Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, 2023, Iss. 92, pp. 28–40

УДК 621.3:681.5

Метод зберігання елементів службових складових криптокомпресійних кодограм відеозображень

Бараннік В. В.[1], *Сідченко С. О.*[2], *Бараннік Д. В.*[3], *Чорномаз І. К.*[4], *Гуржій П. М.*[5], *Григор'ян М. Б.*[4]

[1]Харківський національний університет імені В. Н. Каразіна, Україна
[2]Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна
[3]Харківський національний університет радіоелектроніки, Україна
[4]Національний університет цивільного захисту України, Україна
[5]Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Україна

E-mail: *vvbarannik@karazin.ua*

В статті проводиться обґрунтування вимог до якісних характеристик відеоінформаційного ресурсу у разі його використання для інформаційного забезпечення функціонування систем критичної інфраструктури. Тут одночасно висуваються вимоги щодо: своєчасності доставки та конфіденційності відеоінформації в умовах заданого рівня її цілісності та повноти. Показується те, що частково такі вимоги зумовлені інтелектуалізацією окремих етапів процесу аналізу та прийняття рішень в системах критичної інфраструктури. Надається системне обґрунтування наявності проблемних питань, до яких відноситься: дисбаланс між рівнями продуктивності інфокомунікаційних систем та бітової інтенсивності відеоінформаційних потоків. Для зменшення такого дисбалансу використовуються технології компресійного кодування. Вони дозволяють зменшити бітовий об'єм відеоданих. Однак самі по собі не забезпечують потрібного рівня конфіденційності інформації. Звідси доводиться актуальність науково-прикладної проблеми відносно необхідності забезпечення потрібного рівня оперативності доставки конфіденційної інформації з використанням бездротових інфокомунікаційних технологій в системах критичної інфраструктури.

В статті показано, що напрямком вирішення існуючої проблеми є створення та застосування технологій кодування, які дозволяють забезпечити конфіденційність відеоінформації в процесі скорочення надмірності. При цьому одними з представників даного класу методів є такі, що будуються на основі технологій криптокомпресійного кодування. Для таких технологій формується система службових відомостей. З одного боку це створює умови для забезпечення конфіденційності відеоінформації в процесі зменшення її бітового об'єму. З іншого боку виникає деструктивний вплив на стримування росту коефіцієнту стиснення. Звідси мета статті полягає у розробці методу зберігання елементів службових складових криптокомпресійних кодограм. Запропоновано три способи зберігання елементів службових складових криптокомпресійних кодограм зображень. Перший полягає у зберіганні службових даних у вигляді мінімальних та максимальних значень. Другий спосіб передбачає зниження динамічного діапазону максимальних значень. Третій спосіб передбачає зберігання проміжних елементів або елементів службових складових у вигляді напівсуми та напіврізниці. Для реалізації третього способу зберігання елементів службових даних розроблено метод, який організує примусове зниження якості вихідних зображень. Зниження якості організується за рахунок внесення помилки у вихідні зображення для формування парних і непарних значень елементів службових даних в межах усієї площини зображення, окремих її блоків або для кожного рядка блоку окремо. Пікове співвідношення сигналу до шуму (PSNR) реконструйованих зображень не нижче 56,5 dB, а значення коефіцієнта кореляції становить 0,99997. Позитивним ефектом від реалізації розробленого методу є підвищення конфіденційності кодограм за рахунок порушення взаємозв'язку між елементами службових даних, підвищення коефіцієнту компресії до 2–3% та зниження обсягу службових складових кодограм на 6,25%.

Ключові слова: захист інформації; зображення; конфіденційність; криптокомпресія; стиснення; шифрування

DOI: 10.20535/RADAP.2023.92.28-40

Вступ. Постановка проблеми

Питання стосовно досягнення потрібного рівня конфіденційності та доступності інформаційних ресурсів є ключовими компонентами національної безпеки держави [1–5].

В загальному випадку інформаційні ресурси можуть представлятися різними типами джерел. Сюди відносяться текстові електроні документи, аудіофайли та відеодані [6–8]. Останнім часом найбільший попит дістають відеоінформаційні ресурси.

Це зумовлено такими факторами [9–12]:

– ростом потужності інфокомунікаційних технологій. Створюється потенціал відносно обробки та передачі великих за бітовим об'ємом масивів даних;

– інтелектуалізацією окремих етапів процесу аналізу та прийняття рішень. Відеоінформація містить найбільшу кількість відомостей щодо об'єктів контролю та управління. Отже має роль ключового ресурсу для ідентифікації та розпізнавання об'єктів, їх класу та поточного стану.

До якісних характеристик щодо відеоінформаційного забезпечення надаються певні вимоги. До них слід віднести такі [13–16]:

– оперативність доставки відеоінформації до користувачів;

– конфіденційність, цілісність та повнота відеоінформаційного ресурсу.

Особливо підвищені вимоги до відеоінформаційного забезпечення висуваються у разі його використання для систем критичної інфраструктури [17–19]. Тут одночасно висуваються вимоги щодо: своєчасності доставки та конфіденційності відеоінформації в умовах заданого рівня її цілісності та повноти.

В той же час на шляху забезпечення таких вимог виникають проблемні питання. Вони стосуються того, що:

1. Інфокомунікаційні системи мають недостатній рівень продуктивності відносно значної за бітовим рівнем інтенсивності відеопотоку. Особливо такий дисбаланс має місце у разі використання бездротових інфокомунікаційних технологій [20–23].

2. Застосування технологій компресійного кодування з одного боку дозволяє зменшити бітовий об'єм відеоданих. Однак, з іншого боку, ці технології самі по собі не забезпечують потрібного рівня конфіденційності інформації [24–26].

Звідси існує актуальна науково-прикладна проблема, яка полягає у необхідності забезпечення потрібного рівня оперативності доставки конфіденційної інформації з використанням бездротових інфокомунікаційних технологій в системах критичної інфраструктури.

Напрямком вирішення існуючої проблеми є створення та застосування технологій кодування, які дозволяють забезпечити конфіденційність відеоінформації в процесі скорочення надмірності. При цьому необхідно дотримуватись вимог щодо цілісності інформації. Базовими представниками даного класу методів є такі, що будуються на основі технологій криптокомпресійного кодування [27–33]. В цьому випадку ключова послідовність формується в процесі стиснення відеоданих. В якості ключової послідовності використовуються системи службових даних. Службові дані тут необхідні для формування компактного представлення відеоданих. Одночасно їх пропонується використовувати для побудови ключових послідовностей для забезпечення криптостійкості.

1 Обґрунтування технології криптокомпресійного кодування

Криптокомпресійне кодування (ККК) організується для кожної окремої площини A зображення розмірністю $M \times N$ елементів, де M – кількість рядків у зображенні, а N – кількість стовпців.

Концептуальний метод плаваючого ККК зображень у диференційованому базисі без втрати якості інформації організує трикаскадну схему формування криптокомпресійних кодограм (КККдг) [29, 30]. На перших двох каскадах забезпечується одночасне формування кодових конструкцій інформаційних складових (ІС), які не вимагають додаткового забезпечення конфіденційності, та ключових елементів як службових складових (СС).

На першому каскаді обробки організується формування ІС з елементів вихідного зображення з формуванням проміжних двовимірних матриць (ПДМ) [29].

Площина A розбивається на однакові блоки $A^{(\gamma;\chi)}$, де γ – координата блоку у зображенні по вертикалі, χ – координата по горизонталі. Розмірність блоків $A^{(\gamma;\chi)}$ складає $m \times n$ елементів, де m – кількість рядків у блоці, а n – кількість стовпців. Блоки $A^{(\gamma;\chi)}$ є двовимірними масивами елементів $a_{i,j}^{(\gamma,\chi)}$, де $\gamma = \overline{1, \left[\frac{M}{m}\right]}$, $\chi = \overline{1, \left[\frac{N}{n}\right]}$, $i = \overline{1,m}$, $j = \overline{1,n}$. Тут $[\bullet]$ – ціла частина числа.

Для кожного блоку $A^{(\gamma;\chi)} = \{a_{i,j}^{(\gamma,\chi)}\}$ в напрямку по рядках визначаються максимальні $\lambda_i^{(\gamma,\chi)}$ та мінімальні $\mu_i^{(\gamma,\chi)}$ значення елементів $a_{i,j}^{(\gamma,\chi)}$ [28, 29]:

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

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

З них будуються вектор-стовпці $\Lambda^{(\gamma;\chi)} = \{\lambda_i^{(\gamma,\chi)}\}$ і $\Theta^{(\gamma;\chi)} = \{\mu_i^{(\gamma,\chi)}\}$, які формують ПДМ $\Lambda = \{\Lambda^{(\gamma;\chi)}\}$ та $\Theta = \{\Theta^{(\gamma;\chi)}\}$.

На першому каскаді обробки при формуванні ІС КККдг двовимірна матриця $A = \{a_{i,j}^{(\gamma,\chi)}\}$ площини

зображення трансформується у векторне представлення $A = \{a_\tau\}$, де $\tau = \overline{1, M \cdot N}$. Трансформація ПДМ $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ та $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ у векторне представлення може бути організована:

– з урахуванням розширення розмірності результуючих векторів до розміру векторного представлення даних. Воно організується за рахунок повторення n раз кожного елементу $\lambda_i^{(\gamma,\chi)}$, $\mu_i^{(\gamma,\chi)}$. Тут формуються вектори $\Lambda' = \{\lambda'_\tau\}$ і $\Theta' = \{\mu'_\tau\}$, де $\tau = \overline{1, M \cdot N}$;

– без організації розширення розмірності векторного представлення ПДМ. Тут формуються вектори $\Lambda = \{\lambda_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]}\}$ і $\Theta = \{\mu_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]}\}$, $\tau = \overline{1, M \cdot N}$.

