Method of Ciphergrams Coding for Increasing the Effectiveness of Selective Cyber-Protection Technologies

Barannik V., Barannik D., Hahanova A., Medvedev D., Strelbtskiy M.

.

Abstract – **The method of increasing the efficiency and confidentiality for the video information stream based on the selective transformation of macroblocks is developed.**

I. Introduction

Method of increasing the efficiency and video data privacy for departmental video conferencing systems based on selective encoding of video frames. To further reduce the amount of transmitted data, that is, reducing the level of information load on the telecommunication network, it is proposed to further process binary ciphers.This need is explained by the following reasons:

1. Growth of the macroblocks with high content of energetically significant components number leads to increasing in the number of ciphergrams formed as selection result for low frequency components the of transformants. But at the same time, the ciphergrams are formed for low-frequency components without additional processing. Accordingly, this leads to increasing the information load on the data transmission channels, and to increase the time delay for the transmission of video information

2. The capacity of the telecommunication network is dynamic. Therefore, in cases of a sharp decrease in bandwidth, it is necessary to use a technological mechanism for regulating the information intensity of the coded stream. In this case, to shorten the processing delays, it is necessary to ensure the availability of such a mechanism at the later stages of processing video information, i.e. including at the stage of forming a ciphergram. In order to reduce the number of the ciphergrams digits, it is proposed to use a structural approach based on the identification the number of binary transitions and the formation the corresponding code description without loss of information.

Manuscript received November 30, 2016.

Barannik V. is with the Kharkiv Air Force University. Address: Ukraine, 61023, Kharkov, st. Sumskaya, 77/79 (corresponding author, e-mail: barannik_v_v@mail.ru).

Barannik D. is with the Kharkiv National University of Radioelectronics. Address: Ukraine, 61166, Kharkov, Nauka Ave, 14.

Hahanova A. is with the Kharkiv National University of Radioelectronics. Address: Ukraine, 61166, Kharkov, Nauka Ave, 14.

Medvedev D. PhD student, is with the Kharkiv National University of Radioelectronics. Address: Ukraine, 61166, Kharkov, Nauka Ave, 14.

Strelbtskiy M., PhD in Eng., doctoral of National Academy of State Border Service of Ukraine named after B. Khmelnytskyi.

This allows to detect such characteristics for their specific content by the fact of the processed ciphergram.

Consider the process of the ciphergrams low-frequency components structural processing for energy-sensitive macroblocks of video frames taking into account the identification of characteristics at binary transitions.

The construction of a ciphergram compact description, taking into account the presence of restrictions on binary transitions, is proposed to be carried out using an approach based on binary structural coding. In this case, the rolling ratio of the weight coefficient system is used (Fig. 1), that is,

$$K = \sum_{\xi=1}^{L} q_\xi \, w_\xi ; \tag{1}$$

Here K – the code of the ciphergram structural description, the length of the bit, as a rule $L = 128;\ 256;\ 512$.

Since the elements cryptogram take binary values, i.e $q_\xi \in [0; 1]$, there are insignificant components $q_\xi \, w_\xi$ of convolution (3.13). Therefore, to reduce the number of operations, we suggest introducing an auxiliary parameter θ_ξ, equal of summand convolution, i.e.:

$$\theta_\xi = q_\xi \, w_\xi .$$

In this case, we obtain:

$$\theta_\xi = \begin{cases} w_\xi , & \rightarrow q_\xi = 1; \\ 0, & \rightarrow q_\xi = 1. \end{cases}$$

Then the expression (1) takes the next form:

