ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.932.1.056.55 **doi: 10.32620/reks.2022.1.11**

Vladimir BARANNIK[1], Serhii SIDCHENKO[2], Dmitriy BARANNIK[3], Andrii YERMACHENKOV[4], Maksym SAVCHUK [4], Gennady PRIS[4]

[1] *V. N. Karazin Kharkiv National University, Kharkiv, Ukraine*
[2] *Ivan Kozhedub National Air Force University, Kharkiv, Ukraine*
[3] *Kharkiv National University of Radio Electronics, Kharkiv, Ukraine*
[4] *Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine*

VIDEO IMAGES' COMPRESSION METHOD BASED ON FLOATING POSITIONAL CODING WITH AN UNEQUAL CODOGRAMS LENGTH

The subject of research *is the video images' compression and encryption processes during the critically important objects managing process.* ***The goal*** *is to develop a method for compressing video images based on floating positional coding with an uneven codegrams length to simultaneously ensure information reliability and confidentiality during its transmission with a given time delay.* ***Objectives****: analyzing existing approaches to ensuring the video images confidentiality; development a method for compressing video images based on floating positional coding with an uneven codegrams length; evaluate the developed method effectiveness. The* ***methods used are****: digital image processing methods, digital image compression methods, image encryption and scrambling methods, structural-combinatorial coding methods, statistical analysis methods. The following* ***results were obtained****. The technology of floating encoding of an uneven sequence of blocks is proposed. Code values are formed from the elements of different video image blocks. For this, a scheme for linearizing image point coordinates from its four-dimensional representation on a plane into a one-dimensional element coordinate in a vector has been developed. The four-dimensional element coordinate on the plane describes the image block coordinates and the coordinates of the element in this block. Code values are formed under conditions of controlling their binary representation's length. Simultaneously, coding is implemented for an indeterminate number of video image elements. The number of elements depends on the length of the code word. Accordingly, codegrams with an indeterminate length are formed. Their length depends on the service data values, generated during the encoding process. Service data act as a key element.* ***Conclusions****. The one-stage polyadic image encoding method in a differentiated basis has been further improved. The developed encoding method provides image compression without information quality loss. The original images volume compression was provided by 3–20 % better compared to the TIFF data presentation format and by 4–15 % compared to the PNG format. The overhead amount was less than 2.5 % of the entire codestream size***.**

Keywords: *authenticity; compression; confidentiality; encoding; encryption; image; lossless; video.*

1. Introduction

The formulation of the problem. Recently, video images are widely used for decision-making in the crisis infrastructure management and during their protection. The volume of images constantly grows and they are required to maintain maximum quality. Simultaneously, there are requirements for ensuring the video data confidentiality. Therefore, there is an urgent need to solve the ***scientific and applied problem*** of increasing video information confidentiality in terms of ensuring its reliability and accessibility.

The state of the art. There are various approaches to ensuring the images confidentiality, including:

– cryptographic protection methods based on data encryption. First, these are the block symmetric encryption algorithms [1–3] and algorithms with public key (asymmetric) encryption [4]. Additionally, schemes are adapted directly for image processing, for example, using reversible cellular automata [5]. These methods are usually used in sequential schemes for executing the compression and encryption functional [6, 7];

– cryptographic protection methods based on data scrambling [8, 9]. These are methods that are focused on processing uncompressed and compressed images. As a rule, chaotic maps are applied to uncompressed images [9, 10]. For example, Sudoku [11] and Rubik's cubic [12]. Ensuring the compressed images security focused on the compression standard features. In the JPEG 2000 technology, using the JPSEC functionality, it organizes wavelet-region coefficients signs scrambling and processing at the packet level [13, 14]. In the JPEG technology, privacy functionality is only being developed [15–17]. It is focused on scrambling of DCT coefficients [17–19] and processing at the packet

level [20–22]. Additionally, alternative schemes are also offered. For example, a non-format compliant scalable RSA-based JPEG encryption algorithm [23]. In other compression technologies, approaches to ensuring security are in the development stages. For example, the GIF format uses 3D Chaotic Baker maps [24];

– steganographic image processing methods to ensure both the built-in and the video data themselves security [25–27];

– using the sharing secrets technology to ensure one [28] or more images security [29–32];

– methods that implement the access rights policy and confidentiality management [8, 16–18];

– transformations that remove critical areas in images [8, 33, 34];

– geometrically inverse image distortions [35, 36].

But they all are characterized by significant problematic shortcomings, among which are the following:

– ensuring video data confidentiality without compression technologies using does not allow to create conditions to increase its accessibility;

– ensuring images confidentiality using compression technologies after and/or between data compression process stages is actually based on the encryption and compression functionality separation. This also reduces the video data availability;

– lack of complexing compression and cryptographic transformation methods, which affect video data availability;

– lack of methods based on non-deterministic encryption algorithm principles implementation and/or non-deterministic approaches to the processed data amount and location. This affects the cryptographic strength level.

To address these shortcomings, cryptocompression representation (CCR) methods have been developed. They are designed to simultaneously provide video information compression and protection. These methods are based on nonequilibrium-positional coding systems in the upper bounds basis [37] and differentiated basis [38]. The two-stage processing scheme was described in the study [39]. Decoding methods are described in the study [40]. Technological features are described in the studies [39, 41]. Articles [39, 42] consider the cryptocompression coding systems key parameters that affect the cryptographic stability and video data availability. Such parameters are the CCR images code constructions nondeterministic length and an uncertainty additional degree presence such as elements nondeterministic number involved in the cryptocompression codograms (CCCdg) formation. Considering these parameters, the service component systems coding method in a differentiated basis on the second stage of the CCR images was developed in the study [38]. The method basis is the developed data linearization scheme from three-dimensional coordinates of the representation in a two-dimensional matrix into a one-dimensional coordinate for a mutually unique element in the vector representation. Linearization is organized in the horizontal direction in rows. After the second coding stage, the generated service data CCCdg are encrypted on the basis camouflage video compression systems service data compression developed method [43].

However, the basic methods [37, 40] of the CCR images encoding the original video data do not fully take into account nondeterministic properties identified in [39–42] and are implemented in [38]. Therefore, it is necessary to develop a cryptocompression coding (CCC) method, which additionally uses the nondetermination property.

Thus, ***the article develops*** a cryptocompression images' coding method based on a floating nondeterministic processing scheme to ensure video data cryptographic stability while maintaining information specified quality without reducing its availability.

2. Development of Image Cryptocompression Method Based on Floating Positional Coding With Different Codegram Lengths

The frame of any original image has a dimension $M \times N$ elements where M is the number of lines in the image, and N is the number of columns, and consists of P planes. Thus, color images presented in RGB color space consist of three planes $P = 3$. Each plane is a two-dimensional matrix A dimension $M \times N$ elements.

The same processing type was organized for all planes. Plane A is divided into equal blocks $A^{(\gamma;\chi)}$, where γ is the block $A^{(\gamma;\chi)}$ coordinate in the plane A vertically, χ is a horizontal coordinate. Each block $A^{(\gamma;\chi)}$ dimension is defined as $m \times n$ elements where m is the row number in the processed block, and n is the column number. Dimensions m and n block $A^{(\gamma;\chi)}$ are chosen multiples of degree 2, i.e. $m, n \in 2, 4, 8, 16$. During handling process array $m \times n$ sides values are usually accepted equal, i.e. $m = n$.

