Methods of Crypto Protection of Color Image Pixels in Different Code Systems

Nataliia Vozna[1], Yaroslav Nykolaichuk[1], Orest Volynskyi[2], Petro Humennyi[1], Andrij Sydor[1]

1. Department of Specialized Computer Systems, Ternopil National Economic University, UKRAINE, Ternopil, 8 Chekhova str., email: nvozna@ukr.net

2. Department of Cyber Security, Ternopil National Economic University, UKRAINE, Ternopil, 8 Chekhova str., email: orestsks@ukr.net

Abstract: **The relevance of the development of theoretical foundations, methods and algorithms for encoding color image pixels by the problem-oriented multifunctional data structuring and the representation of color image code pixels in Rademacher (R), Krestenson (K), Rademacher-Krestenson (RK), Haar-Krestenson (HK) and Galois (G) Systems is substantiated in this article. The purpose of the research is to increase the efficiency of the algorithms for digital image transforms, processing and recognition using modular arithmetic of extended Galois fields on the basis of mathematics of arithmetic operations of a non-positional residue number system.**

Keywords: **crypto protection, color image pixels, Rademacher and Krestenson Systems, Residue Number System.**

I. Introduction

Successful development of modern computer technology, microelectronics and telecommunication systems promotes designing and mass production of color TV displays as well as personal computers, mobile devices, camcorders, tablet PC screens, industrial and large format color displays.

The large-scale application of various types of video equipment in all branches of industry and their wide-spread personal use determines a high level of importance of the solutions to theoretical and applied problems of increasing and optimizing the efficiency of video image structuring during the processes of creation, encoding, transformation, crypto protection, transmission, archiving and access receiving to color images as well as their use.

The examples of setting and successful solving the problems referring to this issue on the basis of the mathematical foundations development, the implementation of the algorithms and hardware and software tools for image processing and recognition were thoroughly highlighted in the works of scientific researches [1-5].

Considerable attention is paid to solving research problems in this field and creating algorithms of the image structural properties and features.

II. Methods of Multifunctional Structuring of Color Image Pixels in the System of Extended Galois Fields

The analysis of the mathematical foundations of the existing algorithms for color image processing and recognition was carried out by segmentation methods on the basis of histogram thresholding and cumulative histograms. It is analysis of the statistic estimates of the mean value, dispersion, asymmetry and the degree of contrast of the intensity histograms homogeneity taking into account the dispersion of pixels coordinates of image fragments and silhouettes, as well as image clustering methods [1-5].

As a result, it was found that the main components of the algorithms of the above-mentioned methods for image processing are the following arithmetic operations: summarizing ($\sum x_i$), division ($P(i) = n_i / n_0$), absolute difference ($|x_i - x_j|$), square (x_i^2), multiplication ($x_i \times x_j$), square difference ($[x_i - x_j]^2$), sum of multiplication ($\sum x_i x_j$), which are commonly performed due to the low-speed arithmetic of the binary number system.

III. The Method for Encoding RGB Pixels in the Rademacher and Krestenson Systems

According to the international RGB color model, colors are presented as a combination of three main colors: red (R), green (G) and blue (B) [4].

In this case in the computer RGB system, the main color has 256 gradations. Thus, the color code of the RGB system is made up of three bytes, that is, 24 bits in the Rademacher system.

The colors of the Hamming distance pixels on a monitor, given in Cartesian coordinates, can be coded in the Residue Number System (K). This is implemented by introducing three relatively simple modules (P_1, P_2, P_3), which allow encoding each pixel of the RGB system in the binary system by forward integer transform of the residue number system (RNS) according to the expression [6]:

$$N_k = res \sum_{i=1}^{3} b_i \cdot B_i (\mathrm{mod}\, P_0) \qquad (1)$$

where B_i - the orthogonal bases of RNS, which are calculated according to diophantine equations:

$$B_1 = P_2 \cdot P_3 \cdot m_1 \equiv 1 (\mathrm{mod}\, P_1); \qquad (2)$$

$$B_2 = P_1 \cdot P_3 \cdot m_2 \equiv 1 (\mathrm{mod}\, P_2); \qquad (3)$$

$$B_3 = P_1 \cdot P_2 \cdot m_3 \equiv 1 (\mathrm{mod}\, P_3), \qquad (4)$$

where m_1, m_2, m_3 - inverse elements of the RNS [8];

$P_0 = P_1 \cdot P_2 \cdot P_3$ - color image pixel encoding range with color depth $K_0 = \hat{E}[\log_2 P_0]$, $\hat{E}[\bullet]$ - integer function with rounding to a larger integer.