Формування кодової величини E_α ІС криптокомпресійного представлення зображення на основі плаваючої схеми кодування в диференційованому базисі для векторного представлення даних задається виразами [28, 29]:

$$E_\alpha = \sum_{\tau=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} \langle (a_\tau - \mu'_\tau) \cdot W_\tau \rangle = \\ = \sum_{\tau=\tau(0)_\alpha}^{\tau(0)_\alpha+\Psi_\alpha-1} \left(\left(a_\tau - \mu_{m\cdot\left[\frac{\tau-1}{m\cdot n}\right]+\tau-m\cdot\left[\frac{\tau-1}{m}\right]} \right) \cdot W_\tau \right), \tag{3}$$

$$W_\tau = \begin{cases} \prod\limits_{\xi=\tau+\mathbf{1}}^{\tau(0)_\alpha+\Psi_\alpha-1} (\lambda'_\xi + 1 - \mu'_\xi) = \prod\limits_{\xi=\tau+\mathbf{1}}^{\tau(0)_\alpha+\Psi_\alpha-1} \left(\lambda_{m\cdot\left[\frac{\xi-1}{m\cdot n}\right]+\xi-m\cdot\left[\frac{\xi-1}{m}\right]} + 1 - \mu_{m\cdot\left[\frac{\xi-1}{m\cdot n}\right]+\xi-m\cdot\left[\frac{\xi-1}{m}\right]} \right), \\ \tau < \tau(0)_\alpha + \Psi_\alpha - 1; \\ 1, \qquad \tau = \tau(0)_\alpha + \Psi_\alpha - 1, \end{cases} \tag{4}$$

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

де α – порядковий номер формованого значення кодової величини E_α ІС ККККдг;

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

$\tau(0)_\alpha$ – стартова координата елементу a_τ у векторному вигляді, з якого починається формування значення кодової величини;

Ψ_α – плаваюча (недетермінована) кількість елементів a_τ, які приймають участь у формуванні кодової величини E_α ІС, що залежить від значень даних, що обробляються;

W_τ – ваговий коефіцієнт для τ-ого елементу a_τ, який є добутком наступних елементів підстав λ'_ξ з урахуванням зниження їх динамічних діапазонів на μ'_ξ.

Кодові величини E_α формують ІС $E = \{E_\alpha\}$ ККККдг після першого каскаду обробки.

На другому каскаді організується додаткова обробка ПДМ Λ та Θ [30].

Спочатку формуються СС ККККдг. Для цього у кожному вектор-стовпці $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ визначаються максимальні елементи $\lambda(\max)^{(\gamma,\chi)}$ та $\mu(\max)^{(\gamma,\chi)}$ і мінімальні елементи $\lambda(\min)^{(\gamma,\chi)}$ та $\mu(\min)^{(\gamma,\chi)}$ за допомогою формул [30]:

$$\lambda(\max)^{(\gamma,\chi)} = \max_{1 \le i \le m} \left(\lambda_i^{(\gamma,\chi)} \right); \tag{5}$$

$$\mu(\max)^{(\gamma,\chi)} = \max_{1 \le i \le m} \left(\mu_i^{(\gamma,\chi)} \right); \tag{6}$$

$$\lambda(\min)^{(\gamma,\chi)} = \min_{1 \le i \le m} \left(\lambda_i^{(\gamma,\chi)} \right); \tag{7}$$

$$\mu(\min)^{(\gamma,\chi)} = \min_{1 \le i \le m} \left(\mu_i^{(\gamma,\chi)} \right). \tag{8}$$

Елементи $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ об'єднуються у відповідні двовимірні масиви даних $\Lambda(\max) = \{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min) = \{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max) = \{\mu(\max)^{(\gamma,\chi)}\}$ і $\Theta(\min) = \{\mu(\min)^{(\gamma,\chi)}\}$. Вони й є СС ККККдг.

Кодування двовимірних матриць Λ та Θ на другому каскаді організується у напрямку по рядках. Пропонується переформатувати двовимірні матриці Λ і Θ в одновимірні вектори, а саме [30]:

$$\Lambda = \{\lambda_\eta\} = \{\lambda_i^{(\gamma,\chi)}\}; \;\; \Theta = \{\mu_\eta\} = \{\mu_i^{(\gamma,\chi)}\},$$

при $\eta = \overline{1, M \cdot \left[\frac{N}{n}\right]}$, $\gamma = \overline{1, \left[\frac{M}{m}\right]}$, $\chi = \overline{1, \left[\frac{N}{n}\right]}$, $i = \overline{1, m}$, де η – одновимірна координата елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ відповідної двовимірної матриці Λ та Θ, переформатованої в одновимірний вектор.

Переформатування двовимірних масивів СС $\Lambda(\max) = \{\lambda(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min) = \{\lambda(\min)^{(\gamma,\chi)}\}$, $\Theta(\max) = \{\mu(\max)^{(\gamma,\chi)}\}$ і $\Theta(\min) = \{\mu(\min)^{(\gamma,\chi)}\}$ в одновимірні вектори можуть бути організовані одним з двох способів, а саме:

– для вихідних розмірів двовимірних масивів СС, кожен із яких дорівнює $\left[\frac{M}{m}\right] \times \left[\frac{N}{n}\right]$ елементів. Тоді формуються вектори

$$\Lambda(\max) = \{\lambda(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\cdot\left[\frac{N}{n}\right]}\},$$

$$\Lambda(\min) = \{\lambda(\min)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\cdot\left[\frac{N}{n}\right]}\},$$

$$\Theta(\max) = \{\mu(\max)_{\eta-\left[\frac{\eta-1}{\left[\frac{N}{n}\right]}\right]\cdot\left[\frac{N}{n}\right]}\},$$

$$\Theta(\min) = \{\mu(\min)_{\eta-[\frac{\eta-1}{[\frac{N}{n}]}]\cdot[\frac{N}{n}]}\},$$

$$\eta = \overline{1, M \cdot \left[\frac{N}{n}\right]};$$

– з урахуванням розширення їх розмірності до розміру $M \times \left[\frac{N}{n}\right]$ елементів, який відповідає розміру двовимірних масивів оброблюваних даних Λ та Θ. В результаті формуються двовимірні матриці $\Lambda'(\max) = \{\lambda'(\max)_i^{(\gamma,\chi)}\}$, $\Lambda'(\min) = \{\lambda'(\min)_i^{(\gamma,\chi)}\}$, $\Theta'(\max) = \{\mu'(\max)_i^{(\gamma,\chi)}\}$ і $\Theta'(\min) = \{\mu'(\min)_i^{(\gamma,\chi)}\}$.

Криптокомпресійне кодування на другому каскаді організується на основі використання технологічного ядра системи криптокомпресійного перетворення даних, описаного виразами (3) та (4).

На третьому каскаді кодування організується забезпечення конфіденційності СС КККдг [32].

Концептуальний метод плаваючого ККК на перших двох каскадах забезпечує формування кодових конструкцій інформаційних складових з одночасним забезпеченням їх конфіденційності та ключових елементів в якості службових складових [30]. Обсяг службової складової в криптокомпресійних кодограмах становить 6,5–8,5% від усього кодового потоку при обробці відеоданих блоками $m \times n$ розмірністю 8×8 елементів, 3–4,5% – для блоків 12×12 елементів, та не перевищує 2,5% – для блоків 16×16 елементів [30]. На третьому каскаді організується забезпечення конфіденційності службової складової з використанням методів шифрування [30, 32].

Службові складові КККдг у відкритому вигляді повністю характеризують зміст оброблюваних зображень. У разі реконструкції зображень тільки на основі елементів СС без використання кодових значень (КЗ) ІС забезпечується коефіцієнт кореляції з вихідними відеоданими на рівні 0,8. Причому, за допомогою СС можна реконструювати вихідне зображення без помилок.

У процесі кодування та формування КККдг можуть використовуватись різні схеми зберігання елементів ПДМ та СС. Вони можуть істотно вплинути на кількість операцій у процесі кодування та декодування, а також на обсяги формованих кодограм.

Значить, метою статті є розробка методу зберігання елементів службових складових криптокомпресійних кодограм зображень.