$$K = \sum_{\xi=1}^{L} q_\xi \, w_\xi = \sum_{\xi=1}^{L} \theta_\xi$$

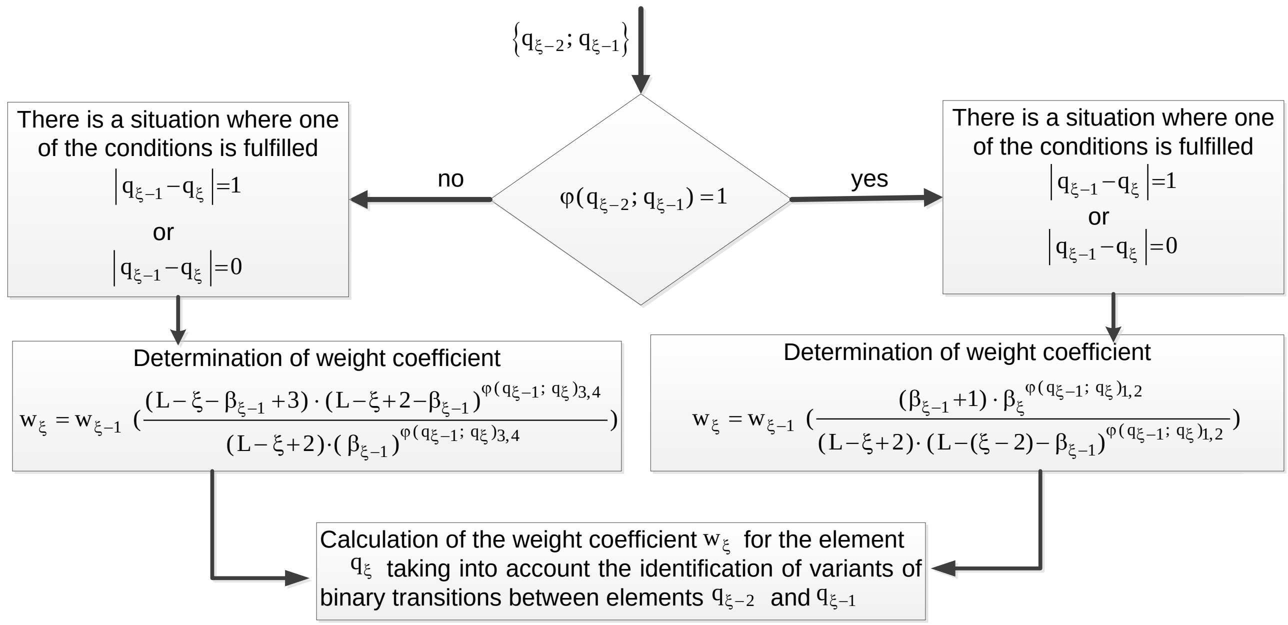

Fig. 1. Structural-functional scheme of identification the variants for binary transitions between elements

As can be seen from the obtained ratio, the value of the code is determined by the weight coefficients of the processed elements. Finding weight coefficients is carried out according to the recurrent approach. In this case, we take into account: weight coefficient obtained in the previous processing step, i.e.

– weight coefficient $w_{\xi-1}$ for the previous element $(\xi-1)$ - of the ciphergram;

– dependence between the three elements, $q_{\xi-2}$, $q_{\xi-1}$ и q_ξ, that is, between the current processed element and the two previous ciphergrams. At the same time, this approach involves the need for a separate consideration for the four situations caused by the transitions between the three elements, $q_{\xi-2}$, $q_{\xi-1}$ и q_ξ, i.e.:

1) $|q_{\xi-2} - q_{\xi-1}| = 1$, $|q_{\xi-1} - q_\xi| = 1$;

2) $|q_{\xi-2} - q_{\xi-1}| = 1$, $|q_{\xi-1} - q_\xi| = 0$;

3) $|q_{\xi-2} - q_{\xi-1}| = 0$, $|q_{\xi-1} - q_\xi| = 1$;

4) $|q_{\xi-2} - q_{\xi-1}| = 0$, $|q_{\xi-1} - q_\xi| = 0$.

As a result, the need to process more operations on the such conditions verification and the appropriate calculation the weight coefficients.

Therefore, in order to operations number reducing associated with the decrease of the video stream information intensity, it is proposed to develop generalizing dependencies for finding weight coefficients in the process of binary uniform ciphergrams structural coding. We consider the develop generalizing functional transitions for the calculation of weight coefficients for the first two cases of dependence between elements $q_{\xi-2}$, $q_{\xi-1}$ и q_ξ, namely:

- $|q_{\xi-2} - q_{\xi-1}| = 1$ и $|q_{\xi-1} - q_\xi| = 1$;

- $|q_{\xi-2} - q_{\xi-1}| = 1$, $|q_{\xi-1} - q_\xi| = 0$;

Let's introduce the functional $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$, which shows the relationship between $(\xi-1)$-th i ξ-th binary elements of the ciphergram __ of the transformants important components, which implements the inversion function, i.e. if

$$|q_{\xi-1} - q_\xi| = 1,\ \varphi(q_{\xi-1};\, q_\xi) = 0.$$

Conversely, for

$$|q_{\xi-1} - q_\xi| = 0$$

the value of the functional will be equal to the component, i.e.