The maximum value of the coordinate the block $A^{(\gamma;\chi)}$ variable vertically γ_{max} and horizontally χ_{max} is determined based on the ratio of dimensions $M \times N$ the processed plane A and dimensions $m \times n$ block $A^{(\gamma;\chi)}$, namely:

$$\gamma_{max} = [\frac{M}{m}], \qquad \chi_{max} = [\frac{N}{n}],$$

where $[\bullet]$ is an integer part number.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Every block $A^{(\gamma;\chi)}$ is a two-dimensional array of $a_{i,j}^{(\gamma,\chi)}$ elements. Here:

– i is the row of the element in $A^{(\gamma;\chi)}$ array, $i=\overline{1,m}$;

– j is the column of the element in $A^{(\gamma;\chi)}$ array, $j=\overline{1,n}$;

– $\gamma=\overline{1,[\frac{M}{m}]}$, $\chi=\overline{1,[\frac{N}{n}]}$;

– $A^{(\gamma;\chi)}=\{a_{i,j}^{(\gamma,\chi)}\}$.

Each item $a_{i,j}^{(\gamma,\chi)}$ contains information about brightness and can take values from 0 to 255.

Each processed plane A is two-dimensional elements $a_{i,j}^{(\gamma,\chi)}$ array $A=\{a_{i,j}^{(\gamma,\chi)}\}$, where is $\gamma=\overline{1,[\frac{M}{m}]}$, $\chi=\overline{1,[\frac{N}{n}]}$, $i=\overline{1,m}$, $j=\overline{1,n}$.

CCCdg formation begins with service components (SC) formation. To do this, in each block $A^{(\gamma;\chi)}$ of the lines direction determines:

– bases $\Lambda^{(\gamma;\chi)}=\{\lambda_i^{(\gamma,\chi)}\}$ systems, where $i=\overline{1,m}$. Basis $\lambda_i^{(\gamma,\chi)}$ for items of i-th line in the block $A^{(\gamma;\chi)}$ defines as the source block maximum line element by the formula:

$$\lambda_i^{(\gamma,\chi)}=\max_{1\le j\le n}(a_{i,j}^{(\gamma,\chi)}); \quad (1)$$

– lowering value systems dynamic range $\Theta^{(\gamma;\chi)}=\{\mu_i^{(\gamma,\chi)}\}$, where $i=\overline{1,m}$. Decreasing value $\mu_i^{(\gamma,\chi)}$ for i-th line in the block $A^{(\gamma;\chi)}$ items defined as the minimum value by the formula:

$$\mu_i^{(\gamma,\chi)}=\min_{1\le j\le n}(a_{i,j}^{(\gamma,\chi)}). \quad (2)$$

Each elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ can take values in the range $[0;255]$.

Base systems $\Lambda^{(\gamma;\chi)}=\{\lambda_i^{(\gamma,\chi)}\}$ and blocks $A^{(\gamma;\chi)}$ plane dynamic range $\Theta^{(\gamma;\chi)}=\{\mu_i^{(\gamma,\chi)}\}$ decreasing values are vector columns with m elements each. Two-dimensional data arrays $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta=\{\mu_i^{(\gamma,\chi)}\}$ are being formed. The size of these arrays is $M\times[\frac{N}{n}]$. Two-dimensional arrays Λ and Θ are SC CCR of the image for plane A. They contain information about the identified structural characteristics of the video data.

Data processing begins with the first block $A^{(\gamma;\chi)}$ with coordinates (1;1) and continues horizontally to the coordinate block $(1;[\frac{N}{n}])$. After that, the processing continues in the block with coordinates (2;1) in the horizontal direction and so on until the last block with coordinates $([\frac{M}{m}];[\frac{N}{n}])$ processing completes. Elements $a_{i,j}^{(\gamma,\chi)}$ inside block $A^{(\gamma;\chi)}$ are processed vertically. The element with coordinates (1;1) is processed first. After the element with coordinates (m;1) is processed, processing of the element with coordinates (1;2) begins. The last element to be processed in block $A^{(\gamma;\chi)}$ is the one with coordinates (m;n).

The next limitations are being considered:

- planes A have dimension $M\times N$;

- planes are uniformly partitioned into blocks $A^{(\gamma;\chi)}$. Each block has dimensions $A^{(\gamma;\chi)}$.

Then next condition is fulfilled:

$$[\frac{M}{m}]=\frac{M}{m}, \qquad [\frac{N}{n}]=\frac{N}{n}.$$

The two-dimensional matrix A is reformatted into a one-dimensional vector to organize floating coding:

$$A=\{a_\tau\}=\{a_{i,j}^{(\gamma,\chi)}\},$$

where $\tau=\overline{1,M\cdot N}$, $\gamma=\overline{1,[\frac{M}{m}]}$, $\chi=\overline{1,[\frac{N}{n}]}$, $i=\overline{1,m}$, $j=\overline{1,n}$,

where τ is the matrix A two-dimensional element $a_{i,j}^{(\gamma,\chi)}$ one-dimensional coordinate, which is reformatted into a one-dimensional vector for one-to-one correspondence.

To do this, the element $a_{i,j}^{(\gamma,\chi)}$ coordinates linearization performs. Reformatting consists in finding the τ coordinate of an element in a one-dimensional sequence, $\tau=\overline{1,M\cdot N}$. Simultaneously, the four-dimensional coordinates of the elements are considered. They are defined by:

- location (i; j) of elements in block $A^{(\gamma;\chi)}$;

- place $(\gamma;\chi)$ of the block in the image A.

This takes into account the data processing organization scheme in the process of CCR image plane. The following expression for this uses:

$$\tau = ((\gamma - 1)\cdot[\frac{N}{n}] + \chi - 1)\cdot m\cdot n + (j-1)\cdot m + i\,. \quad (3)$$

As a result of matrix A reformatting, the form of data representation changes. However, the data itself do not change. Its number remains unchanged and is equal to $M\cdot N$.

The reverse transformation involves determining the two-dimensional coordinates $(\gamma;\chi)$ and $(i;j)$ of element $a_{i,j}^{(\gamma,\chi)}$ on the basis of one-dimensional ones. The input elements are a_τ with a one-dimensional coordinate τ. The following expressions are used for transformation:

$$\gamma = [\frac{[\frac{\tau-1}{m\cdot n}]}{[\frac{N}{n}]}] + 1;$$

$$\chi = [\frac{\tau-1}{m\cdot n}] - [\frac{[\frac{\tau-1}{m\cdot n}]}{[\frac{N}{n}]}]\cdot[\frac{N}{n}] + 1;$$

$$i = \tau - [\frac{\tau-1}{m\cdot n}]\cdot m\cdot n - [\frac{\tau-1-[\frac{\tau-1}{m\cdot n}]\cdot m\cdot n}{m}]\cdot m;$$

$$j = [\frac{\tau-1-[\frac{\tau-1}{m\cdot n}]\cdot m\cdot n}{m}] + 1.$$

The reformatting of the two-dimensional components $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$, $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ of base systems into one-dimensional sequences is carried out on the basis of expression (3). This takes into account that $j = \overline{1,n}$. This takes into account the data processing in the CCC process organization scheme.