2 Визначення способів зберігання елементів службових складових

Зберігання елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ ПДМ Λ та Θ, а також елементів $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ СС $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ і $\Theta(\min)$ в процесі ККК може бути організовано у такі способи:

– у вихідному варіанті подання елементів. Даний варіант передбачає на першому каскаді кодування формування максимальних $\lambda_i^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$ значень по рядках у блоці $A^{(\gamma;\chi)}$ площини A згідно з формулами (1) і (2). На другому каскаді кодування процес знаходження максимальних $\lambda(\max)^{(\gamma,\chi)}$ та $\mu(\max)^{(\gamma,\chi)}$ і мінімальних $\lambda(\min)^{(\gamma,\chi)}$ та $\mu(\min)^{(\gamma,\chi)}$ значень організується в межах векторів-стовпців $\Lambda^{(\gamma;\chi)}$ та $\Theta^{(\gamma;\chi)}$ за формулами (5)–(8). Причому вектори-стовпці $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ відповідно сформовані з мінімальних $\lambda_i^{(\gamma,\chi)}$ та максимальних $\mu_i^{(\gamma,\chi)}$ значень одного блоку $A^{(\gamma;\chi)}$;

– у формі, коли максимальні значення $\lambda_i^{(\gamma,\chi)}$, $\lambda(\max)^{(\gamma,\chi)}$ і $\mu(\max)^{(\gamma,\chi)}$ зберігаються в зниженому динамічному діапазоні, а саме $(\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)})$, $(\lambda(\max)^{(\gamma,\chi)} - \lambda(\min)^{(\gamma,\chi)})$ та $(\mu(\max)^{(\gamma,\chi)} - \mu(\min)^{(\gamma,\chi)})$. При цьому форма зберігання мінімальних значень $\mu_i^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ не змінюється. Як варіант, на другому каскаді кодування може бути організовано зберігання максимальних значень $\lambda(\max)^{(\gamma,\chi)}$ та $\mu(\max)^{(\gamma,\chi)}$ елементів СС у вигляді зниженого діапазону, збільшеного на один, а саме $(\lambda(\max)^{(\gamma,\chi)}+1-\lambda(\min)^{(\gamma,\chi)})$ та $(\mu(\max)^{(\gamma,\chi)}+1-\mu(\min)^{(\gamma,\chi)})$. Це забезпечить зменшення кількості операцій у процесі кодування/декодування та підвищить його оперативність. Однак, на першому каскаді кодування даний спосіб зберігання максимальних значень $\lambda_i^{(\gamma,\chi)}$ у зниженому динамічному діапазоні, а саме $(\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)})$, не є оптимальним. Дана модифікація, з одного боку, призведе до зменшення кількості операцій у процесі кодування/декодування, що позитивно вплине на підвищення оперативності виконання ККК. Однак, з іншого боку, за рахунок нерівномірного зниження динамічного діапазону всіх елементів з вектор-стовбця $\Lambda^{(\gamma;\chi)^*} = \{(\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)})\}$ на другому каскаді перетворення сформуються значення елементів $\lambda(\max)^{(\gamma,\chi)^*} = \max\limits_{1 \le i \le m}(\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)})$ та $\lambda(\min)^{(\gamma,\chi)^*} = \min\limits_{1 \le i \le m}(\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)})$ СС. Це може призвести до збільшення відстані між відповідними максимальними та мінімальними значеннями:

$$(\lambda(\max)^{(\gamma,\chi)^*} - \lambda(\min)^{(\gamma,\chi)^*}) \ge (\lambda(\max)^{(\gamma,\chi)} - \lambda(\min)^{(\gamma,\chi)}).$$

Зрештою зміняться значення сформованих КЗ $E(\Lambda)_{\alpha(\Lambda)}$, їх довжин $q(\Lambda)_{\alpha(\Lambda)}$ та кількості $\Psi(\Lambda)_{\alpha(\Lambda)}$ елементів, що їх сформували. При цьому збільшиться загальна кількість $\alpha(\Lambda)_{\max}$ всіх КЗ $E(\Lambda)_{\alpha(\Lambda)}$ ІС $E(\Lambda) = \{E(\Lambda)_{\alpha(\Lambda)}\}$. Все це призведе до негативного ефекту, пов'язаного зі збільшенням загальної довжини КККдг. Крім того, на першому каскаді кодування у разі зберігання максимальних значень у вигляді $(\lambda_i^{(\gamma,\chi)} + 1 - \mu_i^{(\gamma,\chi)})$ для підвищення оперативності обробки буде потрібна організація примусового зниження якості вихідного зображення.

Це пов'язано з тим, що у разі різкого перепаду між відповідними максимальними $\lambda_i^{(\gamma,\chi)} = 255$ та мінімальними $\mu_i^{(\gamma,\chi)} = 0$ значеннями, сформованими в i-му рядку блоку $A^{(\gamma;\chi)} = \{a_{i,j}^{(\gamma,\chi)}\}$, буде отримано значення $(\lambda_i^{(\gamma,\chi)} + 1 - \mu_i^{(\gamma,\chi)}) = 256$. А це призведе до необхідності виділення для зберігання 9 біт, що неприпустимо. Для усунення цього ефекту всі значення $a_{i,j}^{(\gamma,\chi)}$ даного i-ого рядка, що дорівнює 255, зменшуються на 1. У результаті буде організовано незначне зниження якості. Тут у практичній реалізації значення середньоквадратичної похибки (RSME) будуть не перевищувати 0,05. Організація цього способу зберігання лише на другому каскаді кодування забезпечує підвищення оперативності виконання ККК на етапі декодування. Це не призводить до збільшення довжини КККдг та внесення помилок у реконструйоване зображення;

– зберігання максимальних і мінімальних елементів ПДМ і СС у вигляді напівсум і напіврізниць. Так, на першому каскаді обробки формується напівсума $\left(\frac{\lambda_i^{(\gamma,\chi)}+\mu_i^{(\gamma,\chi)}}{2}\right)$ і напіврізниця $\left(\frac{\lambda_i^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)}}{2}\right)$. На другому каскаді обробки формуються відповідні напівсуми $\left(\frac{\lambda(\max)^{(\gamma,\chi)}+\lambda(\min)^{(\gamma,\chi)}}{2}\right)$, $\left(\frac{\mu(\max)^{(\gamma,\chi)}+\mu(\min)^{(\gamma,\chi)}}{2}\right)$ та напіврізниці $\left(\frac{\lambda(\max)^{(\gamma,\chi)}-\lambda(\min)^{(\gamma,\chi)}}{2}\right)$, $\left(\frac{\mu(\max)^{(\gamma,\chi)}-\mu(\min)^{(\gamma,\chi)}}{2}\right)$. Цей спосіб зберігання є складнішим. З одного боку, він збільшує кількість операцій і призведе до формування навмисних помилок у вихідних даних $a_{i,j}^{(\gamma,\chi)}$. Причому організація цього способу зберігання на двох каскадах обробки одночасно є недоцільною через значне збільшення рівня навмисно сформованих помилок в даному варіанті. З іншого боку, цей спосіб забезпечує зменшення обсягу матриць $\Lambda(\min) = \{\lambda(\min)^{(\gamma,\chi)}\}$ і $\Theta(\min) = \{\mu(\min)^{(\gamma,\chi)}\}$ СС, у яких зберігаються напіврізності, і призводить до зменшення обсягу ІС $E = \{E_\alpha\}$, $E(\Lambda) = \{E(\Lambda)_{\alpha(\Lambda)}\}$ та $E(\Theta) = \{E(\Theta)_{\alpha(\Theta)}\}$. Крім того, він змінює структуру представлення елементів СС.

Розглянемо докладніше останній спосіб зберігання елементів ПДМ та СС у вигляді напівсум та напіврізниць максимальних та мінімальних значень. Для його правильної роботи необхідно забезпечити формування значень напівсум і напіврізниць у цілочисловому вигляді, тобто виконання наступних умов:

$$\frac{\lambda_i^{(\gamma,\chi)} + \mu_i^{(\gamma,\chi)}}{2} = \left[\frac{\lambda_i^{(\gamma,\chi)} + \mu_i^{(\gamma,\chi)}}{2}\right], \tag{9}$$

$$\frac{\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)}}{2} = \left[\frac{\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)}}{2}\right], \tag{10}$$

$$\frac{\lambda(\max)^{(\gamma,\chi)}+\lambda(\min)^{(\gamma,\chi)}}{2}=\left[\frac{\lambda(\max)^{(\gamma,\chi)}+\lambda(\min)^{(\gamma,\chi)}}{2}\right], \tag{11}$$

$$\frac{\lambda(\max)^{(\gamma,\chi)}-\lambda(\min)^{(\gamma,\chi)}}{2}=\left[\frac{\lambda(\max)^{(\gamma,\chi)}-\lambda(\min)^{(\gamma,\chi)}}{2}\right], \tag{12}$$

$$\frac{\mu(\max)^{(\gamma,\chi)}+\mu(\min)^{(\gamma,\chi)}}{2}=\left[\frac{\mu(\max)^{(\gamma,\chi)}+\mu(\min)^{(\gamma,\chi)}}{2}\right], \tag{13}$$

$$\frac{\mu(\max)^{(\gamma,\chi)}-\mu(\min)^{(\gamma,\chi)}}{2}=\left[\frac{\mu(\max)^{(\gamma,\chi)}-\mu(\min)^{(\gamma,\chi)}}{2}\right]. \tag{14}$$

Дані умови (9)–(14) виконуються лише тоді, коли самі елементи $\lambda_i^{(\gamma,\chi)}$, $\mu_i^{(\gamma,\chi)}$, $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ є попарно парними чи непарними. Умови їх парності визначаються так:

$$\frac{\lambda_i^{(\gamma,\chi)}}{2} = \left[\frac{\lambda_i^{(\gamma,\chi)}}{2}\right] \quad \text{та} \quad \frac{\mu_i^{(\gamma,\chi)}}{2} = \left[\frac{\mu_i^{(\gamma,\chi)}}{2}\right], \tag{15}$$

$$\begin{aligned} &\frac{\lambda(\max)^{(\gamma,\chi)}}{2} = \left[\frac{\lambda(\max)^{(\gamma,\chi)}}{2}\right] \text{ та} \\ &\frac{\lambda(\min)^{(\gamma,\chi)}}{2} = \left[\frac{\lambda(\min)^{(\gamma,\chi)}}{2}\right], \end{aligned} \tag{16}$$

$$\begin{aligned} &\frac{\mu(\max)^{(\gamma,\chi)}}{2} = \left[\frac{\mu(\max)^{(\gamma,\chi)}}{2}\right] \text{ та} \\ &\frac{\mu(\min)^{(\gamma,\chi)}}{2} = \left[\frac{\mu(\min)^{(\gamma,\chi)}}{2}\right], \end{aligned} \tag{17}$$

