Ніколаєнко Богдан Анатолійович, кандидат технічних наук, старший викладач спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
E-mail: nikolaenko_iszzi@ukr.net.
Orcid ID: 0000-0002-6888-5947.
Николаенко Богдан Анатольевич, кандидат технических наук, старший преподаватель специальной кафедры № 3 Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".
Nikolaenko Bohdan Anatoliyovych, Candidate of Technical Sciences, Senior Lecturer at the Special Department № 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky".

Бакалинський Олександр Олегович, кандидат технічних наук, заступник директора Департаменту кіберзахисту, начальник відділу Адміністрації Держспецзв'язку, Київ.
E-mail: baov@meta.ua.
Orcid ID: 0000-0001-9712-2036.
Бакалинский Александр Олегович, кандидат технических наук, заместитель директора Департамента киберзащиты, начальник отдела Администрации Госспецсвязи, Киев.
Bakakynskyi Oleksandr Olehovich, Candidate of Technical Sciences, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine, Kyiv, Ukraine.

DOI: 10.18372/2410-7840.23.16403
УДК 621.327:681.5

РОЗРОБКА МЕТОДУ КРИПТОКОМПРЕСІЙНОГО КОДУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ПЛАВАЮЧОЇ НЕДЕТЕРМІНОВАНОЇ СХЕМИ ОБРОБКИ

Володимир Бараннік, Сергій Сідченко, Валерій Бараннік, Дмитро Бараннік, Сергій Шульгін, Сергій Туренко

В процесі управління об'єктами кризової інфраструктури та під час їх охорони використовуються цифрові відеозображення. Їх обсяги постійно зростають та до них висуваються вимоги щодо збереження максимальної якості при необхідності забезпечення конфіденційності. Тому, актуальною є науково-прикладна проблема, яка полягає в підвищенні конфіденційності відеоінформації в умовах забезпечення її достовірності та доступності. Для її вирішення отримав подальше вдосконалення однокаскадний метод криптокомпресійного кодування зображень в диференційованому базисі на основі використання технології нерівноважного позиційного кодування. Відмінність даного методу від відомих полягає в наступному. По-перше, плаваюча схема кодування організується в межах всієї площині зображення, коли у формуванні кодових величин інформаційної складової беруть участь елементи зображення, що належать різним блокам відеоданих. Для цього розроблена схема лінеаризації координат з чотиривимірного представлення елементу в двовимірної матриці, які визначають координати блоку в площині зображення та координати елементу в цьому блоці, в одновимірну координату для взаємно-однозначного уявлення цього елемента у векторі. По-друге, додатково використовуються два ступеня невизначеності, які складаються з недетермінованої довжини криптокомпресійних кодограм і недетермінованої кількості елементів, що беруть участь в їх формуванні. Це дозволяє підвищити криптостійкість та доступність відеоданих без втрати достовірності.

Ключові слова: *криптокомпресійне представлення, захист інформації, шифрування, кодування, компресія, конфіденційність, зображення.*

ВСТУП

Останнім часом відеозображення широко використовуються для прийняття рішень в процесі управління об'єктами кризової інфраструктури та під час їх охорони. Обсяги зображень постійно зростають і до них висуваються вимоги щодо збереження максимальної якості.

При цьому висуваються вимоги щодо забезпечення конфіденційності відеоданих. Тому, необхідно вирішити актуальну науково-прикладну проблему, яка полягає в підвищенні конфіденційності відеоінформації в умовах забезпечення її достовірності та доступності. Існують різні підходи щодо забезпечення конфіденційності зображень, серед яких:

– криптографічні методи захисту на основі шифрування даних [6-8, 11, 23-29, 35-37, 40, 44];

– криптографічні методи захисту на основі скремблювання даних [12, 23, 24, 27-30, 32, 34, 35, 38, 39, 41, 43];

– методи стеганографічної обробки зображень для забезпечення безпеки, як вбудованих в них даних, так і самих відеоданих [1, 13-15];

– з використанням технології поділу секрету щодо забезпечення безпеки одного або декількох зображень [20-22, 33, 35, 42];

– методи, що реалізують політику управління правами доступу та конфіденційності [27, 35];

– перетворення, що видаляють в зображеннях критично важливі області [35];

– геометрично зворотні спотворення зображень [31].

Але їм характерні суттєві проблемні недоліки, серед яких можна відзначити наступні:

– забезпечення конфіденційності відеоданих без використання технологій компресії не дозволяє створити умови для підвищення рівня її доступності;

– забезпечення конфіденційності зображень з використанням технологій компресії після і/або між етапами процесу стиснення даних фактично засноване на поділі функціоналу шифрування і компресії. Це так само призводить до зниження доступності відеоданих;

– відсутність методів комплексування компресійних і криптографічних перетворень, що впливає на доступність відеоданих;

– відсутність методів, побудованих на недетермінованих принципах реалізації алгоритму шифрування і/або недетермінованих підходів щодо кількості та місця розташування оброблюваних даних. Це впливає на рівень криптостійкості.

Для усунення цих недоліків були розроблені методи криптокомпресійного представлення (ККП) зображень. Вони призначені для одночасного забезпечення компресії та захисту відеоінформації. Ці методи будуються на основі нерівноважно-позиційних системах кодування [4, 5, 9, 10, 16–19]. В статті [3] розглянуті ключові параметри систем криптокомпресійного кодування, що впливають на підвищення криптостійкості та доступності відеоданих. Такими параметрами є недетермінована довжина кодових конструкцій ККП зображень та наявність додаткової міри невизначеності такої, як недетермінована кількість елементів, що беруть участь у формуванні криптокомпресійних кодограм (КККдг). З урахуванням цих параметрів в статті [17] було розроблено метод кодування систем службових складових в диференційованому базисі на другому каскаді ККП зображень. Основою методу є розроблена схема лінеаризації даних з тривимірних координат представлення у двовимірної матриці в одновимірну координату для взаємно-однозначного представлення цього елемента у векторі. Лінеаризація організовується в горизонтальному напрямку по рядках. Після другого каскаду кодування сформовані службові данні КККдг піддаються шифруванню на основі розроблено методу маскувального ущільнення службових даних в системах компресії відеозображень [2].

Однак, базові методи [4, 9, 10, 16] ККП зображень, що кодують початкові відеодані, не повністю враховують недетерміновані властивості, що були визначені у [3] та реалізовані в [17]. Тому необхідно розробити такий метод криптокомпресійного кодування (ККК), який додатково використовує властивість недетермінованості.

Метою статті є розробка методу криптокомпресійного кодування зображень на основі плаваючої недетермінованої схеми обробки для забезпечення криптостійкості відеоданих зі збереженням заданої якості інформації без зниження її доступності.

ОСНОВНА ЧАСТИНА

Кадр будь-якого вихідного зображення має розмірність $M \times N$ елементів, де M – кількість рядків в зображенні, а N – кількість стовпців, і складається з P площин. Так, кольорові зображення, представлені в колірному просторі RGB, складаються з трьох площин $P = 3$. Кожна площина являє собою двовимірну матрицю A розмірністю $M \times N$ елементів.

