Along with the widespread use of digital images, an urgent scientific and applied issue arose regarding the need to reduce the volume of video information provided it is confidential and reliable. To resolve this issue, cryptocompression coding methods could be used. However, there is no method that summarizes all processing steps. This paper reports the development of a conceptual method for the cryptocompression coding of images on a differentiated basis without loss of information quality. It involves a three-stage technology for the generation of cryptocompression codograms. The first two cascades provide for the generation of code structures for information components while ensuring their confidentiality and key elements as a service component. On the third cascade of processing, it is proposed to manage the confidentiality of the service component. The code values for the information components of non-deterministic length are derived out on the basis of a non-deterministic number of elements of the source video data in a reduced dynamic range. The generation of service data is proposed to be organized in blocks of initial images with a dimension of 16×16 elements. The method ensures a decrease in the volume of source images during the generation of cryptocompression codograms, by 1.14–1.58 times (12–37 %), depending on the degree of their saturation. This is 12.7–23.4 % better than TIFF technology and is 9.6–17.9 % better than PNG technology. The volume of the service component of cryptocompression codograms is 1.563 % of the volume of the source video data or no more than 2.5 % of the total code stream. That reduces the amount of data for encryption by up to 40 times compared to TIFF and PNG technologies. The devised method does not introduce errors into the data in the coding process and refers to methods without loss of information quality

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

UDC 621.327:681.5
DOI: 10.15587/1729-4061.2021.237359

DEVISING A CONCEPTUAL METHOD FOR GENERATING CRYPTOCOMPRESSION CODOGRAMS OF IMAGES WITHOUT LOSS OF INFORMATION QUALITY

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 Department of Organizing
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
Dmitriy Barannik
Postgraduate Student*
Sergii Shulgin
PhD**
Valeriy Barannik*
Anton Datsun**
*Department of Design Automation***
Department of Information and Network Engineering*
***Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received date 15.06.2021
Accepted date 30.07.2021
Published date 31.08.2021

How to Cite: *Barannik, V., Sidchenko, S., Barannik, D., Shulgin, S., Barannik, V., Datsun, A. (2021). Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. Eastern-European Journal of Enterprise Technologies, 4 (2 (112)), 6–16. doi: https://doi.org/10.15587/1729-4061.2021.237359*

1. Introduction

The modern development of IT technologies is characterized by an increase in the level of intelligence and mobility. This allows them to be used in information and control systems for objects of varying complexity. In particular, they are applied in the process of managing critical infrastructure systems. At the same time, for such systems, one needs to take into consideration the increased level of cyber threats. Given a range of destabilizing factors, this could lead to significant damage. Therefore, it is important to ensure the security of information resources that are involved in managing critical infrastructure systems. An example is a process of acquiring analyzed video information from remote mobile video recording tools.

On the other hand, in terms of improving the efficiency of control systems, such a type of information resource as video information is gaining great importance. Here, additional technological difficulties arise associated with large time delays and significant losses of reliability in the process of delivering video information resources using existing information technologies.

Therefore, an important scientific and applied task is to reduce the volume of video information provided it is confidential and reliable [1].

To resolve this issue, the use of existing standard technological concepts is insufficient. This is because there is an imbalance between the increase in intensity and limited opportunities to reduce the volume of video information.

The imbalance is exacerbated by the transmission of video information in real-time using telecommunication technologies under the conditions of ensuring the necessary level of reliability and confidentiality.

2. Literature review and problem statement

Currently, standardized solutions are used to create conditions regarding efficiency, confidentiality, and reliability. The most elaborate is the sequential scheme [2, 3]. In a given variant, at the first stage, an increase in the efficiency of transmission is achieved through the technology of reducing the amount of video data (compression of video images) [4]. The second step ensures the confidentiality of the compressed representation based on the cryptographic transformation. For this purpose, symmetric and asymmetric encryption algorithms are used. The most known of these is the AES block symmetric encryption standard [5] and the RSA asymmetric algorithm [6]. At the final stage, standardized noise-tolerant coding technologies are used. However, there are certain problematic shortcomings.

First, to ensure the reliability of video information, the use of such technological transformations that at each stage of the sequential scheme ensure the preservation of the required level of reliability. Therefore, in the process of compression (compression coding), in order to ensure the required level of reliability, methods are used without entering information losses. For this reason, the application of compression methods that use frequency conversions is accompanied by the introduction of loss of quality and information in the reconstructed images. Such methods include discrete cosine and wavelet transformations, which, respectively, are implemented in the JPEG [7] and JPEG 2000 methods [8]. Their use leads to significant losses in the reliability of video imagery. At the same time, in critical infrastructure control systems, decisions are made automatically, including using artificial intelligence systems. The presence of even minor distortions could lead to incorrect decision-making. That, under critical conditions, is associated with the infliction of significant damage.

Second, cryptographic encryption technologies apply to the original or all compressed amounts of video data. On the one hand, this is accompanied by additional time costs. On the other hand, it is necessary to organize noise-resistant coding of the entire output volume of information. In this case, significant corrective binary bits are formed because encryption is critical to interference in the communication channel. Therefore, it is proposed to use cryptographic transformations only for key information. That would make it possible, on the one hand, to reduce the processing time (the energy costs of which are allocated to the encryption process). On the other hand, to reduce energy costs in the process of noise-resistant coding, which could be used to ensure noise immunity only for cryptograms of key information.

Third, a reduction in corrective bits is achieved, which leads to an increase in the efficiency of information delivery and a decrease in the related energy costs.

The following alternative approaches could be used in this direction.

Application of scrambling [9] and encrypting [5, 6] transformations to the source video data. Scrambled conversions, although they are fast-acting, provide weak protection. Encryption transformations, on the contrary, could provide guaranteed protection. However, as a result of their application, significant time delays are created when processing large amounts of data. As a result, the transfer of large amounts of information leads to a decrease in availability.

The Encryption-then-Compression scheme, in contrast to the serial scheme, on the contrary, provides for the sequential execution of the steps of perceptual encryption and compression [10]. Its disadvantage is the use of weak, from the point of view of cryptographic strength, scrambled transformations to process the entire volume of source video data. In addition, in the process of managing compression, a controlled loss of video quality is organized. That could lead to a loss of credibility. In addition, as a result of this scheme, there may be a decrease in the compression rate of video data relative to the underlying compression technology.

In works [11, 12], an approach to ensuring the confidentiality of video transmission based on the use of a secret distribution scheme (visual cryptography) is considered. In paper [11], it is considered from the standpoint of processing single images. Its application leads to a significant increase in the volume of original images and, as a result, to a decrease in the efficiency of information delivery. In [12], it is considered from the standpoint of managing the multi-secret exchange of several images. Significant disadvantages are the processing of uncompressed images; the ability to recognize individual objects from the original images in encrypted video data; the requirement for all encrypted video data to properly reconstruct the required images.

In works [13, 14], general approaches to the organization of confidentiality functionality in JPEG technology are proposed. It is implemented using scrambled and encrypting transformations at different stages of compression technology. However, a sequential processing scheme is actually implemented. At the same time, in the process of compression, a loss of information quality is organized, which could affect its reliability.