$$\varphi(q_{\xi-1};\, q_\xi)_{1,2} = 1.$$

Generally, this dependence is given by the following system:

$$\varphi(q_{\xi-1};\, q_\xi)_{1,2} = \begin{cases} 0, & \to |q_{\xi-1} - q_\xi| = 1; \\ 1, & \to |q_{\xi-1} - q_\xi| = 0. \end{cases}$$

To implement such a functional dependence, we will use a sign function $\varphi(x)$, which is set by the next conditions:

$$\varphi(x) = \mathrm{sign}(x) = \begin{cases} 0, & \to x = 0; \\ 1, & \to x > 0; \\ -1, & \to x < 0. \end{cases}$$

We can use the function $\varphi(x)$ to specify a functional relationship $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ by the next way:

$$\varphi(q_{\xi-1};\, q_\xi)_{1,2} = \mathrm{sign}(1 - \mathrm{sign}(|q_{\xi-1} - q_\xi|)). \quad (2)$$

In this case, will be fulfilled the conditions of the functional task $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$, i.e.:

$$\varphi(q_{\xi-1};\, q_\xi)_{1,2} = \mathrm{sign}\,(1 - \mathrm{sign}\,(|q_{\xi-1} - q_\xi|)) = \\ = \begin{cases} 0, & \to |q_{\xi-1} - q_\xi| = 1; \\ 1, & \to |q_{\xi-1} - q_\xi| = 0. \end{cases} \quad (3)$$

Then recursive generalized expression for determining the weight coefficients w_ξ for ξ- th element of the ciphergram using the value of the weight coefficient $w_{\xi-1}$ for $(\xi-1)$-th element for the option, when $(|q_{\xi-2} - q_{\xi-1}| = 1)$, depending on the difference value $(|q_{\xi-1} - q_\xi|)$, will be determined by such a ratio:

$$w_\xi = w_{\xi-1}\ \left(\frac{(\beta_{\xi-1}+1)\cdot \beta_\xi^{\varphi(q_{\xi-1};\, q_\xi)_{1,2}}}{(L-\xi+2)\cdot(L-(\xi-2)-\beta_{\xi-1})^{\varphi(q_{\xi-1};\, q_\xi)_{1,2}}}\right) \quad (4)$$

This relation generalizes cases where: two previously processed elements, create a binary difference, that is, there is a transition either from 0 to 1, or from 1 to 0, namely:

$$q_{\xi-2} = 0 \ \&\ q_{\xi-1} = 1\ ,\ q_{\xi-2} = 1 \ \&\ q_{\xi-1} = 0\,;$$

Thus, the value of the current processed element of the ciphergram can be arbitrary, i.e.

$$q_\xi \in [0;1].$$

Indeed, if the conditions are fulfilled simultaneously

$$\left|\, q_{\xi-2} - q_{\xi-1} \right| = 1,\ \ \left|\, q_{\xi-1} - q_\xi \right| = 1,$$

then according to the relation (3.15) the value of the functional $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ will be equal to zero value, $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$, and weight coefficient w_ξ for current element can be determined by formula:

$$w_\xi = w_{\xi-1}\ \left(\frac{(\beta_{\xi-1}+1)\cdot \beta_\xi^{\ 0}}{(n-\xi+2)\cdot(L-(\xi-2)-\beta_{\xi-1})^0}\right) = \\ = w_{\xi-1}\,(\beta_{\xi-1}+1)/(L-\xi+2)\,. \quad (5)$$

On the contrary, if both conditions are fulfilled simultaneously:

$$\left|\, q_{\xi-2} - q_{\xi-1} \right| = 1,\ \ \text{но}\ \ \left|\, q_{\xi-1} - q_\xi \right| = 0,$$

by the ratio (5) value of the functional $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ will take a “1” value, i.e. $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$, and weight coefficient value w_ξ for current element of the ciphergram determined using this expression:

$$w_\xi = w_{\xi-1}\ \left(\frac{(\beta_{\xi-1}+1)\cdot \beta_\xi^{\ 1}}{(n-\xi+2)\cdot(L-(\xi-2)-\beta_{\xi-1})^1}\right) = \\ = w_{\xi-1}\left(\frac{(\beta_{\xi-1}+1)\beta_\xi}{(n-(\xi-2)-\beta_{\xi-1})(L-\xi+2)}\right). \quad (6)$$