RGB pixels encoding in the Rademacher-Krestenson system is provided by selecting the following values of the encoding range of b_i remainders in the Rademacher system:

$b_1 = b_R$; $0 \le b_R \le 255$; (00000000 ÷ 11111111);

$b_2 = b_G$; $0 \le b_G \le 255$; (00000000 ÷ 11111111);

$b_3 = b_B$; $0 \le b_B \le 255$; (00000000 ÷ 11111111).

In addition, taking into account the coefficients $m = 1.0$, $n = 4.5907$, $p = 0.0601$, in order to achieve the most saturated green color, the range of its change can be set as $0 \le b_G \le 254$ that provides relevant simplicity of the following modules: $P_1 = 256$, $P_2 = 255$, $P_3 = 257$.

To verify the relevant simplicity of the selected modules system, they are factorized into multipliers: $256 = 2^8$, $255 = 5 * 51$, 257 - a prime number, i.e. $P_0 = 16776960$, where $P_0 < 2^{24} = 16777216$. That is, the condition for creating a 24-bit pixel code in the Rademacher-Krestenson System is satisfied.

In binary system module codes are represented as:

$P_1 = 100000000_{(2)}$, $P_2 = 11111111_{(2)}$, $P_3 = 100000001_{(2)}$.

Then: $P_0 = 111111111111111100000001_{(2)}$.

As a module $P_1 = 2^8$ is among the modules P_1, P_2, P_3, then, according to the inverse RNS transform, the remainder of N_k (G – color features) will be presented without decoding it by eight low orders of N_k, which is in the Rademacher system.

According to the Diophantine equations solution (2-4), the following values of the inverse elements m_i and basic numbers B_i are received:

$m_1 = 255$, $B_1 = 16711425$; $m_2 = 128$, $B_2 = 8421376$; $m_3 = 129$, $B_3 = 8421120$

The verification of the calculation accuracy of the RNS transform is performed according to the equation:

$N_k = (b_R \cdot B_1 + b_G \cdot B_2 + b_B \cdot B_3) \cdot (\mathrm{mod}\, P_0) = 1$ when $b_R = 1$, $b_G = 1$, $b_B = 1$.

That is,

$N_k = (1 \cdot 16711425 + 1 \cdot 8421376 + 1 \cdot 8421120) \cdot (\mathrm{mod}\, P_0) = 1$.

For example, $R = 10$, $G = 200$, $B = 100$.

Then

$$N_k = (10 \cdot 16711425 + 200 \cdot 8421376 + 100 \cdot 8421120) \cdot \cdot (\mathrm{mod}\, 16776960) = 9187850,$$

which corresponds to the binary representation of the RGB pixel in the Krestenson System ($100011000011001000001010_2$).

Decoding of such representation is as follows:

$$r_i = resN_k (\mathrm{mod}\, P_1);\ g_i = resN_k (\mathrm{mod}\, P_2);$$
$$b_i = resN_k (\mathrm{mod}\, P_3).$$

IV. The method for color image pixels encoding in the Rademacher-Krestenson and the Haar-Krestenson Systems

The encoding of color image pixels according to the RGB color model is carried out by the 24-bit binary code, when the intensity of each of the colors is represented by the 8-bit binary code of the Rademacher System:

$$R\begin{cases} r_{8-1} \\ \dots \\ r_i \\ \dots \\ r_0 \end{cases}; \quad G\begin{cases} g_{8-1} \\ \dots \\ g_i \\ \dots \\ g_0 \end{cases}; \quad B\begin{cases} b_{8-1} \\ \dots \\ b_i \\ \dots \\ b_0 \end{cases}$$

$0 \le r_i \le 255$; $0 \le g_i \le 255$ $0 \le b_i \le 255$.