In paper [15], the functionality of JPSEC is offered, which implements in the compression technology JPEG 2000 safe image transfer. Packet-level encryption organizes a sequential processing scheme with all its drawbacks. Managing the scramble of the signs of the wavelet region coefficients requires the processing of a reduced amount of data. However, weak data protection is provided. Scrambled images are the blurry representations of the original video data, on which all large details are distinguishable.

Therefore, existing technologies do not make it possible to simultaneously ensure requirements regarding the efficiency, reliability, and confidentiality of video transmission.

To meet these requirements, it is proposed to develop cryptocompression methods. In this case:

1) volume reduction occurs in the process of cryptocompression coding. At the same time, service components are formed, which are key information for the process of video image reconstruction;

2) encryption is carried out for key information;

3) noise-resistant coding is organized on the basis of standardized methods only for cryptograms of key information.

3. The aim and objectives of the study

The aim of this study is to devise a conceptual method to form cryptocompression image codograms without losing the quality of information in order to reduce the volume of video information while ensuring its confidentiality and reliability.

To accomplish the aim, the following tasks have been set:

– to devise the generalized three-cascade technology of cryptocompression image coding;

– to conduct an experimental assessment of the effectiveness of the devised method of cryptocompression coding in comparison with known technologies for the compact representation of video data without losing the quality of information.

4. The study materials and methods

In this study, coding refers to a processing process aimed at reducing the amount of source data without losing information.

As theoretical methods of research, methods of digital image processing, methods of information encoding, methods of compression of digital images, methods of structural and combinatorial coding were used. Statistical analysis methods were employed to assess the adequacy of our results.

The following limitations were accepted in the process of devising the coding method:

– processing is focused on encoding static video imagery presented in the RGB color space. Note that the devised method of cryptocompression coding is basic and could be unified to process any type of digital data;

– the processed planes have the same dimensionality of $M\times N$ elements, where M is the number of lines in the image, and N is the number of columns. Although similar processing could be organized for planes having different dimensionalities. For example, in the color space YCbCr or YUV with sparse color planes;

– the dimensionalities of images consisting of $M\times N$ elements are imposed with limitations when dividing them into the blocks $A^{(\gamma,\chi)}$ of processing with the dimensionalities of $m\times n$ elements, where m is the number of lines in the block $A^{(\gamma,\chi)}$, and n is the number of columns. Here, $\gamma=\overline{1,\left[\frac{M}{m}\right]}$, $\chi=\overline{1,\left[\frac{N}{n}\right]}$. The method does not describe the processing of data that are in the extreme regions of the image. That is, the following conditions are met:

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

where $[\bullet]$ is the integer part of the number;

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

The mathematical statement of the study task: it is required to devise a conceptual method for the cryptocompression image coding, which is given by the functionality $F(I_{RGB}, m, n, L_{cw})$. Here: I_{RGB} is the original image; L_{cw} is the length of a codeword (the maximum number of bits) allocated to control the generation of code values for the information components of cryptocompression codograms. The method under construction must ensure that the following conditions are met:

1) reduction in the volume of compact representation of video imagery without loss of information quality in the cryptocompression coding system:

$$Q_{RGB}>Q_{comp}\geq Q_{CCP},$$

where Q_{RGB} is the volume of the original video image; Q_{comp} is the volume of compact representation of video images, which are formed by known encoding methods without loss of information quality; Q_{CCP} is the volume of compact representation of video imagery in the cryptocompression coding system;

2) reduction in the amount of service data that act as a key element in the cryptocompression coding system and require additional security based on cryptographic transformations:

$$Q_{CCP}>Q_{1\Lambda\Theta}>Q_{2\Lambda\Theta},$$

where $Q_{1\Lambda\Theta}$ is the volume of service components in the cryptocompression codograms for a single-cascade processing scheme; $Q_{2\Lambda\Theta}$ is the volume of service components in the cryptocompression codograms;

3) distortions are not introduced in the process of cryptocompression coding, i.e. the standard deviation RSME should be equal to 0.

To assess the effectiveness of the devised method, the simulation was carried out in the form of a full-scale experiment. To this end, a software package was developed that runs on operating systems from the Microsoft family. No additional libraries by third-party developers are needed for the proper operation of the software package. There are no additional requirements for personal computer equipment.

To assess the effectiveness of processing, three groups of pre-categorized images were used, depending on the degree of saturation with small details, namely low-saturated, medium-saturated, and highly-saturated. The images were taken from standardized databases that are used to test the methods of encoding and processing video information. In the experiments, we used 100 images from each class. In this case, the confidence interval is ±3 %. The 3-sigma rule was used to estimate the confidence interval. The reliability of our results is confirmed by the reconstruction of test images without loss of information, i.e. the standard deviation RSME is 0.

5. The study results regarding the development of a conceptual method for the generation of cryptocompression image codograms

5. 1. Devising a three-cascade technology of cryptocompression image coding

The generalized scheme of the conceptual method for the cryptocompression coding of images without loss of information quality is shown in Fig. 1. In Fig. 1, the main stages of processing are assigned with numbers in the blocks.

The first stage is preliminary. It initializes the parameters responsible for the organization of coding, namely:

– the type of processing is selected – processing in a differentiated basis or a basis along the upper boundaries. A given parameter is responsible both for the number of matrices of service components to be formed and for the degree of data compression. Preferred is the option of processing on a differentiated basis;

– the parameters m and n responsible for the dimensionality of the block $A^{(\gamma,\chi)}$ of processing are selected. These parameters are also responsible for the number of elements and the volume of matrices of service components formed. The greater the values they take, the smaller the volume of service components is formed. In addition, there is an indirect effect on non-deterministic processing parameters. All this significantly affects the degree of compression of the

initial data. For example, for the first processing cascade, the non-deterministic parameters are:

1) the number Ψ_α, $\alpha=\overline{1,\alpha_{max}}$, elements $a_{i,j}^{(\gamma,\chi)}$, $i=\overline{1,m}$, $j=\overline{1,n}$, of the source data involved in the generation of each code value E_α;

2) the length q_α of a given code value;

3) the total number α_{max} of the code values that form the information component $E=\{E_\alpha\}$;

– the length of the codeword L_{cw} is determined, which affects all non-deterministic processing parameters. Moreover, the total value of the length L_{cw} for all processed data could be selected, as well as different for different planes, macro segments, or data segments. A given scheme proposes using a common length value of the codeword L_{cw} to process all data. A given parameter significantly affects all non-deterministic characteristics of cryptocompression codograms.

