УДК 681.322

Н.Я. ВОЗНА, Я.М. НИКОЛАЙЧУК, О.І. ВОЛИНСЬКИЙ

АЛГОРИТМИ РОЗВ'ЯЗАННЯ ЗАДАЧ КРИПТОЗАХИСТУ ПІКСЕЛІВ КОЛЬОРОВИХ ЗОБРАЖЕНЬ У БАЗИСІ РАДЕМАХЕРА ТА ЗАЛИШКОВИХ КЛАСАХ

Анотація. Обґрунтовано актуальність розроблення теоретичних засад, методів та алгоритмів криптозахисту пікселів кольорових зображень шляхом проблемно-орієнтованої поліфункціональної структуризації даних та представлення кодів пікселів кольорових зображень у теоретико-числових базисах Радемахера, Радемахера–Крестенсона, Хаара–Крестенсона та Галуа. Досліджено можливість підвищення швидкодії алгоритмів перетворення, опрацювання та розпізнавання цифрових зображень із застосуванням модульної арифметики залишкових класів на основі математики арифметичних операцій непозиційної системи числення залишкових класів.

Ключові слова: алгоритми, криптозахист, кольорові зображення, теоретико-числові базиси.

ВСТУП

Успішний розвиток сучасної комп'ютерної техніки, мікроелектроніки та телекомунікаційних систем стимулює створення та масовий випуск дисплеїв кольорових зображень для телевізорів, моніторів персональних комп'ютерів, мобільних засобів, відеокамер, планшетів, промислових та великогабаритних табло [1, 2].

Широкомасштабне застосування різних типів відеотехніки у всіх галузях промисловості та в побуті зумовлює високу актуальність теоретичних і прикладних задач з удосконалення, оптимізації та підвищення ефективності структуризації відеозображень у процесах формування, кодування, перетворення, криптозахисту, передавання, архівації, використання кольорових зображень та організації доступу до них.

Приклади постановки та успішного розв'язання цих задач шляхом розроблення математичних основ, реалізації алгоритмів та використання програмно-апаратних засобів опрацювання та розпізнавання зображень представлено у роботах зарубіжних авторів [3–5], українських вчених [6–9] та ін.

Значну увагу в цьому напрямі досліджень приділено розв'язанню задач криптозахисту шляхом удосконалення алгоритмів структурних перетворень цифрових зображень.

1. АНАЛІЗ АЛГОРИТМІВ ОПРАЦЮВАННЯ ЗОБРАЖЕНЬ

У процесах кодування, перетворення, структуризації, кластеризації, класифікації та розпізнавання зображень використовують складні математичні методи та алгоритми опрацювання. Розглянемо найбільш ефективні та широковживані з них [6].

1.1. Алгоритми оцінки ступеня статистичної близькості структур цифрових зображень. Для оцінки ступеня декомпозиції зображення введено алгоритми [6], які характеризують зображення з точки зору його структурних властивостей, зокрема (верхній індекс позначає рівень зображення):

- між сусідніми рівнями зображення:

$$K_S^1 = C / MC,\ K_S^2 = CR / C,\ K_S^{23} = IA / CR;$$

• через один сусідній рівень:

$$K_S^{12} = CR / MC,\ K_S^{23} = IA / C;$$

• усієї сукупності пікселів:

$$K_S^{123}(PX) = IA / PX,$$

де C — кластери; MC — мікрокластери; CR — замкнені ділянки; IA — кількість ступенів декомпозиції зображення; PX — ймовірності інтенсивностей пікселів.

1.2. Структурні оцінки мір близькості зображень. Найбільш поширеними мірами близькості зображень є такі [6]:

• евклідова відстань

$$d(i, j) = \sqrt{\sum (x_i - x_j)^2},$$

x_i, x_j — ознаки зображень;

• манхеттенська відстань

$$d_m(i, j) = \sum_{i=1}^{M} \sum_{j=1}^{N} | x_i - y_j |;$$

• статична відстань

$$d_S(i, j) = \left(\sum_{i=1}^{M} \sum_{j=1}^{N} | x_i - y_j |^P \right)^{1/2},\ P \to \infty;$$

• відстань Чебишова

$$d_c(i, j) = \max \sum | x_i - x_j |;$$

• відстань найменш (D_1) та найбільш (D_2) віддалених сусідів кластерів

$$D_1(A, B) = \min \{d_{ij}\},\ i \to A,\ j \to B,\ D_2(A, B) = \max \{d_{ij}\};$$

• попарне середнє

$$D_S(A, B) = \frac{1}{| A | \times | B |} \sum_{i=1}^{A} \sum_{j=1}^{B} d_S(i, j);$$

• центроїдна відстань

$$D_S(A, B) = (d_S(ic, jc)),$$

де ic, jc — центроїди кластерів зображень A і B;

• відстань Варда

$$D_S(A, B) = d_e / (| A | \times | B |),\ d_e = \sqrt{\sum (x_k - \bar{x})^2},$$

x_k — координати пікселя, $\bar{x}$ — математичне сподівання координат.

2. МЕТОДИ ОПРАЦЮВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ГІСТОГРАМ

2.1. Метод сегментування зображень на основі гістограм з одним порогом згідно із статистичним алгоритмом Оцу [6]. Ідея алгоритму полягає у мінімізації зваженої суми дисперсій інтенсивності двох сегментів зображень [6]:

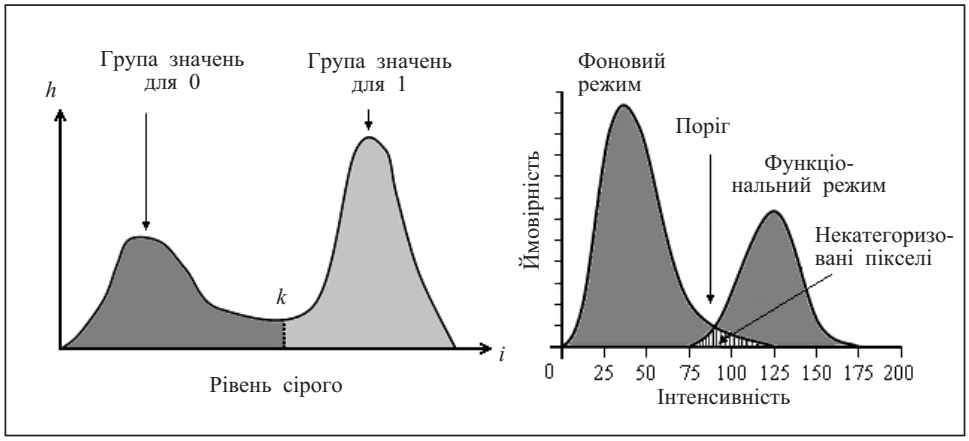


Рис. 1. Приклади гістограм інтенсивностей пікселів зображення

$$\sigma^2_{\text{міжклас.}}(T) = \sigma_0^2 - \sigma^2_{\text{внутр.}}(T) = W_1(t)W_2(t)[M_1(t) - M_2(t)]^2,$$

