The demand for image confidentiality is constantly growing. At the same time, ensuring the confidentiality of video information must be organized subject to ensuring its reliability with a given time delay in processing and transmission. Methods of cryptocompression representation of images can be used to solve this problem. They are designed to simultaneously provide compression and protection of video information. The service component is used as the key of the cryptocompression transformation. However, it has a significant volume. It is 25 % of the original video data volume. A method for coding systems of service components in a differentiated basis on the second cascade of cryptocompression representation of images has been developed. The method is based on the developed scheme of data linearization from three-dimensional coordinates of representation in a two-dimensional matrix into a one-dimensional coordinate for one-to-one representation of this element in a vector. Linearization is organized horizontally line by line. On the basis of the developed method, a non-deterministic number of code values of information components is formed. They have non-deterministic lengths and are formed on a non-deterministic number of elements. The uncertainty of positioning of cryptocompression codograms in the general code stream is provided, which virtually eliminates the possibility of their unauthorized decryption. The method provides a reduction in the volume of the service component of the cryptocompression codogram. The service data volume is 6.25 % of the original video data volume. The method provides an additional reduction in the volume of cryptocompression representation of images without loss of information quality relative to the original video data on average from 1.08 to 1.54 times, depending on the degree of their saturation

Keywords: cryptocompression, service component, information protection, floating scheme, differentiated basis, image

UDC 621.327:681.5
DOI: 10.15587/1729-4061.2021.235521

DEVELOPMENT OF THE METHOD FOR ENCODING SERVICE DATA IN CRYPTOCOMPRESSION IMAGE REPRESENTATION SYSTEMS

Vladimir Barannik
Corresponding author
Doctor of Technical Sciences, Professor
Department of Artificial Intelligence and Software
V. N. Karazin Kharkiv National University
Svobody sq., 4, Kharkiv, Ukraine, 61022
E-mail: vvbar.off@gmail.com
Serhii Sidchenko
PhD, Senior Researcher
Scientific and Organizational Department
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
Natalia Barannik
Scientific and Organizational Department
National University of Civil Defence of Ukraine
Chernyshevska str., 94 Kharkov, Ukraine, 61023
Valeriy Barannik
Department of Design Automation
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received date: 26.04.2021
Accepted date: 02.06.2021
Published date: 30.06.2021

***How to Cite**: Barannik, V., Sidchenko, S., Barannik, N., Barannik, V. (2021). Development of the method for encoding service data in cryptocompression image representation systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 103–115. doi: https://doi.org/10.15587/1729-4061.2021.235521*

1. Introduction

The development of information and control systems allows them to be used to automate control processes, both complex systems and critical infrastructure facilities.

To improve the efficiency of management processes, video information resources are used. At the same time, the following requirements are put forward for them:

– delivery of information in real time;

– ensuring the required level of confidentiality;

– creation of conditions for maintaining a given level of reliability (integrity) of information.

At the same time, two factors must be taken into account here, namely:

1) firstly, the growth in the volume of video images, which is also dictated by the need to increase their resolution. On the one hand, this increases the efficiency of video information analysis and object identification. On the other hand, the load on the telecommunications network increases sharply;

2) secondly, information about control objects, as a rule, is collected remotely. Therefore, for its transmission to control points, mainly wireless data transmission channels are used. Moreover, such channels have insufficient bandwidth to transmit video information in real time.

This imbalance leads to increased time delays in the transmission and processing of video images. This reduces the effectiveness of control systems. Therefore, to localize such an imbalance, video compression technologies are used [1–4]. However, existing video compression technologies do not take into account such issues as confidentiality in their structure [5–7]. This creates conditions for unauthorized access to video information by intruders.

At the same time, video information that is used in critical infrastructure management systems can be classified as information with limited access. For example, information

that reveals the features and structure of the petrochemical complex, nuclear and hydroelectric power plants, airports, train stations, large railway bridges and junctions. Therefore, the loss of the level of confidentiality of video information can lead to serious damage.

Thus, reducing the volume of video information in terms of ensuring its confidentiality and reliability is an urgent scientific and applied research problem.

2. Literature review and problem statement

In works [1–4] video image compression technologies based on the use of methods without loss of information quality and with controlled loss of its quality are presented. The most well-known lossless technologies are TIFF and PNG, and with controlled loss of quality – technologies based on the JPEG platform. In this case, conditions are created to reduce the amount of video data.

At the same time, there are two systemic drawbacks. First, there are no technological mechanisms to protect video information and there is a possibility of using metadata to form key sequences – this is reflected in works [5–7]. Secondly, the insufficient level of compression of video images in the conditions of preserving their required reliability – this is investigated in works [8, 9]. This is what leads to a decrease in the efficiency of the entire process of processing video data.

An option to overcome the first systemic flaw may be the additional use of cryptographic methods. The most widely used approach is defined as sequential. It is used in [10–12] and provides for the sequential execution of compression and encryption transformations. So, in [10], a general version of the sequential scheme for ensuring the safety of different types of data is presented. In [12], it is considered from the standpoint of ensuring the safety of video images. To ensure the confidentiality of video images in the sequential scheme, well-known and well-tested standards for cryptographic transformations are used. Such standards, for example, include the symmetric encryption algorithms AES [13], Kalina [14], GOST 28147 [15] and the asymmetric encryption algorithm RSA [16]. However, a significant drawback of this approach is the increase in the time for processing video data. So, in the conditions of using modern formats for presenting video images, significant time delays occur. This result is shown in [7, 17, 18].

As an alternative to this approach, the Encryption-then-Compression scheme is used, which is considered for various image compression technologies in [19–22]. It provides, on the contrary, first performing the encryption stage, and only then the compression stage. So, in [19], an approach to organizing this scheme together with the JPEG compression technology is considered, in [20] – with the JPEG XR algorithm, in [21] – with the JPEG 2000 algorithm, and in [22] – with an algorithm on based on prediction of compression errors. In these algorithms, encryption is mainly based on permutation operations and is aimed at changing the location of pixels. The use of this scheme leads not only to a decrease in processing time, but also reduces the degree of compression of video images.

Another approach to ensuring the confidentiality of video images is the use of secret distribution schemes (visual cryptography). This scheme originates from work [23], in which it is proposed to organize the splitting of one original uncompressed image into several unrecognizable video data. However, this leads to a significant drawback associated with a significant increase in the volume of the encrypted presentation of video data. To eliminate this drawback, the works [24–27] proposed various variants of the scheme for multi-secret image sharing (MSIS) based on mixing pixels of adjacent images with each other. Thus, in [24, 25], (n; n)-MSIS scheme for generating noisy images based on Boolean algebra and its improved version were developed. In work [26], the image fusion is organized on the basis of the XOR operation and inversion of the bit sequence. These schemes organize the formation of n noisy images from n original video images. In [27], (n; n + 1)-MSIS scheme for the formation of noisy images was developed. It organizes the formation of (n+1) noisy images from n source video data. However, the essential disadvantages of all these schemes are: processing of uncompressed images; the ability to recognize individual objects in the encrypted video data from the original images; the presence of all (or almost all) of the encrypted video data for correct reconstruction of video images.

Much work on video confidentiality is aimed at developing specialized scrambling transformations that are applied to the original uncompressed video images. These works include [28–32]. To ensure the privacy of video images, they use the following various options. The first option is based on the use of various permutations of several consecutive pixels, which are considered in [28–30]. The most interesting variants of them are row and column permutations with cyclic shift of elements [29] and permutation transformation based on the properties of the Rubik's cube [30]. The second option is based on permutation of pixels using two-dimensional and three-dimensional chaotic maps [28, 31]. The most famous approaches are 2D and 3D maps of Arnold's cat and baker [28], as well as permutation based on the properties of the Sudoku puzzle [31]. The third option is based on the use of chaotic mappings to generate pixel permutation tables [32]. A significant drawback of all variants of this approach is the decrease in the availability of large video images due to the processing of uncompressed video data.

Active research is being conducted towards organizing another approach to ensure the confidentiality of video images based on scrambling and encryption transformations, which are organized at different stages of video compression technologies. Thus, work [7] proposes general approaches to organizing the Secure JPEG service, which implements the privacy functionality in JPEG technology, and in [33], in JPEG 2000 technology. Various options for scrambling data in the process of performing compression conversion are presented in [17, 34, 35]. Options regarding the use of encryption transformations in various compression schemes are given in [36, 37]. Options for ensuring the confidentiality of the JPEG bitstream are proposed in [38–40]. However, in these variants, in fact, a sequential processing scheme is implemented, organized at different stages of compression conversions.