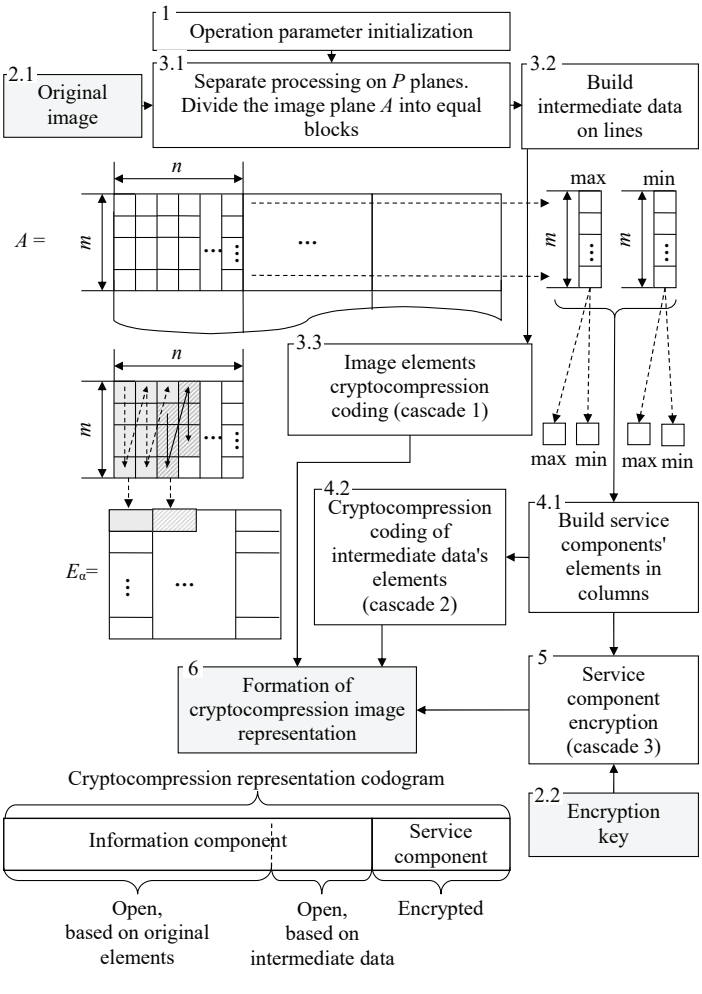


Fig. 1. Generalized scheme of the conceptual method for the cryptocompression coding of images without loss of information quality

At the second stage, video data that requires confidentiality are selected and the user enters the encryption key. The parameters of the encryption key are determined by the requirements of the cryptographic algorithm used in the third processing cascade to ensure the confidentiality of the service components formed as a result of encoding systems.

The headers of the selected video data or other data submitted for processing are used to determine the number P of the processed planes and the dimensionality of their $M\times N$ elements.

Image processing is managed in the RGB color space. The images have the dimensionality of $M\times N$ pixels and consist of P=3 planes A, where $A=\overline{1,P}=\overline{1,3}$, responsible for the red (R), green (G), and blue (B) constituent colors of each pixel. All image planes also have the same dimensionality of $M\times N$ elements, and, therefore, the same volume $Q(A)_{RGB}$. It is determined from the following formula:

$$Q(A)_{RGB}=M\cdot N \text{ [byte]}. \quad (1)$$

Hereinafter, the amount of data is determined in bytes and its value coincides with the value of the number of elements that are formed and processed.

The total volume Q_{RGB} of such an initial image, taking into consideration formula (1), is calculated as follows:

$$Q_{RGB}=\sum_{A=1}^{P}Q(A)_{RGB}=P\cdot M\cdot N=3\cdot M\cdot N \text{ [byte]}.$$

Fig. 2 shows the examples of original test images of varying degrees of saturation with a dimensionality of 512×512 pixels.

Processing begins with the first plane A=1, unless another order is defined, and is organized in all P planes of the image.

At the third stage, the first cascade of cryptocompression coding is performed. The sequence of operations at this stage is described in works [16, 17]. It begins with the partitioning of plane A into uniform blocks $A^{(\gamma,\chi)}$ whose dimensionality is $m\times n$ of elements each. Moreover, the values of the variables m and n are the essential controlled parameters in the generation of a cryptocompression codogram. The n parameter has a significant impact at the first coding cascade; m – at the second cascade. These parameters are directly responsible for the characteristics of the service component of the codogram, namely the number of generated elements and their values. In addition, they determine the order of encoding elements, which is formed using coordinate linearization schemes in the process of reformatting two-dimensional matrices of the processed data into vectors. Consequently, they are indirectly responsible for the number of generated code values for the information component.

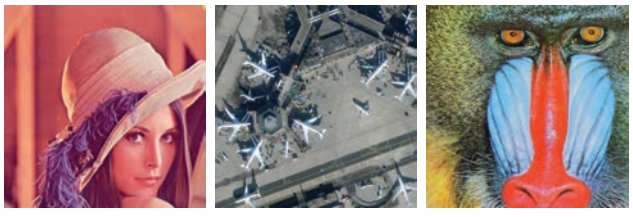
During the first cascade of processing, the value of the n parameter primarily affects the number of elements of the intermediate two-dimensional matrices being formed $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta=\{\mu_i^{(\gamma,\chi)}\}$, from which the service components are formed during the second coding cascade. Here $\lambda_i^{(\gamma,\chi)}$ is defined as the maximum value of the element $a_{i,j}^{(\gamma,\chi)}$ in the line; $\mu_i^{(\gamma,\chi)}$, as the minimum value. The generation of these matrices is carried out by sampling only one element from n in each line of the block $A^{(\gamma,\chi)}=\{a_{i,j}^{(\gamma,\chi)}\}$. As a result, the dimensionality of each matrix is $M\times\left\lceil\frac{N}{n}\right\rceil$ elements; its volume $Q(A)_{1\Lambda\Theta}$ is determined, taking into consideration formula (1), as follows:

$$Q(A)_{1\Lambda\Theta}=\frac{Q(A)_{RGB}}{n}=\frac{M\cdot N}{n} \text{ [byte]}. \quad (2)$$

Within each plane A, two intermediate matrices are formed, namely Λ and Θ. Therefore, for each image, the total volume $Q_{1\Lambda\Theta}$ of such intermediate data, taking into

consideration formula (2), is determined from the following expression:

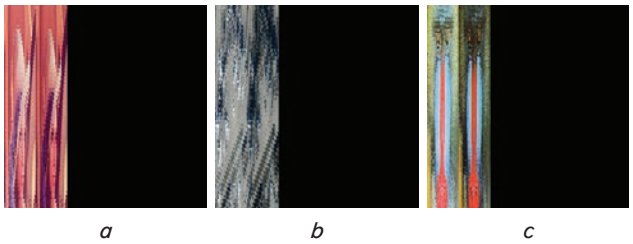
$$Q_{1\Lambda\Theta}=\sum_{P=1}^{3}\left(2\cdot Q(A)_{1\Lambda\Theta}\right)=\frac{6\cdot M\cdot N}{n}\ \text{[byte]}.$$



a *b* *c*

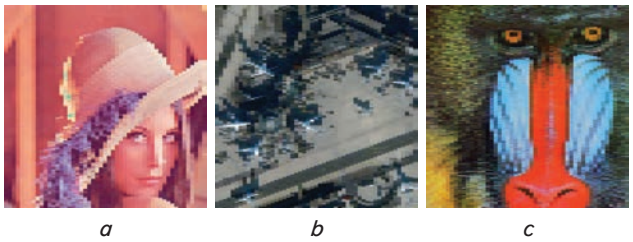
Fig. 2. Examples of original test images: *a* – Lena; *b* – Airport; *c* – Baboon