We will now develop a technological stage for determining the general functional dependences for the weight coefficients of the ciphergram structure coding, taking into account the next relationships between the elements $q_{\xi-2}$, $q_{\xi-1}$ and q_ξ of the ciphergram:

- $\left|\, q_{\xi-2} - q_{\xi-1} \right| = 0$ and $\left|\, q_{\xi-1} - q_\xi \right| = 1$;
- $\left|\, q_{\xi-2} - q_{\xi-1} \right| = 0$ and $\left|\, q_{\xi-1} - q_\xi \right| = 0$.

This situation differs from the previous two by the fact that:

1) for elements $q_{\xi-2}$ and $q_{\xi-1}$ values the condition of equality is fulfilled, ie:

$$q_{\xi-2} = q_{\xi-1} = 0 \ \text{or}\ q_{\xi-2} = q_{\xi-1} = 1;$$

2) with the value of the element q_ξ is selected arbitrarily, ie: $q_\xi \in [0;1]$.

Similar to the previous generalization, we introduce the next functional dependence $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$. Unlike the functional $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ here it is necessary to realize a direct relationship between, on the one hand, the value of the difference and $(|q_{\xi-1} - q_\xi|)$ and functional $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$ value on the other hand. This is displayed as next:

Conditions

$$\left|\, q_{\xi-1} - q_\xi \right| = 1,$$

Need to be provided

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = 1\,.$$

And, accordingly, for:

$$\left|\, q_{\xi-1} - q_\xi \right| = 0$$

the value of the functional must be zero:

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = 0\,.$$

Generally, this dependence shows by the system:

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = \begin{cases} 1, & \to |q_{\xi-1} - q_\xi| = 1; \\ 0, & \to |q_{\xi-1} - q_\xi| = 0. \end{cases}$$

Then using a sign function $\mathrm{sign}(x)$ functional relationship $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$ will be set based on the relationship:

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = \mathrm{sign}\,(|q_{\xi-1} - q_\xi|)\,, \quad (7)$$

so:

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = \mathrm{sign}\,(|q_{\xi-1} - q_\xi|) = \\ = \begin{cases} 1, & \to |q_{\xi-1} - q_\xi| = 1; \\ 0, & \to |q_{\xi-1} - q_\xi| = 0. \end{cases} \quad (8)$$

From the analysis of the obtained ratios shown relationship between functionals $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ and $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$:

$$\varphi(q_{\xi-1};\, q_\xi)_{3,4} = 1 - \varphi(q_{\xi-1};\, q_\xi)_{1,2}\,. \quad (9)$$

A generalized expression for the recurrent calculation of the weight factor w_ξ for ξ-th element of the ciphergram using the weight coefficient value $w_{\xi-1}$ for $(\xi-1)$-th element based on using the binary transition functional $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$ for option, when $(|q_{\xi-2} - q_{\xi-1}| = 0)$, depending on the difference value $(|q_{\xi-1} - q_\xi|)$, will be determined by the next relationship:

$$w_\xi = w_{\xi-1}\left(\frac{(L-\xi-\beta_{\xi-1}+3)\cdot(L-\xi+2-\beta_{\xi-1})^{\varphi(q_{\xi-1};\,q_\xi)_{3,4}}}{(L-\xi+2)\cdot(\beta_{\xi-1})^{\varphi(q_{\xi-1};\,q_\xi)_{3,4}}}\right) \quad (10)$$

The resulting ratio, based on the specific difference value $(|q_{\xi-1} - q_\xi|)$ will take the next look:

1) for the no transition option $(|q_{\xi-1} - q_\xi| = 1)$ the corresponding value of the functional dependence will be equal to the component, $\varphi(q_{\xi-1};\, q_\xi)_{3,4} = 1$. Then the weight factor w_ξ for the current element determines by the formula:

$$w_\xi = w_{\xi-1}\left(\frac{(L-\xi-\beta_{\xi-1}+3)\cdot(L-\xi+2-\beta_{\xi-1})^1}{(L-\xi+2)\cdot(\beta_{\xi-1})^1}\right) =$$

$$= w_{\xi-1}\frac{(L-\xi-\beta_{\xi-1}+3)\cdot(L-\xi+2-\beta_{\xi-1})}{(L-\xi+2)\cdot(\beta_{\xi-1})}. \quad (11)$$

