VIDEO IMAGES’ COMPRESSION METHOD BASED ON FLOATING POSITIONAL CODING WITH AN UNEQUAL CODEGRAMS 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 $A^{(\gamma, x)}$, where $\gamma$ is the block $A^{(\gamma, x)}$ coordinate in the plane $A$ vertically, $x$ is a horizontal coordinate. Each block $A^{(\gamma, x)}$ 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 $A^{(\gamma, x)}$ 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 $A^{(\gamma, x)}$ variable vertically $\gamma_{\max}$ and horizontally $x_{\max}$ is determined based on the ratio of dimensions $M \times N$ the processed plane $A$ and dimensions $m \times n$ block $A^{(\gamma, x)}$, namely:

$$\gamma_{\max} = \left\lfloor \frac{M}{m} \right\rfloor, \quad x_{\max} = \left\lfloor \frac{N}{n} \right\rfloor,$$

where $\left\lfloor \cdot \right\rfloor$ is an integer part number.
Every block $A^{(γ;χ)}$ is a two-dimensional array of
$a_{i,j}^{(γ;χ)}$ elements. Here:

- $i$ is the row of the element in $A^{(γ;χ)}$ array, $i=1\ldots m$;
- $j$ is the column of the element in $A^{(γ;χ)}$ array, $j=1\ldots n$;
- $γ = \lfloor \frac{M}{m} \rfloor$, $χ = \lfloor \frac{N}{n} \rfloor$;
- $A^{(γ;χ)} = \{a_{i,j}^{(γ;χ)}\}$.

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

Each processed plane $A$ is two-dimensional elements
$a_{i,j}^{(γ;χ)}$ array $A = \{a_{i,j}^{(γ;χ)}\}$, where

- $γ = \lfloor \frac{M}{m} \rfloor$, $χ = \lfloor \frac{N}{n} \rfloor$.

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

- bases $A^{(γ;χ)} = \{λ_{i,j}^{(γ;χ)}\}$ systems, where $i=1\ldots m$.

Basis $λ_{i,j}^{(γ;χ)}$ for items of $i$-th line in the block $A^{(γ;χ)}$ defines as the source block maximum line element by the formula:

$$λ_{i,j}^{(γ;χ)} = \max_{1 \leq j \leq n} (a_{i,j}^{(γ;χ)}) ;$$

(1)

- lowering value systems dynamic range $Θ^{(γ;χ)} = \{μ_{i,j}^{(γ;χ)}\}$, where $i=1\ldots m$. Decreasing value $μ_{i,j}^{(γ;χ)}$ for $i$-th line in the block $A^{(γ;χ)}$ items defined as the minimum value by the formula:

$$μ_{i,j}^{(γ;χ)} = \min_{1 \leq j \leq n} (a_{i,j}^{(γ;χ)}) .$$

(2)

Each elements $λ_{i,j}^{(γ;χ)}$ and $μ_{i,j}^{(γ;χ)}$ can take values in the range $[0;255]$.

Base systems $A^{(γ;χ)} = \{λ_{i,j}^{(γ;χ)}\}$ and blocks $A^{(γ;χ)}$ plane dynamic range $Θ^{(γ;χ)} = \{μ_{i,j}^{(γ;χ)}\}$ decreasing values are vector columns with $m$ elements each. Two-dimensional data arrays $Λ = \{λ_{i,j}^{(γ;χ)}\}$ and $Θ = \{μ_{i,j}^{(γ;χ)}\}$ are being formed. The size of these arrays is $M \times \lfloor \frac{N}{n} \rfloor$.

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 $A^{(γ;χ)}$ with coordinates $(1;1)$ and continues horizontally to the coordinate block $(\lfloor \frac{M}{m} \rfloor; \lfloor \frac{N}{n} \rfloor)$ . 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 $(\lfloor \frac{M}{m} \rfloor; \lfloor \frac{N}{n} \rfloor)$ processing completes. Elements $a_{i,j}^{(γ;χ)}$ inside block $A^{(γ;χ)}$ 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 $A^{(γ;χ)}$ 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 $A^{(γ;χ)}$. Each block has dimensions $A^{(γ;χ)}$.