To reduce time delays during processing, it was proposed to create an approach that ensures the confidentiality of video images directly in the process of their compression. This approach is proposed to be called cryptocompression coding and is considered in [41]. The specification of cryptocompression transformations under the conditions of using key sequences in the compression process is reflected in the works [42, 43]. This is what creates a conceptual approach to protecting video information in the process of its compression coding.

To eliminate the second systemic drawback of existing compression technologies, it is proposed to use non-equilibrium

positional coding as a basis for cryptocompression transformations. This approach is studied in [8]. In this case, the key sequence is the base system of the non-equilibrium positional basis. But such bases are formed in absolute space, that is, the lower limit of the dynamic range of video data is not taken into account. This, as shown in [44], reduces the level of confidentiality of information. It is proposed to localize such shortcomings by additionally taking into account the lower boundary of the dynamic ranges of video data in the process of constructing a system of bases for non-equilibrium positional coding. In this case, the base system is created in a differential non-equilibrium positional basis [45]. However, on the other hand, this leads to an increase in the amount of overhead and to an increase in the total volume of compact presentation of video data. This affects the increase in time delays in the process of transmitting video information in a telecommunications network. All this gives grounds to assert that it is expedient to conduct a study devoted to the development of a method for coding the service components of the cryptocompression representation of a video image.

3. The aim and objectives of research

The aim of research is to develop a method for coding the service components of the cryptocompression representation of images to reduce their volume without losing their reliability.

To achieve this aim, it is necessary to solve the following objectives:

– to develop a second stage of cryptocompression coding to further reduce the overhead redundancy;

– to conduct an experimental assessment of the effect of reducing the redundancy of service data on reducing the volume of video information.

4. Materials and methods of research

Methods of digital image processing, methods of information coding, methods of compressing digital images, methods of structural combinatorial coding were used as theoretical research methods. Methods of statistical analysis were used to assess the adequacy of the results obtained.

During the development of the coding method, the following restrictions were used:

– processing is focused on coding static video images presented in RGB color space;

– service components of the cryptocompression codograms are processed, and not the original elements of the video images. Different types of service data of cryptocompression codograms are subjected to the same type of processing;

– restrictions are imposed on the dimensions of the images $M \times N$ elements, where M is the number of lines in the image, and N is the number of columns. The method does not describe the processing of data located in the outer regions of the image and does not form fully filled data blocks with dimensions of $m \times n$ elements, where m is the number of rows in a block, and n is the number of columns. The following conditions are met:

$$\frac{M}{m}=\left[\frac{M}{m}\right] \text{ and } \frac{N}{n}=\left[\frac{N}{n}\right],$$

where [•] is the integer part of the number;

– each color plane of the image is coded separately and does not depend on the processing of the rest of the data.

Mathematical formulation of the research problem. It is necessary to develop a method for coding the service components of cryptocompression codograms, which is specified by the functional $F(S_{CCP1}, m, n, L_{cw})$. Here: S_{CCP1} is the service data of the cryptocompression codogram obtained after the first processing stage; L_{cw} is the length of the codeword (the maximum number of bit digits) allocated to control the formation of code values of the information component. The developed method is the second stage of processing in the cryptocompression coding system. It must ensure that the following conditions are met:

1) reducing the amount of service data in the cryptocompression coding system:

$$Q_{S1}>Q_{S2},$$

where Q_{S1} is the volume of service components of cryptocompression codograms after the first processing stage;

Q_{S2} is the volume of service components of cryptocompression codograms after the second processing stage;

2) reduction of the total volume of compact representation of video data without loss of information quality in the cryptocompression coding system:

$$Q_{img}>Q_{CCP1}>Q_{CCP2};$$

$$Q_{comp}\geq Q_{CCP2},$$

where Q_{img} is the volume of the original video image;

Q_{CCP1} is the volume of compact representation of video data in the cryptocompression coding system after the first processing stage;

Q_{CCP2} is the volume of compact representation of video data in the cryptocompression coding system after the second processing stage, taking into account the volume of the information component received after the first coding stage;

Q_{comp} is the volume of compact representation of video data, which are formed by well-known image coding methods without loss of information quality.

In this case, during the encoding process, it is necessary to exclude the distortion of video images. That is, the standard deviation of the RSME of the reconstructed images relative to the original video data should be equal to 0.

To assess the effectiveness of the developed method, simulation was carried out in the form of a full-scale experiment.

For this, a software implementation of the developed method for encoding service data has been performed. It is implemented as an executable file that runs on operating systems of the Microsoft Windows XP family and above. Additional third-party libraries are not required for the software implementation to work correctly. There are no additional requirements for personal computing equipment and the operating system to ensure the correct functioning of the software implementation.

Experiment plan:

1. Three groups of pre-classified images were used depending on the degree of saturation with fine details, namely, weakly saturated, medium-saturated and highly saturated. The images were taken from standardized databases that are used to test methods for encoding and processing video information.

2. Averaged results were obtained for 100 images of each of the three classes. In this case, the confidence interval is ±3 %. The 3-sigma rule was used to estimate the confidence interval.

The reliability of the results obtained is confirmed by the reconstruction of test images without loss of information. For all reconstructed images, the standard deviation of the RSME is 0.

5. The results of research on the development of a method for coding service data in systems of cryptocompression representation of images

5. 1. Development of the second stage of cryptocompression coding

The results of the implementation of methods of cryptocompression representation of images are the formation of cryptocompression codograms [11, 12]. They consist of information and service components. The information component is a compact representation of the original values of the elements in the image. The service component contains information about the identified structural characteristics of video data. It is used to encode and decode the code values of the information component, that is, it acts as a transformation key. Therefore, to ensure the safety of cryptocompression codograms, the service component must be kept secret. It undergoes a secondary cryptographic transformation using scrambling and/or encryption algorithms.

Cryptocompression coding is organized for each separate plane A of the image with a dimension of $M\times N$ elements. To form the service components, the plane A is divided into identical blocks $A^{(\gamma;\chi)}$, where γ is the vertical coordinate of the block in the image, χ is the horizontal coordinate. The dimension of the blocks $A^{(\gamma;\chi)}$ is $m\times n$ elements. Blocks $A^{(\gamma;\chi)}$ are two-dimensional arrays of elements $a_{i,j}^{(\gamma;\chi)}$, where $\gamma=\overline{1,\left[\frac{M}{m}\right]}$, $\chi=\overline{1,\left[\frac{N}{n}\right]}$, $i=\overline{1,m}$, $j=\overline{1,n}$.

For each block $A^{(\gamma;\chi)}=\left\{a_{i,j}^{(\gamma;\chi)}\right\}$ in the direction along the i-th rows, the maximum $\lambda_i^{(\gamma;\chi)}$ and minimum $\mu_i^{(\gamma;\chi)}$ values of the elements $a_{i,j}^{(\gamma;\chi)}$ are determined. From them, the column vectors of the service data $\Lambda^{(\gamma;\chi)}=\left\{\lambda_i^{(\gamma;\chi)}\right\}$ and $\Theta^{(\gamma;\chi)}=\left\{\mu_i^{(\gamma;\chi)}\right\}$, are constructed, which form the service components $\Lambda=\left\{\Lambda^{(\gamma;\chi)}\right\}$ and $\Theta=\left\{\Theta^{(\gamma;\chi)}\right\}$ of the cryptocompression codogram of the image plane A.