$$\sigma_{\text{внутр.}}(T) = \omega_B(T)\sigma_B^2(T) + \omega_0(T)\sigma_0^2(T),\ \omega_B(T) = \sum_{i=0}^{T-1} P(i),\ \omega_0(T) = \sum_{i=T}^{L-1} P(i),$$

$$\mu_1(T) = \sum_{i=0}^{T-1} P(i)x(i),\ \mu_2(T) = \sum_{i=T}^{L-1} P(i)x(i),$$

де $x(i)$ — значення інтенсивності, μ — середнє арифметичне; σ — середньоквадратичне відхилення; σ_B^2, σ_0^2 — дисперсії пікселів сегмента зображення, відповідно нижче і вище від порогу, $P(i)$ — відносна ймовірність пікселів або абсолютна кількість пікселів на i-му рівні.

Приклад бінаризації зображення таким методом наведено на рис. 1 [6].

Перевага цього методу полягає у простому алгоритмі обчислень на основі адитивних та мультиплікативних операцій над кодами інтенсивностей RGB-пікселів $x(i)$.

2.2. Модифікація методу Оцу. Модифікація базується на визначенні кумулятивної гістограми як суми ймовірностей [6]. Це алгоритм, за яким дисперсію величин обчислюють з обох боків осі інтенсивності і розраховують згідно з виразом

$$V_1(S) = \sum_{i=\overline{n,s}} P_2(i).$$

Для кожного сегмента зображення за ітераційною процедурою обчислюють дисперсію відхилень значень $P_1(i)$ та $P_2(i)$ від середнього арифметичного значення [6]:

$$E_1^2(S) = \frac{1}{S}\sum_{i=1}^{S}[P_1(i) - \overline{P_1}(S)]^2,\ E_2^2(S) = \frac{1}{n-S}\sum_{i=n}^{S}[P_2(i) - \overline{P_2}(S)]^2,$$

$$F_S(V) = \min\{E_1(V_1(S)) + E_2(V_2(S))\}.$$

На рис. 2 наведено приклад результатів розрахунку кумулятивної гістограми [6].

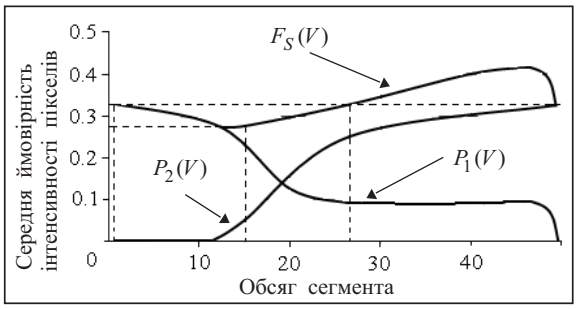


Рис. 2. Кумулятивна гістограма зображення

2.3. Сегментування зображень за кумулятивною гістограмою. Нормовану кумулятивну гістограму для кількості пікселів зображення $N \times M / n$, де N, M — розміри зображення, n — кількість інтервалів кумулятивної гістограми, розраховують за формулою [6]

$$V_{FG}(S) = (1/n)\,S\,,\ S \in \overline{1, 4},$$

де $V_{FG}(S)$ — кількість пікселів зображення в інтервалі інтенсивності $(1–S)$.

На рис. 3 [6] наведено графіки гіпотетичної та реальної кумулятивних гістограм зображення та різниці між ними згідно з виразом

$$D(S) = V_F(S) - V_{FG}(S),\ S \in \overline{1, 4},$$

де $V_F(S)$ — максимальна кількість пікселів на вертикалі зображення.

Реальну кумулятивну гістограму отримують шляхом центрування гіпотетичної гістограми, що спрощує цифрове розпізнавання зображення.

2.4. Розподілені статистичні ознаки зображень. Аналіз та класифікацію зображень виконують на основі розрахунку таких статистичних оцінок [6]:

- середнього значення інтенсивності

$$m = \sum_{i=0}^{L-1} z(i)\,p(i);$$

- центральних моментів порядку n

$$\mu_n[z(i)] = \sum_{i=0}^{L-1} (z(i) - m)^n P(i),$$

$\widetilde{P} = \{\overline{P(i),\ i \in 0, L-1}\}$ — гістограма інтенсивності, L — кількість інтервалів гістограми;

- дисперсії контрасту σ^2 зображення

$$\sigma^2 = \mu_2,\ \mu_3(i) = \sum_{i=0}^{L-1} (z(i) - m)^3 P(i);$$

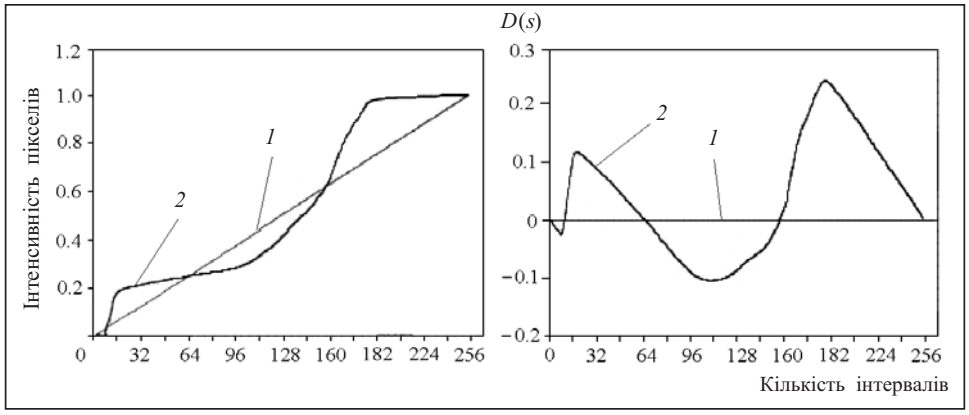


Рис. 3. Кумулятивні гістограми гіпотетичного (*1*) і реального (*2*) зображень та різниці між ними ($D(s)$)

• міри контрастності U однорідності інтенсивності пікселів

$$U = \sum_{i=0}^{L-1} P^2(i).$$

2.5. Перетворення інтенсивності. Кольорове зображення перетворюють на зображення, передане відтінками сірого кольору. Для перетворення використовують алгоритм BT709 [6, 7] з такими коефіцієнтами R, G, B:

$$\mathrm{R} = 0.2125;\ \mathrm{G} = 0.7154;\ \mathrm{B} = 0.0721.$$

Значення яскравості пікселів обчислюють згідно з виразом $b = (256 - C_i) \times \times 100/256$ або у відсотках від білого кольору $b = C_i \times 100/256$, де C_i $(i = 1, 2, 3)$ — значення компонентів сірого кольору RGB-пікселя.