Intermediate matrices Λ and Θ contain information about the identified structural characteristics of the processed image planes. Using them, one can reconstruct the representation of the original image. Examples of visualization of these intermediate matrices are shown in Fig. 3, 4. In the examples, the planes are processed at values m=n=8 of block $A^{(\gamma,\chi)}$. This reduces the total $Q_{1\Lambda\Theta}$ volume of the Λ and Θ matrices for the entire image by 4 times compared to the Q_{RGB} volume of the original image.



a *b* *c*

Fig. 3. Visual representation of the ratio of the volume of intermediate two-dimensional matrices Λ and Θ to the total image volume: *a* – Lena; *b* – Airport; *c* – Baboon



a *b* *c*

Fig. 4. Examples of the visualization of images reconstructed on the basis of elements of the intermediate two-dimensional matrix Λ after the first processing cascade: *a* – Lena; *b* – Airport; *c* – Baboon

Fig. 3 shows the visualized mapping of the volume ratio of intermediate two-dimensional matrices Λ and Θ to the total image volume. In Fig. 3, the black background displays the size of the original video data. Two rectangular images located in the image on the left visualize the matrices Λ and Θ of all planes. The volume of each matrix Λ and Θ in each plane A is $\frac{1}{n}$ of the volume of the plane itself.

Fig. 4 illustrates the semantic correspondence of the values of the intermediate matrix $\Lambda=\left\{\lambda_i^{(\gamma,\chi)}\right\}$ to the original images of varying degrees of saturation. Images are reconstructed from the elements of intermediate two-dimensional matrices $\Lambda=\left\{\lambda_i^{(\gamma,\chi)}\right\}$, formed in all planes of the processed image, provided the dimensionality $M\times\left[\frac{N}{n}\right]$ of the elements is expanded to the level of M×N elements in the original video data. The expansion of dimensionality is organized by repeating n times each element $\lambda_i^{(\gamma,\chi)}$ in the direction horizontally using the rule:

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

where Λ" is the extended representation of the two-dimensional matrix Λ; $\lambda_{i,j}^{(\gamma,\chi)''}$ is the elements of the matrix Λ".

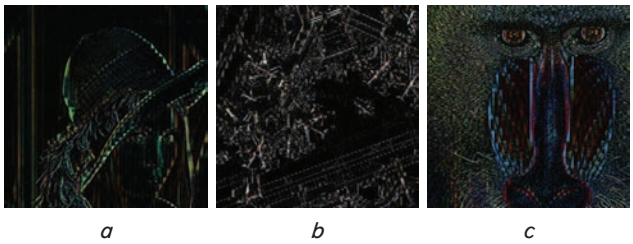
Table 1 gives the results of assessing the quality of the test images shown in Fig. 4. Quantitative assessment of the quality of video data processing is carried out using the quality indicators RSME, PSNR, and a correlation coefficient.

Table 1

Results of quality assessment of the test images formed on the basis of elements of the intermediate two-dimensional matrix Λ after the first processing cascade

Test image	Processing quality indicator		
	RSME	PSNR, dB	correlation coefficient
Lena	25.10	20.14	0.9387
Airport	35.23	17.19	0.8145
Baboon	42.32	15.60	0.8485

Our analysis of the scheme to manage the first cascade of encoding [1, 16, 17] reveals that the code values E_α are formed not for the values of the original elements $a_{i,j}^{(\gamma,\chi)}$, but taking into consideration the decrease in their dynamic range $\left(a_{i,j}^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)}\right)$. The values of the elements $a_{i,j}^{(\gamma,\chi)}$ are subject to a uniform decrease in the dynamic range along the lines within the processed block $A^{(\gamma,\chi)}$. At the same time, within the entire block $A^{(\gamma,\chi)}$, in plane A, and in the entire image as a whole, an uneven decrease in their values is organized. A visualized representation of the test video data in a reduced dynamic range is shown in Fig. 5; the results of the assessment of their quality are given in Table 2.



a *b* *c*

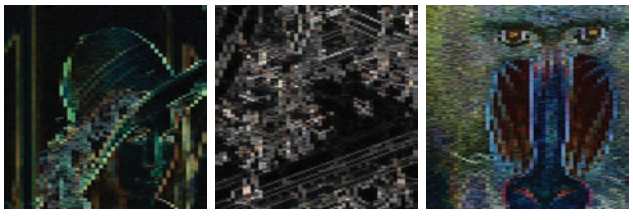
Fig. 5. Examples of the visualization of video data represented in a reduced dynamic range: *a* – Lena; *b* – Airport; *c* – Baboon

Table 2

Results of the evaluation of the quality of video data represented in a reduced dynamic range

Test image	Processing quality indicator		
	RSME	PSNR, dB	correlation coefficient
Lena	129.06	5.92	0.1270
Airport	108.41	7.43	0.2676
Baboon	111.70	7.17	0.3121

The same applies to the values $\lambda_i^{(\gamma,\chi)}$ of the matrix $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$, which, at the first cascade of cryptocompression coding, are involved in the generation of code values E_α in a reduced dynamic range in the form $(\lambda_i^{(\gamma,\chi)}+1-\mu_i^{(\gamma,\chi)})$. Examples of the visualized representation of such data are shown in Fig. 6; the results of the assessment of their quality are given in Table 3.



a *b* *c*

Fig. 6. Examples of the visualization of the matrices $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$, whose elements are represented in a reduced dynamic range in the form $(\lambda_i^{(\gamma,\chi)}+1-\mu_i^{(\gamma,\chi)})$: *a* – Lena; *b* – Airport; *c* – Baboon

Table 3

Results of the evaluation of the quality of video data constructed from the elements of matrices $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$, represented in a reduced dynamic range in the form $(\lambda_i^{(\gamma,\chi)}+1-\mu_i^{(\gamma,\chi)})$

Test image	Processing quality indicator		
	RSME	PSNR, dB	correlation coefficient
Lena	120.73	6.49	–0.1639
Airport	98.24	8.28	–0.1232
Baboon	97.77	8.32	–0.1438

Increasing the number of *n* sample elements for each *i*-th line of the block $A^{(\gamma,\chi)}$ leads to a change in the values of the elements of the intermediate matrices Λ and Θ, namely:

– the matrix $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$ values $\lambda_i^{(\gamma,\chi)}$ increase as they are defined as maximum values in the *i*-th line.

– their corresponding values $\mu_i^{(\gamma,\chi)}$ of the matrix $\Theta=\{\mu_i^{(\gamma,\chi)}\}$, on the contrary, are reduced since they are defined as the minimum values in the same line.