As a result, the three-dimensional coordinates of elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ are converted into one-dimensional. Here the vectors $\Lambda = \{\lambda_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}\}$, $\Theta = \{\mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}\}$, $\tau = \overline{1, M\cdot N}$ are formed.

These vectors consist, respectively, of elements with coordinates:

- from λ_1 to $\lambda_{M\cdot[\frac{N}{n}]}$;
- from μ_1 to $\mu_{M\cdot[\frac{N}{n}]}$.

Reformatting two-dimensional matrices Λ and Θ into one-dimensional vectors has such features:

- values of the elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ do not change;
- their number does not change. In each vector, this number is determined by the value $M\cdot[\frac{N}{n}]$.

It is necessary to provide a one-to-one correspondence between fragment elements and service data. To do this, it is proposed to expand components Λ, Θ of the base system to the power of the image plane. Here, it should be considered that the planes are represented in a one-dimensional vector form.

To do this, the column vectors $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$ are transformed into a two-dimensional matrix $\Lambda'^{(\gamma,\chi)}$ and $\Theta'^{(\gamma,\chi)}$, respectively.

Transformation process is organized by repeating the corresponding column vectors $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$ by n times. Two-dimensional matrices $\Lambda'^{(\gamma,\chi)}$, $\Theta'^{(\gamma,\chi)}$ consist of elements $\lambda'^{(\gamma,\chi)}_{i,j}$, $\mu'^{(\gamma,\chi)}_{i,j}$ accordingly. The value of elements is calculated by expressions:

$$\lambda'^{(\gamma,\chi)}_{i,j} = \lambda_i^{(\gamma,\chi)} \text{ and } \mu'^{(\gamma,\chi)}_{i,j} = \mu_i^{(\gamma,\chi)} \text{ at } j = \overline{1,n}\,.$$

As a result, bases Λ' and lowering values Θ' systems forms which dimension is equal to processed plane A, namely $M\times N$ elements.

Reformat service data systems Λ' and Θ' from two-dimensional matrices to one-dimensional vectors is performed using expression (3) on the image plane A two-dimensional matrix reformatting principle. As a result, one-dimensional vectors forms:

$$\Lambda' = \{\lambda'_\tau\} = \{\lambda'^{(\gamma,\chi)}_{i,j}\} = \{\lambda_i^{(\gamma,\chi)}\}_{j=\overline{1,n}},$$

$$\Theta' = \{\mu'_\tau\} = \{\mu'^{(\gamma,\chi)}_{i,j}\} = \{\mu_i^{(\gamma,\chi)}\}_{j=\overline{1,n}},\ \tau = \overline{1, M\cdot N}\,.$$

Based on the linearization of the coordinates according to expression (3), accordance is ensured between:

- coordinates τ of elements of SC systems Λ' and Θ';
- coordinates $\left(m\cdot[\frac{\tau-1}{m\cdot n}] + \tau - m\cdot[\frac{\tau-1}{m}]\right)$ of elements of SC Λ and Θ.

Such accordance is described as:

$$\lambda'_\tau = \lambda_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]} = \lambda_i^{(\gamma,\chi)},\ \tau = \overline{1, M\cdot N};$$

$$\mu'_\tau = \mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]} = \mu_i^{(\gamma,\chi)},\ \tau = \overline{1, M\cdot N}\,.$$

Code values (CV) E_α of the information component (IC) of the CCR image are formed for:

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

- vector representation of the plane A;

- advanced service data systems Λ' and Θ' (or Λ and Θ).

At the same time, coding is organized according to a floating scheme in a differentiated basis. The CV formation E_α process given by the following expressions:

$$E_\alpha = \sum_{\tau=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} \left\langle (a_\tau - \mu'_\tau)\cdot W_\tau \right\rangle = \sum_{\tau=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} \left\langle (a_\tau - \mu_{m\{\frac{\tau-1}{m\cdot n}\}+\tau-m\{\frac{\tau-1}{m}\}})\cdot W_\tau \right\rangle, \quad (4)$$

$$W_\tau = \begin{cases} \prod_{\xi=\tau+1}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi+1-\mu'_\xi) = \\ = \prod_{\xi=\tau+1}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}+1-\mu_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}), \\ \qquad\qquad \tau < \tau(0)_\alpha+\Psi_\alpha-1; \\ 1, \\ \qquad\qquad \tau = \tau(0)_\alpha+\Psi_\alpha-1, \end{cases} \quad (5)$$

where $\tau \in [\tau(0)_\alpha; \tau(0)_\alpha+\Psi_\alpha-1]$ and $\tau(0)_\alpha+\Psi_\alpha-1 \le M\cdot N$,

where α is a formed CV serial number E_α IC CCCdg;

τ, ξ – linear vector coordinates that determines the data processed in the encoding process position;

$\tau(0)_\alpha$ – the processed plane A element a_τ starting coordinate in the vector form from which the CV E_α formation of the begins;

Ψ_α – floating (indeterminate) plane A elements a_τ number involved in the CV E_α formation;

W_τ – weighting factor for τ-th element a_τ, which is the product of the following bases λ'_ξ elements, taking into account their dynamic ranges reduction by μ'_ξ.

The starting parameters for the first CV E_α are calculated as follows:

– the CV serial number is equal to $\alpha = 1$;

– first element a_τ starting coordinate is equal to $\tau(0)_1 = 1$.

The following starting parameters for the new CV IC formation determines as follows:

– CV serial number increases by one $\alpha = \alpha + 1$;

– starting coordinate $\tau(0)_\alpha$ determines based on:

a) value of coordinate $\tau(0)_{\alpha-1}$ for the previous CV $E_{\alpha-1}$;

b) current amount $\Psi_{\alpha-1}$ of elements a_τ.

This is described by the formula:

$$\tau(0)_\alpha = \tau(0)_{\alpha-1} + \Psi_{\alpha-1}. \quad (6)$$

For the CV E_α IC formation involved are plane A elements a_τ with coordinates $\tau \in [\tau(0)_\alpha; \tau(0)_\alpha + \Psi_\alpha - 1]$. The last CV formation ends after processing all the plane elements, namely $\tau(0)_\alpha + \Psi_\alpha - 1 \le M\cdot N$. After all the CV E_α formation they combine and form IC $E = \{E_\alpha\}$ for the processed plane.

Number Ψ_α of plane A elements a_τ involved to the CV E_α formation, are non-deterministic and depends on the processed data values. It is determined based on the condition that the formation of the CV E_α should not lead to code word overflow (CW) L_{cw}, which is allocated for its storage, i.e.:

$$E_\alpha \le 2^{L_{cw}} - 1,\ \log_2(E_\alpha) \le L_{cw}, \quad (7)$$

where $2^{L_{cw}} - 1$ is the largest number that can be stored in the CW by length of L_{cw} bit.

From the analysis of expressions (4) and (5), the conditions for fulfilling inequality (7) follow. They consist in controlling the accumulated product of bases λ'_ξ considering:

- amount Ψ_α of elements in CV;

- reduced dynamic range μ'_ξ.