2) for the transition option availability $(|q_{\xi-1} - q_\xi| = 0)$ the corresponding value of the functional dependence will be zero, $\varphi(q_{\xi-1};\, q_\xi)_{3,4} = 0$. Here, the value of the weight factor w_ξ of the current ciphergram processed element the will be determined using the relation:

$$w_\xi = w_{\xi-1}\left(\frac{(L-\xi-\beta_{\xi-1}+3)\cdot(L-\xi+2-\beta_{\xi-1})^0}{(L-\xi+2)\cdot(\beta_{\xi-1})^0}\right) =$$

$$= w_{\xi-1}\left(\frac{(L-\xi-\beta_{\xi-1}+3)}{(L-\xi+2)}\right). \quad (12)$$

Thus, the relation (3) and (9) on the basis of taking into account the transitions between the three elements of the binary ciphergram allow us to generalize the process of determining their weight coefficients accordingly for variants where two previously treated elements create a binary transition and variants when there is no binary difference between such elements, with using functional dependencies $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ and $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$ shows the presence of a binary transition between the current and the previous elements.

To form a single relation for obtaining a ciphergram code in the process of its structural coding based on the use of generalized functional dependencies $\varphi(q_{\xi-1};\, q_\xi)_{1,2}$ and $\varphi(q_{\xi-1};\, q_\xi)_{3,4}$ it is necessary to identify situations when:

1) the first two conditions are fulfilled, that is, when two previously processed elements create a binary difference, $|q_{\xi-2} - q_{\xi-1}| = 1$;

2) performed the last two conditions, when two previously processed items missing binary difference, that is, $|q_{\xi-2} - q_{\xi-1}| = 0$.

To implement the identification of binary transitions between elements $q_{\xi-2}$ and $q_{\xi-1}$ proposed to use the next functionality $\varphi(q_{\xi-2};\, q_{\xi-1})$, which describes such a decisive rule:

$$\varphi(q_{\xi-2};\, q_{\xi-1}) = \begin{cases} 1, & \to |q_{\xi-2} - q_{\xi-1}| = 1; \\ 0, & \to |q_{\xi-2} - q_{\xi-1}| = 0. \end{cases}$$

To implement such a decisive rule, it is necessary to use the next adaptation of the sign function:

$$\varphi(q_{\xi-2};\, q_{\xi-1}) = \mathrm{sign}(|q_{\xi-2} - q_{\xi-1}|), \quad (13)$$

Accordingly, if the binary transition between the elements $q_{\xi-2}$ and $q_{\xi-1}$ exists, then the value of the functional will take a “1” value. On the contrary, when such a transition is absent then the value of such functional will be zero. Consequently, in order to organize the weight coefficients calculating switching process, taking into account the appropriate transition option, additional switches must be used:

- coefficient $\varphi(q_{\xi-2};\, q_{\xi-1}) = \mathrm{sign}(|q_{\xi-2} - q_{\xi-1}|)$ for switching to weight coefficient w_ξ in the case of a binary transition between the elements $q_{\xi-2}$ and $q_{\xi-1}$;
- coefficient $(1 - \varphi(q_{\xi-2};\, q_{\xi-1}))$, when between the elements $q_{\xi-2}$ and $q_{\xi-1}$ such a transition is absent.

This will enable the system of switches of ciphergram binary elements weight coefficients determining process for a single technological expression of the finding the structural code K.

Then using the expressions (3) and (9) to find the weight coefficients in two basic cases of the presence and absence binary transition between the two preceding elements and the ratio (12) for identifying such cases, we obtain the following technological formula for calculating the code of the ciphergram (Fig. 2) in the process of its structural coding:

$$K = \sum_{\xi=1}^{L} q_\xi w_\xi =$$

$$= \sum_{\xi=1}^{L} q_\xi \Big(\varphi(q_{\xi-2};\, q_{\xi-1}) \times$$

$$\times w_{\xi-1}\left(\frac{(\beta_{\xi-1}+1)\cdot\beta_\xi^{\varphi(q_{\xi-1};\,q_\xi)_{1,2}}}{(L-\xi+2)\cdot(L-(\xi-2)-\beta_{\xi-1})^{\varphi(q_{\xi-1};\,q_\xi)_{1,2}}}\right) +$$

