ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.932.056.5

doi: 10.32620/reks.2021.2.06

Д. С. ГАВРИЛОВ[1], С. С. БУЧІК[2], Ю. М. БАБЕНКО[2], С. С. ШУЛЬГІН[1], О. В. СЛОБОДЯНЮК[3]

[1] ***Харківський національний університет радіоелектроніки, Украйна***
[2] ***Київський національний університет імені Тараса Шевченко, Украйна***
[3] ***Каменець-Подільський національний університет імені Івана Огієнкка, Украйна***

МЕТОД ОБРОБКИ ВІДЕОДАНИХ З МОЖЛИВІСТЮ ЇХ ЗАХИСТУ ПІСЛЯ КВАНТУВАННЯ

Предметом *досліджень в статті є процеси обробки відеозображення на основі JPEG-платформи для передачі даних у інформаційно-телекомунікаційній мережі.* ***Метою*** *є побудова методу обробки відеозображення з можливістю його захисту на етапі квантування з подальшим арифметичним кодуванням. Це дозволить при збереженні структурно – статистичної закономірності забезпечити необхідний рівень доступності, достовірності та конфіденційності при передачі відеоданих.* ***Завдання:*** *дослідження відомих методів селективної обробки відеозображення з подальшою формалізацією процедури обробки відеозображення на етапі квантування та статистичному кодуванні значимих блоків на основі JPEG-платформи. Використовуваними* ***методами*** *є: алгоритм на основі JPEG-платформи, методи селекції значимих інформативних блоків, арифметичне кодування. Отримані такі* ***результати.*** *Розроблено метод обробки відеозображення з можливістю його захисту на етапі квантування з подальшим арифметичним кодування. Це дозволить при збереженні структурно-статистичної закономірності виконати поставлені вимоги по доступності, достовірності та конфіденційності передачі відеоданих. Забезпечення необхідного рівеня доступності пов'язане зі зменшенням об'єму відеозображення на 30 % у порівнянні з вихідним об'ємом. При цьому, забезпечення необхідного рівня достовірності підтверджується оцінкою пікового відношення сигнал/шум для авторизованого користувача, який складає* $\mathrm{PSNR}_{\text{авт}} \geq 20$ *дБ. Забезпечення необхідного рівня конфіденційності підтверджується оцінкою пікового відношення сигнал/шум при несанкціонованому доступі, який складає* $\mathrm{PSNR}_{\text{нсд}} \leq 9$ *дБ.*

Висновки. *Наукова новизна отриманих результатів полягає в наступному: вперше запропоновано два методи обробки відеозображення на етапі квантування. Варто зазначити, що запропоновані підходи виконують поставлені завдання по забезпеченню необхідного рівня конфіденційності при заданому рівні достовірності. При цьому, метод використання шифрувальних таблиць має вищій рівень криптографічної стійкості ніж метод використання матриці-ключа. Це обумовлено більш складним математичним апаратом. Це свою чергу, це призводить до збільшення часу на обробку даних.З метою виконання вимоги доступності даних запропоновано використовувати арифметичне кодування для інфоормативних блоків, це має вищу ефективність у порівнянні з методами кодових таблиць. Отже, метод використання шифрувальних таблиць має більшу криптографічну стійкість, а метод використання матриці-ключа більшу швидкодію. При цьому, використання арифметичного кодування задовольнить потребу у доступності за рахунок зменшення початкового об'єму.*

Keywords: *квантування; доступність; криптографічний захист; достовірність; обробка даних.*

Вступ

У зв'язку зі збільшенням кількості мобільних пристроїв збирання, обробки, зберігання та передачі даних кількість прийнятих рішень за одиницю часу постійно зростає. При цьому, ефективність прийнятого рішення що залежить від рівня достовірності та конфіденційності зменшується. Під ефективністю прийнятого рішення розуміємо показник, що визначає рівень досягнення поставленої мети після сформованого і доведеного до виконавця рішення. Тож, в останні роки збільшилися вимоги щодо забезпечення конфіденційності та достовірності відеозображень. Приклад технологій, що направлені на вирішення даних вимог розглядаються в працях вчених [1 – 6], а саме:

- технологія на основі використання стандартизованих криптографічних алгоритмів на різних етапах синтаксичного представлення відеозображень [2, 6, 7].

- технологія, що враховує механізми переміщування декількох відеозображень [8 – 12]. Якщо про-

цес перемішування стосується окремих відеокадрів, тобто внутрішне перемішування, то дана технологія розглядається в таких працях, як [13 – 17] – без градієнтних перетворень та [17 – 20] – у разі додаткового використання масок масштабування відео сегментів.

Найбільш розповсюджений варіант таких двох технології - це класична послідовна реалізація компресії та захисту інформації [21 – 23]. Саме послідовна концепція компресії та захисту відеоінформації з використанням методів JPEG реалізовані в праці [24], а із застосуванням методів JPEG 2000 в праці [25]. Їх різні реалізації наводяться відповідно в працях [26 – 32] та [33 – 35].

- технологія щодо захисту інформації в системах селективної обробки полягає у її прихованні. Тут використовуються особливості відеозображень перш за все обумовлені їх аналоговою природою походження. Приклади таких методів розглядаються та досліджуються в працях [36 – 39].

В той же час загальний недолік таких методів полягає у пропуску ключової інформації відеозображень в процесі обробки. Отже, це призводить до виникнення втрат інформації, значних часових затримок на обробку, або до зменшення величини коефіцієнта компресія. Отже, існує проблематика забезпечення необхідного рівня доступності, достовірності та конфіденційності даних в системах обміну інформацією. За основу пропонується використовувати алгоритм JPEG у зв'язку з широкою популярністю та ефективністю його робити.

Дослідження публікацій [40 – 42] вказало на актуальність науково-прикладної задачі забезпечення необхідного рівня доступності, достовірності та конфіденційності даних в системах обміну інформацією. Для вирішення цієї задачі пропонується використовувати селективну технологію. Під селективною технологією розуміємо процес виявлення і подальшу обробку значущих складових відеокадру в процесі його кодування і побудови формату. Переваги селективної технології на етапі колірного перетворення полягають в наступному:

- не потрібно додатково витрачати час на виявлення значимої інформації в складовій яскравості, адже вся компонента яскравості вважається значимою і виділена в ході колірного перетворення;

- у разі потреби забезпечення конфіденційності зображення необхідним є вилучання компоненти яскравості з процесу обробки алгоритмом на основі JPEG-платформи. При цьому, рівень достовірності також збільшиться. В свою чергу, час на обробку цієї компоненти буде прямувати до нуля.

Недоліки селективної технології на етапі колірного перетворення полягають в наступному:

- у разі потреби забезпечення конфіденційності зображення, об'єм вихідних даних після селективної обробки збільшиться у порівнянні з об'ємом вихідних даних після алгоритму на основі JPEG – платформи. При цьому, об'єм колірних компонент після селективної обробки залишається без змін. У зв'язку з цим середній час доведення компоненти яскравості значно більший за середній час на доведення хроматичних компонент.

- відсутня оцінка блоків компоненти яскравості на предмет значимості. Таким чином, має місце надлишковий вплив на всю компоненту яскравості, замість впливу лише на блоки інтересу; можливість отримання несанкціонованим користувачем значимої інформації при аналізі колірних.