To form the information component E of the cryptocompression codogram, the two-dimensional matrix $A=\left\{a_{i,j}^{(\gamma;\chi)}\right\}$ of the image plane is transformed into a vector representation $A=\{a_\tau\}$, where $\tau=\overline{1,M\cdot N}$. The transformation of two-dimensional matrices of service components $\Lambda=\left\{\lambda_i^{(\gamma;\chi)}\right\}$ and $\Theta=\left\{\mu_i^{(\gamma;\chi)}\right\}$ into a vector representation can be organized:

– taking into account the expansion of the dimension of the resulting vectors to the size of the vector representation of the video data. It is organized by repeating each element n times $\lambda_i^{(\gamma;\chi)}$, $\mu_i^{(\gamma;\chi)}$. Then vectors $\Lambda'=\left\{\lambda'_\tau\right\}$ and $\Theta'=\left\{\mu'_\tau\right\}$, $\tau=\overline{1,M\cdot N}$, are formed;

– without organizing the expansion of the dimension of the vectors of service components. Then vectors

$$\Lambda=\left\{\lambda_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]}\right\}\ \text{and}\ \Theta=\left\{\mu_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]}\right\},$$

$\tau=\overline{1,M\cdot N}$, are formed.

Formation of the code value E_α of the information component of the cryptocompression image representation based on a floating coding scheme in a differentiated basis for the vector data representation is given by the following expressions:

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

$$W_\tau=\begin{cases}\prod_{\xi=\tau+1}^{\tau(0)_\alpha+\Psi_\alpha-1}\left(\lambda'_\xi+1-\mu'_\xi\right)=\\ =\prod_{\xi=\tau+1}^{\tau(0)_\alpha+\Psi_\alpha-1}\left(\lambda_{m\cdot\left[\frac{\xi-1}{m\cdot n}\right]+\xi-m\cdot\left[\frac{\xi-1}{m}\right]}+1-\mu_{m\cdot\left[\frac{\xi-1}{m\cdot n}\right]+\xi-m\cdot\left[\frac{\xi-1}{m}\right]}\right), \quad (2)\\ \text{if } \tau<\tau(0)_\alpha+\Psi_\alpha-1;\\ 1,\\ \text{if } \tau=\tau(0)_\alpha+\Psi_\alpha-1,\end{cases}$$

where

$$\tau\in\left[\tau(0)_\alpha;\tau(0)_\alpha+\Psi_\alpha-1\right]$$

and

$$\tau(0)_\alpha+\Psi_\alpha-1\le M\cdot N,$$

where α is the ordinal number of the generated value of the code value E_α of the information component of the cryptocompression codogram;

τ, ξ is linear vector coordinates that determine the position of the data processed during encoding;

$\tau(0)_\alpha$ is the starting coordinate of the element a_τ in vector form, from which the formation of the value of the code value begins;

Ψ_α is a floating (non-deterministic) number of elements a_τ participating in the formation of the code value E_α of the information component, which depends on the values of the processed data;

W_τ is the weighting coefficient for the τ-th element a_τ, which is the product of the base elements λ'_ξ following it, taking into account the decrease in their dynamic ranges by μ'_ξ.

The code values E_α form the information component $E=\{E_\alpha\}$ of the cryptocompression codogram.

From the analysis of the process of forming the systems of service components of cryptocompression codograms, it can be seen that:

– the generated column vectors $\Lambda^{(\gamma;\chi)}$ and $\Theta^{(\gamma;\chi)}$ contain information that characterizes one original data block $A^{(\gamma;\chi)}$. Therefore, elements $\lambda_i^{(\gamma;\chi)}$ and $\mu_i^{(\gamma;\chi)}$ in them can contain values close to each other;

– each of the matrices Λ and Θ of service components has a size equal to $M\cdot\left[\frac{N}{n}\right]$ bytes. Consequently, the volume of the service component of the cryptocompression codogram is 2 times less than the volume of the original image. When the parameter $n=8$ is selected, the volume of the service com-

ponent of the cryptocompression codogram is 25 % of the volume of the original video data. This value continues to be significant. Therefore, it is required to develop a method that will reduce its volume.

To reduce the volume of service components Λ and Θ, their additional cryptocompression coding can be organized. This processing option will be called the second stage of the cryptocompression coding technology. Here, the two-dimensional matrices Λ and Θ are intermediate data generated after the first processing stage.

The formation of cryptocompression codograms at the second stage begins with the formation of new service components for each of the two-dimensional matrices Λ and Θ. To do this, in each column vector $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$ are defined:

– the maximum elements $\lambda(\max)^{(\gamma,\chi)}$ and $\mu(\max)^{(\gamma,\chi)}$ by the formulas:

$$\lambda(\max)^{(\gamma,\chi)} = \max_{1\le i\le m}\left(\lambda_i^{(\gamma,\chi)}\right); \quad (3)$$

$$\mu(\max)^{(\gamma,\chi)} = \max_{1\le i\le m}\left(\mu_i^{(\gamma,\chi)}\right); \quad (4)$$

– minimal elements $\lambda(\max)^{(\gamma,\chi)}$ and $\mu(\max)^{(\gamma,\chi)}$ by the formulas:

$$\lambda(\min)^{(\gamma,\chi)} = \min_{1\le i\le m}\left(\lambda_i^{(\gamma,\chi)}\right); \quad (5)$$

$$\mu(\min)^{(\gamma,\chi)} = \min_{1\le i\le m}\left(\mu_i^{(\gamma,\chi)}\right). \quad (6)$$

Elements $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ and $\mu(\min)^{(\gamma,\chi)}$ are combined into the corresponding two-dimensional data $\Lambda(\max)=\{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min)=\{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max)=\{\mu(\max)^{(\gamma,\chi)}\}$ and $\Theta(\min)=\{\mu(\min)^{(\gamma,\chi)}\}$. They are service components of cryptocompression codograms. The dimension of each array is equal to $\left[\frac{M}{m}\right]\times\left[\frac{N}{n}\right]$ elements. The volume of all matrices of service components of one plane on the second processing stage is equal to $4\cdot\left[\frac{M}{m}\right]\cdot\left[\frac{N}{n}\right]$ bytes. This is $\frac{m}{2}$ times less than the volume of intermediate two-dimensional matrices Λ and Θ and $\frac{m\cdot n}{4}$ times less than the volume of the processed image plane A.

Service components contain information about the structural characteristics of video data and require the organization of a secondary (additional) cryptographic transformation to ensure the security of cryptocompression codograms.

The coding of two-dimensional matrices Λ and Θ on the second stage is organized in the row direction. Each of the matrices has the dimension of the $M\times\left[\frac{N}{n}\right]$ elements. They are uniformly partitioned into the corresponding column vectors $\Lambda^{(\gamma,\chi)}$ or $\Theta^{(\gamma,\chi)}$ with coordinates (γ; χ). Each column vector consists of m elements.

Elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ have a three-dimensional coordinate. It consists of the coordinate (γ; χ) of the corresponding column vector $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$, $\gamma=\overline{1,\left[\frac{M}{m}\right]}$, $\chi=\overline{1,\left[\frac{N}{n}\right]}$, and location ($i$) in it, $i=\overline{1,m}$. Elements are processed sequentially within two-dimensional matrices Λ or Θ in the row direction. Processing starts from the first element $\lambda_1^{(1,1)}$, $\mu_1^{(1,1)}$ for γ=1, χ=1 and i=1. Coordinate variables γ and i are fixed and are responsible for the line number in the processed block Λ or Θ. Processing is organized for all elements $\lambda_1^{(1,\chi)}$, of the line when the value of the coordinate variable $\chi=\overline{1,\left[\frac{N}{n}\right]}$ changes. After that, processing is transferred to the first element $\lambda_2^{(1,1)}$ or $\mu_2^{(1,1)}$ of the second line, and so on. The number of each subsequent processed line is determined as (γ · i), where $\gamma=\overline{1,\left[\frac{M}{m}\right]}$, $i=\overline{1,m}$. Moreover, changing the value of the coordinate variable γ is possible only after the last element in the line with the coordinate variable i=m has been processed. After changing the value of the coordinate variable γ, the value of the coordinate variable i=1. In general, it is possible to write that the processing of elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ is either carried out in a line with a serial number with fixed values of the coordinate variables γ and i when the value of the coordinate variable $\chi=\overline{1,\left[\frac{N}{n}\right]}$ changes from the first element $\lambda_i^{(\gamma,1)}$ or $\mu_i^{(\gamma,1)}$ to the last $\lambda_i^{\left(\gamma\left[\frac{N}{n}\right]\right)}$ or $\mu_i^{\left(\gamma\left[\frac{N}{n}\right]\right)}$. Processing ends when the last element is encoded $\lambda_m^{\left(M\left[\frac{N}{n}\right]\right)}$ or $\mu_m^{\left(M\left[\frac{N}{n}\right]\right)}$.