This is described as:

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi+1-\mu'_\xi) \le 2^{L_{cw}} - 1, \quad (8)$$

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}+1-\mu_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}) \le 2^{L_{cw}} - 1. \quad (9)$$

In practice, to eliminate the error associated with the CW overflow, instead of condition (8) or (9) it is better to use the following inequalities:

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi+1-\mu'_\xi) \le \frac{2^{L_{cw}} - 1}{\lambda'_{\tau(0)_\alpha+\Psi_\alpha}+1-\mu'_{\tau(0)_\alpha+\Psi_\alpha}}, \quad (10)$$

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}+1-\mu_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}) \le \frac{2^{L_{cw}} - 1}{\lambda_{m\{\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}\}+(\tau(0)_\alpha+\Psi_\alpha)-m\{\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}\}}+1-\mu_{m\{\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}\}+(\tau(0)_\alpha+\Psi_\alpha)-m\{\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}\}}} \quad (11)$$

provided that SC system $(\Psi_\alpha + 1)$-th element with the coordinate $(\tau(0)_\alpha + \Psi_\alpha) \le M \cdot N$ exists when checking condition (10) and with the coordinate

$$(m \cdot [\frac{\tau(0)_\alpha + \Psi_\alpha - 1}{m \cdot n}] + (\tau(0)_\alpha + \Psi_\alpha) - $$
$$- \; m \cdot [\frac{\tau(0)_\alpha + \Psi_\alpha - 1}{m}]) \le M \cdot [\frac{N}{n}]$$

when checking condition (11).

Elements Ψ_α number defined as:

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi + 1 - \mu'_\xi)$$

or

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}).$$

Value Ψ_α is an argument of this expressions when:

- their maximum value is reached;
- fulfillment of inequalities (10) or (11).

This is described by the formula:

$$\Psi_\alpha = \arg\max_{\Psi_\alpha}(\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi + 1 - \mu'_\xi)) =$$
$$= \arg\max_{\Psi_\alpha}(\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}} + 1 - \mu_{m\{\frac{\xi-1}{m\cdot n}\}+\xi-m\{\frac{\xi-1}{m}\}}). \quad (12)$$

Elements quantity Ψ_α determination algorithm, which describes the formulas (10)–(12) implementation organization rule, consists of the following stages.

At the previous stage, the introduction of initial parameters is organized. These include:

- sequence number α of CV E_α;
- starting coordinate $\tau(0)_\alpha$ of the first element a_τ;
- length of CW L_{cw}.

Counter of the number of elements involved in the formation of the CV E_α installed to $\Psi_\alpha = 1$.

Stage 1. At the first stage, the reading of the elements is organized λ'_τ, μ'_τ for SC Λ' and Θ'. Or $\lambda_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}$, $\mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}$ for Λ and Θ. Elements have the following properties:

- their coordinates vary between $\tau(0)_\alpha$ and $(\tau(0)_\alpha + \Psi_\alpha)$;
- they correspond to the a_τ elements of the A plane.

Stage 2. The second stage organizes CW L_{cw} overflow checking, allocated for CV E_α storage, in the case of adding another element with a coordinate $(\tau(0)_\alpha + \Psi_\alpha)$ (or

$$(m \cdot [\frac{\tau(0)_\alpha + \Psi_\alpha - 1}{m \cdot n}] + (\tau(0)_\alpha + \Psi_\alpha) -$$
$$- m \cdot [\frac{\tau(0)_\alpha + \Psi_\alpha - 1}{m}])).$$

Namely, the fulfillment of inequality (10) or (11) checks under the condition that the existing element of the SC system is added.

Stage 3. If conditions (10) or (11) met, then during the third stage the elements number counter value involved in the CV E_α formation, increases by 1, i.e. $\Psi_\alpha = \Psi_\alpha + 1$. After that we pass to perform the second stage.

Stage 4. If condition (10) or (11) is not fulfilled, then during the fourth stage it is determined that the number of elements that form the CV E_α, is equal to Ψ_α.

The formation of the CCCdg is organized in four steps. The floating coding scheme in the differentiated basis is considered as well.

Step 1. At the first step, which consists in preparing the initial data and determining the SC:

– output plane A divides into blocks $A^{(\gamma;\chi)}$, consists of $m \times n$ elements each;

– for blocks $A^{(\gamma;\chi)} = \{a_{i,j}^{(\gamma,\chi)}\}$ using formulas (1) and (2) determines the base system $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ and the dynamic range $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$ decreasing values that are vector columns with m elements of each. After processing all blocks $A^{(\gamma;\chi)}$ the resulting vector columns are combined into two-dimensional data sets $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta = \{\mu_i^{(\gamma,\chi)}\}$, dimension $M \times [\frac{N}{n}]$ elements each. These two-dimensional arrays Λ and Θ is an SC CCR image for a plane A;

- formula (3) organizes reformatting of two-dimensional matrices. This includes the following matrices:

a) image A;

b) data system services Λ and Θ;

c) extended data system services Λ' and Θ'.

As a result, corresponding one-dimensional vectors are formed;

– the starting parameters for the formation of CV E_α and the lengths of CW L_{cw}. These include:

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

a) sequence number of CV E_α, $\alpha = 1$;

b) starting coordinate of the first element, $\tau(0)_1 = 1$.

Step 2. The second step calculates the elements Ψ_α number involved to the CV E_α formation. To do this, the elements number counter installs to $\Psi_\alpha = 1$. Then stages 1-4 of the corresponding algorithm are performed.

Step 3. During the third step the CV E_α SC is formed on the basis of expressions (4) and (5). Code value E_α depends on:

– image plane $A = \{a_{i,j}^{(\gamma,\chi)}\}$;

– SC systems $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$.

Step 4. After the CV E_α formation, if not all plane elements $A = \{a_{i,j}^{(\gamma,\chi)}\}$ processed, i.e. $(\tau(0)_\alpha + \Psi_\alpha - 1) \neq M \cdot N$, then the new starting parameters for the new CV formation were determined, namely:

– the CV serial number increases by one $\alpha = \alpha + 1$;

– new start coordinate $\tau(0)_\alpha$ determined by formula (6).

After that, the second stage is performed.

Stage 5. If all plane elements $A = \{a_{i,j}^{(\gamma,\chi)}\}$ are processed, i.e. $(\tau(0)_\alpha + \Psi_\alpha - 1) = M \cdot N$, then all formed CV E_α combines and forms IC $E = \{E_\alpha\}$ for this plane. The last formed CV E_α sequence number α will match the quantity α_{max} of all CV E_α, which forms IS $E = \{E_\alpha\}$ for the plane A.

Writing elements in the code stream can be organized on the uniform or non-uniform length q_α CV E_α basis. Uniform length q_α corresponds to the length of the selected CW L_{cw}, ie $q_\alpha = L_{cw}$. The uneven length q_α is individual for each individual CV E_α. It is determined on the basis of the accumulated product of SC elements. Here systems Λ, Θ or Λ', Θ' are used. Length q_α depends on elements quantity Ψ_α using the formula:

$$q_\alpha = [\log_2 \prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi)] + 1 =$$

$$= [\log_2 \prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]})] + 1.$$

All α_{max} CV E_α total length determines by the formula:

$$q = \sum_{\alpha=1}^{\alpha_{max}} q_\alpha .$$

CCCdg image forms from the code structures obtained for each plane A with P planes, namely:

– information component $E = \{E_\alpha\}$;

– bases $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ systems;

– systems of dynamic range $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ lowering values.