Переваги методу селективної обробки Баранніка – Комолова [40, 41]:

- основна енергетика міститься в низькочастотних компонентах, що дозволяє при обробці лише низькочастотних компонентах зруйнувати основні візуальні ознаки об'єктів зображення, замість впливу на всю трансформанту:

- визначення низькочастотних компонент як значимих з подальшою обробкою має незначний вплив на вихідний об'єм даних;

- зменшення частки надлишкової обробки даних. Це відбувається за рахунок наявності системи класифікації блоків по рівню насиченості (слабо, середьо, сильнонасичений). Це дозволяє дозовано визначити кількість низькочастотних елементів трансформанти, які є значимими і потребують подальшої обробки.

Недоліки методу селективної обробки Баранніка–Комолова [40, 41]:

- збільшення часу на обробку трансформанти на етапі дискретного косинусного перетворення. За рахунок складного математичного апарату та наявності класифікації блоків за рівнем насиченості;

- відсутня чітка границя між низькими і середніми частотами. Це ускладнює процес виявлення значимих компонент і відноситься до всіх подібних методів.

Основним недоліком перших двох етапів є руйнування структурно – статистичної закономірності трансформанти. Часткове усунення недоліків перших двох етапів можливе на етапі квантування.

Отже, **мета статті** полягає у розробленні технології обробки відеозображення з можливістю його захисту на етапі квантування з подальшим арифметичним кодуванням. Це створює умови для збереження структурно-статистичних закономірностей та для забезпечення необхідного рівеня доступності, достовірності, та конфіденційності відеоданих.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Аналіз підходів до обробки даних

Процес квантування включає в себе ділення робочої матриці після дискретного косинусного перетворення на матрицю квантування [9, 10]. Саме на даному етапі відбуваються найбільші втрати інформації за рахунок усунення психовізуальної надмірності, яка включає в себе контурно-текстурну і змістову надмірність. Варто зазначити, що достовірність відеоданих визначається матрицею квантування. Оскільки, після процесу квантування значимою інформацією є вся квантована трансформанта застосування селективної технології неможливе.

Також, після процесу квантування відеозображення отримало необхідний рівень достовірності і важливим є збереження можливості його відтворення на приймальній стороні.

При цьому, з метою забезпечення необхідного рівня конфіденційності можливо два варіанта технологій обробки даних, що представлені на рис. 1.

Перша технологія полягає у поелементному впливі на квантовану трансформанту з метою зміни значень за відомим лише авторизованому користувачу математичним апаратом. При цьому, перетворення має бути зворотним для відтворення початкових даних на приймальній стороні.

Друга технологія полягає у приведенні елементів квантованої матриці до єдиного значення. Для даної технології характерним є побудова матриці – ключа за допомогою якої на прийомній стороні можливе відтворення квантованої трансформанти. Процес відтворення значень квантованої трансформанти на прийомній стороні після обробки з матрицею-ключем представлено на рис. 2. Узагальнена зворотна обробка запропонованих технологій обробки відеоданих на основі алгоритмів JPEG – платформи представлено на рис. 3.

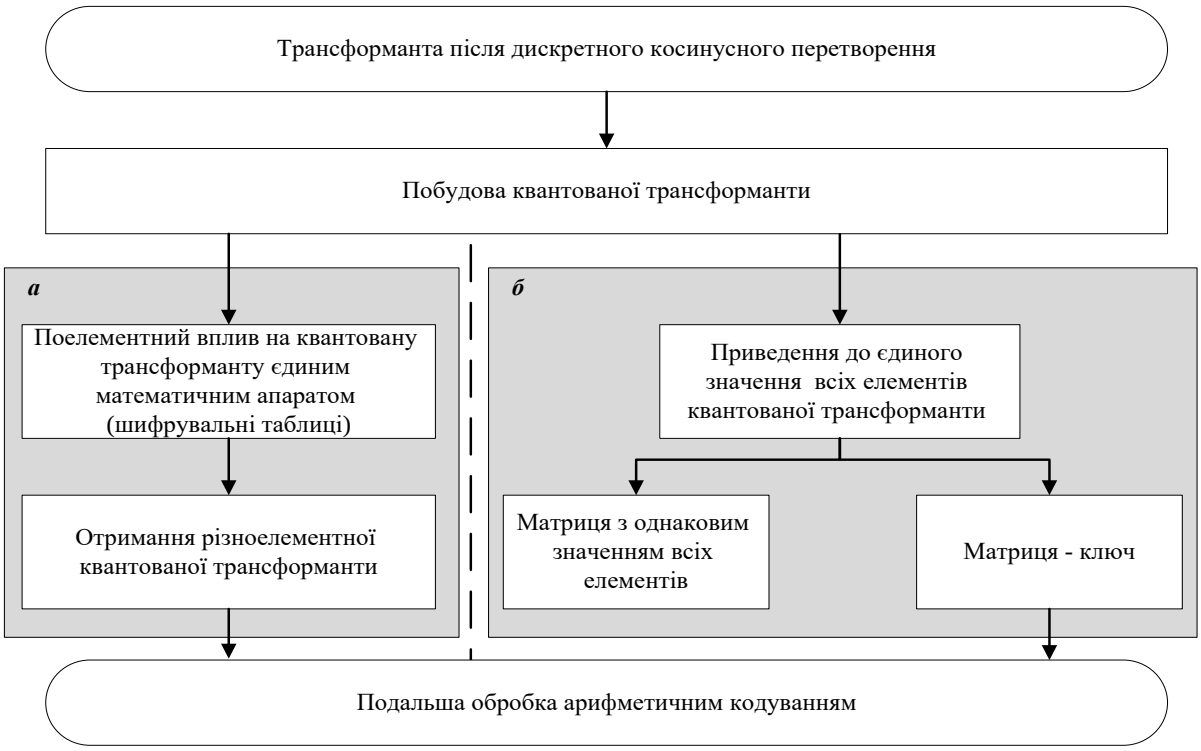


Рис. 1. Можливі варіанти технології обробки відеоданих на етапі квантування трансформанти: а) метод шифрувальних таблиць б) обробка з матрицею-ключем

Рис. 2. Схема відновлення значень квантованої трансформанти на прийомній стороні після обробки з матрицею-ключем

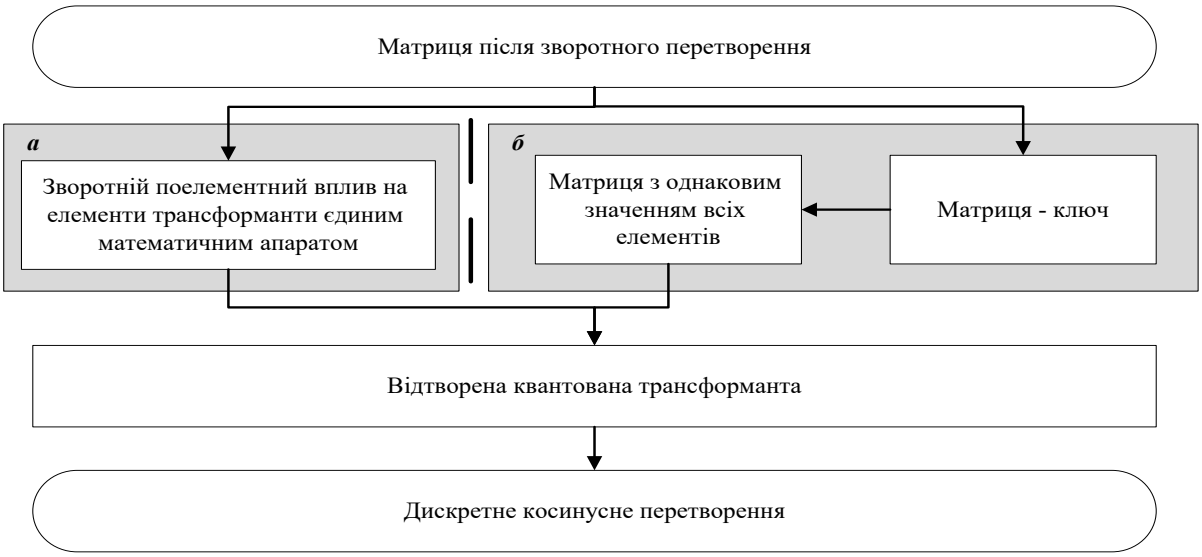


Рис. 3. Зворотна обробка відеоданих на етапі квантування трансформанти:
а) метод шифрувальних таблиць; б) обробка з матрицею-ключем