To organize a floating coding scheme in conditions of reduced computational complexity, it is proposed to reformat the two-dimensional matrices Λ and Θ into one-dimensional vectors, namely:

$$\Lambda=\left\{\lambda_\eta\right\}=\left\{\lambda_i^{(\gamma,\chi)}\right\};\ \ \Theta=\left\{\mu_\eta\right\}=\left\{\mu_i^{(\gamma,\chi)}\right\},$$

where

$$\eta=\overline{1,M\cdot\left[\frac{N}{n}\right]},\ \ \gamma=\overline{1,\left[\frac{M}{m}\right]},\ \ \chi=\overline{1,\left[\frac{N}{n}\right]},\ \ i=\overline{1,m},$$

where η is the one-dimensional coordinate of the elements and the corresponding two-dimensional matrix Λ and Θ, reformatted into a one-dimensional vector.

Linearization of three-dimensional coordinates of elements $\lambda_i^{(\gamma,\chi)}$ and $\lambda_i^{(\gamma,\chi)}$ of the two-dimensional matrices Λ and Θ into one-dimensional is carried out on the basis of the expression:

$$\eta=\left((\gamma-1)\cdot m+i-1\right)\cdot\left[\frac{N}{n}\right]+\chi. \quad (7)$$

On the contrary, the reconstruction of the three-dimensional coordinates of the elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ from the one-dimensional (η) is described by the following expressions:

$$\gamma=\left[\frac{\left[\frac{\eta-1}{m}\right]}{\left[\frac{N}{n}\right]}\right]+1;$$

$$\chi=\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\cdot\left[\frac{N}{n}\right];$$

$$i=\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]+1-\left[\frac{\left[\frac{\eta-1}{m}\right]}{\left[\frac{N}{n}\right]}\right]\cdot m.$$

These relations make it possible to organize a one-to-one correspondence of elements $\lambda_i^{(\gamma,\chi)}$ and $\mu_i^{(\gamma,\chi)}$ between their representations in three-dimensional and one-dimensional spaces.

Reformatting of two-dimensional arrays of service components $\Lambda(\max)=\{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min)=\{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max)=\{\mu(\max)^{(\gamma,\chi)}\}$ and $\Theta(\min)=\{\mu(\min)^{(\gamma,\chi)}\}$ into one-dimensional vectors can be organized in one of two ways, namely:

1) for the initial sizes of two-dimensional arrays of service components, each of which is equal to $\left[\frac{M}{m}\right]\times\left[\frac{N}{n}\right]$ elements;

2) taking into account the expansion of their dimension to the size of $M\times\left[\frac{N}{n}\right]$ elements, which corresponds to the size of two-dimensional arrays of processed data Λ and Θ.

In the first case, vectors are formed:

$$\Lambda(\max)=\left\{\lambda(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}\right\};$$

$$\Lambda(\min)=\left\{\lambda(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}\right\};$$

$$\Theta(\max)=\left\{\mu(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}\right\};$$

$$\Theta(\min)=\left\{\mu(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}\right\},\quad \eta=\overline{1,M\cdot\left[\frac{N}{n}\right]}.$$

They consist of elements from $\lambda(\max)_1$ to $\lambda(\max)_{\left[\frac{M}{m}\right]\left[\frac{N}{n}\right]}$, from $\lambda(\min)_1$ to $\lambda(\min)_{\left[\frac{M}{m}\right]\left[\frac{N}{n}\right]}$, from $\mu(\max)_1$ to $\mu(\max)_{\left[\frac{M}{m}\right]\left[\frac{N}{n}\right]}$ and from $\mu(\min)_1$ to $\mu(\min)_{\left[\frac{M}{m}\right]\left[\frac{N}{n}\right]}$, respectively. Reformatting two-dimensional matrices $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ and $\Theta(\min)$ into one-dimensional vectors does not change the values of their elements and does not change their number.

In the second case, it is proposed to repeat each row in the arrays of service components $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ and $\Theta(\min)$ m times. As a result, two-dimensional matrices

$$\Lambda'(\max)=\left\{\lambda'(\max)_i^{(\gamma,\chi)}\right\},\ \Lambda'(\min)=\left\{\lambda'(\min)_i^{(\gamma,\chi)}\right\},$$
$$\Theta'(\max)=\left\{\mu'(\max)_i^{(\gamma,\chi)}\right\}\ \text{and}\ \Theta'(\min)=\left\{\mu'(\min)_i^{(\gamma,\chi)}\right\}$$

and element dimensions $M\times\left[\frac{N}{n}\right]$ are formed. Their element values are determined according to the expressions:

$$\lambda'(\max)_i^{(\gamma,\chi)}=\lambda(\max)^{(\gamma,\chi)};$$

$$\lambda'(\min)_i^{(\gamma,\chi)}=\lambda(\min)^{(\gamma,\chi)};$$

$$\mu'(\max)_i^{(\gamma,\chi)}=\mu(\max)^{(\gamma,\chi)};$$

$$\mu'(\min)_i^{(\gamma,\chi)}=\mu(\min)^{(\gamma,\chi)},\quad i=\overline{1,m}.$$

As a result of reformatting these two-dimensional matrices, one-dimensional vectors are formed:

$$\Lambda'(\max)=\left\{\lambda'(\min)_\eta\right\}=$$
$$=\left\{\lambda'(\max)_i^{(\gamma,\chi)}\right\}=\left\{\lambda(\max)^{(\gamma,\chi)}\right\}_{i=\overline{1,m}};$$

$$\Lambda'(\min)=\left\{\lambda'(\min)_\eta\right\}=$$
$$=\left\{\lambda'(\min)_i^{(\gamma,\chi)}\right\}=\left\{\lambda(\min)\right\}_{i=\overline{1,m}};$$

$$\Theta'(\max)=\left\{\mu'(\min)_\eta\right\}=$$
$$=\left\{\mu'(\max)_i^{(\gamma,\chi)}\right\}=\left\{\mu(\max)\right\}_{i=\overline{1,m}};$$

$$\Theta'(\min)=\left\{\mu'(\min)_\eta\right\}=$$
$$=\left\{\mu'(\min)_i^{(\gamma,\chi)}\right\}=\left\{\mu'(\min)\right\}_{i=\overline{1,m}},$$

$$\eta=\overline{1,M\cdot\left[\frac{N}{n}\right]},$$

with the number of $M\cdot\left[\frac{N}{n}\right]$ elements in each.

At the same time, an unambiguous correspondence of one-dimensional coordinates is organized for the elements of arrays of service components, formed taking into account the expansion of their dimension and without its organization, namely:

$$\lambda'(\max)_\eta=\lambda(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]};$$

$$\lambda'(\min)_\eta=\lambda(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]};$$

$$\mu'(\max)_\eta=\mu(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]};$$

$$\mu'(\min)_\eta=\mu(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]},\quad \eta=\overline{1,M\cdot\left[\frac{N}{n}\right]}.$$

Taking into account the created methods of linearization of the coordinates of two-dimensional matrices Λ and Θ, as well as the service components $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ and $\Theta(\min)$, cryptocompression coding at the second stage is organized based on the use of basic expressions (1), (2). These expressions form the technological core of the cryptocompression data conversion system. The input and output

parameters of the technological core depend on the type of data being processed.