2.6. Розбиття інтенсивності компонентів RGB-пікселів з урахуванням дисперсії координат пікселів. Кількість пікселів з однаковою інтенсивністю у гістограмі не враховує різниці між їхніми координатами, тому для підвищення роздільної здатності під час класифікації зображень застосовують статистичні оцінки координат пікселів у сегментах згідно з визначенням [6]:

• математичних сподівань координат пікселів

$$\bar{x}(S) = \frac{1}{K_S} \sum x_i(S),\ \ \bar{y}(S) = \frac{1}{K_S} \sum y_i(S),$$

де $x_i \in x(S)$, $y_i \in Y(S)$, K_S — кількість пікселів у фрагменті;

• дисперсії координат пікселів

$$E^2(x,\ y,\ s) = (1/K_S) \times \sum_{x_i, y_i} ((x_i - \bar{x}(S))^2 + (y_i - \bar{y}(S))^2);$$

• оцінки дисперсії координат пікселів шляхом обчислення площі фігур прямокутника або круга, що покриває пікселі фрагмента,

$$S_K(S) = 9\pi E^2(S),\ \ G(S) = K_S / S_K(S),$$

де $G(S)$ — ознака щільності пікселів у такому фрагменті.

2.7. Опрацювання зображень на основі кластеризації. Метою кластеризації є пошук певних структур у сукупності об'єктів. Кластеризація, як показано в [6], є описовою процедурою, що уможливлює розвідувальний аналіз і вивчення «структури даних». Кластер можна охарактеризувати як групу об'єктів з подібними властивостями, які мають внутрішню однорідність та зовнішню ізольованість.

Кластерний аналіз виконують на основі зваженої суми модулів різниць між характеристиками образів (кластерів), що є кандидатами на об'єднання в один кластер згідно з виразами зважених сум:

— модульних різниць між характеристиками і ознаками образів [6]

$$F_{ij} = W_1 | a_i - a_j | + W_2 | b_i - b_j | + W_3 | c_i - c_j | + \ldots;$$

— квадратів різниць між характеристиками

$$F_{ij} = W_2 [a_i - a_j]^2 + W_2 [b_i - b_j]^2 + W_3 [c_i - c_j]^2 + \ldots$$

для мінімуму ключів початкових образів $F[\cdot] = \min \{F_{kj}\}$, $k, j \in I$, де I — множина всіх можливих пар ключів початкових зображень, W_i — коефіцієнти зваженості сум модульних та квадратичних різниць.

2.8. Метод оцінки «близькості» зображень. У методі оцінки «близькості» зображень за евклідовою відстанню використовується матриця [6]

$$m(i, j) = \frac{1}{n}\sum_{S=1}^{n}(f_i(S) - f_j(S))^2,\ i \in \overline{1, d},\ j \in \overline{1, l},$$

де $f_i(S), f_j(S)$ — ознаки i-го та j-го зображень, d, l — довільні значення розміру матриці.

Наведені в пп. 2.1–2.8 приклади методів та алгоритмів цифрового структурного опрацювання та розпізнавання зображень свідчать про виняткове застосування простих статистичних оцінок математичного сподівання (середнє арифметичне), дисперсії, евклідової відстані та зважених сум таких оцінок.

Як показано у роботах [10, 11], застосування двійкової позиційної арифметики теоретико-числового базису (ТЧБ) Радемахера (R) за наявності наскрізних переносів для обчислення сум, модульних різниць, квадратів добутків, квадратів різниць та зважених ознак

$$\sum_{i=1}^{n} x_i,\ |x_i - x_j|,\ x_i^2,\ x_i \times x_j,\ [x_i - x_j]^2,\ W_i \times |x_i - x_j|,$$
$$W_i \times [x_i - x_j]^2,\ \sum_{i,j} x_i \times x_j, \tag{1}$$

а також більш складних алгоритмів на їхній основі, зумовлює відповідно низьку швидкодію опрацювання цифрових масивів даних, які описують зображення.

3. МЕТОДИ КОЛЬОРОУТВОРЕННЯ ТА КОДУВАННЯ ПІКСЕЛІВ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Представлення кольору згідно з міжнародним стандартом RGB здійснюється як композиція трьох основних кольорів: червоного (R — red), зеленого (G — green) та синього (B — blue). Результатом є стандартна RGB-система кольороутворення, де використано монохроматичні випромінювання з довжиною хвилі:

$\lambda_{\mathrm{R}} = 0.700$ мкм (червоне), $\lambda_{\mathrm{G}} = 0.5461$ мкм (зелене), $\lambda_{\mathrm{B}} = 0.4358$ мкм (синє).

Оскільки різним довжинам хвиль (частотам) відповідають різні значення енергії, випромінювання рівноенергетичного білого кольору, формуються шляхом змішування у пропорції [7]

$$\overline{\Phi} = \overline{\Phi}_{\mathrm{R}} + \overline{\Phi}_{\mathrm{G}} + \overline{\Phi}_{B},$$

де $\overline{\Phi}_{\mathrm{R}} = m\Phi_{\mathrm{R}}$, $\overline{\Phi}_{\mathrm{G}} = n\Phi_{\mathrm{G}}$, $\overline{\Phi}_{\mathrm{B}} = p\Phi_{\mathrm{B}}$, а $m = 1.0$, $n = 4.5907$, $p = 0.0601$.

У комп'ютерній RGB-системі основний колір має 256 градацій, тобто у двійковій системі числення змінюється у діапазоні 0–255, що відповідає об'єму даних 8 біт або 1 байт.