Для всіх площин організовується однотипна обробка. Площина A розбивається на однакові блоки $A^{(\gamma;\chi)}$, де γ – координата блоку $A^{(\gamma;\chi)}$ в

площині A по вертикалі, χ – координата по горизонталі. Розмірність кожного блоку $A^{(\gamma;\chi)}$ визначається як $m \times n$ елементів, де m – кількість рядків в оброблюваному блоці, а n – кількість стовпців. Розміри m і n блоку $A^{(\gamma;\chi)}$ вибираються кратними ступеня 2, тобто $m,n \in$ 2, 4, 8, 16. Зазвичай в процесі обробки значення сторін масиву $m \times n$ приймаються рівними, тобто $m = n$.

Максимальне значення координатної змінної блоку $A^{(\gamma;\chi)}$ по вертикалі γ_{max} і по горизонталі χ_{max} визначається виходячи із співвідношення розмірності $M \times N$ оброблюваної площини A і розмірності $m \times n$ блоку $A^{(\gamma;\chi)}$, а саме:

$$\gamma_{max} = [\frac{M}{m}], \qquad \chi_{max} = [\frac{N}{n}],$$

де $[\bullet]$ – ціла частина числа.

Кожен блок $A^{(\gamma;\chi)}$, де $\gamma = \overline{1,[\frac{M}{m}]}$, $\chi = \overline{1,[\frac{N}{n}]}$, являє собою двомірний масив елементів $a_{i,j}^{(\gamma,\chi)}$, де i – місце розташування елемента в рядку масива (координата в блоці $A^{(\gamma;\chi)}$ по вертикалі), j – місце розташування в стовпці масива (координата в блоці $A^{(\gamma;\chi)}$ по горизонталі), тобто:

$$A^{(\gamma;\chi)} = \{a_{i,j}^{(\gamma,\chi)}\},$$

де $i = \overline{1,m}$, $j = \overline{1,n}$.

Кожен елемент $a_{i,j}^{(\gamma,\chi)}$ містить інформацію про яскравість і може приймати значення від 0 до 255.

Кожна оброблювана площину A являє собою двомірний масив елементів $a_{i,j}^{(\gamma,\chi)}$:

$$A = \{a_{i,j}^{(\gamma,\chi)}\},$$

де $\gamma = \overline{1,[\frac{M}{m}]}$, $\chi = \overline{1,[\frac{N}{n}]}$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Формування ККК$_{дг}$ починається з формування службових складових (СС). Для цього, в кожному блоці $A^{(\gamma;\chi)}$ в напрямку по рядках визначаються:

– системи підстав $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$, де $i = \overline{1,m}$. Підстава $\lambda_i^{(\gamma,\chi)}$ для елементів i-го рядка в блоці $A^{(\gamma;\chi)}$ визначається, як максимальний елемент рядка вихідного блоку за формулою:

$$\lambda_i^{(\gamma,\chi)} = \max_{1 \le j \le n}(a_{i,j}^{(\gamma,\chi)}); \qquad (1)$$

– системи понижуючих значень динамічного діапазону $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$, де $i = \overline{1,m}$. Понижуюче значення $\mu_i^{(\gamma,\chi)}$ для елементів i-го рядка в блоці $A^{(\gamma;\chi)}$ визначається, як мінімальне значення за формулою:

$$\mu_i^{(\gamma,\chi)} = \min_{1 \le j \le n}(a_{i,j}^{(\gamma,\chi)}). \qquad (2)$$

Кожен з елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ може приймати значення в діапазоні $[0;255]$.

Системи підстав $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ і понижуючих значень динамічного діапазону $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$ в блоках $A^{(\gamma;\chi)}$ площині є вектор-стовпці з m елементів кожен. Вони об'єднуються в двовимірні масиви даних $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ і $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ і мають розмірності $M \times [\frac{N}{n}]$ елементів кожен. Дані двовимірні масиви Λ і Θ є СС ККП зображення для площині A і містять інформацію про виявлені структурні характеристики в відеоданих.

Обробка даних починається з першого блоку з координатами $(1;1)$ і триває в напрямку по горизонталі до блоку з координатами $(1;[\frac{N}{n}])$. Після цього обробка триває в блоці з координатами $(2;1)$ в напрямку по горизонталі і так далі, поки не закінчиться обробка останнього блоку з координатами $([\frac{M}{m}];[\frac{N}{n}])$. Обробка елементів $a_{i,j}^{(\gamma,\chi)}$ всередині блоку $A^{(\gamma;\chi)}$ здійснюється, починаючи з першого елемента з координатами $(1;1)$ в напрямку по вертикалі до елемента з координатами $(m;1)$.

Після цього в обробці бере участь елемент з координатами $(1;2)$ і далі триває в напрямку по вертикалі. Обробка блоку $A^{(\gamma;\chi)}$ закінчується після обробки останнього елемента з координатами $(m;n)$.

В якості обмежень приймається той факт, що площині A зображень з розмірами $M \times N$ елементів рівномірно розбиваються на блоки $A^{(\gamma;\chi)}$ з розмірами $m \times n$, тобто виконується умова:

$$[\frac{M}{m}] = \frac{M}{m}, \qquad [\frac{N}{n}] = \frac{N}{n}.$$

Для організації плаваючою схеми кодування в межах всього зображення пропонується здійснити переформатування двовимірної матриці A в одновимірний вектор:

$$A = \{a_\tau\} = \{a_{i,j}^{(\gamma,\chi)}\},$$

де $\tau = \overline{1, M \cdot N}$, $\gamma = \overline{1, [\frac{M}{m}]}$, $\chi = \overline{1, [\frac{N}{n}]}$, $i = \overline{1, m}$, $j = \overline{1, n}$,

де τ – одномірна координата елемента $a_{i,j}^{(\gamma,\chi)}$ двовимірної матриці A, яка переформатована в одновимірний вектор для взаємно-однозначної відповідності.

Для цього здійснюється лінеаризація координат елементу $a_{i,j}^{(\gamma,\chi)}$. Вона полягає в їх переформатуванні з чотиривимірної координати, виходячи з місця розташування $(i; j)$ даного елемента в блоці $A^{(\gamma;\chi)}$ і координати $(\gamma; \chi)$ самого блоку в площині A зображення, в одновимірну координату τ, де $\tau = \overline{1, M \cdot N}$. При цьому враховується схема організації обробки даних в процесі ККП площини зображення. Для цього використовується наступний вираз:

$$\tau = ((\gamma - 1) \cdot [\frac{N}{n}] + \chi - 1) \cdot m \cdot n + (j - 1) \cdot m + i. \qquad (3)$$

В результаті переформатування двовимірної матриці A в одновимірний вектор змінюється тільки форма представлення даних, при цьому самі дані не змінюються і їх кількість залишається незмінною і дорівнює $M \cdot N$ елементів. Для зворотного перетворення, що здійснює визначення координат $(\gamma; \chi)$ і $(i; j)$ елемента $a_{i,j}^{(\gamma,\chi)}$ зображення в двовимірної матриці A виходячи з одновимірної координати τ його векторного представлення a_τ, використовуються наступні вирази:

$$\gamma = [\frac{[\frac{\tau - 1}{m \cdot n}]}{[\frac{N}{n}]}] + 1;$$

$$\chi = [\frac{\tau - 1}{m \cdot n}] - [\frac{[\frac{\tau - 1}{m \cdot n}]}{[\frac{N}{n}]}] \cdot [\frac{N}{n}] + 1;$$

$$i = \tau - [\frac{\tau - 1}{m \cdot n}] \cdot m \cdot n - [\frac{\tau - 1 - [\frac{\tau - 1}{m \cdot n}] \cdot m \cdot n}{m}] \cdot m;$$

$$j = [\frac{\tau - 1 - [\frac{\tau - 1}{m \cdot n}] \cdot m \cdot n}{m}] + 1 \cdot$$

Переформатування систем підстав $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ і понижуючих значень $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ з двовимірних матриць в одномірні вектора здійснюється за допомогою виразу (3) за умови, що $j = \overline{1, n}$. При цьому враховується схема організації обробки даних в процесі ККК.

