦП

В.М. Тигарев, В.И. Салий, Ю.И. Бабич, Е.В. Киценко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044,Украина; e-mail: volodymyr_t@ukr.net,
svi099svi@gmail.com

Информационное проектирование инженерных объектов базируется на использовании информационных моделей объектов. Информационная модель упрощает разработку алгоритма проектирования и ускоряет процесс изготовления объекта. Целью работы является разработка информационной модели и ее применение для создания адаптивно-параметрической модели объекта. Проведен анализ существующих моделей опоры и выявлены их преимущества и недостатки. Предложено прототип конструкции, отвечающий требованиям успешной социально-бытовой адаптации ребенка. В статье предложена технология создания информационной модели опоры для ходьбы детей, больных ДЦП, и подробно рассмотрено восемь уровней проектирования опоры с использованием информационной модели. Разработан адаптивно-параметрическую модель опоры в современной САПР Autodesk Inventor Professional, которая рассчитывает и модифицирует конструкцию в зависимости от входных антропометрических данных ребенка (вес и рост). Выявлены зависимости размеров конструктивных элементов опоры от антропометрических данных ребенка, которые были приведены в табличной форме. В работе было проведено моделирование статических и динамических нагрузок на созданную конструкцию и исследовано влияние механических нагрузок на ее элементы. Результаты моделирования нагрузок позволяют оптимизировать и усовершенствовать конструкцию путем изменения количества стоек и выбора материала, из которого будет изготовлено объект. Предложенная информационная модель может быть использована для различных инженерных объектов. Использование информационной модели сокращает время и повышает надежность проектирование объекта. Дальнейшим развитием работы является создание программного приложения для автоматизации проектирования в среде iLogic САПР Autodesk Inventor Professional на основе полученной информационной модели.

Ключевые слова: информационная модель, параметризация, адаптивно-параметрическая модель, статические нагрузки, динамические нагрузки.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 9, номер 1-2, 2019. Одеса – 106 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 9, номер 1-2, 2019. Одесса – 106 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 9, No. 1-2, 2019. Odesa – 106 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 26.03.2019)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com