а відповідні умови непарності мають вигляд:

$$\frac{\lambda_i^{(\gamma,\chi)}}{2} \neq \left[\frac{\lambda_i^{(\gamma,\chi)}}{2}\right] \quad \text{та} \quad \frac{\mu_i^{(\gamma,\chi)}}{2} \neq \left[\frac{\mu_i^{(\gamma,\chi)}}{2}\right], \tag{18}$$

$$\begin{aligned} &\frac{\lambda(\max)^{(\gamma,\chi)}}{2} \neq \left[\frac{\lambda(\max)^{(\gamma,\chi)}}{2}\right] \text{ та} \\ &\frac{\lambda(\min)^{(\gamma,\chi)}}{2} \neq \left[\frac{\lambda(\min)^{(\gamma,\chi)}}{2}\right], \end{aligned} \tag{19}$$

$$\begin{aligned} &\frac{\mu(\max)^{(\gamma,\chi)}}{2} \neq \left[\frac{\mu(\max)^{(\gamma,\chi)}}{2}\right] \text{ та} \\ &\frac{\mu(\min)^{(\gamma,\chi)}}{2} \neq \left[\frac{\mu(\min)^{(\gamma,\chi)}}{2}\right]. \end{aligned} \tag{20}$$

Формування максимальних $\lambda_i^{(\gamma,\chi)}$, $\lambda(\max)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$,

$\mu(\min)^{(\gamma,\chi)}$ значень у парному вигляді, коли виконуються умови (15)–(17), або непарному вигляді, коли виконуються умови (18)–(20), можливе лише у разі формування навмисних помилок в елементах $a_{i,j}^{(\gamma,\chi)}$ вихідних блоків $A^{(\gamma;\chi)}$ відеоданих. Причому значення помилки в елементах $a_{i,j}^{(\gamma,\chi)}$ не буде перевищувати одиничного значення, тобто забезпечуватиметься умова:

$$\left|a_{i,j}^{(\gamma,\chi)} - a_{i,j}^{(\gamma,\chi)^*}\right| \le 1, \tag{21}$$

де $a_{i,j}^{(\gamma,\chi)^*}$ – значення елемента $a_{i,j}^{(\gamma,\chi)}$ з навмисно внесеною помилкою на формування парного чи непарного значення.

Напівсуми та напіврізниці з використанням умов цілісності (9)–(14) можна формувати на одному з двох каскадів обробки:

– лише на першому каскаді обробки для елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$;

– тільки на другому каскаді для попарних елементів $\lambda(\max)^{(\gamma,\chi)}$ та $\lambda(\min)^{(\gamma,\chi)}$, а також $\mu(\max)^{(\gamma,\chi)}$ та $\mu(\min)^{(\gamma,\chi)}$.

Якщо на першому каскаді в межах одного блоку $A^{(\gamma;\chi)}$ сформовані тільки парні чи непарні значення елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ для всіх $i = \overline{1,m}$ (тобто, якщо виконується відповідна умова (15) або (18)), то їх напівсуми $\left(\frac{\lambda_i^{(\gamma,\chi)}+\mu_i^{(\gamma,\chi)}}{2}\right)$ та напіврізниці $\left(\frac{\lambda_i^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)}}{2}\right)$ завжди будуть цілими. А саме, виконуватиметься відповідна умова (9) та (10). В результаті сформовані вектори-стовпці $\Lambda^{(\gamma;\chi)^*}$ і $\Theta^{(\gamma;\chi)^*}$ будуть складатися з відповідних елементів $\lambda_i^{(\gamma,\chi)^*}$ та $\mu_i^{(\gamma,\chi)^*}$, які перевизначаються за допомогою формул:

$$\lambda_i^{(\gamma,\chi)^*} = \frac{\lambda_i^{(\gamma,\chi)} + \mu_i^{(\gamma,\chi)}}{2}, \tag{22}$$

$$\mu_i^{(\gamma,\chi)^*} = \frac{\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)}}{2}, \tag{23}$$

де $\lambda_i^{(\gamma,\chi)^*}$ – максимальне значення $\lambda_i^{(\gamma,\chi)}$, що зберігається у вигляді напівсуми; $\mu_i^{(\gamma,\chi)^*}$ – мінімальне значення $\mu_i^{(\gamma,\chi)}$, що зберігається у вигляді напіврізниці.

Формування парних значень максимальних $\lambda_i^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$ елементів, коли виконуються умови (15), або непарних значень, коли виконуються умови (18), забезпечує одну з двох можливостей, а саме:

– сформувати на першому каскаді значення напівсум $\lambda_i^{(\gamma,\chi)^*}$ та напіврізниць $\mu_i^{(\gamma,\chi)^*}$ на основі виразів (22) та (23), а на другому каскаді забезпечити зберігання елементів $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ та $\mu(\min)^{(\gamma,\chi)}$ СС у вихідному форматі;

– зберігати проміжні елементи $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ у вихідному вигляді, що забезпечить на другому каскаді формування відповідних парних чи непарних значень елементів $\lambda(\max)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$ та $\mu(\min)^{(\gamma,\chi)}$ СС, які задовольняють умовам парності (16)–(17) або непарності (19)–(20). А це дозволить зберігати їх у вигляді напівсум та напіврізниць та сформувати відповідні цілочисельні значення, які задовольняють умовам (11)–(14).

3 Розробка методу зберігання елементів службових складових у форматі напівсуми та напіврізниці

Для внесення навмисних помилок в елементи $a_{i,j}^{(\gamma,\chi)}$ вихідних блоків $A^{(\gamma;\chi)}$ відеоданих з метою формування одночасно парних чи непарних значень елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ на першому каскаді обробки пропонується такий метод обробки.

Даний метод дозволяє організувати такі чотири варіанти внесення навмисної помилки в елементах $a_{i,j}^{(\gamma,\chi)}$, які забезпечують:

1) формування лише парних значень проміжних елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ для всього зображення;

2) формування лише непарних значень проміжних елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ для всього зображення;

3) формування лише парних чи непарних значень проміжних елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ в межах блоку $A^{(\gamma;\chi)}$, залежно від того, які початкові значення переважають. Це дозволить знизити кількість елементів $a_{i,j}^{(\gamma,\chi)}$, в які навмисно вноситься поодинока помилка. Проте, збільшується кількість операцій при розрахунках. Це пов'язано з тим, що необхідно організувати аналіз всіх значень елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ в межах блоку $A^{(\gamma;\chi)}$ на парність (або непарність);

4) формування лише парних чи непарних значень проміжних елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ для кожного окремого i-ого рядку блоку $A^{(\gamma;\chi)}$. Це ще більше дозволить знизити кількість елементів $a_{i,j}^{(\gamma,\chi)}$, в які навмисно вноситься поодинока помилка. Однак, формування напівсум і напіврізниць буде можливим лише на першому каскаді кодування. Причому, які значення будуть сформовані перестає бути принциповим, оскільки зміні піддається лише один елемент.

Метод передбачає такі основні етапи обробки.

На першому етапі організується обчислення максимальних $\lambda_i^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$ значень по рядках у блоці $A^{(\gamma;\chi)}$ згідно з формулами (1), (2) і формуються вектори-стовпці $\Lambda^{(\gamma;\chi)}$ та $\Theta^{(\gamma;\chi)}$.

На другому етапі здійснюється вибір одного з чотирьох варіантів формування навмисної помилки в елементах $a_{i,j}^{(\gamma,\chi)}$ у блоці $A^{(\gamma;\chi)}$. Наступний етап обробки в залежності від обраного способу, а саме:

– для першого способу на етапі чотири;
– для другого способу на етапі п'ять;
– для третього способу на етапі три;
– для четвертого способу на етапі шість.

На третьому етапі здійснюється перевірка всіх значень елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$, при $i = \overline{1,m}$, векторів-стовпців $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ на парність згідно з умовами (15). Необхідно визначити яких значень $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ у сумі більше: парних чи непарних. Для цього введемо додаткову змінну *even*. Відповідність елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ умові (15) організується роздільно для векторів-стовпців $\Lambda^{(\gamma;\chi)}$ та $\Theta^{(\gamma;\chi)}$. Перед початком аналізу значення $even = 0$. У процесі аналізу значення змінюється на $even = even + 1$, якщо виконуються умови (15). Результуюче значення *even* буде визначати кількість парних елементів у двох векторах-стовбцях $\Lambda^{(\gamma;\chi)}$ та $\Theta^{(\gamma;\chi)}$. Якщо значення $even > 2 \cdot m$, то парних значень $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ більше. В іншому випадку непарні значення переважають. Це необхідно для внесення меншої кількості навмисних спотворень у вихідні елементи $a_{i,j}^{(\gamma,\chi)}$ блоку $A^{(\gamma;\chi)}$. Якщо вектори-стовпці $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ сформовані з переважної кількості парних значень $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$, то зміні піддаються непарні значення $a_{i,j}^{(\gamma,\chi)}$ вихідних елементів, рівні непарним значенням $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$. Для цього обробка продовжується на четвертому етапі. Якщо ж вектори-стовпці $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ сформовані з переважної кількості непарних значень $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$, то зміні навпаки піддаються парні значення $a_{i,j}^{(\gamma,\chi)}$ вихідних елементів, рівні парним значенням $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$. Для цього обробка продовжується на п'ятому етапі.