After organizing the linearization of coordinates and reformatting the two-dimensional matrices Λ and Θ into the vectors Λ' and Θ', these values $\lambda_i^{(\gamma,\chi)}=\lambda'_\tau$, $\mu_i^{(\gamma,\chi)}=\mu'_\tau$ take part in the cryptocompression coding in the following form: $(\lambda'_\tau+1-\mu'_\tau)$ and $(a_\tau-\mu'_\tau)$. Accordingly, the obtained values $(\lambda'_\tau+1-\mu'_\tau)$ and $(a_\tau-\mu'_\tau)$ would increase. And they take part in the following calculations:

– in the calculation of the number Ψ_α of the elements $a_\tau=a_{i,j}^{(\gamma,\chi)}$ of the plane *A* that form the code values E_α. This would reduce a given amount Ψ_α;

– in the generation of the code value E_α for the information component. Suppose that an unchanged number Ψ_α of the elements $a_\tau=a_{i,j}^{(\gamma,\chi)}$ takes part in the generation of the code value E_α and the elements themselves have not changed. However, increasing the values $(\lambda'_\tau+1-\mu'_\tau)$ and $(a_\tau-\mu'_\tau)$ would still lead to an increase in a given code value E_α. In addition, that could lead to an increase in the number of q_α bits for its storage. However, this condition is local. In practice, an increase in the values of $(\lambda'_\tau+1-\mu'_\tau)$ and $(a_\tau-\mu'_\tau)$ would lead to a change in all code values E_α and their lengths q_α;

– reducing the number Ψ_α of the elements would lead to an increase in the number α_{max} of all code values that formed the information component $E=\{E_\alpha\}$ at the first coding cascade. Consequently, the total length of the information component $E=\{E_\alpha\}$ increases.

As a result of the first cascade of cryptocompression transformation for plane *A*, the following are formed:

– an information component $E=\{E_\alpha\}$ of the first processing cascade, which participates in the generation of a cryptocompression codogram;

– two intermediate two-dimensional matrices $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta=\{\mu_i^{(\gamma,\chi)}\}$, the processing of which continues at the next stage.

At the fourth stage, the second cascade of cryptocompression coding is performed. The procedure for performing this step is described in work [1]. Here, an essential controlled parameter that is responsible for the number of elements of the generated matrices of service components and establishes the order of encoding elements is the value of *m*. It simultaneously determines the number of lines in the block $A^{(\gamma,\chi)}$ of the source data and the number of elements in the column vectors $\Lambda^{(\gamma,\chi)}=\{\lambda_i^{(\gamma,\chi)}\}$ and $\Theta^{(\gamma,\chi)}=\{\mu_i^{(\gamma,\chi)}\}$, the elements of which are encoded at this stage.

A value of the parameter *m* reduces the number of elements in the formed matrices Λ(max), Λ(min), Θ(max), and Θ(min) of the service components of cryptocompression codograms. It is organized by sampling only one element from *m* in each column vector $\Lambda^{(\gamma,\chi)}$ and $\Theta^{(\gamma,\chi)}$. In fact, from the elements $a_{i,j}^{(\gamma,\chi)}$ of each block $A^{(\gamma,\chi)}$ whose dimensionality is *m*×*n* elements, four elements of service components are formed, namely $\lambda(max)^{(\gamma,\chi)}$, $\lambda(min)^{(\gamma,\chi)}$, $\mu(max)^{(\gamma,\chi)}$ and $\mu(min)^{(\gamma,\chi)}$. As a result, the dimensionality of each matrix of service constituents is $\left[\frac{M}{m}\right]\times\left[\frac{N}{n}\right]$ elements, and its volume $Q(A)_{2\Lambda\Theta}$ is determined taking into consideration formula (2) using the expression:

$$Q(A)_{2\Lambda\Theta}=\frac{Q(A)_{1\Lambda\Theta}}{m}=\frac{M\cdot N}{m\cdot n}\ \text{[byte]}. \quad (3)$$

Within each plane *A*, four matrices of service components are built. Therefore, for each image, the total volume $Q_{2\Lambda\Theta}$ of the service components, taking into consideration formula (3), is determined from the following expression:

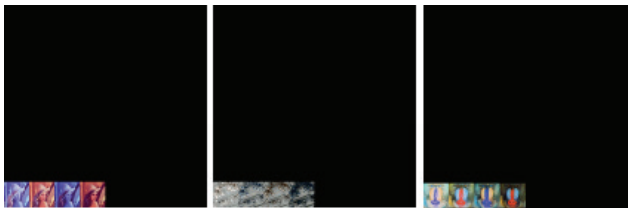
$$Q_{2\Lambda\Theta}=\sum_{P=1}^{3}\left(4\cdot Q(A)_{2\Lambda\Theta}\right)=\frac{12\cdot M\cdot N}{m\cdot n}\ \text{[byte]}. \quad (4)$$

The matrices Λ(max), Λ(min), Θ(max) and Θ(min) of the service components contain information about the revealed structural characteristics of the processed image planes. Using them, it is also possible to reconstruct the representation of the original image. Examples of the visualization of service components are shown in Fig. 7, 8; the results of assessing their quality are given in Table 4.

Table 4

Results of quality assessment of test images formed on the basis of elements of the matrix Λ(min) of the service component of the cryptocompression codogram

Test image	Processing quality indicator		
	RSME	PSNR, dB	correlation coefficient
Lena	20.68	21.82	0.9438
Airport	29.52	18.73	0.7827
Baboon	33.83	17.55	0.8165



a *b* *c*

Fig. 7. Examples of visualization of the volume of service components in the cryptocompression codograms without loss of information quality: *a* — Lena; *b* — Airport; *c* — Baboon

a *b* *c*

Fig. 8. Examples of the visualization of image reconstruction based on elements of the matrix Λ(min) of the service component of the cryptocompression codogram: *a* — Lena; *b* — Airport; *c* — Baboon

In Fig. 8, images are reconstructed only from the elements of the matrix $\Lambda(\min)=\lambda(\min)^{(\gamma,\chi)}$ of the service component of the cryptocompression codogram. In the process of reconstruction, in all planes of the image, the expansion of the dimensionality of the matrices of the service data of $\left[\frac{M}{m}\right]\times\left[\frac{N}{n}\right]$ elements to the dimensionality of the image consisting of $M\times N$ elements is organized. The extension of dimensionality is organized by repeating n times each element $\lambda(\min)^{(\gamma,\chi)}$ in the direction horizontally, and m times in the direction vertically using the rule:

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

where Λ(min)'' is the extended representation of the two-dimensional matrix Λ(min); $\lambda(\max)_{i,j}^{(\gamma,\chi)}{}''$ is the elements of the matrix Λ(min)''.

As a result of the second cascade of the cryptocompression transformation for plane A, the following are formed:

– information components $E(\Lambda)=\{E(\Lambda)_{\alpha(\Lambda)}\}$ and $E(\Theta)=\{E(\Theta)_{\alpha(\Theta)}\}$ of the second coding cascade;

– the service components of cryptocompression codograms consisting of two-dimensional matrices $\Lambda(\max)=\{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min)=\{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max)=\{\mu(\max)^{(\gamma,\chi)}\}$ and $\Theta(\min)=\{\mu(\min)^{(\gamma,\chi)}\}$.

At the fifth stage, the third processing cascade is performed, which involves ensuring the confidentiality of the service components of cryptocompression codograms. Cryptographic data encryption transformations could be used to this end. For example, encryption standards AES [5], Kalina [18], GOST 28147-89 [19], RSA [6]. The key for such conversions is set in the second step.

For the case of data processing in a reduced dynamic range, it is proposed to use the method of masking compaction of service data in compression systems [20].