В результаті тривимірні координати елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ перетворюються в одномірні і формуються вектори

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

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

що складаються з елементів від λ_1 до $\lambda_{M \cdot [\frac{N}{n}]}$ та від μ_1 до $\mu_{M \cdot [\frac{N}{n}]}$, відповідно. Переформатування двовимірних матриць Λ і Θ в одномірні вектори не призводить до зміни значень елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ та не змінює їх кількість, яка дорівнює $M \cdot [\frac{N}{n}]$ елементів в кожному з векторів. Для визначення взаємно-однозначної відповідності елементів фрагмента зображення з елементами службових даних пропонується розширити систему підстав Λ і систему понижувальних значень Θ до потужності оброблюваної площини зображення в одновимірному векторному вигляді. Для цього кожен вектор-стовпець $\Lambda^{(\gamma,\chi)}$ і $\Theta^{(\gamma,\chi)}$ для всіх $\gamma = \overline{1, [\frac{M}{m}]}$ і $\chi = \overline{1, [\frac{N}{n}]}$ перетворюється в двовимірну матрицю $\Lambda'^{(\gamma,\chi)}$ і $\Theta'^{(\gamma,\chi)}$ відповідно.

Перетворення організовується за рахунок повторення відповідних векторів-стовпців $\Lambda^{(\gamma,\chi)}$ і $\Theta^{(\gamma,\chi)}$ n раз. Двовимірні матриці $\Lambda'^{(\gamma,\chi)}$ і $\Theta'^{(\gamma,\chi)}$

складаються з відповідних елементів $\lambda'^{(\gamma,\chi)}_{i,j}$ і $\mu'^{(\gamma,\chi)}_{i,j}$, значення яких визначаються за допомогою виразів:

$$\lambda'^{(\gamma,\chi)}_{i,j}=\lambda^{(\gamma,\chi)}_{i} \text{ та } \mu'^{(\gamma,\chi)}_{i,j}=\mu^{(\gamma,\chi)}_{i} \text{ при } j=\overline{1,n}.$$

В результаті формуються системи підстав Λ' і понижуючих значень Θ', які мають розмірність оброблюваної площини A, а саме $M\times N$ елементів. Переформатування систем службових даних Λ' і Θ' з двовимірних матриць в одномірні вектора здійснюється за допомогою виразу (3) за принципом переформатування двовимірної матриці площині A зображення.

В результаті формуються одномірні вектори

$$\Lambda'=\{\lambda'_{\tau}\}=\{\lambda'^{(\gamma,\chi)}_{i,j}\}=\{\lambda^{(\gamma,\chi)}_{i}\}_{j=\overline{1,n}},$$

$$\Theta'=\{\mu'_{\tau}\}=\{\mu'^{(\gamma,\chi)}_{i,j}\}=\{\mu^{(\gamma,\chi)}_{i}\}_{j=\overline{1,n}},\ \tau=\overline{1,M\cdot N}.$$

У процесі організації лінеаризації координат на основі виразу (3) організовується однозначна відповідність координат τ елементів систем СС Λ' і Θ' у векторному вигляді з координатами $\left(m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]\right)$ елементів систем СС Λ і Θ у векторному вигляді. Тобто організується однозначна відповідність значень елементів, а саме:

$$\lambda'_{\tau}=\lambda_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}=\lambda^{(\gamma,\chi)}_{i},\ \tau=\overline{1,M\cdot N};$$

$$\mu'_{\tau}=\mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}=\mu^{(\gamma,\chi)}_{i},\ \tau=\overline{1,M\cdot N}.$$

Формування кодових значень (КЗ) E_{α} інформаційної складової (ІС) ККП зображення на основі плаваючої схеми кодування в диференційованому базисі організовується для векторного представлення площини A і розширених систем службових даних Λ' і Θ' (або вихідного їх векторного представлення Λ і Θ). Процес формування КЗ E_{α} задається наступними виразами:

$$E_{\alpha}=\sum_{\tau=\tau(0)_{\alpha}}^{\tau(0)_{\alpha}+\Psi_{\alpha}-1}\left\langle(a_{\tau}-\mu'_{\tau})\cdot W_{\tau}\right\rangle=$$

$$\sum_{\tau=\tau(0)_{\alpha}}^{\tau(0)_{\alpha}+\Psi_{\alpha}-1}\left\langle(a_{\tau}-\mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]})\cdot W_{\tau}\right\rangle, \quad (4)$$

$$W_{\tau}=\begin{cases}\prod_{\xi=\tau+1}^{\tau(0)_{\alpha}+\Psi_{\alpha}-1}(\lambda'_{\xi}+1-\mu'_{\xi})=\prod_{\xi=\tau+1}^{\tau(0)_{\alpha}+\Psi_{\alpha}-1}(\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}+1-\mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}), & \tau<\tau(0)_{\alpha}+\Psi_{\alpha}-1;\\ 1, & \tau=\tau(0)_{\alpha}+\Psi_{\alpha}-1,\end{cases} \quad (5)$$

де $\tau\in[\tau(0)_{\alpha};\tau(0)_{\alpha}+\Psi_{\alpha}-1]$ і $\tau(0)_{\alpha}+\Psi_{\alpha}-1\le M\cdot N$,

де α – порядковий номер формованого КЗ E_{α} ІС ККК$_{дг}$;

τ, ξ – лінійні векторні координати, які визначають положення оброблюваних в процесі кодування даних;

$\tau(0)_{\alpha}$ – стартова координата елемента a_{τ} оброблюваної площини A у векторному вигляді, з якого починається формування КЗ E_{α};

Ψ_{α} – плаваюча (недетермінована) кількість елементів a_{τ} площині A, що беруть участь у формуванні КЗ E_{α};

W_{τ} – ваговий коефіцієнт для τ-ого елемента a_{τ}, який є добутком наступних за ним елементів підстав λ'_{ξ} з урахуванням зниження їх динамічних діапазонів на μ'_{ξ}.

При формуванні першого КЗ E_{α} стартові параметри кодування визначаються наступним чином:

– порядковий номер КЗ дорівнює $\alpha=1$;

– стартова координата першого елементу a_{τ} дорівнює $\tau(0)_1=1$.

Наступні стартові параметри для формування нового КЗ ІС визначаються наступним чином:

– порядковий номер КЗ збільшується на один $\alpha = \alpha + 1$;

– стартова координата $\tau(0)_\alpha$ визначається виходячи із значення стартової координати $\tau(0)_{\alpha-1}$ для формування попереднього КЗ $E_{\alpha-1}$ і кількості $\Psi_{\alpha-1}$ елементів a_τ, які його сформували. Для цього використовується формула:

$$\tau(0)_\alpha = \tau(0)_{\alpha-1} + \Psi_{\alpha-1}. \quad (6)$$

У формуванні КЗ E_α ІС беруть участь елементи a_τ площині A з координатами $\tau \in [\tau(0)_\alpha; \tau(0)_\alpha + \Psi_\alpha - 1]$.