На четвертому етапі виконується навмисне спотворення елементів $a_{i,j}^{(\gamma,\chi)}$ у блоці $A^{(\gamma;\chi)}$ з метою створення умови для формування векторів-стовпців $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ тільки з парних та нульових значень елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$, які задовольняють умовам (15). Для цього використовується правило:

$$a_{i,j}^{(\gamma,\chi)*} = \begin{cases} a_{i,j}^{(\gamma,\chi)} - 1, \to & a_{i,j}^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)} \text{ та } \dfrac{\lambda_i^{(\gamma,\chi)}}{2} \neq [\dfrac{\lambda_i^{(\gamma,\chi)}}{2}] \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)} - 1, \to & a_{i,j}^{(\gamma,\chi)} = \mu_i^{(\gamma,\chi)} \text{ та } \dfrac{\mu_i^{(\gamma,\chi)}}{2} \neq [\dfrac{\mu_i^{(\gamma,\chi)}}{2}] \text{ та } \mu_i^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)} \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)} + 1, \to & a_{i,j}^{(\gamma,\chi)} = \mu_i^{(\gamma,\chi)} \text{ та } \dfrac{\mu_i^{(\gamma,\chi)}}{2} \neq [\dfrac{\mu_i^{(\gamma,\chi)}}{2}] \text{ та } \mu_i^{(\gamma,\chi)} < \lambda_i^{(\gamma,\chi)} \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)}, \to & \text{інше,} \end{cases} \quad (24)$$

$$\text{для всіх} \quad i = \overline{1,m} \text{ та } j = \overline{1,n}.$$

Подальша обробка продовжується на сьомому етапі.

На п'ятому етапі виконується навмисне спотворення елементів $a_{i,j}^{(\gamma,\chi)}$ у блоці $A^{(\gamma;\chi)}$ з метою створення умови для формування векторів-стовпців $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ тільки з непарних значень елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$, які задовольняють умовам (18). Для цього використовується правило:

$$a_{i,j}^{(\gamma,\chi)*} = \begin{cases} a_{i,j}^{(\gamma,\chi)} - 1, \to & a_{i,j}^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)} \text{ та } \dfrac{\lambda_i^{(\gamma,\chi)}}{2} = [\dfrac{\lambda_i^{(\gamma,\chi)}}{2}] \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)} - 1, \to & a_{i,j}^{(\gamma,\chi)} = \mu_i^{(\gamma,\chi)} \text{ та } \dfrac{\mu_i^{(\gamma,\chi)}}{2} = [\dfrac{\mu_i^{(\gamma,\chi)}}{2}] \text{ та } \mu_i^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)} \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)} + 1, \to & a_{i,j}^{(\gamma,\chi)} = \mu_i^{(\gamma,\chi)} \text{ та } \dfrac{\mu_i^{(\gamma,\chi)}}{2} = [\dfrac{\mu_i^{(\gamma,\chi)}}{2}] \text{ та } \mu_i^{(\gamma,\chi)} < \lambda_i^{(\gamma,\chi)} \text{ та } a_{i,j}^{(\gamma,\chi)} > 0; \\ 1, \to & a_{i,j}^{(\gamma,\chi)} = 0; \\ a_{i,j}^{(\gamma,\chi)}, \to & \text{інше?} \end{cases} \quad (25)$$

$$\text{для всіх} \quad i = \overline{1,m} \text{ та } j = \overline{1,n}.$$

Наступна обробка продовжується на сьомому етапі.

На шостому етапі організується змішана обробка, коли для кожного окремого i-ого рядка блоку $A^{(\gamma;\chi)}$ виконується навмисне спотворення елементів $a_{i,j}^{(\gamma,\chi)}$ з метою створення умови для формування лише парних чи непарних значень проміжних елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ в межах даного рядка. Причому, у нових сформованих векторах-стовбцях $\Lambda^{(\gamma;\chi)}$ і $\Theta^{(\gamma;\chi)}$ не будуть дотримуватися значення парності чи непарності для всіх елементів $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$.

Для цього для елементів СС i-ого рядка виконується перевірка однієї з умов, коли максимальне $\lambda_i^{(\gamma,\chi)}$ значення парне, а мінімальне $\mu_i^{(\gamma,\chi)}$ непарне:

$$\frac{\lambda_i^{(\gamma,\chi)}}{2} = \left[\frac{\lambda_i^{(\gamma,\chi)}}{2}\right] \quad \text{та} \quad \frac{\mu_i^{(\gamma,\chi)}}{2} \neq \left[\frac{\mu_i^{(\gamma,\chi)}}{2}\right]. \qquad (26)$$

Або навпаки, коли максимальне $\lambda_i^{(\gamma,\chi)}$ значення непарне, а мінімальне $\mu_i^{(\gamma,\chi)}$ парне:

$$\frac{\lambda_i^{(\gamma,\chi)}}{2} \neq \left[\frac{\lambda_i^{(\gamma,\chi)}}{2}\right] \quad \text{та} \quad \frac{\mu_i^{(\gamma,\chi)}}{2} = \left[\frac{\mu_i^{(\gamma,\chi)}}{2}\right]. \qquad (27)$$

Якщо обрана умова (26) або (27) виконується, то виконується навмисне спотворення елементів $a_{i,j}^{(\gamma,\chi)}$ даного i-ого рядка згідно з одним з наступних правил для всіх $j = \overline{1,n}$:

– змінюється елемент $a_{i,j}^{(\gamma,\chi)}$, який відповідає максимальному $\lambda_i^{(\gamma,\chi)}$ значенню:

$$a_{i,j}^{(\gamma,\chi)^*} = \begin{cases} a_{i,j}^{(\gamma,\chi)} - 1, & a_{i,j}^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)} \quad \text{та} \quad \lambda_i^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)}, & \text{інше}, \end{cases} \qquad (28)$$

– змінюється елемент $a_{i,j}^{(\gamma,\chi)}$, який відповідає мінімальному $\mu_i^{(\gamma,\chi)}$ значенню:

$$a_{i,j}^{(\gamma,\chi)^*} = \begin{cases} a_{i,j}^{(\gamma,\chi)} + 1, & a_{i,j}^{(\gamma,\chi)} = \mu_i^{(\gamma,\chi)} \quad \text{та} \quad \lambda_i^{(\gamma,\chi)} > 0; \\ a_{i,j}^{(\gamma,\chi)}, & \text{інше}. \end{cases} \qquad (29)$$

Після обробки всіх рядків $i = \overline{1,m}$, обробка продовжується на сьомому етапі.

На сьомому етапі організується перевірка обробки всіх блоків $A^{(\gamma;\chi)}$. Якщо оброблені не всі блоки площини A, то змінюються координати блоку $(\gamma;\chi)$, де $\gamma = \overline{1,\left[\frac{M}{m}\right]}$, $\chi = \overline{1,\left[\frac{N}{n}\right]}$, та обробка триває на першому етапі. Причому на другому етапі варіант способу формування навмисної помилки в елементах $a_{i,j}^{(\gamma,\chi)}$ у блоці $A^{(\gamma;\chi)}$ залишається тим, який був обраний під час обробки першого блоку $A^{(1;1)}$. Обробка закінчується після формування навмисної помилки в елементах $a_{i,j}^{(\gamma,\chi)}$ останнього блоку $A^{\left(\left[\frac{M}{m}\right];\left[\frac{N}{n}\right]\right)}$.

Внаслідок виконання методу внесення навмисних помилок в елементах $a_{i,j}^{(\gamma,\chi)}$ буде сформована площина $A^* = \{a_{i,j}^{(\gamma,\chi)^*}\}$. Для уніфікації подальших процесів ККК розглядатимемо її як вихідну площину $A = \{a_{i,j}^{(\gamma,\chi)}\}$.

Використання правил (24), (25), (28) та (29) для внесення навмисних помилок в елементах $a_{i,j}^{(\gamma,\chi)}$ призводить до зменшення відстані між максимальними $\lambda_i^{(\gamma,\chi)}$ та відповідними їм мінімальними $\mu_i^{(\gamma,\chi)}$ значеннями, що дозволяє зменшити довжину ІС КККдг на обох каскадах обробки.

У блоках $A^{(\gamma;\chi)}$ знову сформованої площини організується обчислення нових значень $\lambda_i^{(\gamma,\chi)}$ та $\mu_i^{(\gamma,\chi)}$ за рядками відповідно до формул (1) та (2) та формуються нові вектори-стовпці $\Lambda^{(\gamma;\chi)}$ та $\Theta^{(\gamma;\chi)}$. Далі продовжується виконання першого каскаду ККК.

Якщо вибрано схему зберігання значень максимальних $\lambda_i^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$ елементів у вигляді напівсум $\lambda_i^{(\gamma,\chi)^*}$ та напіврізниць $\mu_i^{(\gamma,\chi)^*}$ після першого каскаду ККК, то вона організується у відповідних проміжних матрицях $\Lambda = \{\lambda_i^{(\gamma,\chi)}\}$ і $\Theta = \{\mu_i^{(\gamma,\chi)}\}$ на основі формул (22) та (23). Причому значення елементів $\lambda_i^{(\gamma,\chi)^*}$ ПДМ $\Lambda^* = \{\lambda_i^{(\gamma,\chi)^*}\}$ у вигляді напівсум змінюються в діапазоні $[0,255]$ та вимагають для свого зберігання 8 розрядів. Дійсно, якщо значення $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ є гранично можливими, тобто дорівнюють 255, то їх напівсума $\lambda_i^{(\gamma,\chi)^*}$ дорівнює 255. Нульові значення $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ дадуть нульовий результат напівсуми $\lambda_i^{(\gamma,\chi)^*}$. Значення ПДМ $\Theta^* = \{\mu_i^{(\gamma,\chi)^*}\}$ у вигляді напіврізниць $\mu_i^{(\gamma,\chi)^*}$ знаходяться в діапазоні $[0,127]$ та вимагають для свого зберігання 7 розрядів. Справді, нульові значення $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ дадуть нульовий результат напіврізниці $\mu_i^{(\gamma,\chi)^*}$. Для граничних непарних значень $\lambda_i^{(\gamma,\chi)} = 255$ ($\lambda_i^{(\gamma,\chi)} = 254$) і $\mu_i^{(\gamma,\chi)} = 1$ ($\mu_i^{(\gamma,\chi)} = 0$) напіврізність $\mu_i^{(\gamma,\chi)^*}$ дорівнює 127.