$$+ (1-\varphi(q_{\xi-2};\, q_{\xi-1}))\times$$

$$\times w_{\xi-1}\left(\frac{(L-\xi-\beta_{\xi-1}+3)\cdot(L-\xi+2-\beta_{\xi-1})^{\varphi(q_{\xi-1};\,q_\xi)_{3,4}}}{(L-\xi+2)\cdot(\beta_{\xi-1})^{\varphi(q_{\xi-1};\,q_\xi)_{3,4}}}\right)$$

or

$$K = \sum_{\xi=1}^{L} q_\xi w_\xi =$$

$$= \sum_{\xi=1}^{L} q_{\xi} (\mathrm{sign}(|q_{\xi-2} - q_{\xi-1}|) \times$$

$$\times w_{\xi-1} \left(\frac{(\beta_{\xi-1}+1) \cdot \beta_{\xi}^{(1-\mathrm{sign}(|q_{\xi-1}-q_{\xi}|))}}{(L-\xi+2) \cdot (L-(\xi-2)-\beta_{\xi-1})^{(1-\mathrm{sign}(|q_{\xi-1}-q_{\xi}|))}} \right) +$$

$$+ (1 - \mathrm{sign}(|q_{\xi-2} - q_{\xi-1}|)) \times$$

$$\times w_{\xi-1} \left(\frac{(L-\xi-\beta_{\xi-1}+3) \cdot (L-\xi+2-\beta_{\xi-1})^{\mathrm{sign}(|q_{\xi-1}-q_{\xi}|)}}{(L-\xi+2) \cdot (\beta_{\xi-1})^{\mathrm{sign}(|q_{\xi-1}-q_{\xi}|)}} \right) \quad (14)$$