Encoding of the color image RGB pixels in the Rademacher-Krestenson (RK) and Haar-Krestenson (HK) Systems is carried out by selecting relatively simple modules system (P_1, P_2, P_3), whose product exceeds the range of quantization of the brightness values (r_i, g_i, b_i).

Such a condition can be satisfied by a different set of the RNS discrete transformer modules, for example, $P_1 = 5, P_2 = 7, P_3 = 8$, which provide encoding of r_i, g_i and b_i brightness in $P_0 = 5 * 7 * 8 = 280 > 255$ range. The following code structure is created in the R-K System, which unambiguously represents the corresponding RGB-pixel code:

$$R \vee G \vee B\begin{cases} a_2 \\ a_1 \\ a_0 \end{cases}; \quad \begin{cases} c_2 \\ c_1 \\ c_0 \end{cases} \quad \begin{cases} d_2 \\ d_1 \\ d_0 \end{cases}$$

$P_1 = 5$ $P_2 = 7$; $P_3 = 8$,

where $a_i \in \overline{0,1}$; $c_i \in \overline{0,1}$; $d_i \in \overline{0,1}$; $i \in \overline{0,2}$.

In this case, each value a_i, c_i, d_i is calculated as the remainder according to the expressions: $a_i = res(r_i \bmod P_1)$; $c_i = res(g_i \bmod P_2)$, $d_i = res(b_i \bmod P_3)$.

For a given set of modules, the inverse elements m_i and the basic numbers B_i are determined according to the Diophantine equations solutions (2-4):

$m_1 = 1$, $B_1 = 56$, $m_2 = 3$, $B_2 = 120$, $m_3 = 3$, $B_3 = 105$.

Accuracy of the obtained m_i and B_i values is verified according to the expression (1):

$N_1 = (1 \cdot 56 + 1 \cdot 120 + 1 \cdot 105) \bmod 280 = 1$

For example, the following values of color intensity of the RGB-pixel are set as: $r_i = 10$, $g_i = 100$, $b_i = 37$.

Then, RGB-pixel codes are received in the Rademacher System:

$r_i = 00001010_{(2)}$; $g_i = 01100100_{(2)}$; $b_i = 00100101_{(2)}$;

in the Rademacher-Krestenson system:

$$r_i = (\overbrace{000}^{P_1}\overbrace{011}^{P_2}\overbrace{101}^{P_3})_{(5,7,8)};\ g_i = (\overbrace{000}^{P_1}\overbrace{010}^{P_2}\overbrace{010}^{P_3})_{(5,7,8)};$$

$$b_i = (\overbrace{010}^{P_1}\overbrace{010}^{P_2}\overbrace{101}^{P_3})_{(5,7,8)}.$$

Representation of the RGB pixel code for each r_i, g_i and b_i intensity value in the Haar-Krestenson System is made according to the structure:

$$R \vee G \vee B \begin{cases} a_{P_1-1} \\ .... \\ a_i \\ .... \\ a_0 \end{cases}; \quad \begin{cases} c_{P_2-1} \\ ... \\ c_i \\ ... \\ c_0 \end{cases} \quad \begin{cases} d_{P_3-1} \\ ... \\ d_i \\ ... \\ d_0 \end{cases}$$

$$P_1 = 5 \qquad P_2 = 7; \qquad P_3 = 8,$$

where $i \in \overline{0, P_i - 1}$

For the specified color intensity values of the RGB pixel $r_i = 10$, $g_i = 100$, $b_i = 37$, the following code structure in the H-K system is obtained:

$r_i = (10000..0001000..00000100)$;

$g_i = (10000..0010000..00100000)$;

$b_i = (00100..0010000..00000100)$.

The representation of r_i, g_i and b_i color brightness digital values in different systems leads, correspondingly, to different code length according to the expressions:

1. $K_R = \log_2 2^8 = 8$ bits in the Rademacher System (R).

2. $K_{R-C} = \sum_{i-1}^{3} [\hat{E}(\log_2 P_i - 1)] = 3 + 3 + 3 = 9$ bits in the Rademacher-Krestenson system (R-K).