Then next condition is fulfilled:

$$\frac{M}{m} = \frac{M}{m} \quad \frac{N}{n} = \frac{N}{n} .$$

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

$$A = \{a_{i,j}\} = \{a_{i,j}^{(γ;χ)}\} ,$$

where $τ = \lfloor \frac{M}{m} \rfloor \cdot \lfloor \frac{N}{n} \rfloor$, $γ = \lfloor \frac{M}{m} \rfloor$, $χ = \lfloor \frac{N}{n} \rfloor$, $i=1\ldots m$,

$$j=1\ldots n ,$$

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

To do this, the element $a_{i,j}^{(γ;χ)}$ coordinates linearization performs. Reformattting consists in finding the $τ$ coordinate of an element in a one-dimensional sequence, $τ = \lfloor \frac{M}{m} \rfloor \cdot \lfloor \frac{N}{n} \rfloor$. Simultaneously, the four-dimensional coordinates of the elements are considered. They are defined by:

- location $(i;j)$ of elements in block $A^{(γ;χ)}$;
- place $(γ;χ)$ 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:
The following expressions are used for transformation:

\[
\begin{align*}
\tau &= (\gamma - 1) \cdot \left[ \frac{N}{n} \right] + \chi - 1 \cdot m \cdot n + (j - 1) \cdot m + i. \quad (3)
\end{align*}
\]

As a result of matrix \( A \) reformattting, the form of data representation changes. However, the data itself does 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 \( a_{\tau} \), with a one-dimensional coordinate \( \tau \). The following expressions are used for transformation:

\[
\begin{align*}
\gamma &= \left[ \frac{\tau - 1}{m \cdot n} \right] + 1; \\
\chi &= \left[ \frac{\tau - 1}{m \cdot n} \right] - \left[ \frac{\gamma}{m \cdot n} \right] \cdot \left[ \frac{N}{n} \right] + 1; \\
i &= \tau - \left[ \frac{\tau - 1}{m \cdot n} \right] \cdot m \cdot n - \left[ \frac{\chi}{m \cdot n} \right] \cdot m; \\
j &= \left[ \frac{\tau - 1}{m \cdot n} \right] \cdot m + 1.
\end{align*}
\]

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

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

These vectors consist, respectively, of elements with coordinates:

- from \( \lambda_{1} \) to \( \lambda_{M} \) \( \frac{N}{n} \),
- from \( \mu_{1} \) to \( \mu_{M} \) \( \frac{N}{n} \).

Reformatting two-dimensional matrices \( \Lambda \) and \( \Theta \) 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 \( M \cdot \left[ \frac{N}{n} \right] \).

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 \( \Lambda \), \( \Theta \) 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 \( \Lambda_{j}^{(\gamma, \chi)} \) and \( \Theta_{j}^{(\gamma, \chi)} \) 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 \( \Lambda_{i}^{(\gamma, \chi)} \) and \( \Theta_{j}^{(\gamma, \chi)} \) by \( n \) times. Two-dimensional matrices \( \Lambda^{(\gamma, \chi)} \), \( \Theta^{(\gamma, \chi)} \) consist of elements \( \lambda_{i}^{(\gamma, \chi)} \), \( \mu_{i}^{(\gamma, \chi)} \) accordingly. The value of elements is calculated by expressions:

\[
\begin{align*}
\lambda_{i}^{(\gamma, \chi)} &= \lambda_{i}^{(\gamma, \chi)} \quad \text{and} \quad \mu_{i}^{(\gamma, \chi)} = \mu_{i}^{(\gamma, \chi)} \quad \text{at} \quad j = 1, n.
\end{align*}
\]

As a result, bases \( \Lambda' \) and lowering values \( \Theta' \) systems forms which dimension is equal to processed plane \( \Lambda \), namely \( M \times N \) elements.

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

\[
\begin{align*}
\Lambda' &= \{\lambda'_{j} \} = \{\lambda_{i}^{(\gamma, \chi)}\}_{i=1}^{N}; \\
\Theta' &= \{\mu'_{j} \} = \{\mu_{i}^{(\gamma, \chi)}\}_{i=1}^{N}, \quad \tau = 1, M \cdot N.
\end{align*}
\]

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

- coordinates \( \tau \) of elements of SC systems \( \Lambda' \) and \( \Theta' \);

- coordinates \( \left[ m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right] + \tau - m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right] \right] \) of elements of SC \( \Lambda' \) and \( \Theta' \).