The sixth stage organizes the generation of a cryptocompression image codogram, which is formed for each plane A separately. The cryptocompression codogram of each plane A consists of:

– information component $E=\{E_\alpha\}$, formed from the elements of the image $A=\left\{a_{i,j}^{(\gamma,\chi)}\right\}$ plane on the first cascade of cryptocompression coding;

– information components $E(\Lambda)=\{E(\Lambda)_{\alpha(\Lambda)}\}$ and $E(\Theta)=\{E(\Theta)_{\alpha(\Theta)}\}$, formed at the second cascade of cryptocompression coding from elements of the intermediate two-dimensional matrices $\Lambda=\left\{\lambda_i^{(\gamma,\chi)}\right\}$ and $\Theta=\left\{\mu_i^{(\gamma,\chi)}\right\}$, formed at the first cascade of processing;

– a service component consisting of the two-dimensional matrices $\Lambda(\max)=\{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min)=\{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max)=\{\mu(\max)^{(\gamma,\chi)}\}$ and $\Theta(\min)=\{\mu(\min)^{(\gamma,\chi)}\}$. These matrices are a key element for decoding the generated cryptocompression codogram.

To reduce the number of operations in the coding process at the first processing cascade, it is proposed to use the following sequence of actions when processing blocks $A^{(\gamma,\chi)}$ in plane A, namely:

– finding the minimum $\mu_i^{(\gamma,\chi)}$ value for elements $a_{i,j}^{(\gamma,\chi)}$ along the lines $i=\overline{1,m}$;

– lowering the dynamic range of all values $a_{i,j}^{(\gamma,\chi)}$ at $\mu_i^{(\gamma,\chi)}$. Actually, $a_{i,j}^{(\gamma,\chi)}=a_{i,j}^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)}$, $j=\overline{1,n}$;

– finding on the lines $i=\overline{1,m}$ the maximum $\lambda_i^{(\gamma,\chi)}$ values among the derived elements $a_{i,j}^{(\gamma,\chi)}=a_{i,j}^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)}$ in a reduced dynamic range;

– increase the maximum $\lambda_i^{(\gamma,\chi)}$ value by 1, i.e. $\lambda_i^{(\gamma,\chi)}=\lambda_i^{(\gamma,\chi)}+1$;

– further coding is organized taking into consideration these changes.

At the second cascade of cryptocompression coding, a similar change in finding the minimum and maximum values is proposed.

5. 2. Experimental evaluation of the effectiveness of the devised method of cryptocompression coding

The main control parameters in the conceptual method of cryptocompression encoding are the values of m and n in block $A^{(\gamma,\chi)}$ of video data processing. They affect:

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

– a reduction in the total volume of the compact representation of video data without loss of information quality.

The percentage of the volume of the service component in a cryptocompression codogram without loss of information quality to the volume of the original image at different values of the parameters m and n could be determined using the following ratio:

$$\frac{Q_{2\Lambda\Theta}\cdot 100}{Q_{RGB}}=\frac{400}{n\cdot m}\ [\%].$$

Some resulting estimates at uniform values, when $m=n$, are given in Table 5. Our analysis of the results reveals that with an increase in the dimensionality $m\times n$ of the elements of the processed block $A^{(\gamma,\chi)}$ in the process of cryptocompression coding, the volumes of the service component of the cryptocompression codogram decrease. Moreover, at the dimensionality of block $A^{(\gamma,\chi)}$ of 16×16 elements, the volumes of the service component of the cryptocompression codogram do not exceed 1.6 % of the volume of the original images.

As a result, smaller amounts of data would be subjected to cryptographic transformation at the third cascade of processing.

Evaluation of the effectiveness of ensuring the protection of service components at the third cascade of processing is reported in work [20].

Table 5

Percentage of the volume of the service component of the cryptocompression codogram without loss of information quality to the volume of the original image

Value of parameters m and n under condition $m=n$	4	8	12	16	20	24	28	32
Percentage ratio, %	25	6.25	2.778	1.563	1	0.694	0.51	0.391

The results of estimating the compression ratio of test images by the conceptual method of cryptocompression coding in a differentiated basis without loss of information quality at different parameters m and n of the block $A^{(\gamma,\chi)}$ of video data processing for some test images are given in Table 6. In it, the best values of the compression coefficient for the processed image are marked in gray. The ratios of the volumes of information and service components in cryptocompression codograms are given in Table 7. The following abbreviations are used: IC1 is the information component formed after the first cascade of processing; IC2 – an information component formed after the second cascade of processing; SC is a service component.

Table 6

Results of estimation of the compression ratio of test images by the conceptual method of cryptocompression coding

Test image	Value for parameter m and n provided $m=n$							
	4	8	12	16	20	24	28	32
2.1.01	0.915	1.126	1.174	1.188	1.188	1.187	1.18	1.182
Airplane	1.232	1.543	1.584	1.584	1.53	1.51	1.462	1.511
Airport	0.996	1.21	1.234	1.234	1.209	1.199	1.174	1.189
Baboon	0.87	1.079	1.128	1.145	1.141	1.136	1.13	1.139
Barbara	0.996	1.218	1.244	1.245	1.232	1.226	1.23	1.204
Lena	1.121	1.374	1.399	1.384	1.357	1.326	1.313	1.299
Peppers	1.098	1.352	1.405	1.367	1.352	1.314	1.303	1.284

Table 7

The ratio of the volumes of information and service components in cryptocompression codograms without loss of information quality at different parameters m and n in the block $A^{(\gamma,\chi)}$ of video data processing, %

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

After our experiment, the following conclusions can be drawn:

– from the position of ensuring the greatest reduction in the volume of source video data without loss of information quality, the best values of the sizes m and n in a block of processed video data are 12 or 16 elements, provided $m=n$. This provides for an increase in the compression coefficient for the specified parameters of the dimensionalities of the processing units relative to the dimensionality of the processing block of 8×8 elements, by 2.5 to 6.5 %;

– the volume of the service component, which is a key element in the generation of information components, decreases in cryptocompression codograms with an increase in the dimensionality of the processing units of $m\times n$ elements. That reduces the amount of data that are subjected to cryptographic transformation based on scrambling and/or encryption at the third processing cascade. Thus, taking into consideration ensuring a better degree of compression, the optimal values of sizes m and n are 16 elements. This makes it possible to provide for the volume of the service component in cryptocompression codograms no more than 2.5 % of the volume of the entire code stream;

– the time spent on coding does not change with the increasing dimensionality of processing blocks $m\times n$ elements on the first cascade of processing. On the second processing cascade, the time spent decreases with increasing the value of the n parameter (the number of columns). That is due to the fact that a given parameter is responsible for changing the amount of intermediate data in the form of service components formed after the first processing cascade. On the third processing cascade, increasing the parameters m and n reduces the time spent on cryptographic conversion by reducing the amount of service data processed.