Таким чином, код кольору RGB-системи задають трьома байтами, він становить 24 біти у базисі Радемахера. Найменший елемент кольорового зображення у хеммінговому просторі на дискретному дисплеї представляють одним триколірним пікселем.

З ініціативи фірм Microsoft та Hewlett Packard стандартизованим колірним простором для мережі Інтернет є SRGB (standart RGB), який відповідає простору типового монітора VGA. Основні кольори цього простору збігаються з кольорами, що використовують у телебаченні (HDTV). Модель RGB є стандартною для створення web-сторінок.

У колірному просторі Wide Gamut RGB використовують спектрально чисті основні кольори, білу точку D50 у трикутнику локусу колірностей та гаму 2.2, що дає змогу задати 77.6 % усіх видимих кольорів. Проте він містить 8.1 % нереальних кольорів, а тому на видимі кольори залишається менше градацій [6].

Колірний простір Adobe RGB є стандартною колірною моделлю і містить інтенсивні зелені та блакитні кольори.

Модель Lab, створена Міжнародною комісією з освітлення (GIE), визначає кольори без урахування індивідуальних особливостей пристроїв відображення (монітора, принтера тощо).

Відповідно до моделі Lab колір визначають яскравістю (Luminance) (у діапазоні 0–100 %) і двома хроматичними компонентами:

— параметром a, який змінюється від зеленого до червоного і задається числом до 128 (7 біт у базисі Радемахера);

— параметром b, що змінюється в діапазоні від синього до жовтого і задається числом до 127 (7 біт у базисі Радемахера). Цю модель використовують у друкарстві.

Координати колірностей LCH одержують у стандарті Lab таким чином: L — координата яскравості; C (Chroma) $= (a^2 + b^2)^{1/2}$ — насиченість кольору; H (Hue) = arctg (b/a) — колірний тон.

Калібрування та профілювання пристроїв у колірних просторах *XYZ* або Lab перетворюють на основі спеціальних тестових колірних таблиць (мішеней), які містять певний набір контрольних кольорів. До цього набору включають основні адитивні (червоний, зелений, синій) і базові субтрактивні кольори (жовтий, пурпурний, блакитний та різні їхні градації), до яких додають білий, чорний та градації сірих кольорів. Мішені, що використовуються для профілювання моніторів, відео- та проекційного обладнання, представляють у вигляді координат RGB тестових кольорів згідно із стандартом IT8. Усі тестові таблиці IT8 складено з 144 тестових колірних зв'язків, контрольної шкали сірого і тестового зображення. Кожен колірний зв'язок має номер (від 1 до 22) та індекс (від A до L) [6].

Профілювання фотокамер і контроль кольору фотографій виконують згідно з колірною шкалою ColorChecker SG. Кожен колірний зв'язок має номер (від 1 до 10) та індекс (від A до N) [6].

3.1. Обґрунтування ефективності кодування RGB-пікселів кольорових зображень у базисах Радемахера та Крестенсона. Відсутність умови взаємної простоти модулів у різних розрядах двійкових кодів ТЧБ Радемахера ускладнює алгоритми додавання та множення двійкових чисел. Під час виконання операції додавання між двійковими розрядами виникають наскрізні переноси з молодших розрядів у старші [12]:

$$\begin{array}{ccccccccccc} & & x_{n-1} & \cdots & x_i & \cdots & x_1 & x_0 \\ + & & + & & + & & + & + \\ & & y_{n-1} & \cdots & y_i & \cdots & y_1 & y_0 \\ \hline P_n & \leftarrow & P_{n-1} & \leftarrow & \cdots & \leftarrow & P_i & \leftarrow & \cdots & \leftarrow & P_1 & \leftarrow \\ \downarrow & & \downarrow & & & & \downarrow & & & & \downarrow & \downarrow \\ S_n & & S_{n-1} & & \cdots & & S_i & & \cdots & & S_1 & S_0 \end{array} .$$

Наявність наскрізних переносів під час виконання операції додавання в базисі Радемахера в $2n$ разів знижує швидкодію виконання операції додавання чисел відносно тактової частоти процесорів.

Крім того, виникнення наскрізних переносів під час додавання двійкових чисел суттєво знижує швидкодію та ускладнює структуру пристроїв, які виконують операцію множення згідно з графом (рис. 4, де AND — лінійка операторів, що формує

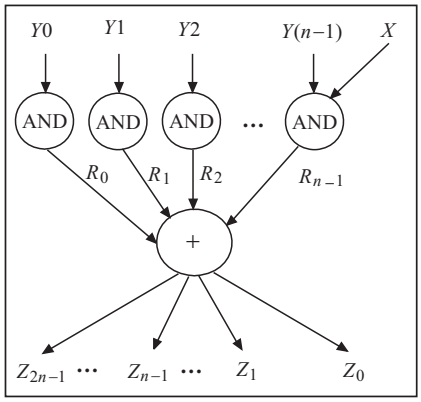


Рис. 4. Граф виконання операції множення в базисі Радемахера

часткові результати множення між двійковими кодами множеного Y на розряди множника X, які зсуваються праворуч на R_i $(i = 1, 2, \ldots, n-1)$ розрядів, відтак отримується результат множення у вигляді коду $(Z_{2n-1} \ldots Z_{n-1} \ldots Z_1 Z_0))$.

За умови взаємної простоти модулів системи залишкових класів (СЗК) базису Крестенсона суттєво спрощуються алгоритми виконання операцій додавання та множення над числами, представленими кодами Радемахера–Крестенсона та Хаара–Крестенсона СЗК: $X = (b_0, b_1, \ldots, b_j, \ldots, b_{k-1})$ та $Y = (a_0, a_1, \ldots, a_j, \ldots, a_{k-1})$ згідно з граф-алгоритмами (рис. 5), де $(+)\text{res}$ відповідає операції $C_j = \text{res}\,(b_j + a_j) \bmod P_j$, а $(\times)\text{res}$ — операції $\gamma_j = \text{res}\,(b_j \cdot a_j) \bmod P_j$.