Формування останнього КЗ закінчується після обробки всіх елементів площини, а саме $\tau(0)_\alpha + \Psi_\alpha - 1 \le M \cdot N$. Після формування всіх КЗ E_α вони об'єднуються і формують ІС $E = \{E_\alpha\}$ для оброблюваної площині.

Кількість Ψ_α елементів a_τ площині A, які беруть участь у формуванні КЗ E_α, є недетермінованою і залежить від значень оброблюваних даних.

Вона визначається виходячи з умови, що формування КЗ E_α повинно не приводити до переповнення кодового слова (КС) L_{cw}, яке виділяється для його зберігання, тобто:

$$E_\alpha \le 2^{L_{cw}} - 1, \quad \log_2(E_\alpha) \le L_{cw}, \quad (7)$$

де $2^{L_{cw}} - 1$ – найбільше число, яке може зберігатися в КС довжиною L_{cw} біт.

Виходячи з аналізу механізму формування КЗ E_α на основі виразів (4) і (5) видно, що умова (7) буде виконуватися, якщо накопичений добуток підстав λ'_ξ в зниженому динамічному діапазоні μ'_ξ для Ψ_α елементів, які беруть участь у формуванні КЗ E_α, не приведе до переповнення КС, тобто:

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi) \le 2^{L_{cw}} - 1, \quad (8)$$

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}) \le 2^{L_{cw}} - 1.$$

На практиці, для виключення помилки, пов'язаної з переповненням КС, замість умови (8) або (9) краще використовувати такі нерівності:

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi) \le \frac{2^{L_{cw}} - 1}{\lambda'_{\tau(0)_\alpha+\Psi_\alpha} + 1 - \mu'_{\tau(0)_\alpha+\Psi_\alpha}}, \quad (10)$$

$$\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}) \le$$

$$\le \frac{2^{L_{cw}} - 1}{\lambda_{m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}]+(\tau(0)_\alpha+\Psi_\alpha)-m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}]} + 1 - \mu_{m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}]+(\tau(0)_\alpha+\Psi_\alpha)-m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}]}}, \quad (11)$$

за умови, що $(\Psi_\alpha + 1)$-й елемент системи СС з координатою $(\tau(0)_\alpha + \Psi_\alpha) \le M \cdot N$ існує при перевірці умови (10) і з координатою $(m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}]+(\tau(0)_\alpha+\Psi_\alpha)-m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}]) \le M\cdot[\frac{N}{n}]$ при перевірці умови (11).

Кількість Ψ_α елементів визначається, як значення аргументу при якому величина $\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi)$ (або $\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]})$) досягає максимуму за умови виконання нерівності (10) або (11) і розраховується за формулою:

$$\Psi_\alpha = \arg\max_{\Psi_\alpha}\Big(\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi)\Big) =$$

$$= \arg\max_{\Psi_\alpha}\Big(\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]} + 1 - \mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]})\Big). \quad (12)$$

Алгоритм визначення кількості Ψ_α елементів, який описує правило організації виконання формул (10)–(12), складається з наступних етапів.

На попередньому етапі організовується введення початкових параметрів, а саме порядкового номера α формованого КЗ E_α, стартової координати $\tau(0)_\alpha$ першого елементу a_τ і довжина КС L_{cw}. Лічильник кількості елементів, які беруть участь у формуванні КЗ E_α, встановлюється $\Psi_\alpha = 1$.

Етап 1. На першому етапі організується зчитування елементів λ'_τ і μ'_τ (або $\lambda_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}$ і $\mu_{m\cdot[\frac{\tau-1}{m\cdot n}]+\tau-m\cdot[\frac{\tau-1}{m}]}$) СС Λ' і Θ' (або Λ і Θ) з координатами від $\tau(0)_\alpha$ до $(\tau(0)_\alpha + \Psi_\alpha)$, які відповідають елементам a_τ початкової площини A, що формує КЗ E_α.

Етап 2. Другий етап організовує перевірку переповнення КС L_{cw}, виділеного для зберігання КЗ E_α, у разі додавання чергового елемента з координатою $(\tau(0)_\alpha + \Psi_\alpha)$ (або $(m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m\cdot n}]+(\tau(0)_\alpha+\Psi_\alpha)-m\cdot[\frac{\tau(0)_\alpha+\Psi_\alpha-1}{m}])$). А саме, перевіряється виконання нерівності (10) або (11) за умови, що додається існуючий елемент системи СС.

Етап 3. Якщо умова (10) або (11) виконується, то на третьому етапі значення лічильника кількості елементів, які беруть участь у формуванні КЗ E_α, збільшується на 1, тобто $\Psi_\alpha = \Psi_\alpha + 1$. Після цього переходимо до виконання другого етапу.

Етап 4. Якщо ж умова (10) або (11) не виконується, то на четвертому етапі визначається, що кількість елементів, що формують КЗ E_α, дорівнює Ψ_α.

Формування КККдг для оброблюваної площини A зображення на основі плаваючої схеми кодування в диференційованому базисі організовується в три етапи.

Етап 1. На першому етапі, що полягає в підготовці вихідних даних і визначенні СС:

– вихідна площина A розбивається на блоки $A^{(\gamma;\chi)}$, розмірністю $m \times n$ елементів кожен;

– в блоках $A^{(\gamma;\chi)} = \{a_{i,j}^{(\gamma,\chi)}\}$ за допомогою формул (1) і (2) визначаються системи підстав $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ і понижуючих значень динамічного діапазону $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$, які представляють собою вектор-стовпці з m елементів кожен. Після обробки всіх блоків $A^{(\gamma;\chi)}$ отримані вектор-стовпці об'єднуються в двовимірні масиви даних $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ і $\Theta = \{\mu_i^{(\gamma,\chi)}\}$, розмірністю $M \times [\frac{N}{n}]$ елементів кожен. Дані двовимірні масиви Λ і Θ є СС ККП зображення для площині A;

– організовується переформатування двовимірних матриць, що містять елементи вихідних даних A зображення і систем службових даних Λ і Θ (або розширених до потужності оброблюваної площини систем службових даних Λ' і Θ'), в одномірні вектора за допомогою формули (3);

– встановлюються стартові параметри кодування для формування першого КЗ E_α ІС, а саме, порядковий номер формованого КЗ дорівнює $\alpha = 1$, стартова координата першого елемента, з якого починається кодування, дорівнює $\tau(0)_1 = 1$ і визначається довжина КС L_{cw}.

Етап 2. На другому етапі розраховується кількість елементів Ψ_α, які беруть участь у формуванні КЗ E_α. Для цього лічильник кількості елементів встановлюється $\Psi_\alpha = 1$. Після цього виконуються етапи 1–4 відповідного алгоритму.

Етап 3. На третьому етапі безпосередньо формується КЗ E_α ІС на основі виразів (4) і (5). Кодове значення E_α є інтегрованим.