For the developed method of cryptocompression coding of two-dimensional matrices Λ and Θ, the input parameters are:

– the values of the initial elements a_τ of the video data, which are determined according to the condition:

$$a_\tau = \begin{cases} \lambda_\eta, & \text{if matrix } \Lambda \text{ is processed;} \\ \mu_\eta, & \text{if matrix } \Theta \text{ is processed;} \end{cases}$$

– values of elements λ'_τ and μ'_τ

$$\left(\lambda_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]} \text{ and } \mu_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]} \right)$$

service components. They are determined depending on the data being processed according to the conditions:

$$\lambda'_\tau = \lambda_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]} =$$

$$= \begin{cases} \lambda'(\max)_\eta = \\ = \lambda(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}, & \text{if matrix } \Lambda \text{ is processed;} \\ \mu'(\max)_\eta = \\ = \mu(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}, & \text{if matrix } \Theta \text{ is processed;} \end{cases}$$

$$\mu'_\tau = \mu_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]} =$$

$$= \begin{cases} \lambda'(\min)_\eta = \\ = \lambda(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}, & \text{if matrix } \Lambda \text{ is processed;} \\ \mu'(\min)_\eta = \\ = \mu(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]}, & \text{if matrix } \Theta \text{ is processed;} \end{cases}$$

– the number τ of the processed service components, which is equal to:

$$\tau = \eta = \overline{1, M\cdot\left[\frac{N}{n}\right]}.$$

At the output of the cryptocompression coding system at the second stage, code values E_α are generated that transform the information component. The type of generated code values is determined depending on the data being processed according to the condition:

$$E_\alpha = \begin{cases} E(\Lambda)_{\alpha(\Lambda)}, & \text{if matrix } \Lambda \text{ is processed;} \\ E(\Theta)_{\alpha(\Theta)}, & \text{if matrix } \Theta \text{ is processed,} \end{cases}$$

where $E(\Lambda)_{\alpha(\Lambda)}$, $E(\Theta)_{\alpha(\Theta)}$ are the values of the code values of the information component of the cryptocompression representation of the image based on a floating coding scheme in a differentiated basis, obtained at the second coding stage as a result of processing the elements of the corresponding two-dimensional matrices Λ or Θ;

$\alpha(\Lambda)$, $\alpha(\Theta)$ are the ordinal numbers of the generated corresponding values of the code values $E(\Lambda)_{\alpha(\Lambda)}$ and $E(\Theta)_{\alpha(\Theta)}$, which are defined as:

$$\alpha = \begin{cases} \alpha(\Lambda), & \text{if matrix } \Lambda \text{ is processed;} \\ \alpha(\Theta), & \text{if matrix } \Theta \text{ is processed.} \end{cases}$$

As a result of encoding, intermediate values are formed and used, namely:

– the number of Ψ_α elements forming the code value. They are determined according to the condition:

$$\Psi_\alpha = \begin{cases} \Psi(\Lambda)_{\alpha(\Lambda)}, & \text{if matrix } \Lambda \text{ is processed;} \\ \Psi(\Theta)_{\alpha(\Theta)}, & \text{if matrix } \Theta \text{ is processed,} \end{cases}$$

where $\Psi(\Lambda)_{\alpha(\Lambda)}$, $\Psi(\Theta)_{\alpha(\Theta)}$ is the corresponding floating (non-deterministic) number of elements λ_η or μ_η participating in the formation of the code value $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$ information component at the second processing stage, which depends on the values of the processed data;

– starting coordinate $\tau(0)_\alpha$ for generating the code value. It corresponds to the type of data being processed according to the conditions:

$$\tau(0)_\alpha = \begin{cases} \tau(\Lambda)_{\alpha(\Lambda)}, & \text{if matrix } \Lambda \text{ is processed;} \\ \tau(\Theta)_{\alpha(\Theta)}, & \text{if matrix } \Theta \text{ is processed,} \end{cases}$$

where $\tau(\Lambda)_{\alpha(\Lambda)}$, $\tau(\Theta)_{\alpha(\Theta)}$ is the corresponding starting coordinate of the element λ_η or μ_η, from which the generated value of the code value $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$.

The quantities $\Psi(\Lambda)_{\alpha(\Lambda)}$ and $\Psi(\Theta)_{\alpha(\Theta}$ of elements are determined based on the condition that the formation of the values of the code values $E(\Lambda)_{\alpha(\Lambda)}$ и $E(\Theta)_{\alpha(\Theta)}$ should not lead to overflow of the codeword $L_{c\bar{w}}$ allocated for their storage. These conditions are written as follows:

$$\log_2\left(E(\Lambda)_{\alpha(\Lambda)}\right) \le L_{c\bar{w}}, \ \log_2\left(E(\Theta)_{\alpha(\Theta)}\right) \le L_{c\bar{w}}. \quad (8)$$

The method of coding the service data in the systems of cryptocompression representation of images is the organization of the second cascade of coding. It consists of the following technological stages.

The input data of the method are:

– service components $\Lambda = \left\{\lambda_i^{(\gamma,\chi)}\right\}$ and $\Theta = \left\{\mu_i^{(\gamma,\chi)}\right\}$ of the cryptocompression codograms obtained after the first stage of processing. They are considered as intermediate two-dimensional matrices and are structurally divided into column vectors $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$. Each intermediate two-dimensional matrix has the dimension of the $M\times\left[\frac{N}{n}\right]$ elements;

– dimensions of processed images M and N;

– dimensions of video processing blocks m and n, selected at the first stage of cryptocompression coding;

– the length of the codeword $L_{c\bar{w}}$, allocated to control the formation of code values of the information component.

Coding for different types of intermediate data Λ and Θ is organized separately or in parallel.

1. At the first stage, in all column vectors $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$:

– using formulas (3) and (4), the maximum elements $\lambda(\max)^{(\gamma,\chi)}$ and $\mu(\max)^{(\gamma,\chi)}$ are determined;

– using formulas (5) and (6), the minimum elements $\lambda(\max)^{(\gamma,\chi)}$ and $\mu(\max)^{(\gamma,\chi)}$ are determined.

These elements are combined into two-dimensional data arrays $\Lambda(\max)=\{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min)=\{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max)=\{\mu(\max)^{(\gamma,\chi)}\}$ and $\Theta(\min)=\{\mu(\min)^{(\gamma,\chi)}\}$. They are new service components of cryptocompression codograms obtained after the second processing stage.

2. At the second stage, reformatting is organized:

– two-dimensional matrices $\Lambda=\left\{\lambda_i^{(\gamma,\chi)}\right\}$ and $\Theta=\left\{\mu_i^{(\gamma,\chi)}\right\}$ into one-dimensional vectors $\Lambda=\{\lambda_\eta\}$ и $\Theta=\{\mu_\eta\}$ based on the linearization of coordinates using expression (7);

– two-dimensional arrays of service components $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ and $\Theta(\min)$ into one-dimensional vectors.

3. At the third stage, the starting coding parameters are set for the formation of the first code values $E(\Lambda)_{\alpha(\Lambda)}$ and $E(\Theta)_{\alpha(\Theta)}$ of the information components obtained after the second coding stage, namely:

– ordinal start numbers $\alpha(\Lambda)=1$ and $\alpha(\Theta)=1$;

– are the starting coordinates of the elements from which the encoding begins, $\tau(\Lambda)_{\alpha(\Lambda)}=1$ and $\tau(\Theta)_{\alpha(\Theta)}=1$.

4. At the fourth stage, code values $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$ are formed, depending on the type of processed service data. The stage consists of four steps. At the first step, the counters of the number of elements involved in the formation of the corresponding code values are set equal to $\Psi(\Lambda)_{\alpha(\Lambda)}=1$ or $\Psi(\Theta)_{\alpha(\Theta)}=1$. At the second step, using the basic expressions (1) and (2) and taking into account the selected correspondences of the processed elements, intermediate code values $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$ are calculated. At the third step, an overflow check of the L_{cw} codeword is organized. Namely, the fulfillment of inequality (8) is verified. If condition (8) is satisfied, then at the fourth step the value of the counter of the number of elements participating in the formation of the code value $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$, is increased by 1, i. e.

$$\Psi(\Lambda)_{\alpha(\Lambda)}=\Psi(\Lambda)_{\alpha(\Lambda)}+1$$

or

$$\Psi(\Theta)_{\alpha(\Theta)}=\Psi(\Theta)_{\alpha(\Theta)}+1.$$

After that, let's move on to the second step. If condition (8) is not met, then at the fifth step it is determined that the maximum number of elements forming the code value $E(\Lambda)_{\alpha(\Lambda)}$ or $E(\Theta)_{\alpha(\Theta)}$ of the information component at the second processing stage is, respectively, $\Psi(\Lambda)_{\alpha(\Lambda)}$ or $\Psi(\Theta)_{\alpha(\Theta)}$, and the previous code values are the resulting ones.