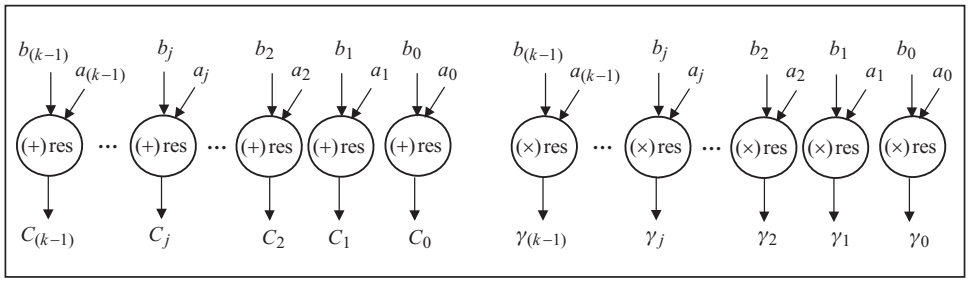


Рис. 5. Графи виконання операцій додавання та множення в базисі Крестенсона

Обґрунтований спосіб кодування RGB-пікселів у базисі Крестенсона дає змогу замінити вектори P_1, P_2, P_3 одним вектором P_0, розрядність якого становить 24 біти і дорівнює розрядності кодів RGB-системи, тобто можна реалізувати представлення RGB-пікселів у хеммінговому просторі (рис. 6) [13].

Представлення цифрових даних у ТЧБ Радемахера–Крестенсона та особливо Хаара–Крестенсона, які базуються на математичних основах модульної арифметики та системи числення залишкових класів, дають змогу на 2–3 порядки підвищити швидкодію виконання алгоритмів згідно з виразами (1) незалежно від розрядності чисел, а саме:

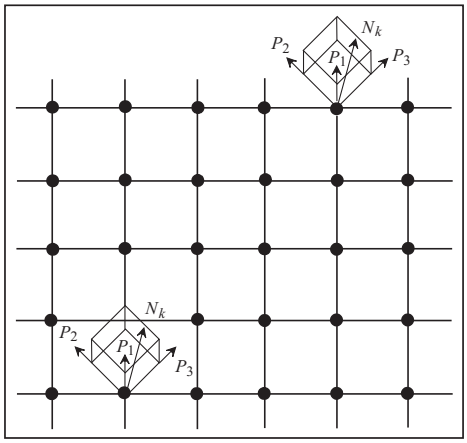


Рис. 6. Представлення RGB-пікселів у хеммінговому просторі

- кожної операції підсумовування $x_i + x_j$ та множення $x_i \times x_j$ — за 2 мікротакти;
- операції піднесення до квадрату — за 1 мікротакт;
- операції визначення квадрату різниці $[x_i - x_j]^2$ — за 5 мікротактів;
- операції модульної різниці $|x_i - x_j|$, яка може бути реалізована шляхом сканування масиву квадратів $(x_i - x_j)^2$ СЗК з представленням мо-

дульних різниць у базисі Хаара–Крестенсона на основі вентильних матриць, що є можливим для $0 \le x_i \le 255$ — за 21 мікротакт.

4. МЕТОДИ ПОЛІФУНКЦІОНАЛЬНОЇ СТРУКТУРИЗАЦІЇ ПІКСЕЛІВ КОЛЬОРОВИХ ЗОБРАЖЕНЬ У ТЧБ РОЗШИРЕНИХ ПОЛІВ ГАЛУА

4.1. Метод кодування пікселів RGB-стандарту у базисах Радемахера та Крестенсона. Кодування кольорів для пікселя хеммінгового простору монітора, заданих у декартових координатах, можна однозначно представити у системі залишкових класів ТЧБ Крестенсона. Таке представлення реалізується за допомогою задання трьох взаємно простих модулів (P_1, P_2, P_3), які дають змогу однозначно закодувати у двійковій системі числення ТЧБ Радемахера кожен піксель RGB-системи шляхом виконання прямого цілочислового перетворення СЗК згідно з виразом [14, 15]

$$N_k = \operatorname{res} \sum_{i=1}^{3} b_i B_i \,(\operatorname{mod} P_0), \tag{2}$$

де B_i — ортогональні базиси СЗК, які розраховують згідно з діофантовими рівняннями

$$\begin{aligned} B_1 &= P_2 P_3 m_1 \equiv 1 (\operatorname{mod} P_1), \\ B_2 &= P_1 P_3 m_2 \equiv 1 \,(\operatorname{mod} P_2), \\ B_3 &= P_1 P_2 m_3 \equiv 1 (\operatorname{mod} P_3), \end{aligned} \tag{3}$$

де m_1, m_2, m_3 — обернені елементи кодової системи СЗК [16], $P_0 = P_1 P_2 P_3$ — діапазон кодування пікселя кольорового зображення з розрядністю $K_0 = \hat{E}[\log_2 P_0]$, $\hat{E}[\cdot]$ — цілочислова функція з округленням до більшого цілого.

Однозначне кодування RGB-пікселів у базисі Радемахера–Крестенсона забезпечують вибором таких значень діапазону кодування залишків b_i у базисі Радемахера:

$$b_1 = b_{\mathrm{R}},\ 0 \le b_{\mathrm{R}} \le 255,\ (00000000–11111111),$$

$$b_2 = b_{\mathrm{G}},\ 0 \le b_{\mathrm{G}} \le 255,\ (00000000–11111111),$$

$$b_3 = b_{\mathrm{B}},\ 0 \le b_{\mathrm{B}} \le 255,\ (00000000–11111111).$$

Крім того, з урахуванням коефіцієнтів $m = 1.0$, $n = 4.5907$, $p = 0.0601$ для найбільш насиченого зеленого кольору діапазон його зміни можна задати як $0 \le b_{\mathrm{G}} \le 254$, що дає змогу забезпечити взаємну простоту модулів $P_1 = 256$, $P_2 = 255$, $P_3 = 257$.

Для перевірки взаємної простоти обраної системи модулів розкладемо їх на множники: $256 = 2^8$, $255 = 5 \cdot 51$, 257 — просте число, тобто $P_0 = 16776960$, де $P_0 < 2^{24} = 16777216$. Отже, задоволено умову формування 24-розрядного коду пікселя у базисі Радемахера–Крестенсона.

У двійковій системі числення базису Радемахера коди модулів мають таке представлення:

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

Тоді $P_0 = 111111111111111100000001_{(2)}$.

Оскільки серед модулів P_1, P_2, P_3 є модуль $P_1 = 2^8$, то залишок числа N_k (G — ознаки кольору), згідно з оберненим перетворенням СЗК можна записати без декодування вісьмома молодшими розрядами числа N_k, представленого у базисі Радемахера.