Such accordance is described as:

\[
\begin{align*}
\lambda'_{\tau} = \lambda_{m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right] + \tau - m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right]}^{(\gamma, \chi)}, \quad \tau = 1, M \cdot N; \\
\mu'_{\tau} = \mu_{m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right] + \tau - m \cdot \left[ \frac{\tau - 1}{m \cdot n} \right]}^{(\gamma, \chi)}, \quad \tau = 1, M \cdot N.
\end{align*}
\]

Code values (CV) \( E_{\alpha} \) of the information component (IC) of the CCR image are formed for:
- vector representation of the plane \( A \);
- advanced service data systems \( \Lambda' \) and \( \Theta' \) (or \( \Lambda \) and \( \Theta \)).

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

\[
E_a = \sum_{n=0}^{\tau(0)} \left( (a_i - \mu_i) \cdot W_i \right) = \sum_{n=0}^{\tau(0)} \left( (a_i - \mu_i) \cdot \frac{1}{m} \right),
\]

(4)

where \( \tau \in [\tau(0)_{a \alpha}, \tau(0)_{a \alpha} + \Psi_{\alpha} - 1] \) and \( \tau(0)_{a \alpha} + \Psi_{\alpha} - 1 \leq M \cdot N \),

where \( \alpha \) is a formed CV serial number \( E_a \) IC CCCdg;

\( \tau(0)_{a \alpha} \) – linear vector coordinates that determines the data processed in the encoding process position;

\( \tau(0)_{a \alpha} \) – the processed plane \( A \) element \( a_\tau \) starting coordinate in the vector form from which the CV \( E_a \) formation of the begins;

\( \Psi_{\alpha} \) – floating (indeterminate) plane \( A \) elements \( a_\tau \) number involved in the CV \( E_a \) formation;

\( W_i \) – weighting factor for \( i \)-th element \( a_i \), which is the product of the following bases \( \lambda_i \) elements, taking into account their dynamic ranges reduction by \( \mu_i \).

The starting parameters for the first CV \( E_a \) are calculated as follows:

- the CV serial number is equal to \( \alpha = 1 \);
- first element \( a_1 \) starting coordinate is equal to \( \tau(0)_{a \alpha} = 1 \).

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

- CV serial number increases by one \( \alpha = \alpha + 1 \);
- starting coordinate \( \tau(0)_{a \alpha} \) determines based on:
  a) value of coordinate \( \tau(0)_{a \alpha} - 1 \) for the previous CV \( E_{\alpha - 1} \);
  b) current amount \( \Psi_{\alpha - 1} \) of elements \( a_\tau \).

This is described by the formula:

\[
\tau(0)_{a \alpha} = \tau(0)_{a \alpha-1} + \Psi_{\alpha-1}.
\]

(6)

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

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

\[
E_a \leq 2^{L_{cw} - 1}, \log_2(E_a) \leq L_{cw},
\]

(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 \( \lambda_i \), considering:

- amount \( \Psi_{\alpha} \) of elements in CV;
- reduced dynamic range \( \mu_i \).

This is described as:

\[
\tau(0)_{a \alpha} + \Psi_{\alpha} \leq 2^{L_{cw} - 1},
\]

(8)

\[
\tau(0)_{a \alpha} + \Psi_{\alpha} \leq 2^{L_{cw} - 1} - 1,
\]

(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:

\[
\tau(0)_{a \alpha} + \Psi_{\alpha - 1} \leq 2^{L_{cw} - 1} - 1,
\]

(10)

\[
\tau(0)_{a \alpha} + \Psi_{\alpha - 1} \leq 2^{L_{cw} - 1} - 1,
\]

(11)
provided that SC system \( \Psi_{a} + 1 \) -th element with the coordinate \( (\tau(0)_{a} + \Psi_{a}) \leq M \cdot N \) exists when checking condition (10) and with the coordinate

\[
(m \cdot \left( \frac{\tau(0)_{a} + \Psi_{a} - 1}{m \cdot n} \right) + (\tau(0)_{a} + \Psi_{a}) - m \cdot \left( \frac{\tau(0)_{a} + \Psi_{a} - 1}{m \cdot n} \right)) \leq M \cdot \left[ \frac{N}{n} \right]
\]

when checking condition (11).