5. At the fifth stage, the presence of uncoded data in one-dimensional vectors $\Lambda=\{\lambda_\eta\}$ and $\Theta=\{\mu_\eta\}$ is checked using the condition

$$\left(\tau(\Lambda)_{\alpha(\Lambda)}+\Psi(\Lambda)_{\alpha(\Lambda)}-1\right)<M\cdot\left[\frac{N}{n}\right]$$

or

$$\left(\tau(\Theta)_{\alpha(\Theta)}+\Psi(\Theta)_{\alpha(\Theta)}-1\right)<M\cdot\left[\frac{N}{n}\right].$$

If all the elements have not been processed, then processing continues at the sixth stage. Otherwise, the processing proceeds to the seventh stage.

6. At the sixth stage, new starting parameters are determined for the formation of a new code value, namely:

– the serial number of the code is increased by one:

$$\alpha(\Lambda)=\alpha(\Lambda)+1$$

or

$$\alpha(\Theta)=\alpha(\Theta)+1;$$

– new starting coordinates are determined using the formula:

$$\tau(\Lambda)_{\alpha(\Lambda)}=\tau(\Lambda)_{\alpha(\Lambda)-1}+\Psi(\Lambda)_{\alpha(\Lambda)-1}$$

or

$$\tau(\Theta)_{\alpha(\Theta)}=\tau(\Theta)_{\alpha(\Theta)-1}+\Psi(\Theta)_{\alpha(\Theta)-1}.$$

After this, the fourth stage is performed.

7. At the seventh stage, all obtained code values $E(\Lambda)_{\alpha(\Lambda)}$ and $E(\Theta)_{\alpha(\Theta)}$ are combined and form the corresponding information code streams $E(\Lambda)=\{E(\Lambda)_{\alpha(\Lambda)}\}$ and $E(\Theta)=\{E(\Theta)_{\alpha(\Theta)}\}$ based on non-uniform lengths $q(\Lambda)_{\alpha(\Lambda)}$ and $q(\Theta)_{\alpha(\Theta)}$.

The lengths $q(\Lambda)_{\alpha(\Lambda)}$ and $q(\Theta)_{\alpha(\Theta)}$ are individual for each individual code value. They do not exceed the maximum length of the selected codeword L_{cw} and are determined on the basis of the accumulated product of the number of elements of service components using the expressions:

$$q(\Lambda)_{\alpha(\Lambda)}=\left[\log_2\sum_{\xi=\tau(\Lambda)_{\alpha(\Lambda)}}^{\tau(\Lambda)_{\alpha(\Lambda)}+\Psi(\Lambda)_{\alpha(\Lambda)}-1}\begin{pmatrix}\lambda'(\max)+\\+1-\lambda'(\min)\end{pmatrix}\right]+1=$$
$$=\left[\log_2\sum_{\xi=\tau(\Lambda)_{\alpha(\Lambda)}}^{\tau(\Lambda)_{\alpha(\Lambda)}+\Psi(\Lambda)_{\alpha(\Lambda)}-1}\begin{pmatrix}\lambda(\max)-\left[\frac{-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]+1-\\-\lambda(\min)-\left[\frac{-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]\end{pmatrix}\right]+1; \quad (9)$$

$$q(\Theta)_{\alpha(\Theta)}=\left[\log_2\sum_{\xi=\tau(\Theta)_{\alpha(\Theta)}}^{\tau(\Theta)_{\alpha(\Theta)}+\Psi(\Theta)_{\alpha(\Theta)}-1}\begin{pmatrix}\mu'(\max)+\\+1-\mu'(\min)\end{pmatrix}\right]+1=$$
$$=\left[\log_2\sum_{\xi=\tau(\Theta)_{\alpha(\Theta)}}^{\tau(\Theta)_{\alpha(\Theta)}+\Psi(\Theta)_{\alpha(\Theta)}-1}\begin{pmatrix}\mu(\max)-\left[\frac{-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]+\\+1-\mu(\min)-\left[\frac{-1}{\left[\frac{N}{n}\right]}\right]\left[\frac{N}{n}\right]\end{pmatrix}\right]+1. \quad (10)$$

The last values $\alpha(\Lambda)$ and $\alpha(\Theta)$ of the serial numbers correspond to the quantities $\tau(\Lambda)_{\max}$ and $\tau(\Theta)_{\max}$ of the generated code values of the information components after the second coding stage.

The output of the method is:

– service components $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ and $\Theta(\min)$ of cryptocompression codograms;

– information components $E(\Lambda)=\{E(\Lambda)_{\alpha(\Lambda)}\}$ and $E(\Theta)=\{E(\Theta)_{\alpha(\Theta)}\}$ of cryptocompression codograms obtained after the second processing stage.

Consequently, the formation of the code values $E(\Lambda)_{\alpha(\Lambda)}$ and $E(\Theta)_{\alpha(\Theta)}$ of the information component at the second coding stage is organized based on the use of two degrees of uncertainty, namely:

– the non-deterministic number $\Psi(\Lambda)_{\alpha(\Lambda)}$ and $\Psi(\Theta)_{\alpha(\Theta)}$ of the elements involved in the formation of these code values;

– non-deterministic length $q(\Lambda)_{\alpha(\Lambda)}$ and $q(\Theta)_{\alpha(\Theta)}$ of binary digits used to store the corresponding codograms.

As a result, the corresponding indefinite number $\alpha(\Lambda)_{\max}$ and $\alpha(\Theta)_{\max}$ of the generated code values of information components $E(\Lambda)=\{E(\Lambda)_{\alpha(\Lambda)}\}$ and $E(\Theta)=\{E(\Theta)_{\alpha(\Theta)}\}$. Moreover, it is possible to correctly position the code values $E(\Lambda)_{\alpha(\Lambda)}$ and $E(\Theta)_{\alpha(\Theta)}$ in the corresponding code streams $E(\Lambda)$ and $E(\Theta)$ of information components only if authentic service components of cryptocompression codograms are used.

5. 2. Experimental evaluation of the impact of reducing the redundancy of service data on reducing the volume of video information

The effectiveness of the developed coding method was evaluated from the position:

– assessing the degree of reduction in the amount of service data in the cryptocompression coding system;

– assessing the degree of reduction of the total volume of compact presentation of video data without loss of information quality.

Based on the analysis of the scheme for the formation of cryptocompression codograms in the encoding process, it can be seen that the volumes of service components are fixed for images of the same dimension. They do not depend on the degree of saturation of the video data with small objects. Depending on the number of cascades of cryptocompression transformation, the volumes of service components of cryptocompression codograms are determined for images presented in RGB color space using the following formulas:

– for one cascade of processing:

$$Q_{S1}=\frac{6\cdot M\cdot N}{m}; \quad (11)$$

– for two cascades of processing:

$$Q_{S2}=\frac{12\cdot M\cdot N}{m\cdot n}. \quad (12)$$

From the analysis of formulas (11) and (12) it can be seen that the volumes of the service components of the cryptocompression codograms depend on the dimensions of $M\times N$ images and the dimensions of $m\times n$ data blocks selected in the encoding process.

The developed method made it possible to form the volume of service components of cryptocompression codograms, which:

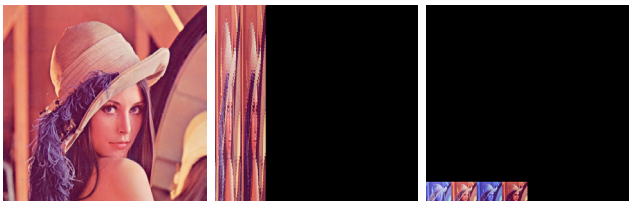
– $\frac{m\cdot n}{4}$ times less than the volume of the original image;

– $\frac{n}{2}$ times less than the volume of service components of cryptocompression codograms after the first processing stage.

The recommended parameters of $m\times n$ dimensions of the processed data blocks are 8×8 elements. These parameters are obtained empirically.

In this case, the total volume of service components of the cryptocompression codograms of the image is 16 times less than the original volume of video data, which is 6.25 %. Consequently, in comparison with the first cascade of processing, the volume of key information has decreased by 4 times. This significantly reduces the amount of data that undergoes additional cryptographic transformation. There are significantly fewer options for using standardized approaches to ensure information security. So, in the case of encryption of the original video data, it is necessary to organize a cryptographic transformation of the entire uncompressed volume of video data. And in the case of organizing a sequential security scheme, the volume of a compact representation of a video image that is encrypted also significantly exceeds the volume of service data in cryptocompression codograms.