3. $K_{H-C} = \sum_{i=1}^{n} P_i = 5 + 7 + 8 = 20$ bits in the Haar-Krestenson System (H-K).

V. Structure Development and Experimental Studies of Structural, Time and Hardware Complexity of ADC With the R and H-K Output Codes.

It is expedient to make multifunctional encoding of RGB pixels in the R-K and H-K systems at the level of analog-to-digital conversion of the analog signals intensity of the RGB sensors. Such a principle of multifunctional data structuring in color formation is implemented by parallel ADC, the structure of which is shown in Fig 1.

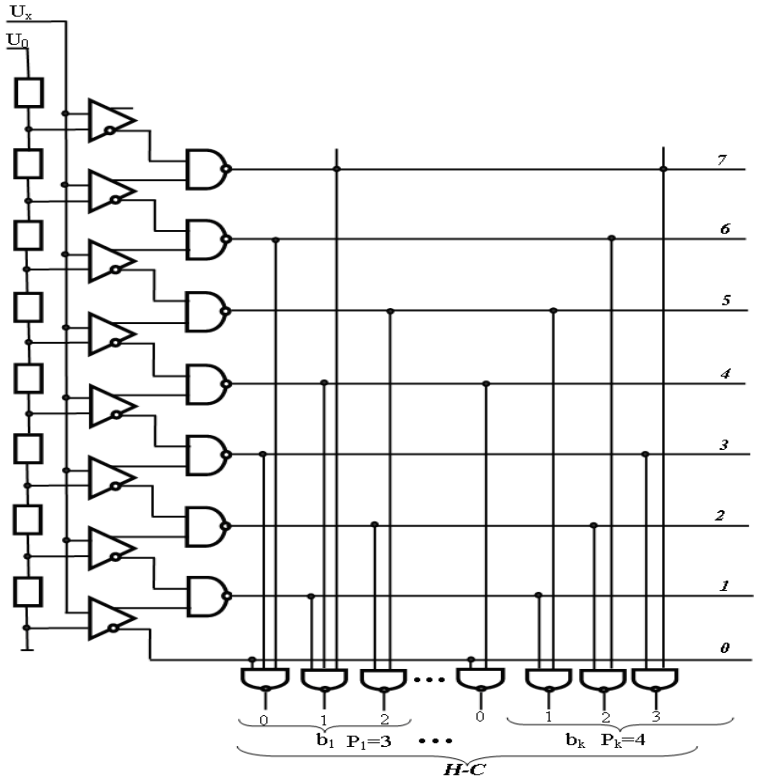

Fig.1. The structure of a multi-purpose parallel ADC with output codes in the Haar-Krestenson System.

ADC consists of 1 – input analogue bus; 2 – paraphase comparators; 3 – input reference bus; 4– exemplary resistors; 5 – the first logic elements "AND-NOT"; 6 – the second logic elements "AND-NOT", 7 – output ADC bus.

ADC efficiency is determined according to the expression:

$$\tau_{ADC_2} = \tau_{k_2} + \tau_{LE_2} + \tau_{LE_3},$$

where $\tau_{k_2} = 2\upsilon$ - switching time for paraphase comparator;

$\tau_{LE_2} = 1\upsilon$ - switching time for two-input logic element "AND-NOT";

$\tau_{LE_3} = 1\upsilon$ - switching time for multi-input logic element (LE) "AND-NOT";

That is, the efficiency of ADC is determined by the total delay of signals:

$$\tau_{ADC_2} = (2+1+1)\upsilon = 4 \text{ micro cycles.}$$

When calculating the time complexity of the ADC components, it is taken into account that the switching time of the paraphase comparator is 2.5 times less in comparison with the single-phase comparator due to positive trigger feedback between the direct and inverse outputs.

VI. The Method of Crypto Protection of Color Image RGB Pixels.

Crypto protection of the RGB image pixels is performed in order to restrict unauthorized access to color images that are generated in real time. It's encoded in different number systems, transmitted via communication channels, recorded in database storage, and displayed on the user monitors. There are different methods for encrypting files containing color image data and data arrays, which include a certain amount of color images. In this case, information systems use standard algorithms for data arrays protection from unauthorized access on the basis of hashing, symmetric and asymmetric RSA algorithms, elliptic curves, etc. [7, 8].