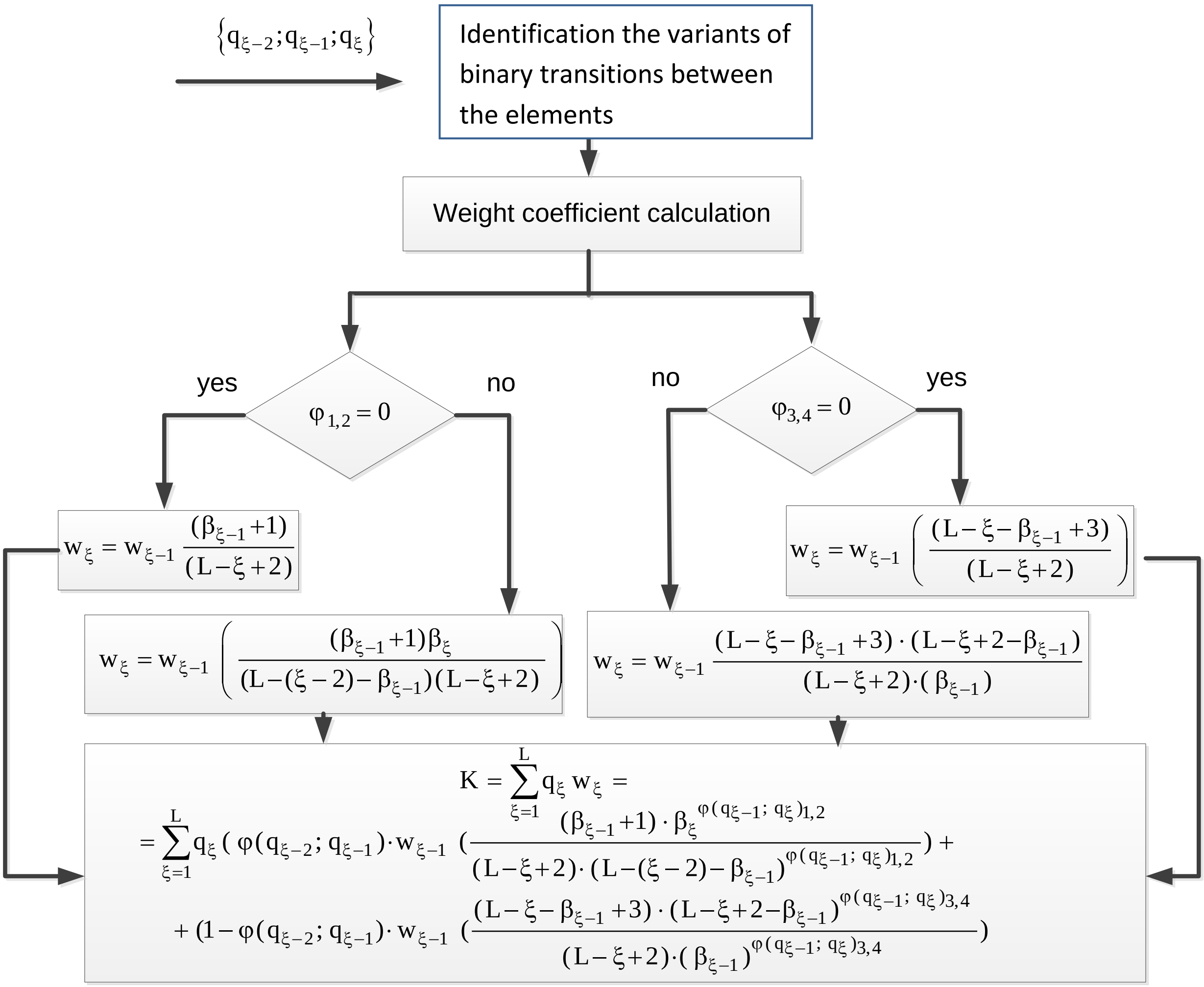

Fig. 2. A structural scheme for calculating the ciphergram code K in the process of its structural coding

Here L – the length of the processed binary ciphergram; q_{ξ} – ξ-th element; β_{ξ} – a recurrence parameter equal to the number of binary drops (the transitions between "0" and "1") for the sequence, consisting of $(L-\xi+1)$ ciphergram raw elements:

$$\beta_{\xi} = \beta_{\xi-1} - \left| q_{\xi-1} - q_{\xi} \right| . \quad (15)$$

Binary structural coding provides a reduction in the ciphergram bits number.

Generalized dependencies for finding weight coefficients in the process of binary uniform ciphergrams structural coding are developed. This allows to reduce the number of transactions, which is associated with decreasing in the information intensity of the video stream. The switches of the weight coefficients calculating process were developed, taking into account the transition options for determining the ciphergram binary elements weight coefficients.

II. Creation a video frame reconstruction method in the conditions of their selective processing and closing of significant components

It is proposed to develop an encrypted video stream decoding method, based on intra-frame selection, which is based on the detection of closed meaningful structural components of the base video frame. To do this, it is proposed to decode an encrypted base video frame K_I taking into account the definition of significant $S_{зн}^{(\xi,\gamma)}$ structural components. The block diagram of the encrypted video stream decoding method includes the next basic steps:

1. Isolation the code structure of the frames group ofrom the binary sequence of the video data stream.
2. Define the type of video frames in the frame group.
3. Selection the digital representation of the closed base video frame from the digital representation of the frames group.
4. Detection closed $S_{sig}^{(\xi,\gamma)}$ and not closed $S_{unsig}^{(\xi,\gamma)}$ structural components. This happens as a result of the label M analysis, the value of which is stored in the digital description of the structural component additional data. If label value M=1, then the structural unit is defined as significant $S^{(\xi,\gamma)} = S_{sig}^{(\xi,\gamma)}$. If label value M=0, then the structural unit is defined as insignificant $S^{(\xi,\gamma)} = S_{unsig}^{(\xi,\gamma)}$.
5. Reverse structural coding.
6. Decoding of closed significant $S_{sig}^{(\xi,\gamma)}$ structural components, in which the values of the components of transformation of the DCT blocks $B(Y)_{L_{row},L_{col}}^{(\xi,\gamma)}$, $B(Cr)_{L_{row},L_{col}}^{(\xi,\gamma)}$ and $B(Cb)_{L_{row},L_{col}}^{(\xi,\gamma)}$ are deciphered.
7. Decoding of unsignificant $S_{unsig}^{(\xi,\gamma)}$ structural components, which includes such stages:
7.1. Reverse linearization of the DCT blocks transformatnts for the component of brightness and color $B(Y)_{L_{row},L_{col}}^{(\xi,\gamma)}$, $B(Cr)_{L_{row},L_{col}}^{(\xi,\gamma)}$ and $B(Cb)_{L_{row},L_{col}}^{(\xi,\gamma)}$ for the unsignificant ctructural components.
7.2. Dequantization the DCT transformants of insignificant blocks.
8. Reverse DCT of significant and insignificant blocks for the brightness and color component of $B(Y)_{L_{row},L_{col}}^{(\xi,\gamma)}$, $B(Cr)_{L_{row},L_{col}}^{(\xi,\gamma)}$ and $B(Cb)_{L_{row},L_{col}}^{(\xi,\gamma)}$.
9. Construction of structural components composition $S^{(\xi,\gamma)}$ for base video frame K_I, which includes the next steps:
9.1. Decode the service information for the structural components formation $S^{(\xi,\gamma)}$:
9.2. Formation of macroblock compositions $M(Y)^{(\xi,\gamma)}$, $M(C_r)^{(\xi,\gamma)}$ and $M(C_b)^{(\xi,\gamma)}$.
10.2. Formation the video from blocks $B(Y)_{L_{row},L_{col}}^{(\xi,\gamma)}$, $B(Cr)_{L_{row},L_{col}}^{(\xi,\gamma)}$ and $B(Cb)_{L_{row},L_{col}}^{(\xi,\gamma)}$.
10. Converting the digital planes of an I-frame video from an YUV format to RGB format (forming one YCrCb image be three digital planes).
11. Обернена диференціальна імпульсно-кодова модуляція для відновлення P-кадрів.
12. Backward differential pulse-code modulation to restore B-frames:
12.1 Convert digital video planes of P i B-frames from YUV to format RGB.
13. Formation group of video frames from the restored I, P and B-frames.