На другому каскаді організується обробка нових перевизначених значень проміжних матриць Λ^* та Θ^*. Причому, за рахунок зменшення динамічного діапазону значень $\mu_i^{(\gamma,\chi)^*}$ у ПДМ Θ^* до рівня $[0,127]$ забезпечується додаткове зменшення довжини ІС $E(\Theta^*) = \{E(\Theta^*)_{\alpha(\Theta^*)}\}$. Це відбувається за рахунок збільшення кількості $\Psi(\Theta^*)_{\alpha(\Theta^*)}$ елементів, що сформували одне КЗ $E(\Theta^*)_{\alpha(\Theta^*)}$, та зменшення кількості $\alpha(\Theta^*)_{\max}$ всіх КЗ.

Довжина ІС $E(\Lambda^*) = \{E(\Lambda^*)_{\alpha(\Lambda^*)}\}$ також зменшиться. Це при тому, що кодуванню піддаються не вихідні елементи $\lambda_i^{(\gamma,\chi)}$, а елементи $\lambda_i^{(\gamma,\chi)^*}$ із меншими значеннями. Дійсно:

$$\lambda_i^{(\gamma,\chi)} \geq \lambda_i^{(\gamma,\chi)^*} = \frac{\lambda_i^{(\gamma,\chi)} + \mu_i^{(\gamma,\chi)}}{2}.$$

У результаті у формуванні кожного окремого КЗ $E(\Lambda^*)_{\alpha(\Lambda^*)}$ приймає участь більша кількість $\Psi(\Lambda^*)_{\alpha(\Lambda^*)}$ елементів $\lambda_i^{(\gamma,\chi)^*}$, а кількість $\alpha(\Theta^*)_{\max}$ всіх КЗ зменшується.

Для уніфікації процесів ККК на другому каскаді обробки ПДМ $\Lambda^* = \{\lambda_i^{(\gamma,\chi)^*}\}$ та $\Theta^* = \{\mu_i^{(\gamma,\chi)^*}\}$ будемо розглядати, як не перевизначені, а саме Λ та Θ. Зберігання, сформованих за допомогою виразів (5)–(8), елементів максимальних $\lambda(\max)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ та мінімальних $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\min)^{(\gamma,\chi)}$ значень у матрицях $\Lambda(\max) = \{\lambda(\max)^{(\gamma,\chi)}\}$, $\Theta(\max) = \{\mu(\max)^{(\gamma,\chi)}\}$, $\Lambda(\min) = \{\lambda(\min)^{(\gamma,\chi)}\}$ та $\Theta(\min) = \{\mu(\min)^{(\gamma,\chi)}\}$ СС КККдг організується у

вихідному вигляді. При цьому з урахуванням обробки на першому каскаді кодування елементи матриць $\Lambda(\max) = \{\lambda(\max)^{(\gamma,\chi)}\}$ і $\Lambda(\min) = \{\lambda(\min)^{(\gamma,\chi)}\}$ змінюються у діапазоні $[0, 255]$ та вимагають для свого зберігання 8 розрядів. А елементи матриць $\Theta(\max) = \{\mu(\max)^{(\gamma,\chi)}\}$ і $\Theta(\min) = \{\mu(\min)^{(\gamma,\chi)}\}$ змінюються у діапазоні $[0, 127]$ та вимагають для свого зберігання 7 розрядів. Це забезпечує зменшення обсягу СС на 6,25%.

Якщо вибрано схему зберігання значень елементів $\lambda(\max)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ СС у вигляді напівсум та напіврізниць, то проміжні значення максимальних $\lambda_i^{(\gamma,\chi)}$ та мінімальних $\mu_i^{(\gamma,\chi)}$ елементів зберігаються у вихідному форматі.

При цьому обробка на першому та другому каскаді кодування не змінюється. Зберігання елементів СС, сформованих за допомогою виразів (5)–(8), організується за допомогою відповідних формул:

$$\lambda(\max)^{(\gamma,\chi)^*} = \frac{\lambda(\max)^{(\gamma,\chi)} + \lambda(\min)^{(\gamma,\chi)}}{2}, \quad (30)$$

$$\mu(\max)^{(\gamma,\chi)^*} = \frac{\mu(\max)^{(\gamma,\chi)} + \mu(\min)^{(\gamma,\chi)}}{2}, \quad (31)$$

$$\lambda(\min)^{(\gamma,\chi)^*} = \frac{\lambda(\max)^{(\gamma,\chi)} - \lambda(\min)^{(\gamma,\chi)}}{2}, \quad (32)$$

$$\mu(\max)^{(\gamma,\chi)^*} = \frac{\mu(\max)^{(\gamma,\chi)} - \mu(\min)^{(\gamma,\chi)}}{2}. \quad (33)$$

Значення елементів матриць $\Lambda(\max)^*$ і $\Theta(\max)^*$, що сформовані за допомогою виразів (30) та (31), змінюються в діапазоні $[0, 255]$ та вимагають для свого зберігання 8 розрядів. А значення елементів матриць $\Lambda(\min)^*$ і $\Theta(\min)^*$, що сформовані за допомогою виразів (32) та (33), змінюються в діапазоні $[0, 127]$ та вимагають для свого зберігання 7 розрядів. Все це так само, як і в попередньому варіанті схеми зберігання, забезпечує зменшення обсягу СС на 6,25%.

У процесі декодування ККККдг організується відновлення значень мінімальних та максимальних елементів з їх представлень у вигляді напівсум та напіврізностей тільки перед виконанням тих каскадів, на яких дане зберігання (перевизначення значень) було організовано. При цьому процес декодування не змінюється. Так, при декодуванні ІС ККККдг, отриманих на другому каскаді кодування, відновлення елементів матриць $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ і $\Theta(\min)$ СС, якщо вони були представлені у вигляді напівсум та напіврізностей за допомогою формул (30)–(33), здійснюється з використанням відповідних виразів:

$$\lambda(\max)^{(\gamma,\chi)} = \lambda(\max)^{(\gamma,\chi)^*} + \lambda(\min)^{(\gamma,\chi)^*},$$

$$\lambda(\min)^{(\gamma,\chi)} = \lambda(\max)^{(\gamma,\chi)^*} - \lambda(\min)^{(\gamma,\chi)^*},$$

$$\mu(\max)^{(\gamma,\chi)} = \mu(\max)^{(\gamma,\chi)^*} + \mu(\min)^{(\gamma,\chi)^*},$$

$$\mu(\max)^{(\gamma,\chi)} = \mu(\max)^{(\gamma,\chi)^*} - \mu(\min)^{(\gamma,\chi)^*}.$$

При декодуванні КЗ E_α ІС $E = \{E_\alpha\}$, отриманого на першому каскаді кодування, для відновлення елементів проміжних матриць Λ і Θ, якщо вони були представлені у вигляді напівсум та напіврізностей за допомогою формул (22)–(23), використовуються такі вирази:

$$\lambda_i^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)^*} + \mu_i^{(\gamma,\chi)^*},$$

$$\mu_i^{(\gamma,\chi)} = \lambda_i^{(\gamma,\chi)^*} - \mu_i^{(\gamma,\chi)^*}.$$

В результаті декодування КЗ E_α будуть реконструйовано елементи, значення яких відповідатимуть значенням елементів з навмисно внесеною помилкою $a_{i,j}^{(\gamma,\chi)^*}$.

В даному варіанті зберігання елементів СС забезпечується зменшення вихідного обсягу ККККдг. Однак, воно забезпечується за рахунок внесення навмисної помилки у вихідні дані та збільшення кількості математичних операцій у процесі кодування.

4 Порівняльне оцінювання характеристик способів зберігання елементів службових складових

Приклад оцінки якості обробки сильнонасичених дрібними об'єктами відеоданих, розмірністю 512×512 елементів, при використанні різних способів зберігання елементів СС ККККдг зображень без втрати якості інформації представлений в Таблиці 1. Криптокомпресійні кодограми формувалися в умовах розбиття площин зображення на блоки розмірністю 8×8 елементів. У таблиці використовуються такі скорочення: k_{cor} – коефіцієнт кореляції; k_{compr} – коефіцієнт компресії.