The method for encryption of color images RGB pixels, which are represented by R, R-K and H-K codes of the described methods, is proposed. In this case, structured R-K and H-K codes are problem-oriented to increasing the efficiency of the image transform, processing and recognition in accordance with the modular arithmetic of the Residue Number System.

It is expedient to apply an effective method based on hashing of certain code positions and logic combination of bits of generated Galois sequences [9] according to the following graphs as the main method of crypto protection of RGB pixel codes:

$$\begin{array}{cccccc} a_n & a_{n-1} & \dots & a_i & \dots & a_0 \\ & \searrow & & \swarrow & & \\ b_n & b_{n-1} & \dots & b_i & \dots & b_0 \end{array} \quad (1)$$

$$\oplus \quad \oplus \quad \oplus \quad \oplus \quad (2)$$

$$G_{n+j} \quad G_{n-1+j} \dots G_{i+j} \dots G_{0+j}$$

$$(P_n \quad P_{n-1} \quad \dots \quad P_i \quad \dots \quad P_0) = \{PX\},$$

where a_i - bits of R-K or H-K pixel codes; 1 – hashing procedure ($b_i := b_j, i \neq j, i \in \overline{0,n}$), $P_i, i \in \overline{0,n}$ - created code of crypto protected pixel PX.

Bits of Galois $\{G_i\}$ codes are generated according to secret keys.

VII. Conclusions

The relevance of the development of the theory, methods and algorithms for encoding color image pixels and their representation in different systems has been substantiated. This allows to increase the efficiency of algorithms for digital image transform, processing and recognition on the basis of the mathematics of arithmetic operations of the non-positional Residue Number System.

The analysis of the mathematical foundations of existing algorithms for color image processing and recognition was carried out by segmentation methods on the basis of histogram thresholding and cumulative histograms, statistic estimates of the mean value, dispersion, asymmetry and the degree of contrast of the intensity of histograms. This is exemple homogeneity taking into account the dispersion of pixels coordinates of image fragments and silhouettes, as well as image clustering methods.

It is proposed to carry out structured encoding of color image pixels by the codes of non-positional number systems of R-K, H-K and G. This allows to increase the efficiency of algorithms for image processing by 2-3 orders.

References

[1] Otsu N., A threshold selection method from grey level histograms, *IEEE Trans. Systems Man Cybernet*, No.9, pp.62-66, 1979..

[2] Zhang Yudong and Wu Lenan., Fast Document Image Binarization Based on an Improved Adaptive Otsu`s Method and Destination Word Accumulation, *Jornal of Computational Information Systems, No.6*, pp.1886-1892, 2011.

[3] U. Ramer, "An Iterative Procedure for the Polygonal Approximation of Plane Curves," *Computer Graphics Image Processing, Vol. 1, No. 3*, pp. 244-256, 1972.

[4] R. Melnyk Algorithms and methods for image processing: Teaching manual., Lviv*: Lviv Politechnika Publishing House*, 220 pp., 2017.

[5] N. Lotoshynska. Theory of color and color formation: Teaching manual, Lviv: *Lviv Politechnika Publishing House*, 204p., 2014.

[6] N. Vozna., Y. Nykolaichuk and N. Shyrmovska, "Method of formation of structured data of quasi-stationary objects on the basis of the Residue Number System of the Krestenson basis", *Scientific and Technical Journal "Exploration and Development of Oil and Gas Fields, No. 3 (40)*, pp.62-65,2011.

[7] Ya. Nykolaychuk, M. Kasianchuk and I.Yakymenko, "Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation", *Cybernetics and Systems Analysis, Volume 50, Issue 5*, pp. 649-654, September, 2014.

[8] Ya. Nykolaychuk, M. Kasianchuk and I.Yakymenko, "Theoretical Foundations of the Modified Perfect form of Residue Number System", *Cybernetics and Systems Analysis, Volume 52, Issue 2*, pp. 219-223, March, 2016.

[9] Y. Nykolaichuk, Galois Field Codes: Theory and Application, Ternopil: *Ltd.: Terno-graf*, 576 pp., 2012.