Service information of a structural features sequence – the value of θ for components series identified for the matrix of signs.
The decoding process is to restore the elements q_{k+1} of binary matrixes.
After getting the service information on the receiving side, the DCT transformants components reconstruction is organized.
So:
1. Proved necessary service information required to mutually unambiguous binary data recovery.
2. A recurrent restoration of binary array elements based on one-dimensional floating structural binary sequences decoding constructed. This decoding differs from other approaches in that:
– decoding is performed for code structures formed for a variable number of binary elements;
– weight factors calculates by recursive expressions based on known values of the two previous reconstructed elements and the previous element weighting factor.

III. CONCLUSIONS

The method of increasing the efficiency and confidentiality for the video information stream based on the selective transformation of macroblocks is developed.
Improved the information technology for closing the video stream, based on the technological direction of processing and closing significant blocks with the additional application of structural coding modernization. This method is based on the macroblocks classification improvement using their previous transformation. This allows to detect significant structural components based on the analysis of the indicators values on the set of low-frequency and high-frequency components of the transformant for the DC-block of the bright component, which is then used for cryptographic protection.
Performs the elimination of statistical and psycho-visual redundancy is based on the consideration of the various peculiarities of frequency component transformants. This leads to a reduction in the information intensity of the frames stream. This allows to provide the departmental requirements for the video resource confidentiality.
The method of binary structural coding is based on the use of a structural approach, which is based on the number of binary transitions identification and the corresponding code formation description without loss of information, provides a reduction of the digits number for the presentation of ciphergrams. This method bases on a preliminary estimation of the binary series distribution in a ciphergram. Depending on this, division the binary digits number into the converted representation of the ciphergram is carried out. The basic stage of the structural method of coding is the different modes identification of binary transitions between the ciphergram elements. This ensures a reduction in the number of digits on the ciphergrams. This reduces the information load on the data transmission channels and reduces the time delay for the transmission of video information.

REFERENCES

[1] R.Gonzalez Digital image processing / R. Gonzalez, R. Woods. M .: Technosphere, 2005. 1072 p.

[2] M.D. Adams The JPEG-2000 Still Image Compression 1 N 2412, Sept. 2001.

[3] O.Yudin, O.Frolov, R.Ziubina Quantitative quality indicators of the invariant spatial method of compressing video data //Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference. IEEE, 2015.P. 227-229.doi: 10.1109/INFOCOMMST.2015.7357320

[4] V. Barannik, S. Podlesny, A. Krasnorutskyi, A. Musienko and V. Himenko, “The ensuring the integrity of information streams under the cyberattacks action”, 2016 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, 2016. P. 1-5. doi: 10.1109/EWDTS.2016.7807752

[5] V.Barannik, I.Hahanova, N.Kulbakova. Dynamic coding of transforms of the images in two level polyadic space Modern Problems of Radio Engineering, Telecommunications and Computer Science - International Conference, TCSET 2008; Lviv-Slavsko. Ukraine. 19 February 2008. 23 February. P. 320-325.