Ensuring the video data cryptographic stability based on the developed method is provided by:

– formation CV E_α on variable elements a_τ quantity Ψ_α based on the CW L_{cw} overflow control. Elements a_τ number Ψ_α, which forms the CV E_α, depends only on the structure of the processed data;

– formation IC $E = \{E_\alpha\}$ using CV E_α. Code values are formed for uneven sequences with uneven lengths q_α. It is determined on the basis of the accumulated product of SC elements. Simultaneously, the number of elements is equal to Ψ_α. On the one hand, this reduces the overall length q IC $E = \{E_\alpha\}$. On the other hand, without knowledge of the SC Λ and Θ (Λ' and Θ') it is impossible to allocate each individual CV E_α from the total code stream of the IC $E = \{E_\alpha\}$;

– in fact CV E_α formation performs non-source involved elements a_τ, but its representation in the reduced dynamic range $(a_\tau - \mu'_\tau)$. This allows significantly increase elements number Ψ_α that forms the CV E_α, and reduce number α_{max} CV E_α IC $E = \{E_\alpha\}$;

– bases $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ and lowering the dynamic range $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ systems are subject to additional encryption and/or scrambling. The volume was much smaller than that of the original image.

Evaluation of the developed method effectiveness was carried out from the standpoint:

– reconstructed images quality assessments compared with the original;

– video data compression quality evaluation;

– SC CCCdg volumes estimates, which are subject to additional encryption;

– IC CCCdg statistical characteristics estimates.

The developed method of non-deterministic floating CCC of images is proposed to be used for the for-

mation of CCCdg. This forms the first stage of the corresponding conceptual method. Here, processing is carried out without loss of information. The relevant material is given in [37].

Therefore, we will evaluate the effectiveness in two directions:

- for a single-stage implementation scheme of the developed method;

- for a two-stage implementation scheme. Here, the use of the developed method in the process of formation of CCCdg is considered.

3. Results and Discussion

Coding methods without loss of information were used for comparison. The comparative evaluation was carried out according to the indicator of the reduction of video data volume. Simultaneously, encoding methods implemented in TIFF and PNG formats were chosen [44, 45].

The developed method, as well as control methods, does not make errors in the data during the coding process and refers to methods without loss of information quality.

The standard RSME deviation of all reconstructed images of different saturation classes of small objects and different sizes relative to the original video data is 0, and the correlation coefficient is 1.

The compression ratio of images based on single-stage and two-stage processing scheme estimates the results presented in Fig. 1. Here the processed data blocks dimension was performed at values $m = n = 8$. Specific results for some images shown in table. 1.

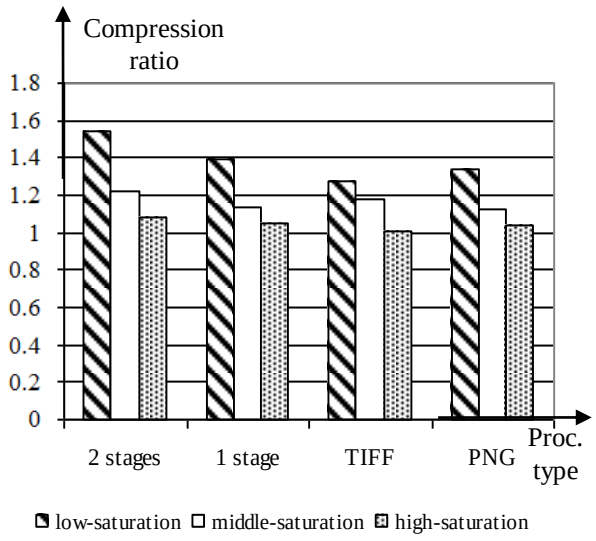

Fig. 1. The images compression ratio estimating the results

The analysis of the data in fig. 1 shows the following. The best result in terms of the degree of image compression was shown by the two-stage implementation scheme of the CCC image method. Simultaneously, images with different degrees of saturation were taken into account. The average value of the compression ratio is:

– for highly saturated images – at the level of 1.08 with decrease in data by 7.14 %;

– for medium-saturated images – at the level of 1.22 with decrease in data by 18 %;

– for weakly saturated images – at the level of 1.54 with decrease in data by 35.06 %.

This is on average 3–20 % better than the TIFF data format and 4–15 % better than the PNG format. Simultaneously, two-stage processing exceeds the single-stage approach by 4–5.2 %.

Therefore, the code constructions of indeterminate length formation:

– from the standpoint of confidentiality ensuring provides uncertainty in the uneven codograms positioning in the overall code stream, which actually eliminates the possibility of their unauthorized decryption;

– from the standpoint of accessibility ensuring provides images CCR amount reduction relative to the original video on average from 1.08 to 1.54 times, depending on the degree of their saturation.

The information and service components in the CCCdg volume ratio are presented by table. 2. The following abbreviations are used here IC1, IC2 – IC, formed after the first and second processing stage.

Table 2 analysis shows that the SC CCCdg volume decreases with processing units m and n increasing dimension. This reduces the amount of data that undergoes additional cryptographic transformation based on scrambling and/or encryption. So, if $m = n = 16$ elements the SC in CCCdg volume the level no more than 2.5 % of all code stream volume provided.

From the IC CCCdg bit sequences statistical testing seen that:

– the number of 1 in bit sequences is greater than the number 0 from 2 to 5 %, and the probability of occurrence of units deviates from $1/2$ only by 1–2.5 %;

– the number 1 in each of 64-bit subsequence will differ from the number 0 by an average of two, which exceeds the reference value by one and satisfies Golombe's postulates (ideally, the number 1 in each period should differ from 0 by no more than one);

– there is the same number of series 0 and 1 in the sequences, which differs from the estimated value of 50 % less than 1 %;

– the probability of series-pairs distribution (00, 01, 10, 11) in the sequences is in the range of 0.223–0.272 with a calculated value of 0.25, and series of threes (000, 001, 010, 100, 011, 110, 10 111) – in the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Table 1

Assessing the degree of test images compression results examples

Tests image	Processing option							
	PNG		TIFF		CCR 1 stage		CCR 2 stage	
	odds compr.	% change volume	odds compr.	% change volume	odds compr.	% change volume	odds compr.	% change volume
2.1.01	1.08	7.41	0.92	-11.11	1.086	7.92	1.126	11.19
Airplane	1.34	25.26	1.28	21.88	1.39	28.06	1.54	35.06
Baboon	1.04	3.85	0.83	-20.48	1.05	4.76	1.08	7.41
Barbara	1.13	11.50	1.18	15.25	1.14	12.28	1.22	18.03
Lena	1.07	6.54	1.08	7.41	1.25	20.00	1.37	27.01
Airport area	1.25	20.00	1.26	20.63	1.16	13.79	1.21	17.36