Розв'язуючи діофантові рівняння (3), отримаємо такі значення обернених елементів m_i та базисних чисел B_i:

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

Перевірку правильності розрахунків даних перетворення СЗК виконуємо згідно з рівнянням

$$N_k = (b_{\mathrm{R}} B_1 + b_{\mathrm{G}} B_2 + b_{\mathrm{B}} B_3) \cdot (\mathrm{mod}\ P_0) = 1 \text{ для } b_{\mathrm{R}} = 1,\ b_{\mathrm{G}} = 1,\ b_{\mathrm{B}} = 1,$$

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

Нехай, наприклад, $R = 10,\ G = 200,\ B = 100.$ Тоді

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

що відповідає двійковому представленню RGB-пікселя у базисі Крестенсона $(100011000011001000001010_2)$.

Декодування такого представлення має такий вигляд:

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

4.2. Метод кодування пікселів кольорових зображень у ТЧБ Радемахера–Крестенсона та Хаара–Крестенсона. Кодування пікселів кольорових зображень у стандарті RGB здійснюється 24-розрядним двійковим кодом, де інтенсивності кожного з кольорів представляють 8-бітними двійковими кодами базису Радемахера:

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

$$0 \le r_i \le 255,\quad 0 \le g_i \le 255,\quad 0 \le b_i \le 255.$$

Кодування RGB-пікселів кольорових зображень у ТЧБ Радемахера–Крестенсона (R–C) та Хаара–Крестенсона (H–C) виконуємо шляхом вибору системи взаємно простих модулів (P_1, P_2, P_3), добуток яких перевищує діапазон квантування значень яскравості (r_i, g_i, b_i). Цю умову може задовольняти різний набір модулів дискретного перетворення СЗК, наприклад: $P_1 = 5$, $P_2 = 7$, $P_3 = 8$, який забезпечує однозначне кодування яскравостей r_i, g_i та b_i у діапазоні $P_0 = 5 \cdot 7 \cdot 8 = 280 > 255$. При цьому формується наведена нижче кодова структура у базисі R–C, яка однозначно представляє відповідний код RGB-пікселя:

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

$$P_1 = 5,\quad P_2 = 7,\quad P_3 = 8,$$

де $a_i = \overline{0,1}$, $c_i = \overline{0,1}$, $d_i = \overline{0,1}$, $i = \overline{0,2}$. До того ж кожне значення a_i, c_i, d_i розраховують як залишок згідно з виразами $a_i = \mathrm{res}\,(r_i \bmod P_1)$, $c_i = \mathrm{res}\,(g_i \bmod P_2)$, $d_i = \mathrm{res}\,(b_i \bmod P_3)$.

Для заданого набору модулів знаходимо обернені елементи m_i та базисні числа B_i, розв'язуючи діофантові рівняння (3). У результаті отримуємо

$$m_1 = 1,\ B_1 = 56,\ m_2 = 3,\ B_2 = 120,\ m_3 = 3,\ B_3 = 105. \qquad (4)$$

Виконаємо перевірку правильності отриманих значень m_i та B_i згідно з виразом (2):

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

Розглянемо приклад. Нехай задано значення інтенсивностей кольорів RGB-пікселя: $r_i = 10,\ g_i = 100,\ b_i = 37.$

Тоді отримаємо коди RGB-пікселя у базисах

1) Радемахера:

$$r_i = 00001010_{(2)},\ g_i = 01100100_{(2)},\ b_i = 00100101_{(2)}.$$

2) Радемахера–Крестенсона:

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

Представлення коду RGB-пікселя у базисі Хаара–Крестенсона для кожного значення інтенсивності r_i, g_i та b_i виконують згідно з такою структурою:

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

$$P_1 = 5, \quad P_2 = 7, \quad P_3 = 8,$$

де $a_i \vee c_i \vee d_i = \overline{0, P_i - 1}$.

Для заданих значень інтенсивності кольорів RGB-пікселя $r_i = 10$, $g_i = 100$, $b_i = 37$ отримаємо відповідну структуру коду у базисі Н–С:

$$r_i = (10000\ldots0001000\ldots00000100),$$

$$g_i = (10000\ldots0010000\ldots00100000),$$

$$b_i = (00100\ldots0010000\ldots00000100).$$

Представлення цифрових значень яскравостей кольорів r_i, g_i та b_i у різних ТЧБ зумовлює відповідно різну розрядність структур кодів згідно з виразами:

1) у базисі Радемахера (R)

$$K_{\mathrm{R}} = \log_2 2^8 = 8 \text{ біт};$$

2) у базисі Радемахера–Крестенсона (R–C)

$$K_{\mathrm{R-C}} = \sum_{i-1}^{3} [\hat{E}(\log_2 P_i - 1)] = 3 + 3 + 3 = 9 \text{ біт};$$

3) у базисі Хаара–Крестенсона (H–C)

$$K_{\mathrm{H-C}} = \sum_{i=1}^{n} P_i = 5 + 7 + 8 = 20 \text{ біт}.$$

4.3. Метод кодування зразків кольороутворення у стандартних мішенях.

4.3.1. Стандартна мішень IT8.7/2. Розглянемо процеси структуризації даних у базисах R, R–C та H–C під час кодування стандартних мішеней кольороутворення [7]. Колірна шкала мішені IT8.7/2 для номерів від 1 до 22, числа індексів від A до L (12) та 22 відтінків сірого, утворює 286 колірних зразків. Колірні зраз-

ки від A20 до L22 не регламентуються стандартом IT8.7/2 і можуть бути заповнені на розсуд виробника. Так, фірма Kodak розміщує тут 12 контрольних кольорів. Таким чином, загальна кількість колірних зразків цієї стандартної мішені (з урахуванням 12 контрольних) становить 262 колірних зразки. Таким чином, кодування цієї мішені не виходить за межі діапазону кодування чисел у базисах R–C та H–C з аналогічним набором модулів кодування RGB-пікселів ($P_1 = 5$, $P_2 = 7$, $P_3 = 8$), добуток яких перевищує кількість колірних зразків мішені ($280 > 262$). Отже, кодування цієї колірної мішені у базисах R–C та H–C буде виконуватися згідно з розрахованими оберненими елементами m_1, m_2, m_3 і базисними числами B_1, B_2, B_3 з (4), а розрядність R, R–C та H–C кодів становитиме відповідно 9, 9 та 20 біт.