Our method does not introduce errors into the data in the coding process and refers to methods without loss of information quality. Let us call it Method 1. To assess the quality of its operation from the standpoint of reducing the volume of the original video image, the following alternative encoding methods were used:

– a method of cryptocompression image coding based on a single-cascade floating processing scheme on a differentiated basis using a non-deterministic processing scheme (Method 2);

– a method of cryptocompression image coding based on a floating processing scheme on a differentiated basis using deterministic processing schemes (Method 3);

– an encoding algorithm based on RLE series length code and the LZW prefix code. It is implemented in the format of TIFF video data representation;

– a deflate compression algorithm based on LZ77 code (built on the principle of sliding window and match encoding mechanism) and Huffman code. It is implemented in the format of PNG video data presentation.

Compression methods based on frequency transformations (such as discrete cosine and wavelet transformations) were not used in the comparison, given the fact that they organize a reduction in the volume of video data under the conditions of loss of quality and information.

The results of assessing the compression coefficient for images of varying degrees of saturation for the analyzed methods of compact representation of images are shown in Fig. 9.

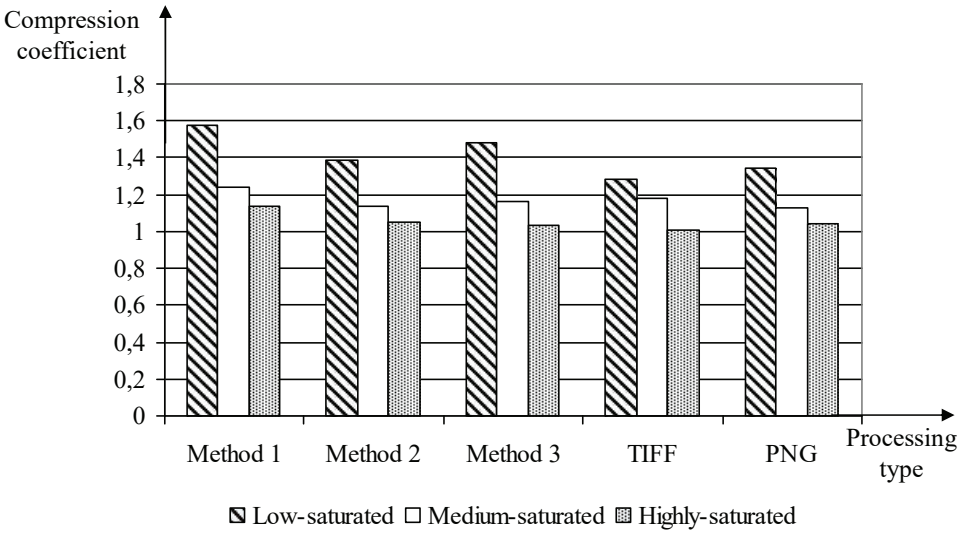


Fig. 9. Image compression coefficient estimation results

Our analysis of the data in Fig. 9 reveals that the best result in terms of compression ratio for video data of different saturation degrees was shown by the developed conceptual method of cryptocompression coding (Method 1). The average value of the compression coefficient for it is:

– for highly saturated images – at the level of 1.14, which ensures a decrease in the volume of original video data by 12.28 %;

– for medium-saturated images – at the level of 1.24, which ensures a decrease in the volume of original video data by 19.35 %;

– for low-saturated images – at the level of 1.58, which ensures a reduction in the volume of source video data by 36.71 %.

That, on average, is:

– 12.7–23.4 % better than the TIFF data representation format;

– 9.6–17.9 % better than the PNG format;

– 8.5–13.7 % better than single-cascade processing;

– 6.7–10.7 % better than a two-cascade deterministic approach.

6. Discussion of results of devising a conceptual method for the cryptocompression representation of images

A conceptual method for the cryptocompression representation of images has been built. It organizes a three-cascade technology for the generation of cryptocompression codograms:

– on the first cascade, information components are formed from the elements of the original images;

– on the second cascade, information components are formed from elements of intermediate key data and the service component of the cryptocompression codogram;

– on the third stage, the encryption of the service component is organized.

The generation of the key element is organized as follows. On the first cascade of processing, the key is formed in the process of compression (non-equilibrium positional coding) and is directly a system of bases. It is the key information, without which it is impossible to reconstruct the original video data. To further improve the efficiency of information delivery, on the second cascade, a decrease in the volume of assembled arrays of service data is carried out. In turn, the third cascade organizes a cryptographic transformation of service components. In this case, the additional costs of the number of arithmetic operations on the second cascade are compensated for by a decrease in the amount of data transferred and a decrease in the number of operations on the third cascade. At the same time, the number of operations is linearly dependent on the size of the processed data blocks. Due to this, a gain is achieved taking into consideration the stages of processing and transmitting information in the infocommunication network.

Images represented in the RGB color space are processed. The experiments used 100 images of three classes, namely low-saturated, medium-saturated, and highly-saturated. To visualize the intermediate data generated at different stages of the developed method, three test images of Lena, Airport, and Baboon were used as examples. Fig. 2–8 show the visualized results; Tables 1–4 give the results of qualitative assessments. The qualitative estimates were obtained on the basis of the comparison of the formed visualized data with the original images. When choosing the optimal parameters for the devised method, Tables 6, 7 give the example of the results from processing 7 test images. The results given as examples are typical for all images processed in the experiment. The conclusions were drawn regarding the processing of all test images. Fig. 9 shows the average results from estimating the value of the compression coefficient of images from different classes.

Examples of the initial test images of varying degrees of saturation with a dimensionality of 512×512 pixels are shown in Fig. 2. The images are clear, one can distinguish individual small objects. The properly reconstructed images, when using the developed conceptual method, can be restored without errors (bit to bit) and completely coincide with the original ones.

After the first processing cascade, intermediate two-dimensional matrices Λ and Θ are formed, which are the key elements for the proper decoding of the information components of the first processing cascade. Examples of the visualization of these intermediate matrices are shown in Fig. 3, 4; their qualitative characteristics are given in Table 1.

Our analysis of the images and the scheme of construction of intermediate two-dimensional matrices Λ and Θ demonstrates that they fully characterize the content of the processed images and include information about the brightness characteristics and low-frequency characteristics of the image. They transmit information about large objects and contours, up to full semantic correspondence to the original video data. At the same time, small objects are destroyed or lost completely, and large objects are blurred. This indicates the concealment of some of the information in the information component $E=\{E_\alpha\}$ in each plane A.

The results of the qualitative assessment of such experimental data indicate that:

– in low-saturated images, there is the least loss of video quality. In such images, the correlation coefficient is above 0.9, although the PSNR values are at 20 dB and below;

– for medium-saturated and highly-saturated images, the correlation coefficient decreases to 0.8, and the PSNR values decrease below 20 dB.

Such characteristics correspond to compressed images with a high level of information quality reduction. The quantitative estimates once again confirmed that the intermediate two-dimensional matrices Λ and Θ fully characterize the content of the processed images.

The generation of information components is organized for video data in a reduced dynamic range. Examples of the visualized representation of such data are shown in Fig. 5, and the results of the assessment of their quality are given in Table 2. Our analysis of the images reveals that only the shapes (contours) of large objects are displayed against a dark background. All the small details of the objects and color characteristics are lost. For such images, the correlation coefficient is below 0.34 and the PSNR value is below 8 dB. Moreover, the correlation coefficients and PSNR for highly-saturated images take values higher than those for low-saturated and medium-saturated video data.