Table 2

The CCCdg information and service components volume ratio without information quality loss for different block $A^{(\gamma;\chi)}$ video data processing parameters m and n, %

Tests image	The parameter m and n value provided that m = n											
	8			12			16			20		
	IC1	IC2	SS	IC1	IC2	SS	IC1	IC2	SS	IC1	IC2	SS
2.1.01	75.53	17.44	7.03	84.02	12.72	3.26	88.23	9.91	1.86	90.75	8.06	1.19
Airplane	72.81	17.55	8.64	82.52	13.08	4.4	86.97	10.55	2.48	89.92	8.55	1.53
Baboon	75.83	17.42	6.75	84.38	12.49	3.13	88.43	9.78	1.79	91.03	7.83	1.14
Barbara	76.29	16.1	7.61	84.76	11.79	3.46	88.79	9.26	1.95	91.22	7.54	1.23
Lena	75.71	15.7	8.59	84.55	11.57	3.88	88.83	9.01	2.16	91.29	7.35	1.36
Peppers	74.63	16.73	8.64	83.65	12.45	3.9	88.03	9.8	2.17	90.73	7.92	1.35
Airport area	74.24	18.23	7.54	82.99	13.58	3.43	87.3	10.77	1.93	90.06	8.73	1.21

range of 0.103–0.146 with an estimated value of 0.125. The best results were obtained for saturated realistic images;

– there is no correlation between the elements in the IC;

– there is no redundancy in the IC, additional compression by ZIP and RAR archivers is not provided.

4. Conclusions

Scientific novelty. The images in a differentiated on the basis of single-stage cryptocompression coding method based on the nonequilibrium positional coding technology using has been further improved. The difference between this method and the known ones is the follows:

– organization of a floating coding scheme for the entire image plane. Here, the information component is formed for the image elements of different blocks. A linearization scheme was developed for this purpose. It allows representing two-dimensional coordinates of elements through four-dimensional ones. Mutually unambiguous mapping between the elements of service components and video images is ensured. For this, the two-dimensional matrices of service components are reformatted into one-dimensional vectors;

– information component code value formation eliminates the code word length overflow, which is allocated for its storage;

– additional using of two degrees of uncertainty, which consist of the nondeterministic length of cryptocompression codograms and the nondeterministic number of elements involved in their formation.

This allows to increase the cryptographic strength and video data availability without losing credibility.

Further research will deal with the development of methods of storage and processing of service components of cryptocompression codegrams of video images.

Research results can be applied as follows:

1) as a component of complex image compression and encryption technologies;

2) for systems of video monitoring at crisis infrastructure facilities in terms of ensuring the conditions for images protection;

3) for on-board complexes in the systems of formation and transmission of protected images.

Contribution of the authors: the review and analysis of information sources – **Andrii Yermachenkov**, **Maksym Savchuk**; the analysis of approaches to ensuring the images confidentiality – **Serhii Sidchenko**, **Dmitriy Barannik**, **Gennady Pris**; the justification of problematic shortcomings of the images confi-

dentiality methods – **Vladimir Barannik**, **Serhii Sidchenko**; the analysis of cryptocompression representation methods of video images – **Dmitriy Barannik**; the justification of the approach to improving the method of cryptocompression coding of images – **Vladimir Barannik**; development of an approach to the organization of a floating position coding scheme within the entire image by reformatting a two-dimensional matrix into a one-dimensional vector, creating an approach for linearizing the four-dimensional coordinates of a two-dimensional matrix into a one-dimensional vector coordinate – **Serhii Sidchenko**; creating an approach to the formation of floating length codegrams – **Serhii Sidchenko**, **Dmitriy Barannik**; creating a images cryptocompression method based on floating positional coding with an unequal codograms length – **Serhii Sidchenko**, **Vladimir Barannik**; software implementation, evaluation of the effectiveness of the method of cryptocompression coding of images, the analysis of the results of the comparison of different methods – **Serhii Sidchenko**, **Andrii Yermachenkov**, **Maksym Savchuk**; the text of the previous version of the article – **Vladimir Barannik**, **Serhii Sidchenko**; editing and post-editing – **Serhii Sidchenko**, **Andrii Yermachenkov**, **Maksym Savchuk**; formulation of conclusions – **Vladimir Barannik**, **Serhii Sidchenko**, **Dmitriy Barannik**.

All authors have read and agreed to the published version of the manuscript.

References

1. FIPS 197. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication, 2001. 51 p.

2. DSTU GOST 28147:2009: *Systema obrobky informatsii. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (HOST 28147-89)* [Information processing system. Cryptographic protection. Cryptographic transformation algorithm (GOST 28147-89)], State Committee for Technical Regulation and Consumer Policy (Derzhspozhivstandart) of Ukraine, 2008. 20 p. (In Ukrainian).

3. DSTU 7624:2014: *Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia* [Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm]. Ministry of Economic Development of Ukraine, 2015. 39 p. (In Ukrainian).

4. Rivest, R. L., Shamir, A., Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, iss. 2, pp. 120-126. DOI: 10.1145/359340.359342.

5. Latif, A., Mehrnahad, Z. A Novel Image Encryption Scheme Based on Reversible Cellular Automata. *Journal of Electronic & Information Systems*, 2019, vol. 1, iss. 1, pp. 18-25. DOI: 10.30564/jeisr.v1i1.1078.

6. Sharma, R., Bollavarapu, S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, 2015, vol. 117, no. 14, pp. 15-18. DOI: 10.5120/20621-3342.

7. Rasheed, M. H., Salih, O. M., Siddeq, M. M. Joint image encryption and compression schemes based on hexa-coding. *Periodicals of Engineering and Natural Sciences*, 2021, vol. 9, no 2, pp. 569-580. DOI: 10.21533/pen.v9i2.1839.

8. Ramakrishnan, S. et al. *Cryptographic and Information Security Approaches for Images and Videos*. CRC Press Publ., 2018. 986 p. DOI: 10.1201/9780429435461.

9. Farajallah, M. *Chaos-based crypto and joint crypto-compression systems for images and videos*, 2015, 211 p. Available at: https://hal.archives-ouvertes.fr/tel-01179610. (accessed 11 January 2022).

10. Zia, U., McCartney, M., Scotney, B. et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 2022, vol. 21, pp. 917–935. DOI: 10.1007/s10207-022-00588-5.

11. Wu, Yu., Zhou, Y., Agaian, S., Noonan, J. 2D Sudoku associated bijections for image scrambling. *Information Sciences*, 2016, vol. 327, pp. 91–109. DOI: 10.1016/j.ins.2015.08.013.

12. Patanwadia, R., Mangrulkar, R. Divide and Scramble - A Recursive Image Scrambling algorithm utilizing Rubik's Cube. *Proc. Int. Conf. "Recent Trends on Electronics, Information, Communication & Technology" (RTEICT)*. Bangalore, India, 2021, pp. 859-863, DOI: 10.1109/RTEICT52294.2021.9573949.

13. *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*, International Standard ISO/IEC 15444-8, ITU-T Recommendation T.807, 2007. 108 p.