Elements \( \Psi_{a} \) number defined as:

\[
\tau(0)_{a} + \Psi_{a} - 1 \prod_{\xi = 1}^{\tau(0)_{a}} (\lambda_{\xi} + 1 - \mu_{\xi})
\]

or

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

Value \( \Psi_{a} \) is an argument of this expressions when:
- their maximum value is reached;
- fulfillment of inequalities (10) or (11).

This is described by the formula:

\[
\Psi_{a} = \arg \max \left( \prod_{\xi = 1}^{\tau(0)_{a}} (\lambda_{\xi} + 1 - \mu_{\xi}) \right) = \arg \max \left( \prod_{\xi = 1}^{\tau(0)_{a}} \left( \lambda_{\xi} \left( \frac{\xi - 1}{m \cdot n} \right) + 1 - \mu_{\xi} \left( \frac{\xi - 1}{m \cdot n} \right) \right) \right)
\]

\( \Psi_{a} = \arg \max \left( \prod_{\xi = 1}^{\tau(0)_{a}} \left( \lambda_{\xi} \left( \frac{\xi - 1}{m \cdot n} \right) + 1 - \mu_{\xi} \left( \frac{\xi - 1}{m \cdot n} \right) \right) \right) \) (12)

Elements quantity \( \Psi_{a} \) 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 \( a \) of CV \( E_{a} \);
- starting coordinate \( \tau(0)_{a} \) of the first element \( a_{1} \);
- length of CV \( L_{cw} \).

Counter of the number of elements involved in the formation of the CV \( E_{a} \) installed to \( \Psi_{a} = 1 \).

Stage 1. At the first stage, the reading of the elements is organized \( \lambda_{1} \), \( \mu_{1} \) for SC \( \Lambda' \) and \( \Theta' \). Or

\[
\begin{align*}
\lambda_{m \left( \frac{\xi - 1}{m} \right), m \left( \frac{\xi - 1}{m} \right)} & \quad \mu_{m \left( \frac{\xi - 1}{m} \right), m \left( \frac{\xi - 1}{m} \right)}
\end{align*}
\]

Elements have the following properties:
- their coordinates vary between \( \tau(0)_{a} \) and \( \tau(0)_{a} + \Psi_{a} \);
- they correspond to the \( a_{e} \) elements of the A plane.

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

\[
(m \cdot \left( \frac{\tau(0)_{a} + \Psi_{a} - 1}{m \cdot n} \right) + (\tau(0)_{a} + \Psi_{a}) - m \cdot \left( \frac{\tau(0)_{a} + \Psi_{a} - 1}{m \cdot n} \right)).
\]

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 \( E_{a} \) formation, increases by 1, i.e. \( \Psi_{a} = \Psi_{a} + 1 \). 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 \( E_{a} \), is equal to \( \Psi_{a} \).

The formation of the CCCdg is organized in four stages. 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 \( \Lambda \) divides into blocks \( \Lambda^{(y,z)} \), consists of \( m \times n \) elements each;
- for blocks \( \Lambda^{(y,z)} = \{a_{j}^{(y,z)} \} \) using formulas (1) and (2) determines the base system \( \Lambda^{(y,z)} = \{\lambda_{i}^{(y,z)} \} \) and the dynamic range \( \Theta^{(y,z)} = \{\mu_{i}^{(y,z)} \} \) decreasing values that are vector columns with \( M \times N \) elements of each. After processing all blocks \( \Lambda^{(y,z)} \) the resulting vector columns are combined into two-dimensional data sets
- formula (3) organizes reformattting of two-dimensional matrices. This includes the following matrices:
  a) image \( \Lambda \);
  b) data system services \( \Lambda \) and \( \Theta \);
  c) extended data system services \( \Lambda' \) and \( \Theta' \). As a result, corresponding one-dimensional vectors are formed;
- the starting parameters for the formation of CV \( E_{a} \) and the lengths of CW \( L_{cw} \). These include:
a) sequence number of CV $E_\alpha$, $\alpha = 1$;
b) starting coordinate of the first element, $\tau(0) = 1$.

Step 2. The second step calculates the elements $\Psi_\alpha$ number involved in the CV $E_\alpha$ 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 $E_\alpha$ SC is formed on the basis of expressions (4) and (5). Code value $E_\alpha$ depends on:
- image plane $A = [a_{i,j}^{(\alpha)}]$;
- SC systems $\Lambda^{(\alpha)} = \{\lambda_i^{(\alpha)}\}$ and $\Theta^{(\alpha)} = \{\mu_i^{(\alpha)}\}$.