Examples of visualization of the service components of the intermediate two-dimensional matrices Λ and Θ and the service components Λ(max), Λ(min), Θ(max) and Θ(min) of the cryptocompression codogram of the Lena test image are shown in Fig. 1 provided it is processed in 8×8 blocks. The black background in the images represents the total size of the original video data. From the analysis of the visualized representation of the service components, it can be seen that they fully characterize the image and represent its reduced copies. And therefore, they require confidentiality based on cryptographic methods.



a *b* *c*

Fig. 1. Examples of visualization of service components of the cryptocompression representation of the Lena image: *a* – the original image; *b* – visual display of intermediate two-dimensional matrices Λ and Θ; *c* – visual display of the service components of the cryptocompression codogram

The developed method does not introduce errors into the data during the encoding process and refers to methods without loss of information quality. The standard deviation RSME of all reconstructed images of different saturation classes with small objects and different sizes relative to the original video data is 0.

To assess the quality of the developed method from the standpoint of reducing the volume of the original video data without losing the quality of information, the following well-known coding methods were used:

– method of cryptocompression coding of images based on a single-stage floating processing scheme in a differentiated basis;

– coding algorithm, which is implemented in the TIFF video data presentation format. It implements the RLE series length code and the LZW prefix code;

– deflate compression algorithm, which is implemented in the PNG video data format. It combines LZ77 sliding window code with Huffman code.

The results of a comparative assessment of the developed and existing coding methods in terms of the compression ratio for images of different degrees of saturation are shown in Fig. 2.

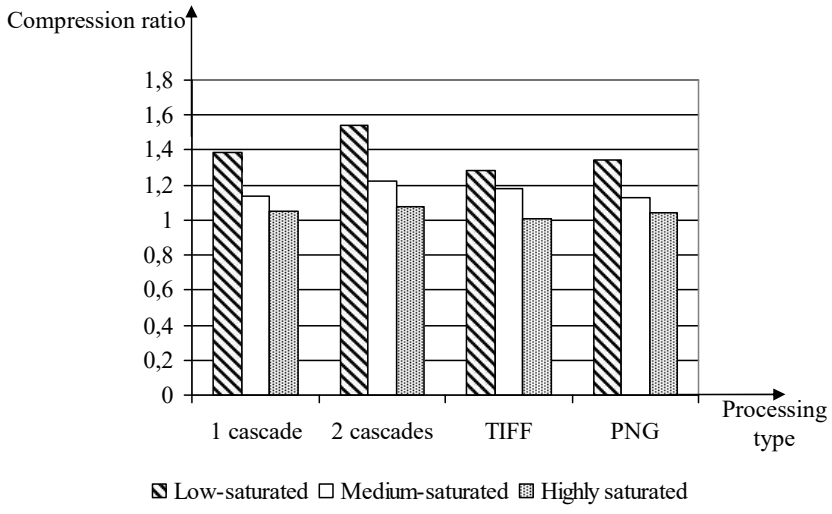


Fig. 2. The results of a comparative assessment of the developed and existing coding methods in terms of the compression ratio

From the analysis of the data in Fig. 2 that the best result in terms of the degree of image compression was shown by the method of cryptocompression coding of images in a differential basis based on two-stage coding. The average value of the compression ratio for it is 1.08 for highly saturated images, 1.22 for moderately saturated and 1.54 weakly saturated images. This is on average 4–5.2 % better than the single-stage processing method, 3–20 % better than the TIFF data format and 4–15 % better than the PNG format.

6. Discussion of the results regarding the method of encoding the service data in the systems of cryptocompression representation of images

A method for coding service data in systems of cryptocompression representation of images has been developed. It is the second stage of cryptocompression coding and is designed to reduce the amount of overhead received after the first stage of processing. Coding is organized on the basis of expressions (1) and (2), which form the technological core of the cryptocompression data conversion system. The technology of non-equilibrium positional coding is used as a basis.

For the correct operation of the method, a scheme for linearizing data from three-dimensional coordinates of the representation of service data in a two-dimensional matrix into a one-dimensional coordinate is proposed. For this, expression (7) is used. Elements of service components of cryptocompression codograms obtained after the second processing stage are determined using expressions (3), (6). The code values generated in the second processing stage are formed on a variable non-deterministic number of elements using condition (8). The length of the code values is also non-deterministic and is determined using expressions (9), (10). These non-deterministic parameters determine the correct positioning of the code value in the codestream of the information component of the cryptocompression codogram.

The volume of service components of cryptocompression codograms after the second processing stage is determined using formula (12). It is 16 times less than the original volume of video data, which is 6.25 %, and 4 times less compared to the first processing stage. The visualization of this result is shown in Fig. 1. The results of a comparative assessment of the developed and existing coding methods in terms of the compression ratio for images of different degrees of saturation are shown in Fig. 2. The developed method provides encoding of video images without loss of information quality.

The results are explained by the possibility of using a non-equilibrium positional basis simultaneously:

– to ensure the compression of service data by reducing the structural and combinatorial redundancy;

– to ensure confidentiality of video images by generating service data, which carry information about the number of elements that formed the code value of the information component, about the length of the code value and determine the positioning of the code value in the code stream of the information component.

This creates conditions for the non-determinism of the processing process and the use of this data as a transformation key. Without knowledge of this information, the possibility of correct reconstruction of video images is excluded.

Distinctive features of the developed method for encoding service components in a differentiated basis on the second stage of cryptocompression image representation are:

– organization of coding of service components, which are formed after the first stage of cryptocompression transformation;

– construction of a data linearization scheme from three-dimensional coordinates of a representation in a two-dimensional matrix into a one-dimensional coordinate for a one-to-one representation of this element in a vector. The three-dimensional coordinate of an element in a two-dimensional matrix is described by the coordinates of the block represented as a column vector in the matrix and the coordinates of the element in this column vector. Linearization is organized horizontally along the lines;

– formation of a non-deterministic number of code values of information components, which have non-deterministic lengths and are formed on a non-deterministic number of elements.

As a limitation of this research is the development of a method focused on processing static video data.

The disadvantage of this study is the unresolved issue of ensuring the safety of the generated service component in cryptocompression codograms after the second cascade of coding. This is due to the fact that the service data contains information about the structural characteristics of the video data, and therefore requires the organization of additional cryptographic transformation.

The development of this research can be aimed both at improving the method from the standpoint of processing dynamic video data, and at ensuring the cryptographic strength of service data using scrambling and encryption methods.

7. Conclusions

1. A method for coding service data has been developed, which is based on the second stage of cryptocompression

coding. It is based on the developed scheme of linearization of the coordinates of the initial and service data from the three-dimensional coordinate to the two-dimensional matrix into the one-dimensional coordinate of the vector for their one-to-one correspondence. Linearization is organized horizontally line by line. Coding is organized within the entire set of processed data. This allows to reduce the overhead of cryptocompression codograms.

2. As a result of the experimental studies, the following results were obtained:

– from the standpoint of ensuring confidentiality – the uncertainty of the positioning of uneven codograms in the general code stream is ensured, which actually eliminates the possibility of their unauthorized decryption. This is achieved through the use of non-deterministic parameters in the encoding process;

– from the point of view of ensuring accessibility – the volume of cryptocompression representation of images relative to the original video data is reduced on average from 1.08 to 1.54 times, depending on the degree of their saturation;

– from the standpoint of ensuring reliability – video information is encoded without loss of its quality, while the standard deviation RSME of all reconstructed images of different saturation classes with small objects and different sizes relative to the original video data is equal to 0;

– the total volume of service components of cryptocompression codograms is reduced by 16 times in comparison with the original volume of video data, provided it is processed in blocks of 8×8 elements. This significantly reduces the amount of key data that requires additional cryptographic transformation.