Переваги з позиції процесу обробки на етапі квантування полягають у наступному:

- усунення психовізуальної надмірності відеозображення, що створює умови для зменшення обсягу переданої інформації; не порушуються структурно - статистичні закономірності трансформанти. Отже, не порушується структура потоку JPEG;
- можливість додаткового криптографічного захисту таблиць квантування, що не впливає на втрату достовірності та часу доведення;
- використання шифрувальних таблиць чи матриці-ключа, забезпечить необхідний рівень конфіденційності.

Порівняльна оцінка методів

Порівняльну оцінку запропонованих технологій проведемо, дослідивши їх криптографічну стійкість та достовірність. Для кількісної оцінки достовірності та конфіденційності пропонується використовувати пікове відношення сигнал/шум:

$$PSNR = 20\lg(255/\sigma_A) \text{ (дБ)},$$

де σ_A – середньоквадратичне відхилення значень пікселів відновленого зображення щодо початкового, яке визначається на основі наступної формули:

$$\sigma_A = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij} - a'_{ij})^2 / m \times n}\ .$$

де a_{ij}, a'_{ij} – елементи відповідно початкового і відновленого зображень на приймальній стороні;

$m \times n$ – відповідно кількість рядків і стовпців в кадрі зображення.

При цьому слід зауважити, що низька якість зображення обумовлює незначну величину пікового відношення сигнал/шум $PSNR$, і як наслідок, зниження ймовірності прийняття ефективного рішення в процесі управління об'єктами критичної інфраструктури. Таким чином, для виконання вимоги достовірності пікове відношення сигнал/шум $PSNR_{авт}$ для авторизованого користувача має бути більше, ніж необхідне $PSNR_{необ.авт}$ значення пікового відношення сигнал/шум:

$$PSNR_{авт} \geq PSNR_{необ.авт} \text{ (дБ)}.$$

Відповідно, для забезпечення умов щодо конфіденційного доведення даних до користувача необхідне виконання умови, що пікове відношення сигнал/шум $PSNR_{нсд}$ при несанкціонованому доступі має бути нижчим допустимого $PSNR_{доп.нсд}$ пікового відношення сигнал/шум для несанкціонованого користувача:

$$PSNR_{нсд} \leq PSNR_{доп.нсд} \text{ (дБ)}.$$

В графічному вигляді порівняльна оцінка запропонованих технологій представлена на рис. 4. Дані отримані в результаті експериментальної обробки реалістичних зображнь з використанням програмних моделей створених технологій. Аналіз діаграм на рис. 4 вказує, що запропоновані технології задовольняють вимозі криптографічного доведення даних при заданому рівні достовірності. При цьому, технологія використання шифрувальних таблиць має вищій рівень криптографічної стійкості, ніж техно-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

логія використання матриці-ключа. Це обумовлено більш складним математичним апаратом. В свою чергу, це призводить до збільшення часу на обробку даних технологією шифрувальних таблиць.

Отже, технологія використання шифрувальних таблиць має більшу криптографічну стійкість, а технологія використання матриці-ключа більшу швидкодію.

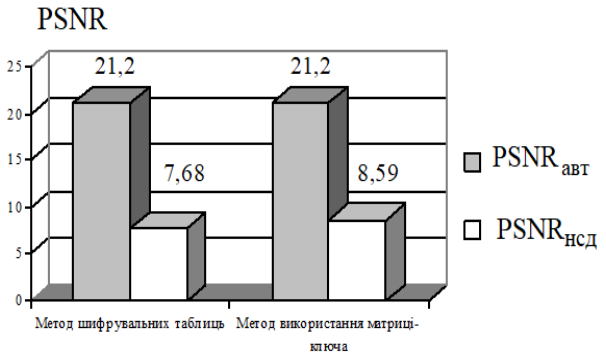


Рис. 4. Порівняльна оцінка запропонованих технологій

З метою зменшення вихідного об'єму пропонується застосовувати алгоритм арифметичного кодування (рис. 5) та декодування (рис. 6). Принцип даного алгоритму полягає у тому, що частоти символів, що поступають на вхід кодера, формуються перед початком процесу кодування та мають бути передані декодеру.

Довжина початкового потоку визначається за формулою:

$$\eta_i = \eta_i^{(0)} + \eta_i^{(1)} + \eta_i^{(w)},$$

де η_i – частота на і-му кроці, $\eta_i^{(0)}$ – частота «0» на і-му кроці, $\eta_i^{(1)}$ – частота «1» на і-му кроці, $\eta_i^{(w)}$ – частота «w» на і-му кроці;

Величина сегмента ρ_i на і-му кроці знаходиться за формулою:

$$\rho_i = \frac{h_i - l_i}{\eta_i},$$

Заключним етапом є знаходження кодового числа варіантом визначення середнього арифметичного числа між початком і кінцем робочого інтервалу останнього кодованого символу в повідомленні:

$$Z = \frac{l_i + h_i}{2},$$

де Z – кодове число повідомлення.

Застосування запропонованої технології в системах криптографічного захисту базується на тому, що:

- у зв'язку з важливістю значень частоти появи $\eta_i^{(w)}$ елемента «w» на і-му кроці можна зробити висновок, що дана інформація є ключовою. Вилучення чи заміна значень частоти появи $\eta_i^{(w)}$ елемента «w» на і-му кроці унеможливить коректне відтворення закодованої послідовності. При цьому варто відзначити, що величина частоти появи $\eta_i^{(w)}$ елемента «w» на кожному кроці рівна:

$$\eta_1^{(w)} = \eta_2^{(w)} = \eta_3^{(w)} = ... = \eta_i^{(w)}.$$

Дана особливість дає можливість вважати, що застосування криптографічних даних для значень частоти появи $\eta_i^{(w)}$ елемента «w» може збільшити ступінь захищеності даних;

- у зв'язку з необхідністю проходу для визначення частоти появи $\eta_i^{(w)}$ елемента «w» застосування методу арифметичного кодування збільшує час на обробку даних.

Для загального аналізу проведено оцінку ефективності алгоритму арифметичного кодування у системі криптографічного захисту інформації (рис.7).

Аналіз рис. 7 вказав на те, що арифметичне кодування є більш прийнятним рішенням для застосування в системах криптографічного захисту інформації у порівнянні з методами компресії на основі побудови таблиць кодування.

Висновки

Розроблено технологію обробки відеозображення з можливістю його захисту на етапі квантування з подальшим арифметичним кодуванням. Це дозволить при збереженні структурно – статистичної закономірності виконати поставлені вимоги. Забезпечення необхідного рівеня доступності пов'язане з використанням алгоритму арифметичногокодування. Результатом робити цього алгоритму є зменшенням об'єму відеозображення на 30 % у порівнянні з початковим об'ємом.