Воно формується з урахуванням елементів, як оброблюваної площини $A = \{a_{i,j}^{(\gamma,\chi)}\}$ зображення, так і СС $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ і $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$.

Етап 4. Після формування КЗ E_α, якщо не оброблені всі елементи площині $A=\{a_{i,j}^{(\gamma,\chi)}\}$, тобто $(\tau(0)_\alpha+\Psi_\alpha-1)\neq M\cdot N$, то визначаються нові стартові параметри для формування нового КЗ, а саме:

– порядковий номер КЗ збільшується на один $\alpha=\alpha+1$;

– нова стартова координата $\tau(0)_\alpha$ визначається формулою (6).

Після цього виконується другий етап.

Етап 5. Якщо оброблені все елементи площині $A=\{a_{i,j}^{(\gamma,\chi)}\}$, тобто $(\tau(0)_\alpha+\Psi_\alpha-1)=M\cdot N$, то всі сформовані КЗ E_α об'єднуються і формують ІС $E=\{E_\alpha\}$для цієї площини. Порядковий номер α останнього сформованого КЗ E_α буде відповідати кількості α_{max} всіх КЗ E_α, які сформували ІС $E=\{E_\alpha\}$ для площині A.

Запис елементів в кодовий потік може бути організовано на основі рівномірної або нерівномірної довжини q_α КЗ E_α. Рівномірна довжина q_α відповідає довжині обраного КС L_{cw}, тобто $q_\alpha=L_{cw}$.

Нерівномірна довжина q_α є індивідуальною для кожного окремого КЗ E_α і визначається на основі накопиченого добутку кількості Ψ_α елементів СС Λ і Θ (Λ' і Θ') за допомогою формули:

$$q_\alpha=[\log_2\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda'_\xi+1-\mu'_\xi)]+1=$$

$$=[\log_2\prod_{\xi=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1}(\lambda_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]}+1-\mu_{m\cdot[\frac{\xi-1}{m\cdot n}]+\xi-m\cdot[\frac{\xi-1}{m}]})]+1.$$

Загальна довжина всіх α_{max} КЗ E_α визначається за формулою:

$$q=\sum_{\alpha=1}^{\alpha_{max}}q_\alpha.$$

КККдг зображення формується з кодових конструкцій отриманих для кожної площині A з P площин, а саме:

– інформаційної складової $E=\{E_\alpha\}$;

– системи підстав $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$;

– системи понижуючих значень динамічного діапазону $\Theta=\{\mu_i^{(\gamma,\chi)}\}$.

$$A^{(\gamma;\chi)}=\{a_{i,j}^{(\gamma,\chi)}\},$$

де $i=\overline{1,m}$, $j=\overline{1,n}$.

Кожен елемент $a_{i,j}^{(\gamma,\chi)}$ містить інформацію про яскравість і може приймати значення від 0 до 255. Кожна оброблювана площина A являє собою двомірний масив елементів $a_{i,j}^{(\gamma,\chi)}$:

$$A=\{a_{i,j}^{(\gamma,\chi)}\},$$

де $\gamma=\overline{1,[\frac{M}{m}]}$, $\chi=\overline{1,[\frac{N}{n}]}$, $i=\overline{1,m}$, $j=\overline{1,n}$.

Забезпечення криптостійкості відеоданих на основі розроблено методу забезпечується за рахунок:

– формування КЗ E_α на змінній кількості Ψ_α елементів a_τ на основі контролю переповнення КС L_{cw}. Кількість Ψ_α елементів a_τ, що сформували КЗ E_α, залежить тільки від структури даних, що оброблюються;

– формування ІС $E=\{E_\alpha\}$ з КЗ E_α нерівномірної довжини q_α, яка є індивідуальною для кожного з них і визначається на основі накопиченого добутку кількості Ψ_α елементів СС Λ та Θ (Λ' та Θ'). З одного боку, це дозволяє зменшити загальну довжину q ІС $E=\{E_\alpha\}$. З іншого боку, без знання СС Λ та Θ (Λ' та Θ') неможливо виділити кожне окреме КЗ E_α із загального кодового потоку ІС $E=\{E_\alpha\}$;

– фактично у формуванні КЗ E_α беруть участь не вихідні елементи a_τ, а її представлення у зниженому динамічному діапазоні $(a_\tau-\mu'_\tau)$. Це дозволяє значно збільшити кількість Ψ_α елементів, що сформували КЗ E_α, та зменшити кількість α_{max} КЗ E_α ІС $E=\{E_\alpha\}$;

– системи підстав $\Lambda=\{\lambda_i^{(\gamma,\chi)}\}$ та понижуючих значень динамічного діапазону $\Theta=\{\mu_i^{(\gamma,\chi)}\}$ під-

даються додатковому шифруванню та/або скремблюванню. Їх обсяг значно менший за обсяг початкового зображення. Оцінка ефективності розробленого методу проводилася з позиції:

– оцінки якості реконструйованих зображень порівняно з вихідними;

– оцінки якості компресії відеоданих;

– оцінки обсягів СС КККдг, що піддаються додатковому шифруванню;

– оцінки статистичних характеристик ІС КККдг.

Розроблений метод ККК зображень на основі плаваючої недетермінованої схеми обробки доцільно використовувати на першому каскаді концептуального методу формування КККдг зображень без втрати якості інформації, що запропоновано в [19]. Тому, оцінку ефективності будимо проводити, як для однокаскадної схеми обробки на основі розроблено методу, так й для двокаскадної схеми з урахуванням використання розроблено методу в концептуального методу формування КККдг. Для порівняльної оцінки якості роботи розробленого методу формування КККдг зображень з позиції зменшення обсягу вихідних відеоданих без втрати якості інформації використовувалися алгоритми кодування, що реалізовані у форматах представлення відео TIFF і PNG.Розроблений метод, як і контрольні методи, не вносить помилок у дані в процесі кодування та відноситься до методів без втрати якості інформації.

Середньоквадратичне відхилення RSME всіх реконструйованих зображень різного класу насиченості дрібними об'єктами та різних розмірів щодо вихідних відеоданих дорівнює 0, коефіцієнт кореляції дорівнює 1.

Результати оцінки коефіцієнта компресії зображень на основі однокаскадної та двокаскадної схеми обробки представлені на рис. 1. Тут розмірність оброблюваних блоків даних проводилася при значеннях $m = n = 8$.Конкретні результати деяких зображень наведено в табл. 1.