14. Fawaz, Z., Noura, H., Mostefaoui, A. Securing JPEG-2000 images in constrained environments: a dynamic approach. *Multimedia Systems*, 2018, vol. 24, iss. 6, pp. 669–694. DOI: 10.1007/s00530-018-0591-z.

15. *JPEG Privacy & Security Abstract and Executive Summary*, 2015. Available at: https://jpeg.org/items/20150910_privacy_security_summary.html. (accessed 11 January 2022).

16. Temmermans, F., Ebrahimi, T., Foessel, S. et al. JPEG Privacy and Security framework for social networking and GLAM services. *EURASIP Journal on Image and Video Processing*, 2017, vol. 68, pp. 1-9. DOI: 10.1186/s13640-017-0216-z.

17. Cao, X., Huang, Y., Wu, H.-T., Cheung, Y.-m. Content and Privacy Protection in JPEG Images by Re-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

versible Visual Transformation. *Applied Sciences, MDPI*, 2020, vol. 10, iss. 19, article id: 6776, pp. 1-12. DOI: 10.3390/app10196776.

18. Yuan, L., Korshunov, P., Ebrahimi, T. Secure JPEG Scrambling enabling Privacy in Photo Sharing. *Proc. 11 th IEEE Int. Conf. and Workshops "Automatic Face and Gesture Recognition" (FG)*. Ljubljana, Slovenia, 2015, pp. 1-6. DOI: 10.1109/FG.2015.7285022.

19. Ruchaud, N., Dugelay, J.-L. JPEG-based scalable privacy protection and image data utility preservation. *IET Signal Processing*, 2018, vol. 12, iss. 7, pp. 881-887. DOI: 10.1049/iet-spr.2017.0413.

20. Minemura, K., Moayed, Z., Wong, K., Qi, X., Tanaka, K. JPEG image scrambling without expansion in bitstream size. *Proc. 19 th IEEE Int. Conf. "Image Processing"*. Orlando, FL, USA, 2012, pp. 261-264. DOI: 10.1109/ICIP.2012.6466845.

21. Auer, S., Bliem, A., Engel, D., Uhl, A., Unterweger, A. Bitstream-based JPEG Encryption in Real-time. *Int. Journal of Digital Crime and Forensics*, 2013, vol. 5, iss. 3, pp. 1-14. DOI: 10.4018/jdcf.2013070101.

22. Kobayashi, H., Kiya, H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. *Proc. 7 th IEEE Global Conf. "Consumer Electronics" (GCCE)*. Nara, Japan, 2018, pp. 1-4. DOI: 10.1109/gcce.2018.8574605.

23. Phatak, A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*, 2016, vol. 8, no. 6, pp. 64-71. DOI: 10.5815/ijigsp. 2016.06.08.

24. Ji, Sh., Tong, X., Zhang, M. Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator, 2012. Available at: https://arxiv.org/abs/1208.0999. (accessed 11 January 2022).

25. Barannik, V., Barannik, N., Khimenko, V. Metod nepriamoho prykhovuvannia informatsii v protsesi stysnennia videozobrazhen [Method of indirect information hiding in the process of video compression]. *Radioelectronic and Computer Systems*, 2021, no. 4, pp. 119–131. DOI: 10.32620/reks.2021.4. (In Ukrainian).

26. Belikova, T. Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. *Proc. 2nd IEEE Int. Conf. "Advanced Trends in Information Theory" (IEEE ATIT 2020)*, 2020, pp. 87–91. DOI: 10.1109/ATIT50783. 2020.9349300.

27. Barannik, V. V., Barannik, D., Podlesny, S., Tarasenko, D., Kulitsa, O. The video stream encoding method in infocommunication systems. *Proc. 14th Int. Conf. "Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering" (TCSET)*, 2018, pp. 538-541. DOI: 10.1109/TCSET.2018. 8336259.

28. Naor, M., Shamir, A. Visual Cryptography. *Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science*, 1995, vol. 950, pp. 1-12. DOI: 10.1007/bfb0053419.

29. Bisht, K., Deshmukh, M. A novel approach for multilevel multi-secret image sharing scheme. *The Journal of Supercomputing*, 2021, vol. 77, pp. 12157-12191. DOI: 10.1007/s11227-021-03747-y.

30. Kabirirad, S., Eslami, Z. Improvement of (n, n)-multi-secret image sharing schemes based on Boolean operations. *Journal of Information Security and Applications*, 2019, vol. 47, pp. 16-27. DOI: 10.1016/j.jisa.2019.03.018.

31. Huang, S.-Y., Lo, A.-h., Juan, J.S.-T. XOR-Based Meaningful (n, n) Visual Multi-Secrets Sharing Schemes. *Applied Sciences, MDPI*, 2022, vol. 12, iss. 20, article id: 10368, pp. 1-22. DOI: 10.3390/app122010368.

32. Liu, L., Lu, Yu., Yan, X. A novel (k1,k2,n)-threshold two-in-one secret image sharing scheme for multiple secrets. *Journal of Visual Communication and Image Representation*, 2021, vol. 74, article id: 102971. DOI: 10.1016/j.jvcir.2020.102971.

33. Erdelyi, A., Barat, T., Valet, P., Winkler, T., Rinner, B. Adaptive cartooning for privacy protection in camera networks. *Proc. 11th IEEE Int. Conf. "Advanced Video and Signal Based Surveillance" (AVSS)*. Seoul, Korea, 2014, pp. 44–49. DOI: 10.1109/AVSS.2014. 6918642.

34. Hassan, E. T., Hasan, R., Shaffer P., Crandall, D., Kapadia, A. Cartooning for Enhanced Privacy in Lifelogging and Streaming Videos. *Proc. IEEE Conf. "Computer Vision and Pattern Recognition Workshops" (CVPRW)*. Honolulu, USA, 2017, pp. 1333–1342. DOI: 10.1109/CVPRW.2017.175.

35. Korshunov, P., Ebrahimi, T. Using warping for privacy protection in video surveillance. *Proc. 18th IEEE Int. Conf. "Digital Signal Processing" (DSP)*. Fira, Greece, 2013, pp. 1-6. DOI: 10.1109/ ICDSP.2013.6622791.

36. Korshunov, P., Ebrahimi, T. Using face morphing to protect privacy. *Proc. 10th IEEE Int. Conf "Advanced Video and Signal Based Surveillance"*. Krakow, Poland, 2013, pp. 208–213. DOI: 10.1109/ AVSS.2013.6636641.

37. Alimpiev, A. N., Barannik, V. V., Sidchenko, S. A. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. *Telecommunications and Radio Engineering*, 2017, vol. 76, no. 6, pp. 521-534. DOI: 10.1615/TelecomRadEng.v76.i6.60.

38. Barannik, V., Sidchenko, S., Barannik, N., Barannik, V. Development of the method for encoding

service data in cryptocompression image representation systems. *Eastern-European Journal of Enterprise Technologies*, 2021, vol. 3, no. 9(111), pp. 103-115. DOI: 10.15587/1729-4061.2021.235521.

39. Barannik, V., Sidchenko, S., Barannik, D., Shulgin, S., Barannik, V., Datsun, A. Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. *Eastern-European Journal of Enterprise Technologies*, 2021, vol. 4, no. 2(112), pp. 6-17. DOI: 10.15587/1729-4061.2021.237359.