Забезпечення необхідного рівня достовірності підтверджується оцінкою пікового відношення сигнал/шум для авторизованого користувача, який складає $PSNR_{авт} \geq 20$ дБ. Забезпечення необхідного рівня конфіденційності підтверджується оцінкою

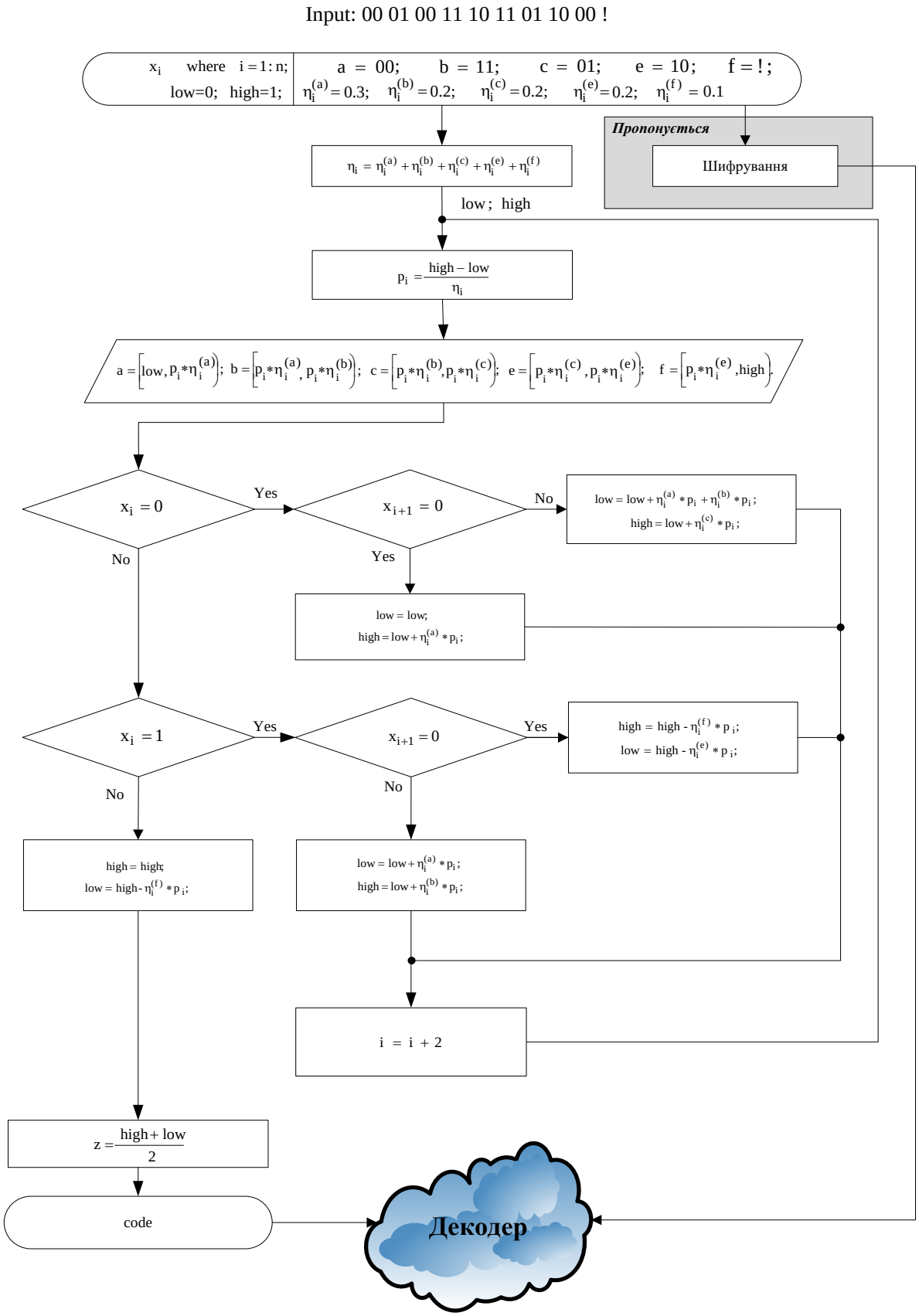
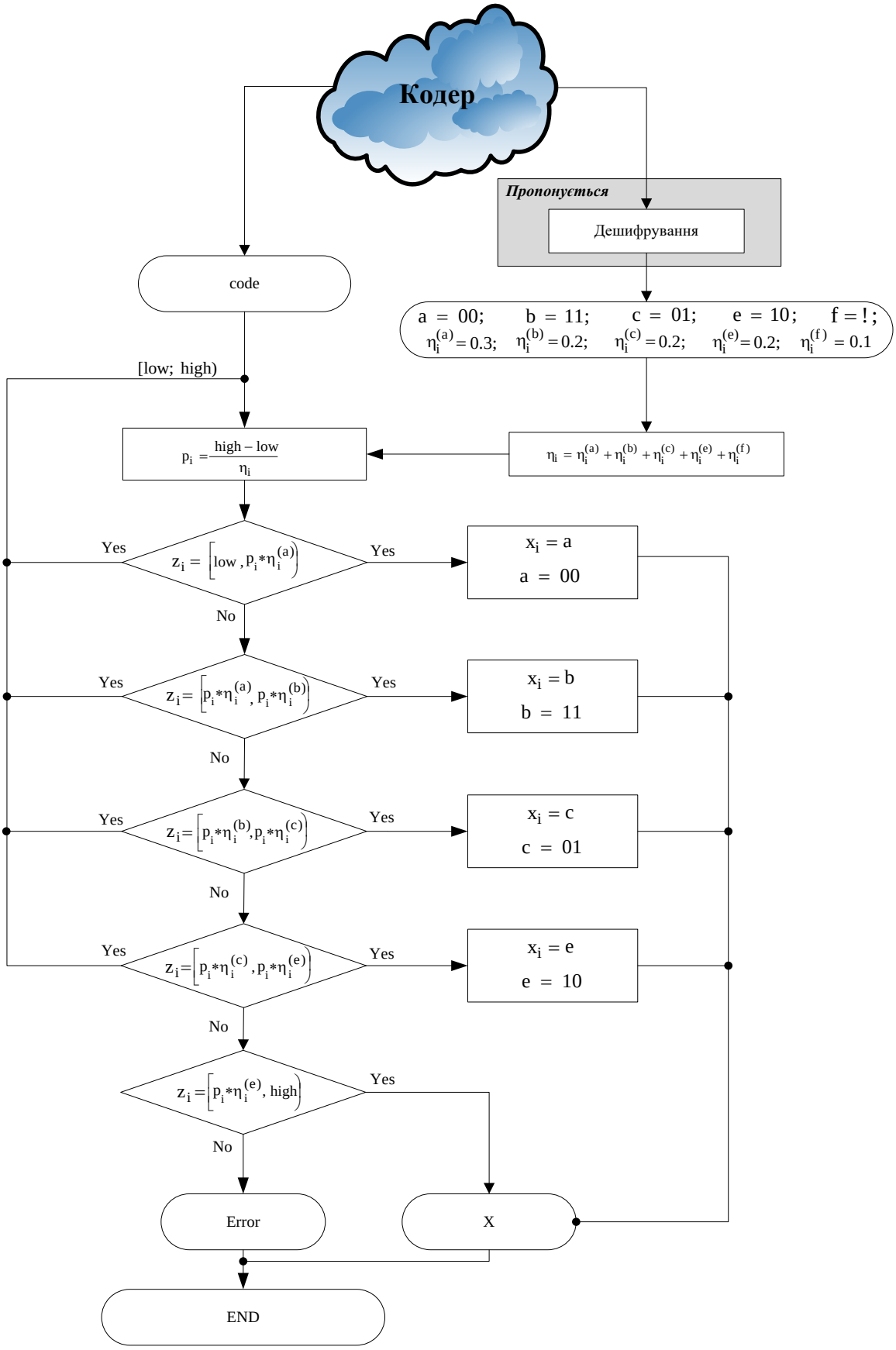


Рис. 5. Приклад роботи арифметичного кодування
для бінарної послідовності з маркером стопу “!”