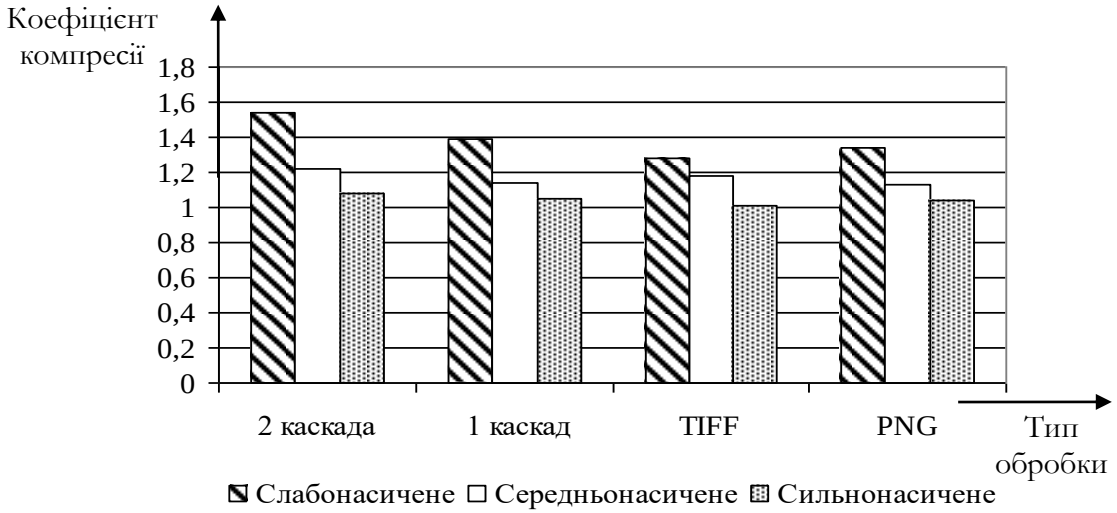

Рис. 1. Результати оцінки коефіцієнта компресії зображень

Таблиця 1

Приклади результатів оцінки ступеня стиснення тестових зображень

Тестове зображення	Варіант обробки							
	PNG		TIFF		ККП 1 каскад		ККП 2 каскада	
	коеф. компр.	% змен. обсягу	коеф. компр.	% змен. обсягу	коеф. компр.	% змен. обсягу	коеф. компр.	% змен. обсягу
2.1.01	1,08	7,41	0,92	-11,11	1,086	7,92	1,126	11,19
Airplane	1,34	25,26	1,28	21,88	1,39	28,06	1,54	35,06
Baboon	1,04	3,85	0,83	-20,48	1,05	4,76	1,08	7,41
Barbara	1,13	11,50	1,18	15,25	1,14	12,28	1,22	18,03
Lena	1,07	6,54	1,08	7,41	1,25	20,00	1,37	27,01
Зона аэропорта	1,25	20,00	1,26	20,63	1,16	13,79	1,21	17,36

З аналізу даних на рис. 1 видно, що найкращий результат за ступенем стиснення зображень показала двокаскадна схема обробки методу ККК зображень різного ступеня насиченості.

Усереднене значення коефіцієнта компресії знаходиться:

– для сильнонасичених зображень – на рівні 1,08 при зниженні обсягу даних на 7,14 %;

– для середньонасичених зображень – на рівні 1,22 при зниженні обсягу даних на 18 %;

– для слабонасичених зображень – на рівні 1,54 при зниженні обсягу даних на 35,06 %.

Це в середньому на 3–20 % краще за формат подання даних TIFF і на 4–15 % краще за формат PNG. При цьому двокаскадна обробка перевищує однокаскадний підхід на 4–5,2 %.

Отже, формування кодових конструкцій недетермінованої довжини:

– з позиції забезпечення конфіденційності – забезпечує невизначеність позиціонування нерівномірних кодограм у загальному кодовому потоці, що фактично усуває можливість їхнього несанкціонованого дешифрування;

– з позиції забезпечення доступності – забезпечує зменшення обсягу ККП зображень щодо вихідних відео в середньому від 1,08 до 1,54 рази в залежності від ступеня їх насиченості.

Співвідношення обсягів інформаційних та службових складових у КККдг представлені в табл. 2. Тут застосовуються такі скорочення: ІС1 – ІС, сформована після першого каскаду обробки; ІС2 – ІС, сформована після другого каскаду обробки. З аналізу табл. 2 видно, що об'єм СС КККдг зменшується зі збільшенням розмірності блоків обробки елементів m та n. Це забезпечує зниження обсягу даних, які зазнають додаткового криптографічного перетворення на основі скремблювання та/або шифрування. Так, при $m = n = 16$ елементів забезпечується обсяг СС в КККдг на рівні не більше 2,5 % від обсягу всього кодового потоку.

Таблиця 2

Співвідношення обсягів інформаційних та службових складових КККдг без втрати якості інформації при різних параметрах m та n блоку $A^{(\gamma;\chi)}$ обробки відеоданих, %

Тестове зображення	Значення параметру m та n за умови, що $m = n$											
	8			12			16			20		
	ІС1	ІС2	СС	ІС1	ІС2	СС	ІС1	ІС2	СС	ІС1	ІС2	СС
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
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
Зона аеропорту	74,24	18,23	7,54	82,99	13,58	3,43	87,3	10,77	1,93	90,06	8,73	1,21

З результатів статистичного тестування бітових послідовностей ІС КККдг видно, що:

– кількість 1 у бітових послідовностях більша від кількості 0 від 2 до 5 %, а ймовірність появи одиниць відхиляється від $1/2$ усього на 1–2,5 %;

– кількість 1 у кожній 64-бітовій підпослідовності відрізнятиметься від кількості 0 у середньому на два, що перевищує на одиницю еталонне значення та задовольняє постулатам Голомба (в ідеальному варіанті кількість 1 у кожному періоді має відрізнятися від кількості 0 не більше ніж на одиницю);

– у послідовностях спостерігається однакова кількість серій 0 і 1, що відрізняється від розрахункового значення 50 % менше 1 %;

– ймовірність розподілу серій-пар (00, 01, 10, 11) у послідовностях знаходиться в межах 0,223–0,272 при розрахунковому значенні в 0,25, а серій-трійок (000, 001, 010, 100, 011, 110, 10 111) – у межах 0,103–0,146 при розрахунковому значенні в 0,125. Найкращі результати отримані для насичених реалістичних зображень;

– в ІС відсутня кореляційна залежність між елементами;

– в ІС відсутня надмірність, додаткове стиснення архіваторами ZIP і RAR не забезпечується.

ВИСНОВКИ

Отримав подальше вдосконалення однокаскадний метод криптокомпресійного кодування зображень в диференційованому базисі на основі використання технології нерівноважного позиційного кодування.

Відмінність даного методу від відомих полягає в:

– організації плаваючою схеми кодування в межах всієї площині зображення, коли у формуванні кодових величин інформаційної складової беруть участь елементи зображення, що належать різним блокам. Для цього розроблена схема лінеаризації з чотиривимірних координат представлення елементу в двовимірної матриці, які визначають координати блоку в площині зображення та координати елементу в цьому блоці, в одновимірну координату для взаємно-однозначного уявлення цього елемента у векторі. Для взаємно-однозначного зіставлення елементів службових складових з елементами зображення у векторному вигляді, двовимірні матраци службових складових переформатуються в одномірні вектори;

– формування кодового значення інформаційної складової виключає переповнення довжини кодового слова, яке виділяється для його зберігання;

– додатковому використанні двох ступенів невизначеності, які складаються з недетермінованої довжини криптокомпресійних кодограм і недетермінованої кількості елементів, що беруть участь в їх формуванні.

Це дозволяє підвищити криптостійкість та доступність відеоданих без втрати достовірності.

ЛІТЕРАТУРА

[1] Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base // *IEEE 2 nd International Conference on Advanced Trends in Information Theory (ATIT 2020)*, 2020. – pp. 83-86.

[2] Бараннік В.В., Сідченко С.О., Бараннік Н.В., Хіменко А.М. Метод маскувального ущільнення службових даних в системах компресії відеозображень. *Радіоелектронні і комп'ютерні системи*. 2021, № 2. – С. 51-63.