З аналізу результатів експерименту можна зробити такі загальні висновки:

– у схемах зберігання елементів $\lambda_i^{(\gamma,\chi)}$ і $\mu_i^{(\gamma,\chi)}$ проміжних матриць Λ та Θ, а також елементів $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ СС $\Lambda(\max)$, $\Lambda(\min)$, $\Theta(\max)$ і $\Theta(\min)$ в процесі ККК у вихідному вигляді та у разі зниження динамічного діапазону максимальних значень $\lambda_i^{(\gamma,\chi)}$, $\lambda(\max)^{(\gamma,\chi)}$ і $\mu(\max)^{(\gamma,\chi)}$ не забезпечується зниження якості вихідних відеоданих. Однак, у випадку використання схеми зберігання проміжних значень $\lambda_i^{(\gamma,\chi)}$ у зниженому діапазоні у вигляді ($\lambda_i^{(\gamma,\chi)} - \mu_i^{(\gamma,\chi)}$) знижується ступінь стиснення відеоданих. При цьому обсяги СС ККККдг не змінюються. Тому з урахуванням схеми організації кодування та

декодування ККККдг для підвищення оперативності обробки рекомендується максимальні значення $\lambda(\max)^{(\gamma,\chi)}$ і $\mu(\max)^{(\gamma,\chi)}$ СС зберігати в зниженому діапазоні у вигляді $(\lambda(\max)^{(\gamma,\chi)}+1-\lambda(\min)^{(\gamma,\chi)})$ та $(\mu(\max)^{(\gamma,\chi)}+1-\mu(\min)^{(\gamma,\chi)})$. При цьому проміжні елементи $\lambda_i^{(\gamma,\chi)}$, сформовані на першому каскаді кодування, потрібно зберігати у вихідному вигляді. А оскільки зниження ступеня компресії у разі зберігання проміжних значень $\lambda_i^{(\gamma,\chi)}$ у зниженому діапазоні у вигляді $(\lambda_i^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)})$ є незначним і не перевищує 1%, то для підвищення оперативності кодування/декодування на першому каскаді кодування може додатково використовуватися запропонована схема зберігання ПДМ, саме у вигляді $(\lambda_i^{(\gamma,\chi)}-\mu_i^{(\gamma,\chi)})$ або $(\lambda_i^{(\gamma,\chi)}+1-\mu_i^{(\gamma,\chi)})$;

– у випадках зберігання проміжних елементів $\lambda_i^{(\gamma,\chi)}$, $\mu_i^{(\gamma,\chi)}$ або елементів $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ СС у вигляді напівсуми та напіврізниці організується примусове зниження якості вихідних зображень. Воно є незначним. Якість реконструйованих зображень перевищує якість відеоданих після кольорового перетворення YCbCr або YUV. Навмисне внесення помилок у вихідні відеодані для формування парних і непарних значень елементів СС забезпечує однаковий рівень якості реконструйованих зображень. Він знаходиться на рівні, коли значення RSME не перевищує 0,37, значення пікового співвідношення сигналу до шуму (PSNR) не нижче 56,5 dB, а значення коефіцієнта кореляції становить 0,99997. Спотворенню піддаються в середньому до 13,35% елементів вихідних відеоданих з одиничною помилкою;

– схема зберігання проміжних елементів $\lambda_i^{(\gamma,\chi)}$, $\mu_i^{(\gamma,\chi)}$ у вигляді напівсум та напіврізниць на основі змішаного варіанта парних і непарних значень по рядках, організована на першому каскаді обробки, забезпечує якість реконструйованих зображень на рівні, коли значення RSME не перевищує 0,27, значення PSNR не нижче 60 dB, а значення коефіцієнта кореляції знаходиться на рівні 0,99999, що майже дорівнює 1. Спотворенню з одиничною помилкою піддаються у середньому до 6,7% елементів вихідних відеоданих. Дані показники якості перевершують варіанти зберігання значень в однотипному парному або непарному форматах;

– із аналізу різних варіантів схем зберігання проміжних елементів $\lambda_i^{(\gamma,\chi)}$, $\mu_i^{(\gamma,\chi)}$ або елементів $\lambda(\max)^{(\gamma,\chi)}$, $\lambda(\min)^{(\gamma,\chi)}$, $\mu(\max)^{(\gamma,\chi)}$ і $\mu(\min)^{(\gamma,\chi)}$ СС у вигляді напівсум та напіврізниць, видно, що схема зберігання, організована на першому каскаді кодування, є кращою. Вона забезпечує підвищення коефіцієнта компресії до 2% щодо схеми зберігання, організованої на другому каскаді кодування. При тому, що кількість операцій у процесі обробки та якість реконструйованих зображень залишається незмінною. Щодо варіантів зберігання елементів СС у вихідному вигляді та у разі зниження динамічного діапазону максимальних значень $\lambda_i^{(\gamma,\chi)}$, $\lambda(\max)^{(\gamma,\chi)}$ та $\mu(\max)^{(\gamma,\chi)}$ забезпечується підвищення коефіцієнта компресії до 2–3%. Як додатковий позитивний ефект, дані схеми забезпечують зниження обсягу СС ККККдг на 6,25%, що знижує обсяг даних, які вимагають забезпечення конфіденційності. Причому обсяг ІС також знизився.

Результати оцінки коефіцієнту компресії k_{compr} зображень різного ступеня насиченості для концептуального методу ККК зображень у диференційованому базисі при зберіганні службових даних у вихідному форматі та у вигляді напівсуми та напіврізниці представлені на Рисунку 1. З аналізу даних на Рисунку 1 видно, що найкращий результат за ступенем стиснення зображень показав концептуальний метод ККК зображень при зберіганні службових даних у вигляді напівсуми та напіврізниці.

Табл. 1 Оцінка якості обробки сильнонасичених відеоданих у різних способах зберігання елементів службових складових

Варіант схеми	Показники якості обробки				
	RSME	PSNR, dB	k_{cor}	k_{compr} 1 каскад	k_{compr} 2 каскад
Вихідні дані	0	–	1	–	1,079
Зниження динамічного діапазону максимальних значень	0	–	1	1,074	1,079
Напівсуми та напіврізниці:					
Парні значення	0,365	56,89	0,99997	1,106	1,091
Непарні значення	0,366	56,86	0,99997	1,106	1,091
Змішаний варіант	0,259	59,87	0,99999	1,102	–

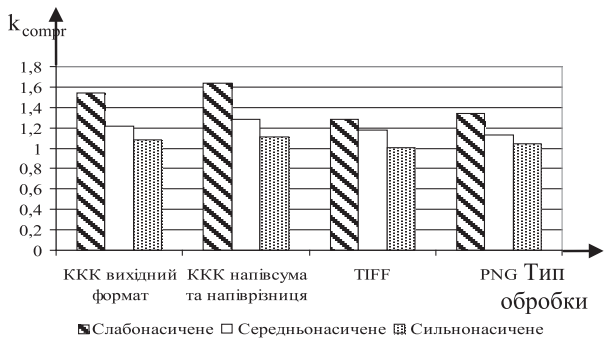
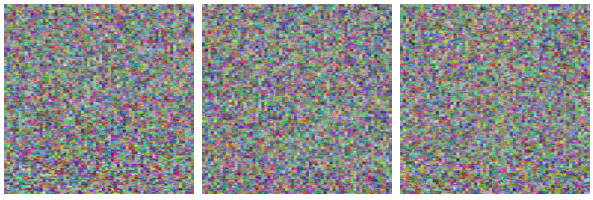


Рис. 1. Результати оцінки коефіцієнта компресії зображень для концептуального методу ККК зображень при $m = n = 8$

Результати оцінки якості забезпечення конфіденційності відеоданих на основі використання схеми ККК зображень із зашифрованими СС на третьому каскаді обробки представлені на Рисунку 2 та в Таблиці 2. На Рис. 2, а представлені вихідні тестові зображення [34]. На Рис. 2, б наведено результат реконструкції (декодування) КККдг зображень без розшифрування СС (варіант, коли зловмиснику не відомий ключ шифрування). Криптокомпресійні кодограми зображень сформовані з використанням розробленого методу зберігання СС.

(а)



(б)

Рис. 2. Приклади візуалізації реконструкції тестових зображень із зашифрованими СС в КККдг: (а) – вихідне зображення, (б) – реконструйоване зображення

З аналізу отриманих результатів можна зробити такі висновки:

– реконструйовані на основі зашифрованих СС зображення (Рисунок 2) повністю зруйновані. Вони практично стали схожі один до одного і не залежать від ступеня насиченості вихідних відеоданих;

– значення показників якості (Таблиця 2) повністю підтверджують результати візуальної оцінки про повне руйнування відеоданих. Для всіх типів зображень RSME знаходиться вище 80, PSNR – нижче 10 dB, а коефіцієнт кореляції – близький до 0;

– кількість пікселів NPCR, що змінюються (Таблиця 2), для всіх зображень знаходиться вище теоретичного порогового значення 99,5341% [35]. Це свідчить про високу стійкість зашифрованих відеоданих до диференціальних атак.

Табл. 2 Результати оцінки якості ККК тестових зображень із зашифрованими службовими складовими

Тестове зображення	Показники якості обробки			
	RSME	PSNR, dB	k_{cor}	NPCR, %
Baboon	88,68	9,17	0,0022	99,5743
Lena	91,12	8,94	-0,0012	99,5981
Аеропорт	84,38	9,61	-0,0103	99,6094

Висновки

Запропоновані три способи зберігання елементів СС КККдг зображень, а саме:

– у вихідному вигляді їх подання, як мінімальні та максимальні значення, що в залежності від каскаду обробки визначаються у напрямку по рядках або по стовпцях оброблюваних блоків відеоданих;

– за умови зниження динамічного діапазону максимальних значень та не зміні способу зберігання мінімальних значень. Як варіант, тут пропонується організувати зберігання максимальних елементів на другому каскаді обробки у зниженому динамічному діапазоні на величину мінімального значення за умови збільшення значення результату на один. При цьому проміжні дані, сформовані на першому каскаді кодування, пропонується зберігати у вихідному вигляді. Цей спосіб зберігання дозволить підвищити оперативність обробки;

– у варіантах зберігання проміжних елементів або елементів службових складових у вигляді напівсуми та напіврізниці.

Для реалізації третього способу зберігання елементів СС розроблено метод, який організує примусове зниження якості вихідних зображень. Зниження якості організується за рахунок внесення помилки у вихідні відеодані для формування парних і непарних значень елементів СС в межах усієї площини зображення, окремих її блоків або для кожного рядка блоку окремо. Воно є незначним. Якість реконструйованих зображень перевищує якість відеоданих після кольорового перетворення YCbCr або YUV. Навмисне внесення помилок у вихідні відеодані для формування парних і непарних значень елементів СС забезпечує однаковий рівень якості реконструйованих зображень. Він знаходиться на рівні, коли значення RSME не перевищує 0,37, значення PSNR не нижче 56,5 dB, а значення коефіцієнта кореляції становить 0,99997. Спотворенню піддаються в середньому до 13,35% елементів вихідних відеоданих з одиничною помилкою. Позитив-

ним ефектом від реалізації розробленого методу є підвищення конфіденційності кодограм за рахунок порушення взаємозв'язку між елементами службових даних, підвищення коефіцієнту компресії до 2–3% та зниження обсягу службових складових кодограм на 6,25%. Це знижує обсяг даних, які потребують забезпечення конфіденційності.