Step 4. After the CV $E_\alpha$ formation, if not all plane elements $A = [a_{i,j}^{(\alpha)}]$ are processed, i.e. $(\tau(0) + \Psi_\alpha - 1) \neq M \cdot N$, 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 $A = [a_{i,j}^{(\alpha)}]$ are processed, then formed CV $E_\alpha$ combines and forms IC $E = \{E_\alpha\}$ for this plane. The last formed CV $E_\alpha$ sequence number $\alpha$ will match the quantity $\alpha_{\text{max}}$ of all CV $E_\alpha$, 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 $q_\alpha$ CV $E_\alpha$ basis. Uniform length $q_\alpha$ corresponds to the length of the selected CV $L_{cw}$, i.e. $q_\alpha = L_{cw}$. The uneven length $q_\alpha$ is individual for each individual CV $E_\alpha$. It is determined on the basis of the accumulated product of SC elements. Here systems $\Lambda$, $\Theta$ or $\Lambda'$, $\Theta'$ are used. Length $q_\alpha$ depends on elements quantity $\Psi_\alpha$ using the formula:

$$q_\alpha = \log_2 \prod_{\xi = \tau(0)_{\alpha}}^{\tau(0)_{\alpha} + \Psi_\alpha - 1} (\lambda_\xi^{(\alpha)} + 1 - \mu_\xi^{(\alpha)}) + 1 = \log_2 \prod_{\xi = \tau(0)_{\alpha}}^{\tau(0)_{\alpha} + \Psi_\alpha - 1} (\lambda_\xi^{(\alpha)} + 1 - \mu_\xi^{(\alpha)}) + 1.$$ 

All $\alpha_{\text{max}}$ CV $E_\alpha$ total length determines by the formula:

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

CCCdg image forms from the code structures obtained for each plane $A$ with $P$ planes, namely:
- information component $E = \{E_\alpha\}$;
- bases $\Lambda = \{\lambda_i^{(\alpha)}\}$ systems;
- systems of dynamic range $\Theta = \{\mu_i^{(\alpha)}\}$ lowering values.

Ensuring the video data cryptographic stability based on the developed method is provided by:
- formation CV $E_\alpha$ on variable elements $a_{\alpha}$ quantity $\Psi_\alpha$ based on the CW $L_{cw}$ overflow control. Elements $a_{\alpha}$ number $\Psi_\alpha$, which forms the CV $E_\alpha$, depends only on the structure of the processed data;
- formation IC $E = \{E_\alpha\}$ using CV $E_\alpha$. Code values are formed for uneven sequences with uneven lengths $q_\alpha$. It is determined on the basis of the accumulated product of SC elements. Simultaneously, the number of elements is equal to $\Psi_\alpha$. On the one hand, this reduces the overall length $q$ IC $E = \{E_\alpha\}$. On the other hand, without knowledge of the SC $\Lambda$ and $\Theta$ ($\Lambda'$ and $\Theta'$) it is impossible to allocate each individual CV $E_\alpha$ from the total code stream of the IC $E = \{E_\alpha\}$;
- in fact CV $E_\alpha$ formation performs non-source involved elements $a_{\alpha}$, but its representation in the reduced dynamic range $(a_{\alpha} - \mu_{\alpha}')$. This allows significantly increase elements number $\Psi_\alpha$ that forms the CV $E_\alpha$, and reduce number $\alpha_{\text{max}}$ CV $E_\alpha$ IC $E = \{E_\alpha\}$;
- bases $\Lambda = \{\lambda_i^{(\alpha)}\}$ and lowering the dynamic range $\Theta = \{\mu_i^{(\alpha)}\}$ 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](image)

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, 111) – in the
Assessing the degree of test images compression results examples