[3] Баранник В., Сидченко С., Баранник Д., Баранник В. Оценка влияния недетерминированных характеристик на эффективность криптокомпрессионного кодирования изображений в дифференцированном базисе. *Безпека інформації*, 2020. – Том 26, № 3. – С. 168-180.

[4] Баранник В.В., Сидченко С.А., Баранник Д.В. Метод криптокомпрессионного представления изображений на основе двухкаскадного обобщенного позиционного кодирования в базисе по верхним границам. *Радиоэлектроника и информатика*. 2017. № 1(76). – С. 22-27.

[5] Баранник В.В., Сидченко С.А., Тупица И.М. Технология наслоения битовых зон в методе криптосемантического представления изображений на основе плавающей схемы. *Автоматизированные системы управления и приборы автоматики*. 2015. Вып. 171. – С. 22-28.

[6] Васильев В.Б., Оков И.Н., Стрежик Ю.Н., Устинов А.А., Швецов Н.В. Сжатие и защита видеоданных в радиоканалах обмена информацией БЛА. *Перспективы развития и применения комплексов с беспилотными летательными аппаратами*: науч.-практ. конф. Коломна: 924 Государственный центр беспилотной авиации Министерства Обороны Российской Федерации, 2016. – С. 202-204.

[7] ДСТУ 7624:2014. *Інформаційні технології. Криптографічний захист інформації.* Алгоритм симетричного блокового перетворення. Чинний від 01.03.2016. Вид. офіц. Київ, Держспоживстандарт України, 2016. – 228 с.

[8] ДСТУ ГОСТ 28147:2009. *Система обробки інформації. Захист криптографічний.* Алгоритм криптографічного перетворення (ГОСТ 28147-89). Чинний від 01.02.2009. Вид. офіц. Київ, Держспоживстандарт України, 2009. – 20 с.

[9] Сідченко С.О., Бараннік Д.В. Метод криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі. *Наукоємні технології*. 2017. № 1 (33). – С. 46-53.

[10] Alimpiev A.N., Barannik V.V., Sidchenko S.A. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. *Telecommunications and Radio Engineering*. 2017. Vol. 76. No. 6. – pp. 521-534.

[11] Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197. NIST, November 26, 2001. – 51 p.

[12] Auer S., Bliem A., Engel D., Uhl A., Unterweger A. Bitstream-based JPEG Encryption in Real-time. *International Journal of Digital Crime and Forensics*. 2013. Vol. 5. Iss. 3. – pp. 1-14.

[13] Barannik V., Barannik D., Fustii V., Parkhomenko M. Evaluation of Effectiveness of Masking Methods of Aerial Photographs. *Advanced Information and Communications Technologies (AICT)*: proceedings of 3rd Intern. Conf. Lviv, 2019. pp. 415-418.

[14] Barannik V., Barannik N., Ryabukha Yu., Barannik D. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System. *Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET' 2020)*: proceedings of 15th IEEE Intern.Conf. Lviv -Slavske, 2020. – pp. 699-702.

[15] Barannik V.V., Ryabukha Yu.N., Kulitsa O.S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. *Telecommunications and Radio Engineering*. 2017. Vol. 76. No. 9. – pp. 785-797.

[16] Barannik V., Sidchenko S., Barannik N., Barannik D., Shulgin S. Methods for Decoding Informational Codes of Cryptocompression Codegrams to Improve Information Security. *CEUR Workshop Proceedings (CEUR-WS.org)*. 2021. Vol.2923. – pp. 143-152.

[17] Barannik V., Sidchenko S., Barannik N., Barannik V. Development of the method for encoding service data in cryptocompression image representation systems. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 3. No. 9(111). – pp. 103-115.

[18] Barannik V., Sidchenko S., Barannik D. Technology for protecting video information resources in the info-communication space. *Advanced Trends in Information Theory (ATIT 2020)*: proceedings of IEEE 2nd Intern. Conf. Kyiv, 2020. – pp. 29-33.

[19] Barannik V., Sidchenko S., Barannik D., Shulgin S., Barannik V., Datsun A. Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 4. No. 2(112). – pp. 6-17.

[20] Chen Ch.-Ch., Wu, W.-J. A secure Boolean-based multi-secret image sharing scheme. *Journal of Systems and Software*. 2014. Vol. 92. – pp. 107-114.

[21] Belikova*, T. Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. Advanced Trends in Information Theory (ATIT), Proceedings of the 2nd IEEE International Conference, Kyiv, Ukraine, 87–91. URL: https://ieeexplore.ieee.org/document/9349300.*

[22] Deshmukh M., Nain N., Ahmed M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. *Advanced Information Networking and Applications (AINA)*: proceedings of IEEE 30th Intern. Conf. Crans-Montana, 2016. – pp. 690-697.

[23] Dufaux F., Ebrahimi T. Toward a Secure JPEG. *Applications of Digital Image Processing XXIX*. 2006. Vol. 6312. – pp. 1-8.

[24] Farajallah M. Chaos-based crypto and joint cryptocompression systems for images and videos. Universite de Nantes, 2015. – 211 p.

[25] Faraoun K.M. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology*. 2014. Vol. 17. – pp. 85-94.

[26] Honda T., Murakami Y., Yanagihara Y., Kumaki, T., Fujino, T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection. *Circuits and Systems (MWSCAS)*: proceedings of IEEE 56th Intern. Midwest Symposium. Columbus, 2013. – pp. 1371-1374.

[27] Information technology – JPEG 2000 image coding system: Secure JPEG 2000. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807. Approved on 29 May 2006 by ITU-T Study Group 16 (2005-2008). Switzerland, Geneva, 2007. – 108 p.

[28] Ji Sh., Tong X., Zhang M. Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator. 2012. URL: https://arxiv.org/abs/1208.0999.

[29] JPEG Privacy & Security Abstract and Executive Summary. JPEG.ORG. September 10, 2015. URL: https://jpeg.org/items/0150910_privacy_security_summary.html.

[30] Kobayashi H., Kiya H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. *Consumer Electronics (GCCE)*: proceedings of IEEE 7th Global Conf. Nara, 2018. – pp. 1-4.

[31] Korshunov P., Ebrahimi T. Using warping for privacy protection in video surveillance. *Digital Signal Processing (DSP)*: proceedings of 18th Intern. Conf. Fira, 2013. – pp. 1-6.

[32] Minemura K., Moayed Z., Wong K., Qi X., Tanaka K. JPEG image scrambling without expansion in bitstream size. *Image Processing*: proceedings of 19th IEEE Intern. Conf. Orlando, 2012. – pp. 261-264.

[33] Naor M., Shamir A. Visual Cryptography. In: Proceedings of the Advances in Cryptology. EUROCRYPT'94. *Lecture Notes in Computer Science*. 1995. Vol. 950. – pp. 1-12.

[34] Phatak A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*. 2016. Vol. 8. No. 6. – pp. 64-71.

[35] Ramakrishnan, S. et al.. Cryptographic and Information Security Approaches for Images and Videos. CRC Press, 2018. – 962 p.

[36] Rivest R.L., Shamir A., Adleman L.M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978. Vol. 21. No. 2. – pp. 120-126.

[37] Sharma R., Bollavarapu S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*. 2015. Vol. 117. No. 14. – pp. 15-18.