References

[1] Schneier B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. *Wiley*, 784 p.

[2] Ramakrishnan S. (2018). Cryptographic and Information Security Approaches for Images and Videos. *CRC Press, Taylor & Francis Group*, 962 p. doi:10.1201/9780429435461.

[3] Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197 (2001). *Defense Technical Information Center*.

[4] Information technology – JPEG 2000 image coding system: Secure JPEG 2000. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807. (2007). 108 p.

[5] Dufaux F., Ebrahimi T. (2006). Toward a Secure JPEG. *Applications of Digital Image Processing XXIX* , Vol. 6312. DOI: 10.1117/12.686963.

[6] Miano J. (1999). *Compressed image file formats: JPEG, PNG, GIF, XBM, BMP*. ACM Press/Addison-Wesley Publishing Co., 264 p.

[7] Joint Photographic Experts Group (JPEG). Information technology – digital compression and coding of continuous-tone still images: Requirements and guidelines. ISO/IEC 10918-1:1994, ITU/CCITT Recommendation T.81. (1992–2017). 182 p.

[8] Sharma R., Bollavarapu S. (2015). Data Security using Compression and Cryptography Techniques. *International Journal of Computer Application*, Vol. 117, № 14, pp. 15–18. DOI: 10.5120/20621-3342.

[9] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022. (2019). *Cisco*. 33 p.

[10] Cisco Annual Internet Report (2018–2023). (2020). *Cisco*. 35 p.

[11] Yuan L., Korshunov P., Ebrahimi T. (2015). Secure JPEG Scrambling enabling Privacy in Photo Sharing. *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, pp. 1-6. DOI: 10.1109/FG.2015.7285022.

[12] Wong, K.-W. (2009). Image Encryption Using Chaotic Maps. In: Kocarev, L., Galias, Z., Lian, S. (eds) Intelligent Computing Based on Chaos. Studies in Computational Intelligence, Vol. 184. *Springer*. doi: 10.1007/978-3-540-95972-4_16.

[13] Phatak A.G. (2016). A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*, Vol. 8, № 6, pp. 64–71. DOI: 10.5815/ijigsp.2016.06.08.

[14] Yang Y., Zhu B., Li S., Yu N. (2007). Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, Iss. 1, 13 p. DOI:10.1186/1687-417X-2007-056365.

[15] Chen Ch., Wu W. (2014). A secure Boolean-based multi-secret image sharing scheme. *Journal of Systems and Software*, Vol. 92, pp. 107–114. DOI: 1016/j.jss.2014.01.001.

[16] Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. (2012). Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. *IEEE International Carnahan Conference on Security Technology ICCST*, pp. 135–139. DOI: 10.1109/CCST.2012.6393548.

[17] Tverdokhlib V., Zakomorna K., Dvukhglavov D., Oleksin O., Zhuikov D., Kryvonos V. (2021). Technology Increasing Capacity Protected Channel Delivery Video Data Telecommunication Systems Critical Infrastructure. *IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, pp. 57-60. DOI: 10.1109/ATIT54053.2021.9678736.

[18] Dick K., Russell L., Dosso Y., Kwamena F., Green J. (2019). Deep Learning for Critical Infrastructure Resilience. *Journal of Infrastructure Systems*, Vol. 25, Iss. 2, 11 p. DOI: 10.1061/(ASCE)IS.1943-555X.0000477.

[19] Isern J., Barranco F., Deniz D., Lesonen J., Hannuksela J., Carrillo R. (2020). Reconfigurable cyber-physical system for critical infrastructure protection in smart cities via smart video-surveillance. *Pattern Recognition Letters*, Vol. 140, pp. 303-309. DOI: 10.1016/j.patrec.2020.11.004.

[20] Gonzalez R., Woods R. (2018). *Digital Image Processing*. Pearson, 1168 p.

[21] Salomon D. (2007). *Data Compression: The Complete Reference*. Springer, 1092 p.

[22] Gore A, Gupta S. (2015). Full reference image quality metrics for JPEG compressed images. *AEU – International Journal of Electronics and Communications*, Vol. 69, Iss. 2, pp. 604–608. DOI: 10.1016/j.aeue.2014.09.002.

[23] Cogranne R. (2018). Determining JPEG Image Standard Quality Factor from the Quantization Tables, 6 p. *Cornell University*.

[24] Wu Yu., Agaian S., Noonan J. (2012). Sudoku Associated Two Dimensional Bijections for Image Scrambling. *Cornell University*.

[25] Auer S., Bliem A., Engel D. et al. (2013). Bitstream-based JPEG Encryption in Real-time. *International Journal of Digital Crime and Forensics*, Vol. 5, Iss. 3, pp. 1-14. DOI: 10.4018/jdcf.2013070101.

[26] Minemura K., Moayed Z., Wong K. et al. (2012). JPEG image scrambling without expansion in bitstream size. *2012 19th IEEE International Conference on Image Processing*, pp. 261–264. DOI: 10.1109/ICIP.2012.6466845.

[27] Barannik V., Sidchenko S., Barannik D. (2020). Technology for Protecting Video Information Resources in the Info-Communication Space. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, pp. 29–33. DOI: 10.1109/ATIT50783.2020.9349324.

[28] Alimpiev A., Barannik V., Sidchenko S. (2017). The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. *Telecommunications and Radio Engineering*, Vol. 76, № 6, pp. 521–534. DOI: 10.1615/TelecomRadEng.v76.i6.60.

[29] Barannik V., Sidchenko S., Barannik N., Barannik V. (2021). Development of the method for encoding service data in cryptocompression image representation systems. *Eastern-European Journal of Enterprise Technologies*, Vol. 3, № 9(111), pp. 103–115. DOI: 10.15587/1729-4061.2021.235521.

[30] Barannik V., Sidchenko S., Barannik D., Shulgin S., Barannik V., Datsun A. (2021). Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. *Eastern-European Journal of Enterprise Technologies*, Vol. 4, № 2(112), pp. 6–17. DOI: 10.15587/1729-4061.2021.237359.

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

[32] Barannik V., Sidchenko S., Barannik N., Khimenko A. (2021). The method of masking overhead compaction in video compression systems. *Radioelectronic and Computer Systems*, No. 2, pp. 51–63. DOI: 10.32620/reks.2021.2.05.

[33] Barannik V., Sidchenko S., Barannik D., Barannik V., Hurzhii I., Babenko Y. (2021). Evaluating of the Resistance of Crypto-Compression Image Codograms to Errors in the Data Transmission Channel. *2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, pp. 52–56. DOI: 10.1109/ATIT54053.2021.9678774.

[34] School of Electronic Engineering and Computer Science. ECS605U/ECS776P – Image Processing. *http://www.eecs.qmul.ac.uk/ phao/IP/Images/*.

[35] Wu Y., Noonan J. P., Agaian S. (2011). NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, pp. 31–38.

Saving Elements Methods for Service Components of Images Cryptocompression Codograms

Barannik V. V., Sidchenko S. O., Barannik D. V., Chornomaz I. K., Hurzhii P. M., Grygorian M. B.

The article substantiates the requirements for the quality characteristics of the video information resource in the case of its use for information support of the functioning of critical infrastructure systems. At the same time, requirements are put forward regarding: timeliness of delivery and confidentiality of video information under conditions of a given level of its integrity and completeness. It is shown that, in part, such requirements are due to the intellectualization of individual stages of the process of analysis and decision-making in critical infrastructure systems. System justification for the existence of problematic issues is provided, which include: imbalance between the levels of productivity of information communication systems and the bit intensity of video information streams. Compression coding technologies are used to reduce this imbalance. They allow you to reduce the bit volume of video data. However, they do not provide the required level of information privacy by themselves. This proves the relevance of the scientific and applied problem regarding the need to ensure the required level of promptness of delivery of confidential information using wireless information communication technologies in critical infrastructure systems.

The article shows that the direction of solving the existing problem is the creation and application of coding technologies that allow ensuring the confidentiality of video information in the process of reducing redundancy. At the same time, one of the representatives of this class of methods are those built on the basis of cryptocompression coding technologies. A service information system is being formed for such technologies. On the one hand, this creates conditions for ensuring the confidentiality of video information in the process of reducing its bit volume. On the other hand, there is a destructive effect on restraining the growth of the compression ratio. Hence, the purpose of the article is to develop a method of storing the elements of service components of cryptographic codegrams.

Three methods of storing service components of cryptographic codegrams of images are proposed. The first consists in storing service data in the form of minimum and maximum values. The second method involves reducing the dynamic range of maximum values. The third method involves storing intermediate elements or elements of service components in the form of a half-sum and a half-difference. To implement the third method of storing elements of service data, a method has been developed that organizes a forced reduction in the quality of output images. The reduction in quality is organized by introducing an error into the source images to form even and odd values of the service data elements within the entire plane of the image, its individual blocks or for each line of the block separately. The peak signal-to-noise ratio (PSNR) of the reconstructed images is at least 56.5 dB, and the value of the correlation coefficient is 0.99997. A positive effect of the implementation of the developed method is an increase in the confidentiality of codegrams due to the violation of the relationship between service data elements, an increase in the compression ratio to 2-3% and a decrease in the volume of service components of codegrams by 6.25%.

Keywords: compression; cryptocompression; encryption; image; information protection; privacy