40. Barannik, V., Sidchenko, S., Barannik, N., Barannik, D., Shulgin, S. Methods for Decoding Informational Codes of Cryptocompression Codegrams to Improve Information Security. *CEUR Workshop Proceedings (CEUR-WS.org)*, 2021, vol. 2923. pp. 143-152. Available at: CEUR-WS.org/Vol-2923/paper16.pdf. (accessed 11 January 2022).

41. Barannik, V., Sidchenko, S., Barannik, D. Technology for Protecting Video Information Resources in the Info-Communication Space. *Proc. IEEE 2 nd Int. Conf. "Advanced Trends in Information Theory" (IEEE ATIT 2020)*. Kyiv, Ukraine, 2020, pp. 29-33. DOI: 10.1109/ATIT50783.2020.9349324.

42. Barannik, V., Sidchenko, S., Barannik, D., Barannik, V., Hurzhii, I., Babenko, Y. Evaluating of the resistance of crypto-compression image codograms to errors in the data transmission channel. *Proc. IEEE 3 rd Int. Conf. "Advanced Trends in Information Theory" (IEEE ATIT 2021)*. Kyiv, Ukraine, 2021, pp. 52-56. DOI: 10.1109/ATIT54053.2021.9678774.

43. Barannik, V. V., Sidchenko, S. O., Barannik, N. V., Khimenko, A. M. Metod maskuvalnoho ushchilnennia sluzhbovykh danykh v systemakh kompresii videozobrazhen [The Method of Masking Overhead Compaction in Video Compression Systems]. *Radioelectronic and Computer Systems*, 2021, № 2, pp. 51-63. DOI: 10.32620/reks.2021.2.05. (In Ukrainian).

44. Li, F., Krivenko, S., Lukin, V. Two-step providing of desired quality in lossy image compression by SPIHT. *Radioelectronic and computer systems*, 2020, no. 2, pp. 22-32. DOI: 10.32620/reks.2020.2.02.

45. Ieremeiev, O., Lukin, V., Okarma, K. Combined visual quality metric of remote sensing images based on neural network. *Radioelectronic and computer systems*, 2020, no. 4, pp. 4-15. DOI: 10.32620/reks.2020.4.01.

Надійшла до редакції 21.12.2022, розглянута на редколегії 20.02.2023.

МЕТОД СТИСНЕННЯ ВІДЕОЗОБРАЖЕНЬ НА ОСНОВІ ПЛАВАЮЧОГО ПОЗИЦІЙНОГО КОДУВАННЯ З НЕРІВНОМІРНОЮ ДОВЖИНОЮ КОДОГРАМ

Володимир Бараннік, Сергій Сідченко, Дмитро Бараннік, Андрій Єрмаченков, Максим Савчук, Геннадій Прис

Предметом вивчення у статті є процеси стиснення та шифрування відеозображень у процесі управління критично важливими об'єктами. **Метою** є розробка методу стиснення відеозображень на основі плаваючого позиційного кодування з нерівномірною довжиною кодограм для одночасного забезпечення достовірності та конфіденційності інформації в процесі її передачі із заданою часовою затримкою. **Завдання**: провести аналіз існуючих підходів до забезпечення конфіденційності відеозображень; розробити метод стиснення відеозображень на основі плаваючого позиційного кодування з нерівномірною довжиною кодограм; провести оцінку ефективності розробленого методу. **Методами**, що використовуються, є: методи цифрової обробки зображень, методи стиснення цифрових зображень, методи шифрування та скремблювання зображень, методи структурно-комбінаторного кодування, методи статистичного аналізу. Отримано такі **результати**. Плаваюча схема кодування не обмежується обробкою окремих блоків. Формування кодових значень організується для елементів із різних блоків зображення. Для цього розроблена схема лінеаризації координат точки зображення з чотиривимірного її представлення на площині в одномірну координату елемента у векторі. Чотиривимірна координата елемента на площині описує координати блоку у зображенні та координати елемента у цьому блоці. Формування кодових значень організується з урахуванням контролю переповнення довжини кодового слова, що виділяється для їх зберігання. При цьому кодування забезпечується для недетермінованої кількості елементів вихідного зображення. Їх кількість залежить від значень елементів, які формують блоки обробки. Внаслідок кодування формуються кодові значення недетермінованої довжини. Їх довжина залежить від значень службових даних, сформованих у процесі кодування. Службові дані виступають як ключовий елемент. **Висновки**. Отримав подальше удосконалення однокаскадний метод поліадичного кодування зображень у диференційованому базисі. Розроблений метод кодування забезпечує стиснення зображень без втрати якості інформації. Забезпечується стиснення обсягу вихідного зображення краще на 3–20 % в порівнянні з форматом представлення даних TIFF і на 4–15 % щодо формату PNG. Обсяг службових даних не перевищує 2,5 % від розміру всього кодового потоку.

Ключові слова: без втрат; відео; достовірність; зображення; кодування; конфіденційність; стиснення; шифрування.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Бараннік Володимир Вікторович – д-р техн. наук, проф., проф. каф. штучного інтелекту та програмного забезпечення, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.

Сідченко Сергій Олександрович – канд. техн. наук, старш. наук. співроб., начальник науково-дослідної лабораторії, Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна.

Бараннік Дмитро Володимирович – асп., каф. автоматизації проектування обчислювальної техніки, Харківський національний університет радіоелектроніки, Харків, Україна.

Єрмаченков Андрій Володимирович – викл. каф. телекомунікаційних систем та мереж Військового інституту телекомунікаційних систем та мереж імені Героїв Крут, Київ, Україна.

Савчук Максим Васильович – старш. викл. каф. телекомунікаційних систем та мереж Військового інституту телекомунікаційних систем та мереж імені Героїв Крут, Київ, Україна.

Прис Геннадій Петрович – заст. начальника наукового центру зв'язку та інформатизації, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Vladimir Barannik – Doctor of Technical Sciences, Professor, Professor of the Department of Artificial Intelligence and Software, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: vvbar.off@gmail.com, ORCID: 0000-0002-2848-4524, Scopus Author ID: 27867503300.

Serhii Sidchenko – PhD, Senior Scientific Researcher, Head of Research Laboratory, Ivan Kozhedub National Air Force University, Kharkiv, Ukraine,
e-mail: sidserg72@gmail.com, ORCID: 0000-0002-1319-6263, Scopus Author ID: 35796112800.

Dmitriy Barannik – PhD student, Department Computer Design Automation, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine,
e-mail: d.v.barannik@gmail.com, ORCID: 0000-0002-7074-9864.

Andrii Yermachenkov – lecturer at the Department Telecommunication Systems and Networks Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine,
e-mail: andrii.yermachenkov@viti.edu.ua, ORCID: 0000-0003-1979-6128.

Maksym Savchuk – lecturer at the Department Telecommunication Systems and Networks Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine,
e-mail: maksym.savchuk@viti.edu.ua, ORCID: 0000-0001-9869-7202.

Gennady Pris – deputy head of the Scientific Communication and Informatization Center, Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine,
e-mail: gennadij.prys@viti.edu.ua; ORCID: 0000-0002-8081-4391.