[38] Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. *Security*

Technology (ICCST): proceedings of IEEE Intern. Carnahan Conf. Newton, 2012. pp. 135-139.

[39] Wong K.-W. Image encryption using chaotic maps. *Intelligent Computing Based on Chaos*. 2009. Vol. 184. pp. 333-354.

[40] Wong K., Tanaka K. DCT based scalable scrambling method with reversible data hiding functionality. *Communications, Control and Signal Processing (ISCCSP)*: proceedings of 4th Intern. Symposium. Limassol, 2010. – pp. 1-4.

[41] Wu Y., Zhou Y., Agaian S., Noonan J.P. 2D Sudoku associated bijections for image scrambling. *Information Sciences*. 2016. Vol. 327. – pp. 91-109.

[42] Yang Ch.-N., Chen Ch.-H., Cai S.-R. Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*. 2016. Vol. 116. pp. 22-34.

[43] Yang Y., Zhu B.B., Li S., Yu N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*. 2008. Vol. 2007. Article ID 56365. – 13 p.

[44] Yuan L., Korshunov P., Ebrahimi T. Secure JPEG Scrambling enabling Privacy in Photo Sharing. *Automatic Face and Gesture Recognition (FG)*: proceedings of 11th IEEE Intern. Conf. and Workshops. Ljubljana, 2015. – pp. 1-6.

РАЗРАБОТКА МЕТОДА КРИПТОКОМПРЕССИОННОГО КОДИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЛАВАЮЩЕЙ НЕДЕТЕРМИНИРОВАННОЙ СХЕМЫ ОБРАБОТКИ

В процессе управления объектами кризисной инфраструктуры и во время их охраны используются цифровые видеоизображения. Их объемы постоянно растут и к ним предъявляются требования относительно сохранения максимального качества при необходимости обеспечения конфиденциальности. Поэтому актуальной является научно-прикладная проблема, которая заключается в повышении конфиденциальности видеоинформации в условиях обеспечения ее достоверности и доступности. Для ее решения получил дальнейшее совершенствование однокаскадный метод криптокомпрессионного кодирования изображений в дифференцированном базисе на основе использования технологии неравновесного позиционного кодирования. Отличие данного метода от известных заключается в следующем. Во-первых, плавающая схема кодирования организуется в пределах всей плоскости изображения, когда в формировании кодовых величин информационной составляющей участвуют элементы изображения, принадлежащие разным блокам видеоданных. Для этого разработана схема линеаризации координат с четырехмерного представления элемента в двумерной матрице, которые определяют координаты блока в плоскости изображения и координаты элемента в этом блоке, в одномерную координату для взаимно-однозначного представления этого элемента в векторе. Во-вторых, дополнительно используются две степени неопределенности, которые состоят из недетерминированной длины кодовых значений криптокомпрессионных кодограмм и недетерминированного количества элементов, участвующих в их формировании. Это позволяет повысить криптостойкость и доступность видеоданных без потери достоверности.

Ключевые слова: криптокомпресионное представление, защита информации, шифрование, кодирование, компрессия, конфиденциальность, изображение.

DEVELOPMENT OF THE METHOD OF CRYPTOCOMPRESSION CODING OF IMAGES BASED ON A FLOATING NONDETERMINISTIC PROCESSING SCHEME

In the process of managing the objects of crisis infrastructure and during their protection, digital video images are used. Their volumes are constantly growing and requirements are imposed on them to maintain maximum quality while maintaining confidentiality. Therefore, a scientific and applied problem is relevant, which consists in increasing the confidentiality of video information in the conditions of ensuring its reliability and availability. To solve it, the one-stage method of cryptocompression coding of images in a differentiated basis based on the use of non-equilibrium positional coding technology was further improved. The difference between this method and the known ones is as follows. First, the floating coding scheme is organized within the entire image plane, when image elements belonging to different blocks of video data participate in the formation of the code values of the information component. For this, a scheme has been developed for linearizing coordinates from a four-dimensional representation of an element in a two-dimensional matrix, which determine the coordinates of a block in the image plane and coordinates of an element in this block, into a one-dimensional coordinate for one-to-one representation of this element in a vector. Secondly, two degrees of uncertainty are additionally used, which consist of the non-deterministic length of the code values of the cryptocompression codograms and the non-deterministic number of elements involved in their formation. This makes it possible to increase the cryptographic strength and availability of video data without loss of credibility.

Keywords: cryptocompression representation, information protection, encryption, encoding, compression, confidentiality, image.

Бараннік Володимир Вікторович, доктор технічних наук, професор, професор кафедри штучного інтелекту та програмного забезпечення, Харківський національний університет імені В.Н. Каразіна.
E-mail: vvbar.off@gmail.com.
Orcid ID: 0000-0002-2848-4524.

Баранник Владимир Викторович, доктор технических наук, профессор, профессор кафедры искусственного интеллекта и программного обеспечения, Харьковский национальный университет имени В.Н. Каразина.
Barannik Vladimir, doctor of technical sciences, professor, professor of the department of artificial intelligence and software, V.N. Karazin Kharkiv National University.

Сідченко Сергій Олександрович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідної лабораторії, Харківський національний університет Повітряних Сил імені І. Кожедуба.
E-mail: sidserg72@gmail.com.
Orcid ID: 0000-0002-1319-6263.
Сидченко Сергей Александрович, кандидат технических наук, старший научный сотрудник, начальник научно-исследовательской лаборатории, Харьковский национальный университет Воздушных Сил имени И. Кожедуба.
Sidchenko Serhii, candidate of technical sciences, senior scientific researcher, head of research laboratory, Ivan Kozhedub National Air Force University.

Бараннік Дмитро Володимирович, аспірант, Харківського національного університету радіоелектроніки.
E-mail: d.v.barannik@gmail.com.
Orcid ID: 0000-0002-7074-9864.
Баранник Дмитрий Владимирович, аспирант, Харьковского национального университета радиоэлектроники.
Dmitriy Barannik, PhD student, Kharkov National University of Radio Electronics.

Бараннік Валерій Володимирович, студент, Харківський національний університет радіоелектроніки.
E-mail: valera462000@gmail.com.
Orcid ID: 0000-0003-3516-5553.
Баранник Валерий Владимирович, студент Харьковского национального университета радиоэлектроники, Харків, Україна,
Barannik Valery, student, Kharkov National University of Radio Electronics.

Шульгін Сергій Сергійович, кандидат технічних наук, докторант Харківського національного університету радіоелектроніки.
E-mail: barannik_v_v@ukr.net.
Orcid ID: 0000-0001-5174-290X.
Шульгин Сергей Сергеевич, кандидат технических наук, докторант Харьковского национального университета радиоэлектроники.
Shulgin Sergii, candidate of technical sciences, associate professor, Doctoral Student in Kharkov National University of Radio Electronics.

Туренко Сергій Вікторович, кандидат технічнихнаук, викладач Харківського національного університетурадіоелектроніки.
E-mail: mercuryserg@gmail.com.
Orcid ID: 0000-0003-0985-7660.
Туренко Сергей Викторович, кандидат технических наук, преподаватель Харьковского национального университета радиоэлектроники.
Turenko Serhii PhD, Kharkiv National University radioelectronics, Kharkov, Ukraine.