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)



Output: 00 01 00 11 10 11 01 10 00

Рис. 6. Приклад роботи декодера арифметичного кодування для бінарної послідовності

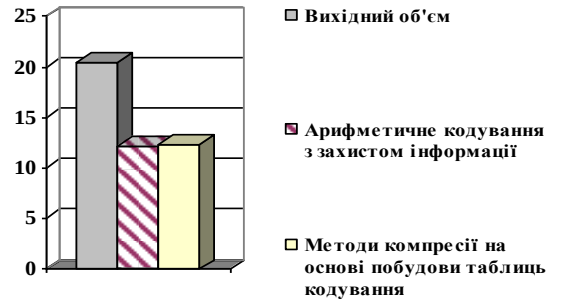


Рис. 7. Оцінка ефективності розробленої технології за критерієм вихідного об'єму

пікового відношення сигнал/шум при несанкціонованому доступі, який складає $PSNR_{нсд} \le 9$ дБ.

Вперше запропоновано два варіанта технології обробки відеозображення на етапі квантування. Це дозволить при збереженні структурно – статистичної закономірності забезпечити необхідний рівень доступності, достовірності та конфіденційності при передачі відеоданих.

Принцип обробки наближається до послідовної схеми. Дана особливість незначною мірою впливає на час доведення даних до користувача, оскільки обробка відбувається після основних етапів компресії. Адже, основна кількість надмірностей усунуто на етапах колірного перетворення, дискретного косинусного перетворення та за рахунок квантування.

Практична реалізація з використанням безпілотних літальних апаратів дає змогу зробити висновок що метод з використанням шифрувальних таблиць $PSNR_{МШТ} = 7{,}68$ має вищій рівень криптографічної стійкості за рахунок меншого співвідношення сигнал/шум, ніж метод з використанням матриці-ключа $PSNR_{ММК} = 8{,}59$. Це обумовлено більш складним математичним апаратом. В свою чергу, це призводить до збільшення часу на обробку даних.

Тож, мета статті по забезпечинню необхідного рівеня доступності, достовірності та конфіденційності при передачі відеоданих вважається досягнутою.

Література

1. JPEG Privacy & Security Abstract and Executive Summary [Electronic resource]. – 2015. – Access mode: https://jpeg.org/items/20150910_privacy_ security_summary.html. – 7.04.2021.

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

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

4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 2015-07-01. – Київ : Мінекономрозвитку України, 2015. – 39 с.

5. Data Encryption Standard (DES) [Text]. – Federal Information Processing Standards Publication 46-3, 1999. – 26 p.

6. ДСТУ ГОСТ 28147:2009. Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89) [Текст]. – Введ. 2009-02-01. – Київ : Держспоживстандарт України, 2008. – 20 с.

7. Rivest, R. L. A method for obtaining digital signatures and public-key cryptosystems [Text] / R. L. Rivest, A. Shamir, L. M. Adleman // Communications of the ACM. – 1978. – Vol. 21, Iss. 2. – P. 120–126. DOI: 10.1145/359340.359342.

8. Barannik, V. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource [Text] / V. Barannik, Yu. Babenko, O. Kulitsa, V. Barannik, A. Khimenko, O. Matviichuk-Yudina // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). – 2020. – P. 52–56. DOI: 10.1109/ATIT50783.2020.9349256.

9. Chen, T.-H. Efficient multi-secret image sharing based on Boolean operation [Text] / T.-H. Chen, Ch.-S. Wu // Signal Processing. – 2011. – Vol. 91, Iss. 1. – P. 90–97. DOI: 10.1016/j.sigpro.2010.06.012.

10. Barannik, V. Methodological Fundamentals of Deciphering Coding of Aerophotography Segments on Special Equipment of Unmanned Complex [Text] / V. Barannik, S. Shulgin, A. Krasnorutsky, O. Slobodyanyuk, P. Gurzhii, N. Korolyova // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). – 2020. – P. 38–43. DOI: 10.1109/ATIT50783.2020.9349257.

11. Li, F. Two-step providing of desired quality in lossy image compression by SPIHT [Текст] / F. Li, S. Krivenko, V. Lukin // Радіоелектронні і комп'ютерні системи. – 2020. – №. 2(94). – С. 22-32. DOI: 10.32620/reks.2020.2.02.

12. Еремеев, О. І. Комбінована метрика візуальної якості зображень дистанційного зондування на основі нейронної мережі [Текст] / О. І. Еремеев, В. В. Лукин, К. Окарма // Радіоелектронні і

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

комп'ютерні системи. – 2020. – № 4 (96). – С. 4-15. DOI: 10.32620/reks.2020.4.01.

13. Barannik, V. A Model for Representing Significant Segments of a Video Image Based on Locally Positional Coding on a Structural Basis [Text] / V. Barannik, D. Jancarczyk, Yu. Babenko, O. Stepanko, J. Nikodem, S. Zawislak // IEEE 5nd International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IEEE IDAACS-SWS 2020). – 2020. – P. 1–5. DOI: 10.1109/IDAACS-SWS50031.2020. 9297068.

14. Barannik, V. Technology of Composite Code Forming in The Spatial-Spectral Description Significant Microsegments [Text] / V. Barannik, V. Himenko, Yu. Babenko, A. Hahanova, V. Fustii // IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (IEEE TCSET 2020). – 2020. – P. 703–706. DOI: 10.1109/TCSET49122.2020.235523.

15. Wu, Yu. Sudoku Associated Two Dimensional Bijections for Image Scrambling [Text] / Yu. Wu, S. Agaian, J. Noonan // IEEE Transactions on multimedia. – 2012. – 30 p. – Access mode: https://arxiv.org/abs/1207.5856v1. – 7.04.2021.

16. Barannik, V. A method to control bit rate while compressing predicted frames [Text] / V. Barannik, N. Kharchenko; O. Othman Shadi; A. Musienko // IEEE International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics (IEEE CADSM 2015). – 2015. – P. 36–38. DOI: 10.1109/CADSM.2015.7230789.

17. Coding tangible component of transforms to provide accessibility and integrity of video data [Text] / Vladimir Barannik, Anna Hahanova, Vladimir Krivonos // International Symposium on East-West Design & Test Symposium (EWDTS). – 2013. – P. 1-5. DOI: 10.1109/EWDTS.2013.6673179.

18. A fast image encryption algorithm based on chaotic map and lookup table [Text] / P. Cheng, H. Yang, P. Wei, W. Zhang // Nonlinear Dynamics. – 2015. – Vol. 79, Iss. 3. – P. 2121–2131. DOI: 10.1007/s11071-014-1798-y.

19. A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2 [Text] / R. Guesmi, M.A.B. Farah, A. Kachouri, M. Samet // Nonlinear Dynamics. – 2016. – Vol. 83, Iss. 3. – P. 1123–1136. DOI: 10.1007/s11071-015-2392-7.