4.3.2. Стандартна мішень Color Checker SG. Кодування колірної мішені стандарту Color Checker SG виконують аналогічно з використанням номерів від 1 до 10 та індексів від A до N (14) і в результаті забезпечують 140 колірних зразків. Кодування зразків цієї колірної мішені у базисі Радемахера не перевищує 8 біт розрядності двійкових чисел. Для системи взаємно простих модулів базису R–C $P_1 = 4$, $P_2 = 5$, $P_3 = 7$, що задовольняє умову однозначного кодування колірних зразків мішені стандарту Color Checker SG $P_0 = P_1 \cdot P_2 \cdot P_3 = 140$, необхідна розрядність коду становить 8 біт, а у базисі H–C ($P_1 + P_2 + P_3 = 16$) — 16 біт.

Збільшення розрядності структур кодів, якими представлено RGB-пікселі кольорових зображень, є доцільним і ефективним для прискорення подальших логічних або обчислювальних операцій над RGB-кодами. Такі операції виконують у процесі перетворень для різних стандартів кольороутворення, цифрового телебачення, друку зокрем, для дисплеїв, модемів, принтерів тощо [6, 7]. Основна перевага R–C та H–C кодів, як показано у роботах [16, 17], полягає у суттєвому (на 23 порядки) збільшенні швидкодії обчислень у зазначених кодах на основі модульної арифметики порівняно з двійковими кодами базису Радемахера, де застосовуються операції з наскрізними переносами.

Наприклад, виконання операції додавання двох 32-розрядних двійкових чисел потребує понад 100 мікротактів, операції множення — більше 500 мікротактів, а виконання аналогічних операцій у базисі H–C незалежно від розрядності виконується за 2 мікротакти.

Вказана перевага H–C-базису реалізується шляхом застосування швидкодіючого АЦП паралельного типу з розширеними функціональними можливостями, запропонованого в [18].

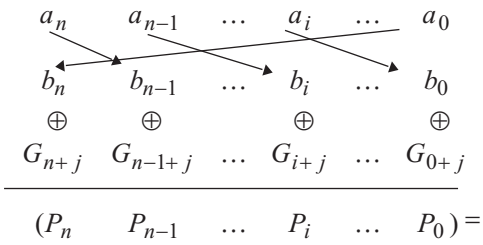
Поліфункціональне кодування RGB-пікселів у базисах R–C та H–C є доцільним на рівні аналого-цифрового перетворення інтенсивностей аналогових сигналів RGB-сенсорів. Такий принцип поліфункціональної структуризації даних для кольороутворення здійснюється з використанням АЦП паралельного типу [19].

5. СПОСІБ КРИПТОЗАХИСТУ RGB-ПІКСЕЛІВ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Криптозахист RGB-пікселів зображень здійснюють з метою обмеження несанкціонованого доступу до кольорових зображень, які формуються в реальному часі, кодуються в різних системах числення, передаються каналами зв'язку, реєструються у накопичувачах баз даних та відображаються на моніторах користувачів. Існують різні методи криптозахисту файлів даних окремих кольорових зображень та масивів даних, що представляють певні обсяги кольорових зображень. До того ж в інформаційних системах використовуються стандартні алгоритми захисту масивів даних від несанкціонованого доступу, побудовані на основі хешування, симетричних та асиметричних алгоритмів RSA, еліптичних кривих тощо [20, 21].

Запропоновано метод шифрозахисту окремих RGB-пікселів кольорових зображень, представлених R, R–C та H–C кодами з використанням зазначених методів. структуризовані R–C та H–C коди є проблемно-орієнтованими на підвищення швидкодії подальших операцій перетворення, опрацювання та розпізнавання зображень згідно з модульною арифметикою системи числення залишкових класів базису Крестенсона.

Як базовий метод криптозахисту кодів RGB-пікселів доцільно застосувати ефективний метод на основі процедур хешування окремих розрядів їхніх кодів та логічного додавання з бітами генерованих послідовностей Галуа згідно з графами [11]



(1) — операція хешування

(2) — додавання за модулем 2

де a_i — біти R–C або H–C кодів пікселів; I — операція хешування ($b_i := b_j$, $i \neq j$, $i = \overline{0, n}$); P_i, $i = \overline{0, n}$, — утворений код криптозахищеного пікселя PX.

Генерація бітів кодів Галуа $\{G_i\}$ виконується згідно з таємними ключами. Позитивним результатом запропонованого методу є ефективний шифрозахист пікселів кольорових зображень на основі сумісного застосування алгоритмів високої швидкодії у залишкових класах та рекурентних кодів поля Галуа.

ВИСНОВКИ

Обґрунтовано актуальність розроблення теорії, методів та алгоритмів кодування пікселів кольорових зображень та їхнє представлення у різних теоретико-числових базисах, що дає змогу підвищити швидкодію алгоритмів перетворення, опрацювання та розпізнавання цифрових зображень на основі математики арифметичних операцій непозиційної системи числення залишкових класів.

Виконано аналіз математичних основ сучасних алгоритмів опрацювання та розпізнавання кольорових зображень з використанням методів сегментування на основі гістограм з одним порогом та кумулятивних гістограм, статистичних оцінок середнього значення, дисперсії, асиметрії та міри контрастності однорідності гістограм інтенсивності, врахування дисперсії координат пікселів фрагментів та силуетів зображень, а також методів кластеризації зображень. За результатами аналізу встановлено, що базовими компонентами алгоритмів зазначених методів опрацювання зображень є арифметичні операції $\sum x_i$, $P(i) = n_i / n_0$, $|x_i - x_j|$, x_i^2, $x_i \times x_j$, $[x_i - x_j]^2$, $\sum [x_i - x_j]^2$, $\sum x_i x_j$, які традиційно виконуються згідно з правилами арифметики двійкової системи числення теоретико-числового базису Радемахера. Запропоновано здійснювати структуризоване кодування пікселів кольорових зображень у кодах непозиційних систем числення Радемахера–Крестенсона, Хаара–Крестенсона та Галуа, що дає змогу на 2–3 порядки підвищити швидкодію виконання перелічених обчислювальних компонентів алгоритмів опрацювання зображень. Наведено приклади алгоритмів кодування та криптозахисту пікселів кольорових зображень у теоретико-числових базисах Радемахера, Радемахера–Крестенсона, Хаара–Крестенсона та Галуа.