References

1. Gonzalez, R., Woods, R. (2018). Digital Image Processing. Published by Pearson, 1168.
2. Salomon, D. (2007). Data Compression: The Complete Reference. Springer Science & Business Media, 1092.
3. Vatolin, D., Ratushnyak, A., Smirnov, M., Yukin, V. (2002). Metody szhatiya dannyh. Ustroystvo arhivatorov, szhatie izobrazheniy i video. Moscow, 384.
4. Wallace, G. K. (1991). The JPEG still picture compression standard. Communications of the ACM, 34 (4), 30–44. doi: https://doi.org/10.1145/103085.103089
5. JPEG Privacy & Security Abstract and Executive Summary (2015). Available at: https://jpeg.org/items/20150910_privacy_security_summary.html
6. Barannik, V., Ryabukha, Y., Barannik, N., Barannik, D. (2020). Indirect Steganographic Embedding Method Based on Modifications of the Basis of the Polyadic System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). doi: https://doi.org/10.1109/tcset49122.2020.235522
7. Dufaux, F., Ebrahimi, T. (2006). Toward a Secure JPEG. Applications of Digital Image Processing XXIX, 6312. doi: https://doi.org/10.1117/12.686963
8. Barannik, V. V., Karpinski, M. P., Tverdokhleb, V. V., Barannik, D. V., Himenko, V. V., Aleksander, M. (2018). The technology of the video stream intensity controlling based on the bit-planes recombination. 2018 IEEE 4th International Symposium on Wireless Systems Within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). doi: https://doi.org/10.1109/idaacs-sws.2018.8525560
9. Gore, A., Gupta, S. (2015). Full reference image quality metrics for JPEG compressed images. AEU - International Journal of Electronics and Communications, 69 (2), 604–608. doi: https://doi.org/10.1016/j.aeue.2014.09.002
10. Sharma, R., Bollavarapu, S. (2015). Data Security using Compression and Cryptography Techniques. International Journal of Computer Applications, 117 (14), 15–18. doi: https://doi.org/10.5120/20621-3342
11. Belikova, T. (2020). Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), 87–91. Available at: https://ieeexplore.ieee.org/document/9349300
12. Barannik, V., Barannik, V., Havrylov, D., Sorokun, A. (2019). Development Second and Third Phase of the Selective Frame Processing Method. 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT). doi: https://doi.org/10.1109/aiact.2019.8847897
13. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197 (2001). NIST, 51. Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
14. DSTU 7624:2014. Informatsiyni tekhnolohiyi. Kryptohrafichnyi zakhyst informatsiyi. Alhorytm symetrychnoho blokovoho peretvorennia (2014). Kyiv, 39.
15. DSTU HOST 28147:2009. Systema obrobky informatsiyi. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (HOST 28147-89) (2008). Kyiv, 20.
16. Rivest, R. L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2), 120–126. doi: https://doi.org/10.1145/359340.359342
17. Yuan, L., Korshunov, P., Ebrahimi, T. (2015). Secure JPEG scrambling enabling privacy in photo sharing. 2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG). doi: https://doi.org/10.1109/fg.2015.7285022

18. Barannik, V., Belikova, T., Gurzhii, P. (2019). The Model of Threats to Information and Psychological Security, Taking into Account the Hidden Information Destructive Impact on the Subconscious of Adolescents. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit49449.2019.9030432
19. Kurihara, K., Shiota, S., Kiya, H. (2015). An encryption-then-compression system for JPEG standard. 2015 Picture Coding Symposium (PCS). doi: https://doi.org/10.1109/pcs.2015.7170059
20. Kurihara, K., Watanabe, O., Kiya, H. (2016). An encryption-then-compression system for JPEG XR standard. 2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). doi: https://doi.org/10.1109/bmsb.2016.7521997
21. Watanabe, O., Uchida, A., Fukuhara, T., Kiya, H. (2015). An Encryption-then-Compression system for JPEG 2000 standard. 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi: https://doi.org/10.1109/icassp.2015.7178165
22. Zhou, J., Liu, X., Au, O. C., Tang, Y. Y. (2014). Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation. IEEE Transactions on Information Forensics and Security, 9 (1), 39–50. doi: https://doi.org/10.1109/tifs.2013.2291625
23. Naor, M., Shamir, A. (1995). Visual cryptography. Lecture Notes in Computer Science, 1–12. doi: https://doi.org/10.1007/bfb0053419
24. Chen, C.-C., Wu, W.-J. (2014). A secure Boolean-based multi-secret image sharing scheme. Journal of Systems and Software, 92, 107–114. doi: https://doi.org/10.1016/j.jss.2014.01.001
25. Chen, T.-H., Wu, C.-S. (2011). Efficient multi-secret image sharing based on Boolean operations. Signal Processing, 91 (1), 90–97. doi: https://doi.org/10.1016/j.sigpro.2010.06.012
26. Deshmukh, M., Nain, N., Ahmed, M. (2016). An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). doi: https://doi.org/10.1109/aina.2016.56
27. Yang, C.-N., Chen, C.-H., Cai, S.-R. (2016). Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and Software, 116, 22–34. doi: https://doi.org/10.1016/j.jss.2015.01.031
28. Ramakrishnan, S. (2019). Cryptographic and Information Security. Approaches for Images and Videos. CRC Press, 986. doi: https://doi.org/10.1201/9780429435461
29. Wong, K.-W. (2009). Image Encryption Using Chaotic Maps. Intelligent Computing Based on Chaos, 333–354. doi: https://doi.org/10.1007/978-3-540-95972-4_16
30. Tsai, C.-L., Chen, C.-J., Hsu, W.-L. (2012). Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. 2012 IEEE International Carnahan Conference on Security Technology (ICCST). doi: https://doi.org/10.1109/ccst.2012.6393548
31. Wu, Y., Agaian, S., Noonan, J. (2012). Sudoku Associated Two Dimensional Bijections for Image Scrambling. IEEE Transactions on multimedia. Available at: https://arxiv.org/abs/1207.5856v1
32. Cheng, P., Yang, H., Wei, P., Zhang, W. (2015). A fast image encryption algorithm based on chaotic map and lookup table. Nonlinear Dynamics, 79 (3), 2121–2131. doi: https://doi.org/10.1007/s11071-014-1798-y
33. Information technology – JPEG 2000 image coding system – XML representation and reference. Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-T.813-201206-I!!PDF-E&type=items
34. Honda, T., Murakami, Y., Yanagihara, Y., Kumaki, T., Fujino, T. (2013). Hierarchical image-scrambling method with scramble-level controllability for privacy protection. 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS). doi: https://doi.org/10.1109/mwscas.2013.6674911
35. Wong, K., Tanaka, K. (2010). DCT based scalable scrambling method with reversible data hiding functionality. 2010 4th International Symposium on Communications, Control and Signal Processing (ISCCSP). doi: https://doi.org/10.1109/isccsp.2010.5463307
36. Ji, S., Tong, X., Zhang, M. (2012). Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator. arXiv.org. Available at: https://arxiv.org/abs/1208.0999
37. Phatak, A. G. (2016). A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. International Journal of Image, Graphics and Signal Processing, 8 (6), 64–71. doi: https://doi.org/10.5815/ijigsp.2016.06.08
38. Auer, S., Bliem, A., Engel, D., Uhl, A., Unterweger, A. (2013). Bitstream-Based JPEG Encryption in Real-time. International Journal of Digital Crime and Forensics, 5 (3), 1–14. doi: https://doi.org/10.4018/jdcf.2013070101
39. Kobayashi, H., Kiya, H. (2018). Bitstream-Based JPEG Image Encryption with File-Size Preserving. 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE). doi: https://doi.org/10.1109/gcce.2018.8574605
40. Minemura, K., Moayed, Z., Wong, K., Qi, X., Tanaka, K. (2012). JPEG image scrambling without expansion in bitstream size. 2012 19th IEEE International Conference on Image Processing. doi: https://doi.org/10.1109/icip.2012.6466845

41. Alimpiev, A. N., Barannik, V. V., Sidchenko, S. A. (2017). The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. Telecommunications and Radio Engineering, 76 (6), 521–534. doi: https://doi.org/10.1615/telecomradeng.v76.i6.60
42. Barannik, V., Sidchenko, S., Barannik, D. (2020). Technology for Protecting Video Information Resources in the Info-Communication Space. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). Available at: https://ieeexplore.ieee.org/document/9349324
43. Barannik, V., Barannik, V. (2020). Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). doi: https://doi.org/10.1109/tcset49122.2020.235540
44. Barannik, V. V., Ryabukha, Y. N., Kulitsa, O. S. (2017). The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. Telecommunications and Radio Engineering, 76 (9), 785–797. doi: https://doi.org/10.1615/telecomradeng.v76.i9.40
45. Barannik, V., Tarasenko, D. (2017). Method coding efficiency segments for information technology processing video. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2017.8246460