20. Barannik, V. Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones [Text] / V. Barannik, V. Barannik // 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020). – 2020. - P. 775–780. DOI: 10.1109/TCSET49122.2020.235540.

21. Kurihara, K. An encryption-then-compression system for JPEG XR standard [Text] / K. Kurihara, O. Watanabe, H. Kiya // IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). – 2016. – P. 1–5. DOI: 10.1109/BMSB.2016.7521997.

22. Sharma, R. Data Security using Compression and Cryptography Techniques [Text] / R. Sharma, S. Bollavarapu // International Journal of Computer Applications. – 2015. – Vol. 117, No. 14. – P. 15–18. DOI: 10.5120/20621-3342.

23. Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation [Text] / J. Zhou, X. Liu, O. C. Au, Y. Y. Tang // IEEE Transactions on Information Forensics and Security. 2014. – Vol. 9, No. 1. – P. 39–50. DOI: 10.1109/TIFS.2013.2291625.

24. Barannik, V. The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries [Text] / V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko // IEEE 3rd International Conference on Advanced Information and Communications Technologies (IEEE AICT 2019). – 2019. – P. 415–418. DOI: 10.1109/AIACT.2019. 8847820.

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

26. Barannik, V. V. Structural slotting with uniform redistribution for enhancing trustworthiness of information streams [Text] / V. V. Barannik, Yu. N. Ryabukha, S. A. Podlesnyi // Telecommunications and Radio Engineering. – 2017. – Vol. 76 No. 7. – P. 607-615. DOI: 10.1615/TelecomRadEng.v76.i7.40.

27. Farajallah, M. Chaos-based crypto and joint crypto-compression systems for images and videos [Electronic resource] / M. Farajallah. – 2015. – Access mode: https://hal.archives-ouvertes.fr/tel-01179610. – 7.06.2021..

28. Wong, K. DCT based scalable scrambling method with reversible data hiding functionality [Text] / K. Wong, K. Tanaka // 4th International Symposium on Communications, Control and Signal Processing (ISCCSP). – 2010. – P. 1–4. DOI: 10.1109/ISCCSP.2010. 5463307.

29. The issue of timely delivery of video traffic with controlled loss of quality [Text] / V. Barannik, N. Kharchenko, V. Tverdokhleb, O. Kulitsa // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). - 2016, P. 902-904. DOI: 10.1109/TCSET. 2016.7452220.

30. An Encryption-then-Compression system for JPEG 2000 standard [Text] / O. Watanabe, A. Uchida, T. Fukuhara, H. Kiya // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – 2015. – P. 1226–1230. DOI: 10.1109/ICASSP.2015.7178165.

31. JPEG image scrambling without expansion in bitstream size [Text] / K. Minemura, Z. Moayed, K. Wong, X. Qi, K. Tanaka // 19 th IEEE International Conference on Image Processing. – 2012. – P. 261–264. DOI: 10.1109/ICIP.2012.6466845.

32. The technology of the video stream intensity controlling based on the bit-planes recombination [Text] / V. Barannik, M. Karpinski, V. Tverdokhleb, D. Barannik, V. Himenko, M. Aleksander // IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS`2018). - 2018. – P. 25–28. DOI: 10.1109/IDAACS-SWS.2018.8525560.

33. Ji, Sh. Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator [Text] / Sh. Ji, X. Tong, M. Zhan. – 2012. – Access mode: https://arxiv.org/abs/1208.0999. – 7.04.2021.

34. Barannik Valeriy. Fast Coding of Irregular Binary Binomial Numbers with a Set Number of Units Series [Text] // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). – 2020. – P. 72–76. DOI: 10.1109/ATIT50783.2020.9349356.

35. Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base [Text] // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). – 2020. – P. 83–86. DOI: 10.1109/ATIT50783.2020.9349328.

36. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System [Text] / V. Barannik, N. Barannik, Yu. Ryabukha, D. Barannik // 15 th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020). – 2020. – P. 699–702. DOI: 10.1109/TCSET49122.2020.235522.

37. Barannik, V. The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents [Text] / V. Barannik, T. Belikova, P. Gurzhii // IEEE International Conference on Advanced Trends in Information Theory (ATIT`2019). – 2019. - P. 656–661. DOI: 10.1109/ATIT49449.2019.9030432.

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

39. Development Second and Third Phase of the Selective Frame Processing Method [Text] / V. Barannik, V. Barannik, D. Havrylov, A. Sorokun // 3rd International Conference on Advanced Information and Communications Technologies (AICT`2019). – 2019. – P. 54–57. DOI: 10.1109/AIACT.2019.8847897.

40. Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component [Text] / V. Barannik, D. Komolov, A. Musienko, R. Tarnopolov // 13th International Conference on Modern Problems of Radio Engineering on Telecommunications and Computer Science (TCSET). – 2016. – P. 739-741. DOI: 10.1109/TCSET.2016.7452168.

41. Komolov, D. Selective Method For Hiding Of Video Information Resource In Telecommunication Systems Based On Encryption Of Energy-Significant Blocks Of Reference I-Frame [Text] / D. Komolov, D. Zhurbynskyy, O. Kulitsa // 1st International Conference on Advanced Information and Communication Technologies (AICT'2015). - 2015. – P. 80-83.

42. Wu, Y. NPCR and UACI Randomness Tests for Image Encryption [Text] / Y. Wu, J. P. Noonan, S. Agaian // Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT). – 2011. – Vol. 2. – P. 31–38. DOI: 10.4236/jss.2015.33005.

References

1. *JPEG Privacy & Security Abstract and Executive Summary*, 2015. Available at: https://jpeg.org/items/20150910_privacy_security_summary.html. (accessed 7.04.2021).

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

3. 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*, 2017, vol. 3, no. 9 (111), pp. 103-115. DOI: 10.15587/1729-4061.2021.235521.

4. DSTU 7624:2014: *Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia* [Information Tech-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

nology. Cryptographic protection of information. Symmetric block transformation algorithm]. Ministry of Economic Development of Ukraine, 2015. 39 p.

5. *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, 1999. 26 p.

6. DSTU GOST 28147:2009: *Systema obrobky informatsii. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (HOST 28147-89)* [Information processing system. Cryptographic protection. Cryptographic transformation algorithm (GOST 28147-89)], State Committee for Technical Regulation and Consumer Policy (Derzhspozhivstandart) of Ukraine, 2008. 20 p.

7. 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, iss. 2, pp. 120-126. DOI: 10.1145/359340.359342.

8. Barannik, V., Babenko, Yu., Kulitsa, O., Barannik, V., Khimenko, A., Matviichuk-Yudina, O. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource. *IEEE 2 nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 52-56. DOI: 10.1109/ATIT50783.2020.9349256.

9. Chen, T.-H., Wu, Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, 2011, vol. 91, iss. 1, pp. 90-97. DOI: 10.1016/j.sigpro.2010.06.012.

10. Barannik, V., Shulgin, S., Krasnorutsky, A., Slobodyanyuk, O., Gurzhii, P., Korolyova, N. Methodological Fundamentals of Deciphering Coding of Aerophotography Segments on Special Equipment of Unmanned Complex. *IEEE 2 nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 38-43. DOI: 10.1109/ATIT50783.2020.9349257.

11. Li, F., Krivenko, S., Lukin, V. Two-step providing of desired quality in lossy image compression by SPIHT. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 2 (94), pp. 22-32. DOI: 10.32620/reks.2020.2.02.