<table>
<thead>
<tr>
<th>Tests image</th>
<th>Processing option</th>
<th>PNG</th>
<th>TIFF</th>
<th>CCR 1 stage</th>
<th>CCR 2 stage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>odds compr.</td>
<td>% change volume</td>
<td>odds compr.</td>
<td>% change volume</td>
<td>odds compr.</td>
</tr>
<tr>
<td>2.1.01</td>
<td>1.08</td>
<td>7.41</td>
<td>0.92</td>
<td>-11.11</td>
<td>1.086</td>
</tr>
<tr>
<td>Airplane</td>
<td>1.34</td>
<td>25.26</td>
<td>1.28</td>
<td>21.88</td>
<td>1.39</td>
</tr>
<tr>
<td>Baboon</td>
<td>1.04</td>
<td>3.85</td>
<td>0.83</td>
<td>-20.48</td>
<td>1.05</td>
</tr>
<tr>
<td>Barbara</td>
<td>1.13</td>
<td>11.50</td>
<td>1.18</td>
<td>15.25</td>
<td>1.14</td>
</tr>
<tr>
<td>Lena</td>
<td>1.07</td>
<td>6.54</td>
<td>1.08</td>
<td>7.41</td>
<td>1.25</td>
</tr>
<tr>
<td>Airport area</td>
<td>1.25</td>
<td>20.00</td>
<td>1.26</td>
<td>20.63</td>
<td>1.16</td>
</tr>
</tbody>
</table>

The CCCdg information and service components volume ratio without information quality loss for different block

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 crypto-compression 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 codograms 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 Sidenko, 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; 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, Andriy Yermachenkov, Maksym Savchuk; the text of the previous version of the article – Vladimir Barannik, Serhii Sidchenko; editing and post-editing – Serhii Sidchenko, Andriy 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

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


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


**МЕТОД СТИСНЕННЯ ВІДЕОЗОБРАЖЕНЬ НА ОСНОВІ ПЛAVАЮЧОГО ПОЗIЦIЙНОГО КОДУВАННЯ З НЕРИВНОМІРНОЮ ДОЖIВИНОЮ КОДОГРАМ**

**Володимир Баранник, Сергiй Сiдченко, Дмитро Баранник, Андрiй Єрмаченков, Максим Савчук, Геннадiй Прис**

Предметом вивчення у статтi є процеси стиснення та шифрування відеозображень у процесі управлiння критично важливими об’єктами. Метoю є розробка методу стиснення відеооб’єктiв на основi плаваючого позицiйного кодування з нерiвномiрною довiжиною кодограм для одночасного забезпечення достовiрностi та конфiденцiйностi iнформацiї в процесi її передачi iз заданoю часовою затримкою.

Завдання: провести аналiз iснуючих пiдходiв до забезпечення конфiденцiйностi вiдеооб’єктiв; розробити новий метод стиснення вiдеооб’єктiв на основi плаваючого позицiйного кодування з нерiвномiрною довiжиною кодограм; провести оцiнку ефективностi розробленого методу.

Методами, що використовуються, є: методи цифрової обробки зображення, методи стиснення цифрових зображень, методи шифрування та скремблювання зображень, методи структурно-комбiнаторного кодування, методи статистичного аналiзу. Отримано такi результати. Плаваюча схема кодування не обмежується обробкою окремих блокiв. Формування кодових значень органiзуються для елементiв iз рiзних блокiв зображення. Для цього розроблена схема лiнiеаризацiї координат точки зображення з чотиривiрiмiнного iї представлення на площинi в однiй координатнiй системi векторi. Чотиривiрiмiнне кoординатне iмя на площi описує координати блоку у зображенi та координати імена його площi. Формування кодових значень органiзується з врахуванням контролю переповнення довжини кодового слова, що вiдображається iз урахуванням контрольної кодограми.

Службовi данi виступають як ключовий елемент. Висновки. Отримав подальше удосконалення однокаскадний метод плаваючого позицiйного кодування з нерiвномiрною довiжиною кодограм iз додатковим контрольним кодограмом. Розроблений метод кодування забезпечує стиснення зображень без втрати якостi iнформацiї. Забезпечується стиснення об’єкту вiдеооб’єктiв з додатковим контрольним кодограмом на 3–20 % з порядки з форматом представлення даних TIFF і на 4–15 % з формату PNG. Обсяг службових даних не перевищує 2,5 % вiд розмiру вiдповiдного кадру.

**Ключовi слова:** без втрат; вiдео; достовiрнiсть; зображення; кодування; конфiденцiйнiсть; стиснення; шифрування.
Бараннік Володимир Вікторович – д-р техн. наук, проф., проф. каф. штучного інтелекту та програмного забезпечення, Харківський національний університет імені В.Н. Каразіна, 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.