The key elements for the generation of information components in the form of intermediate two-dimensional matrices Λ and Θ are also represented in a reduced dynamic range. Examples of the visualized representation of such data are shown in Fig. 6, and the results of the assessment of their quality are given in Table 3. Our analysis of the experimental data reveals that only the shapes (contours) of large objects are displayed against a dark background. All the small details of the objects and color characteristics are lost. For such images, the correlation coefficient is below 0.2 and the PSNR value is below 9 dB.

The service components of cryptocompression codograms contain information about the identified structural characteristics of the processed image planes. Examples of the visualization of service components are shown in Fig. 7, 8, and the results of assessing their quality are given in Table 4. Our analysis of the images in Fig. 8 shows that the service components of cryptocompression codograms fully characterize the content of the processed images. The correlation coefficients of such images with the original video data are at the level of 0.8. And, with their help, one could reconstruct the original image. Therefore, they require additional confidentiality. The volume of service components after the second cascade of processing, taking into consideration the partitioning of the image planes into blocks $A^{(\gamma,\chi)}$ with a dimensionality of 8×8 elements would equal $\frac{1}{16}$ the volume of the plane A. That is confirmed by the visual illustration in Fig. 7.

The volume of the service components of cryptocompression codograms is determined using formula (4). It depends on the dimensionality $m\times n$ of the block $A^{(\gamma,\chi)}$ of processing. For the dimensionality of 16×16 elements, the volumes of the service component of the cryptocompression codogram do not exceed 1.6 % of the volume of the original images. The percentage ratio of the volume of the service component of the cryptocompression codogram without loss of information quality to the volume of the original image is given in Table 5. The results of the influence of the dimensionality $m\times n$ of the block $A^{(\gamma,\chi)}$ of processing on the compression coefficient of video data are given in Table 6; on the ratio of the volumes of information and service components in cryptocompression codograms – in Table 7.

The results of the comparative assessment of the developed and existing methods of coding by compression ratio for images of different degrees of saturation are shown in Fig. 9. The devised method ensures the encoding of video imagery without loss of information quality.

Distinctive features of the developed conceptual method for the cryptocompression representation of images are:

– the organization of three-cascade video coding technology. The first two cascades provide the generation of code structures for the information components while ensuring their confidentiality and key elements as a service component. On the third cascade of processing, it is proposed to organize the confidentiality of the service component;

– the use of control parameters responsible for the size of the processing block and the length of a codeword to store the code values of the information components. These parameters affect the degree of compression of video information; a change in the volume of generated service key data, which are encrypted (scrambled) on the third cascade of processing; a change in the non-deterministic processing parameters during the encoding process;

– the generation of code values for the information components of nondeterministic length is organized on the basis of a non-deterministic number of elements of the original video image.

The limitation of this study is its focus on the processing of static video data. The disadvantage of the study is the unresolved issue regarding the choice of a cryptographic method to ensure the confidentiality of service components on the third cascade of processing.

The current study could be advanced in two directions. First, by improving the method from the standpoint of processing dynamic video data. Second, through the development or adaptation of methods for scrambling and/or encryption of service data on the third cascade of processing.

7. Conclusions

1. We have devised a conceptual method for the cryptocompression coding of images on a differentiated basis without loss of information quality. It organizes a

three-cascade technology for the generation of cryptocompression codograms. The first two cascades provide for the generation of code structures of information components while ensuring their confidentiality and key elements as a service component. On the third cascade, it is proposed to organize the confidentiality of the service component using encryption methods.

2. The results of our experimental studies include the following findings on the effectiveness of the developed conceptual method of cryptocompression coding without loss of quality of information relative to PNG and TIFF compression technologies:

– a reduction in the volume of source images during the generation of cryptocompression codograms by 1.14–1.58 times (by 12–37 %) depending on the degree of their saturation when processing video data blocks consisting of 16×16 elements. This is 12.7–23.4 % better than the TIFF data representation format; 9.6–17.9 % better than the PNG format; 8.5–13.7 % better than single-cascade processing; and 6.7 % better than the two-cascade deterministic approach;

– increasing the dimensionality of $m \times n$ blocks of the processed data to 12×12 or 16×16 elements makes it possible to increase the compression coefficient relative to the dimensionality of the processing unit of 8×8 elements, by 2.5 to 6.5 %;

– the volume of the service component in cryptocompression codograms depends on the dimensionality of the block of processed data. Thus, when processing video data in blocks consisting of 8×8 elements, the amount of service data is 6.5–8.5 % of the total code stream. Increasing the dimensionality of the processing block to 12×12 elements forms the amount of service data at the level of 3–4.5 % of the total code stream. When processing video data in blocks of 16×16 elements, the amount of service data in the code stream does not exceed 2.5 %. That reduces the amount of data for encryption by 10 to 40 times compared to TIFF and PNG technologies in a serial scheme using them.

Our method does not introduce errors into the data in the coding process and refers to methods without loss of information quality. The standard deviation RSME of all reconstructed images relative to the original video data is 0; the correlation coefficient is 1.

References

1. 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
2. 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
3. Jasuja, B., Pandya, A. (2015). Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding. International Journal of Computer Applications, 116 (21), 34–41. doi: https://doi.org/10.5120/20463-2831
4. Gonzalez, R., Woods, R. (2018). Digital Image Processing. Pearson, 1168.
5. 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
6. 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
7. 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
8. ISO/IEC 15444-1:2019. Information technology – JPEG 2000 image coding system – Part 1: Core coding system. Available at: https://www.iso.org/standard/78321.html
9. Ramakrishnan, M. (Ed.) (2019). Cryptographic and Information Security. Approaches for Images and Videos. CRC Press, 986. doi: https://doi.org/10.1201/9780429435461
10. 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
11. Naor, M., Shamir, A. (1995). Visual cryptography. Lecture Notes in Computer Science, 1–12. doi: https://doi.org/10.1007/bfb0053419
12. 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
13. Dufaux, F., Ebrahimi, T. (2006). Toward a secure JPEG. Applications of Digital Image Processing XXIX. doi: https://doi.org/10.1117/12.686963
14. 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
15. ISO/IEC 15444-8:2007. Information technology – JPEG 2000 image coding system: Secure JPEG 2000 – Part 8. Available at: https://www.iso.org/standard/37382.html
16. 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

17. 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). Kyiv, 29–33. Available at: https://ieeexplore.ieee.org/document/9349324
18. DSTU 7624:2014. Informatsiyni tekhnolohiyi. Kryptohrafichnyi zakhyst informatsiyi. Alhorytm symetrychnoho blokovoho peretvorennia (2014). Kyiv, 39.
19. DSTU HOST 28147:2009. Systema obrobky informatsiyi. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (HOST 28147-89) (2008). Kyiv, 20.
20. Barannik, V., Sidchenko, S., Barannik, N., Khimenko, A. (2021). The method of masking overhead compaction in video compression systems. Radioelectronic and computer systems, 2, 51–63. doi: https://doi.org/10.32620/reks.2021.2.05