12. Ieremeiev, O., Lukin, V., Okarma, K. Combined visual quality metric of remote sensing images based on neural тetwork. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4 (96), pp. 4-15. DOI: 10.32620/reks.2020.4.01.

13. Barannik, V., Jancarczyk, D., Babenko, Yu., Stepanko, O., Nikodem, J., Zawislak, S. A Model for Representing Significant Segments of a Video Image Based on Locally Positional Coding on a Structural Basis. *IEEE 5nd International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IEEE IDAACS-SWS 2020)*, 2020, pp. 1-5. DOI: 10.1109/IDAACS-SWS50031.2020.9297068.

14. Barannik, V., Himenko, V., Babenko, Yu., Hahanova, A., Fustii V. Technology of Composite Code Forming in The Spatial-Spectral Description Significant Microsegments. *IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (IEEE TCSET 2020)*, 2020, pp. 703-706. DOI: 10.1109/TCSET49122.2020.235523.

15. Wu, Yu., Agaian, S., Noonan, J. Sudoku Associated Two Dimensional Bijections for Image Scrambling. *IEEE Transactions on multimedia*, 2012. 30 p. Available at: https://arxiv.org/abs/1207.5856v1. (accessed 7.04.2021).

16. Barannik, V., Kharchenko, N., Othman Shadi, O., Musienko, A. A method to control bit rate while compressing predicted frames. *IEEE International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics (IEEE CADSM 2015)*, 2015, pp. 36-38. DOI: 10.1109/CADSM.2015.7230789.

17. Vladimir Barannik, Anna Hahanova, Vladimir Krivonos. Coding tangible component of transforms to provide accessibility and integrity of video data. 2013. *International Symposium, East-West Design & Test Symposium (EWDTS)*, 2013, pp. 1-5. DOI**:** 10.1109/EWDTS.2013.6673179.

18. Cheng, P., Yang, H., Wei, P., Zhang, W. A fast image encryption algorithm based on chaotic map and lookup table. *Nonlinear Dynamics*, 2015, vol. 79, iss. 3, pp. 2121-2131. DOI: 10.1007/s11071-014-1798-y.

19. Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M. A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Nonlinear Dynamics*, 2016, vol. 83, iss. 3, pp. 1123-1136. DOI: 10.1007/s11071-015-2392-7.

20. Barannik, V., Barannik, V. Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones. *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020, pp. 775-780. DOI: 10.1109/TCSET49122.2020.235540.

21. Kurihara, K., Watanabe O., Kiya, H. An encryption-then-compression system for JPEG XR standard. *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2016, pp. 1-5. DOI: 10.1109/BMSB.2016.7521997.

22. Sharma, R., Bollavarapu, S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, 2015, vol. 117, no. 14, pp. 15-18. DOI: 10.5120/20621-3342..

23. Zhou, J., Liu, X., Au, O. C., Tang, Y. Y. Designing an Efficient Image Encryption-Then-

Compression System via Prediction Error Clustering and Random Permutation. *IEEE Transactions on Information Forensics and Security*, 2014, vol. 9, no. 1, pp. 39-50. DOI: 10.1109/TIFS.2013.2291625.

24. Barannik, V., Barannik, D., Fustii, V., Parkhomenko, M. Technology for Protecting Video Information Resources in the Info-Communication Space. *IEEE 3rd International Conference on Advanced Information and Communications Technologies (IEEE AICT 2019)*, 2019, pp. 248-250. DOI: 10.1109/AIACT.2019.8847820.

25. *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*, International Standard ISO/IEC 15444-8, ITU-T Recommendation T.807, 2007. 108 p.

26. Barannik, V., Ryabukha, Yu., Podlesnyi, S. Structural slotting with uniform redistribution for enhancing trustworthiness of information streams, Telecommunications and Radio Engineering, 2017, vol. 76, no 7, pp. 607-615. DOI: 10.1615/TelecomRadEng.v76.i7.40.

27. Farajallah, M. *Chaos-based crypto and joint crypto-compression systems for images and videos*, 2015. Available at: https://hal.archives-ouvertes.fr/tel-01179610. (accessed 7.06.2021).

28. Wong, K., Tanaka, K. DCT based scalable scrambling method with reversible data hiding functionality. *4th International Symposium on Communications, Control and Signal Processing (ISCCSP)*, 2010, pp. 1-4. DOI: 10.1109/ISCCSP.2010.5463307.

29. Barannik, V., Kharchenko, N., Tverdokhleb, V., Kulitsa, O. The issue of timely delivery of video traffic with controlled loss of quality. *In: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016, pp. 902-904. doi: 10.1109/TCSET.2016.7452220.

30. Watanabe, O., Uchida, A., Fukuhara, T., Kiya, H. An Encryption-then-Compression system for JPEG 2000 standard. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1226-1230, DOI: 10.1109/ICASSP.2015.7178165.

31. Minemura, K., Moayed, Z., Wong, K., Qi, X., Tanaka, K. JPEG image scrambling without expansion in bitstream size. *19 th IEEE International Conference on Image Processing*, 2012, pp. 261-264. DOI: 10.1109/ICIP.2012.6466845.

32. Barannik, V. V., Karpinski, M. P., Tverdokhleb, V. V., Barannik, D. V., Himenko, V. V., Aleksander, M. The technology of the video stream intensity controlling based on the bit-planes recombination. *4th IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, 2018, pp. 25-28. DOI: 10.1109/IDAACS-SWS.2018.8525560.

33. Ji, Sh., Tong, X., Zhang, M. *Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator*, 2012. Available at: https://arxiv.org/abs/1208.0999. (accessed 7.04.2021).

34. Barannik Valeriy. Fast Coding of Irregular Binary Binomial Numbers with a Set Number of Units Series. *IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 29-33. DOI: 10.1109/ATIT50783.2020.9349356.

35. Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base. *IEEE 2 nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 83-86. DOI: 10.1109/ATIT50783.2020.9349328.

36. Barannik, V., Barannik, N., Ryabukha, Yu., Barannik, D. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System. *15 th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020, pp. 699-702. DOI: 10.1109/TCSET49122.2020.235522.

37. Barannik, V., Belikova, T., Gurzhii, P. The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents. 2019. *IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, 2019, pp. 656-661. DOI: 10.1109/ATIT49449.2019.9030432.

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

39. Barannik, V., Barannik, V., Havrylov, D., Sorokun, A. Development Second and Third Phase of the Selective Frame Processing Method. *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 54-57. DOI: 10.1109/AIACT.2019.8847897.

40. *Barannik, V., Komolov, D., Musienko, A., Tarnopolov, R.* Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component. *13th International Conference on Modern Problems of Radio Engineering on Telecommunications and Computer Science (TCSET), 2016, pp. 739-741. DOI: 10.1109/TCSET.2016.7452168.*

41. *Komolov, D., Zhurbynskyy, D., Kulitsa, O.* Selective Method For Hiding Of Video Information Resource In Telecommunication Systems Based On

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Encryption Of Energy-Significant Blocks Of Reference I-Frame. *1st International Conference on Advanced Information and Communication Technologies (AICT'2015*), 2015, pp. 80-83.

42. Wu, Y., Noonan, J. P., Agaian, S. NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, 2011, vol. 2, pp. 31-38. DOI: 10.4236/jss.2015.33005.