СПИСОК ЛІТЕРАТУРИ

1. Burd S.D. Systems architecture. 7th ed. Boston: Cengage Learning, 2015. 656 p.
2. Sun D.C. Features of liquid crystal display materials and processes. Scitus Academics LLC, 2016. 264 p.
3. Otsu N. A threshold selection method from grey level histograms. *IEEE Trans. Systems Man Cybernet*. 1979. Vol. 9, N 1. P. 62–66.
4. Zhang Y., Wu L. Fast document image binarization based on an improved adaptive Otsu's method and destination word accumulation. *Journal of Computational Information Systems.* 2011. Vol. 6, N 7. P. 1886–1892.
5. Ramer U. An iterative procedure for the polygonal approximation of plane curves. *Computer Graphics Image Processing*. 1972. Vol. 1, N 3. P. 244256.
6. Мельник Р.А. Алгоритми та методи опрацювання зображень: навч. посібник. Львів: Вид-во Львівської політехніки, 2017. 220 с.
7. Лотошинська Н.Д., Івахів О.В. Теорія кольору та кольороутворення: навч.посібник. Львів: Вид-во Львівської політехніки, 2014. 204 с.
8. Воробель Р.А. Логарифмічна обробка зображень. Київ: Наук. думка, 2012. 231с.
9. Русин Б.П. Варецький Я.Ю. Біометрична аутентифікація та криптографічний захист. Львів: Коло, 2007. 287 с.
10. Гуменний П.В., Волинський О.І. Теоретичні основи визначення залишків на основі лічильників у різних теоретико-числових базисах. *Вісник Хмельницького національного університету*. 2016. № 4 (239). С. 164–173.
11. Николайчук Я.М. Коди поля Галуа: теорія і застосування. Тернопіль: ТзОВ «Терно-граф», 2012. 576 с.
12. Nykolaychuk Y., Volynskyy O., Borovyi A. Rademacher–Krestenson's method of between-bases transformations in designing processors. *Proc. IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications,* IDAACS 2011, Prague, Czech Republic, September 15–17, 2011. Vol. 1. P. 310–314.
13. Николайчук Я.М., Піх В.Я., Заведюк Т.О., Возна Н.Я. Методи спектрального косинусного перетворення Фур'є для розпізнавання сигналів у хеммінговому просторі на основі різних кореляційних функцій та теоретико-числових базисів. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі.* 2013. № 773. С. 89–98.
14. Круліковський Б.Б., Возна Н.Я., Николайчук Я.М. Теоретичні основи та критерії оцінки структурної складності обчислювальних компонентів процесорів багаторозрядної арифметики. *Тези доповідей III Міжнародної науково-практичної конференції науковців.* Рівне: НУВГП, 2014. С. 65–67.
15. Возна Н.Я., Николайчук Я.М., Ширмовська Н.Г. Метод формування структуризованих даних квазістаціонарних об'єктів на основі системи числення залишкових класів базису Крестенсона. *Розвідка та розробка нафтових і газових родовищ*. 2011. № 3 (40). С. 62–65.
16. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical foundations for the analytical computation of coefficients of basic numbers of Krestenson's transformation. *Cybernetics and Systems Analysis.* 2014. Vol. 50, N 5. P. 649–654.
17. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical foundations of the modified perfect form of residue number system. *Cybernetics and Systems Analysis.* 2016. Vol. 52, N 2. P. 219–223.
18. Аналого-цифровий перетворювач. Пат. 116176 Україна, МПК (2006.01) H03M 1/38. Круліковський Б.Б., Николайчук Я.М., Грига В.М., Піх В.Я. № a 2016 12016 заявл. 28.11.2016; опубл. 12.02.2018, Бюл. №3.
19. Николайчук Я.Н., Возна Н.Я., Круликовский Б.Б., Пих В.Я. Метод структуризации дискретного косинусного преобразования Фурье в модульной арифметике теоретико-числового базиса Хаара–Крестенсона. *Кибернетика и системный анализ.* 2018. Т. 54, № 3. С. 178–188.

20. Задирака В.К., Кудин А.М. Облачные вычисления в криптографии и стеганографии. *Кибернетика и системный анализ.* 2013. № 4. С. 113–119.

21. Задирака В.К., Никитенко Л.Л. Новые подходы к разработке алгоритмов скрытия информации. *Штучний інтелект.* 2008. № 4. С. 353–357.

Надійшла до редакції 24.04.2018

Н.Я. Возна, Я.Н. Николайчук, О.И. Волынский

АЛГОРИТМЫ РЕШЕНИЯ ЗАДАЧ КРИПТОЗАЩИТЫ ПИКСЕЛЕЙ ЦВЕТНЫХ ИЗОБРАЖЕНИЙ В БАЗИСЕ РАДЕМАХЕРА И ОСТАТОЧНЫХ КЛАССАХ

Аннотация. Обоснована актуальность разработки теоретических основ, методов и алгоритмов кодирования пикселей цветных изображений путем проблемно-ориентированной полифункциональной структуризации данных и представления кодов пикселей цветных изображений в теоретико-числовых базисах Радемахера, Радемахера–Крестенсона, Хаара–Крестенсона и Галуа. Исследована возможность повышения быстродействия алгоритмов преобразования, обработки и распознавания цифровых изображений с применением модульной арифметики остаточных классов на основе математики арифметических операций непозиционной системы исчисления остаточных классов.

Ключевые слова: алгоритмы, криптозащита, цветные изображения, теоретико-числовые базисы.

N.Y. Vozna, Y.M. Nykolaychuk, O.I. Volynskyi

ALGORITHMS FOR SOLVING PROBLEMS OF COLOR PIXELS CRYPTIC PROTECTION IN THE RADEMACHER AND RESIDUE NUMBER SYSTEMS

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, Krestenson, Rademacher–Krestenson, Haar–Krestenson, and Galois systems is substantiated in this paper. The purpose of the research is to increase the efficiency of the algorithms for digital image transforms, processing and recognition using modular arithmetics with residue number system on the basis of mathematics of arithmetic operations of a non-positional residue number system.

Keywords: algorithms, cryptic protection, color images, theoretical and numerical bases.

Возна Наталія Ярославівна,
кандидат техн. наук, доцент, доцент кафедри Тернопільского національного економічного університету, e-mail: nvozna@ukr.net.

Николайчук Ярослав Миколайович,
доктор техн. наук, професор, завідувач кафедри Тернопільського національного економічного університету, e-mail: lmnykolaychuk@gmail.com.

Волинський Орест Ігорович,
кандидат техн. наук, старший викладач кафедри Тернопільського національного економічного університету, e-mail: orestsks@ukr.net.