Поступила в редакцию 16.04.2021, рассмотрена на редколлегии 20.05.2021

МЕТОД ОБРАБОТКИ ВИДЕОДАННЫХ С ВОЗМОЖНОСТЬЮ ИХ ЗАЩИТЫ ПОСЛЕ КВАНТОВАНИЯ

Д. С. Гаврилов, С. С. Бучик, Ю. М. Бабенко, С. С. Шульгін, А. В. Слободянюк

Предметом исследований в статье являются процессы обработки видеоизображения на основе JPEG-платформы для передачи данных в информационно-телекоммуникационной сети. Целью является построение метода обробки видеоизображения с возможностью его защиты на этапе квантования с последующим арифметическим кодированием. Что позволит при сохранении структурно - статистической закономерности обеспечить необходимый уровень доступности, достоверности и конфиденциальности при передачи видеоданных. Задача: исследование известных методов селективной обработки видеоизображения с последующей формализацией процедуры обработки видеоизображения на этапе квантования и статистическом кодировании значимых блоков на основе JPEG-платформы. Используемыми методами являются: алгоритм на основе JPEG-платформы, методы селекции значимых информативных блоков, арифметическое кодирование. Получены следующие результаты. Разработано метод обработки видеоизображения с возможностью его защиты на этапе квантования с последующим арифметическим кодированием. Это позволит при сохранении структурно-статистической закономерности выполнить поставленные требования по доступной, достоверной и конфиденциальной передачи видеоданных. Обеспечение необходимого уровня доступности связано с уменьшением объема видеоизображения на 30% по сравнению с исходным объемом. При этом, обеспечение необходимого уровня достоверности подтверждается оценкой пикового отношения сигнал / шум для авторизованного пользователя, которое составляет $PSNR_{авт} \geq 20$ дБ. Обеспечение необходимого уровня конфиденциальности подтверждается оценкой пикового отношение сигнал / шум при несанкционированном доступе, которое составляет $PSNR_{нсд} \leq 9$ дБ. Выводы. Научная новизна полученных результатов заключается в следующем: впервые предложено два метода обробки видеозображення на этапе квантования. Стоит отметить, что предложеные технологии выполняют поставленные задачи по обеспечению необходимого уровня конфиденциальности при заданном уровне достоверности. При этом, метод исспользования таблиц шифрования имеет более высокий урровень криптографической устойчивости чем метод исспользования матрицы ключа. Это обусловлено более сложным математическим апаратом. Что, в свою очередь, приводит к увеличению времени на обробку даних. С целью выполнения требования доступности данных предложено использовать арифметическое кодирование для инфоормативних блоков, что должно более высокую эффективность по сравнению с методами кодовых таблиц. Итак, метод исспользования таблиц штфрования имеет большую криптографическую устойчивость, а метод исспользования матрицы-ключа большее быстродействие. При этом, использования арифметического кодирования удовлетворит потребность в доступности за счет уменьшения первоначального объема.

Ключові слова: квантование; доступность; криптографическая защита; достоверность; обработка даннях.

METHOD OF PROCESSING VIDEO DATA WITH THE POSSIBILITY OF THEIR PROTECTION AFTER QUANTIZATION

D. Havrylov, S. Buchyk, Yu. Babenko, S. Shulgin, O. Slobodyanyuk

The subject of research in the article is the video processing processes based on the JPEG platform for data transmission in the information and telecommunication network. The aim is to build a method for processing a video image with the possibility of protecting it at the quantization stage with subsequent arithmetic coding. That will allow, while preserving the structural and statistical regularity, to ensure the necessary level of accessibility, reliability, and confidentiality when transmitting video data. Task: research of known methods of selective video image

processing with the subsequent formalization of the video image processing procedure at the quantization stage and statistical coding of significant blocks based on the JPEG platform. The methods used are an algorithm based on the JPEG platform, methods for selecting significant informative blocks, arithmetic coding. The following results were obtained. A method for processing a video image with the possibility of its protection at the stage of quantization with subsequent arithmetic coding has been developed. This method will allow, while preserving the structural and statistical regularity, to fulfill the set requirements for an accessible, reliable, and confidential transmission of video data. Ensuring the required level of availability is associated with a 30% reduction in the video image volume compared to the original volume. Simultaneously, the provision of the required level of confidence is confirmed by an estimate of the peak signal-to-noise ratio for an authorized user, which is $PSNR_{авт} \geq 20$ dB. Ensuring the required level of confidentiality is confirmed by an estimate of the peak signal-to-noise ratio in case of unauthorized access, which is equal to $PSNR_{нсд} \leq 9$ dB. Conclusions. The scientific novelty of the results obtained is as follows: for the first time, two methods of processing video images at the quantization stage have been proposed. The proposed technologies fulfill the assigned tasks to ensure the required level of confidentiality at a given level of confidence. Simultaneously, the method of using encryption tables has a higher level of cryptographic stability than the method of using the key matrix. It is due to a a more complex mathematical apparatus. Which, in turn, increases the time for processing the tributes. To fulfill the requirement of data availability, it is proposed to use arithmetic coding for info-normative blocks, which should be more efficient compared with the methods of code tables. So, the method of using the scoring tables has greater cryptographic stability, and the method of using the matrix-key has higher performance. Simultaneously, the use of arithmetic coding will satisfy the need for accessibility by reducing the initial volume.

Keywords: quantization; data transfer efficiency; cryptographic protection; quality; data processing.

Гаврилов Дмитро Сергійович – аспірант, Харьківський національний університет радіоелектроніки, Харків, Україна.

Бучік Сергій Степанович – професор, Київський національний університет імені Тараса Шевченко, Київ, Україна.

Бабенко Юрій Михайлович – аспірант, Київський національний університет імені Тараса Шевченко, Київ, Україна.

Шульгін Сергій Сергійович – докторант, Харьківський національний університет радіоелектроніки, Харків, Україна.

Слободянюк Олександр Васильович – доцент, Каменец-Подільский національний університет імені Івана Огієнко, Каменец-Полдільськ, Україна.

Dmytro Havrylov – PhD student, Kharkiv National University of Radio Electronics, Kharkov, Ukraine, e-mail: havrylov_d@ukr.net, ORCID: 0000-0002-3344-7808, Scopus Author ID: 57201779205, ResearcherID: AAF-6200-2021, https://scholar.google.com.ua/citations?user=Ezi2TLEAAAAJ

Serhii Buchyk – doctor of technical sciences, professor, professor of the Department of Cyber Security and Information Protection Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, e-mail: buchyk@knu.ua, ORCID: 0000-0003-0892-3494, Scopus Author ID: 57211747565, https://scholar.google.com.ua/citations?user=0GceVs8AAAAJ&hl=ru.

Yurii Babenko – PhD student of the department of cybersecurity, Taras Shevchenko National University of Kyiv, Kiev, Ukraine, e-mail: babenkomahalych@gmail.com, ORCID: 0000-0002-8115-3329, Scopus Author ID: 57217113657, https://scholar.google.com/citations?user=ikaRuAoAAAAJ.

Sergii Shulgin – Senior Scientific Researcher, Kharkiv National University of Radio Electronics, Kharkov, Ukraine, e-mail: sssh.sergey@gmail.com, ORCID: 0000-0001-5174-290X, SCOPUS Author ID 57189324397, https://www.scopus.com/authid/detail.uri?authorId=57189324397.

Oleksandr Slobodyanyuk – Kamianets-Podilskyi Ivan Ohiienko National University, Kamianets-Podilskyi, Ukraine, e-mail: slobodyanyuk.olexandr@kpnu.edu.ua, ORCID: 0000-0001-5195-3053, Scopus Author ID: 55976592700, https://scholar.google.com.ua/citations?user=QPjiGA8AAAAJ