# *КРИПТОЛОГІЯ / CRYPTOLOGY*

**DOI: 10.18372/2225-5036.26.15569**

# МЕТОД СКРЕМБЛЮВАННЯ СИСТЕМИ СЛУЖБОВИХ СКЛАДОВИХ КРИПТОКОМПРЕСІЙНИХ КОДОГРАМ

**Володимир Бараннік[1], Сергій Сідченко[2], Валерій Бараннік[3] Андрій Хіменко[3]**

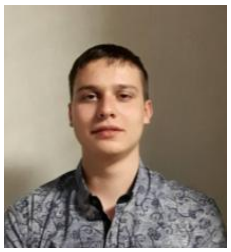
*[1]Харківський національний університет імені В.Н. Каразіна, Україна*
*[2] Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна*
*[3] Харківський національний університет радіоелектроніки, Україна*

**БАРАННІК Володимир Вікторович,** д.т.н., професор.

*Рік та місце народження:* 1971 рік, м. Ізюм, Харківська область, Україна.
*Освіта:* Харківський військовий університет, 1994 рік.
*Посада:* професор кафедрі штучного інтелекту та програмного забезпечення Харківського національного університету імені В.Н. Каразіна.
*Наукові інтереси:* технології кодування, штучний інтелект, інформаційна безпека.
*Публікації:* більше 750 наукових публікацій, серед яких монографії, посібник, навчальні посібники, наукові статті, патенти на винаходи.
*E-mail:* vvbar.off@gmail.com.
*Orcid ID:* 0000-0002-2848-4524.

**СІДЧЕНКО Сергій Олександрович,** к.т.н., с.н.с.

*Рік та місце народження:* 1972 рік, м. Веймар, Німеччина.
*Освіта:* Харківський військовий університет, 1994 рік.
*Посада:* докторант Харківського національного університету Повітряних Сил імені Івана Кожедуба.
*Наукові інтереси:* технології кодування, інформаційна безпека, інформаційна війна.
*Публікації:* більше 250 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях, патенти на винаходи.
*E-mail:* sidserg72@gmail.com.
*Orcid ID:* 0000-0002-1319-6263.



**БАРАННІК Валерій Володимирович**

*Рік та місце народження:* 2000 рік, м. Первомайськ, Миколаївська область, Україна.
*Посада::* студент Харківського національного університету радіоелектроніки.
*Наукові інтереси:* технології цифрової обробки зображень, інформаційна безпека.
*Публікації:* більше 20 наукових публікацій, серед яких наукові статті, монографії, тези та матеріали доповідей на конференціях.
*E-mail:* valera462000@gmail.com.
*Orcid ID:* 0000-0003-3516-5553.

**ІГНАТЬЄВ Олександр Олексійович**

*Рік та місце народження::* 2002 рік, м. Харків, Україна.
*Посада::* студент Харківського національного університету радіоелектроніки.
*Наукові інтереси:* технології цифрової обробки зображень, інформаційна безпека.
*Публікації:* 5 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
*E-mail:* oleksandr.ignatyev10@gmail.com.
*Orcid ID:* 0000-0003-1227-6840.

***Анотація.*** *У системах кризового управління потрібне забезпечення конфіденційності переданих відеоданих зі збереженням заданої якості інформації та без зниження її доступності. Однак, існує проблема пов'язана з тим, що забезпечення конфіденційності відеоданих може бути організовано або за рахунок доступності відеоданих при збереженні заданої їх якості, або за рахунок зниження обсягу корисної інформації для підтримки заданої доступності. Розроблено метод скремблювання системи службових складових в криптокомпресійних кодограмах, сформованих за умови відкидання найменшого значущого розряду в значеннях яскравості пікселів в просторі RGB. Відмінність даного методу від відомих полягає в що, перед виконанням скремблюючих перетворень організовується об'єднання службових даних, представлених в зниженому динамічному діапазоні, в 8-бітові об'єднані елементи. На етапі перестановки об'єднаних 8-бітових даних організовується не лише зміна місця розташування значень вихідних 7-бітних елементів службових складових, але також і зміна їх значень. Це дозволяє підвищити криптографічні характеристики відомих перестановочних перетворень. Розроблений метод забезпечує: підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення; підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів. Скремблюючі перетворення на основі таблиць перестановки, застосовувані до системи службових складових в криптокомпресійних кодограмах, забезпечують стійкість візуальної інформації зображення до помилок в кодограмах, що виникають в каналі зв'язку. Це при тому, що криптокомпресійні кодограми представляють собою стисле представлення вихідних зображень.*

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

**Вступ**

У системах кризового управління потрібне забезпечення конфіденційності переданих відеоданих зі збереженням заданої якості інформації та без зниження її доступності.

Однак, існує проблема пов'язана з тим, що забезпечення конфіденційності відеоданих може бути організовано або за рахунок доступності відеоданих при збереженні заданої їх якості, або за рахунок зниження обсягу корисної інформації для підтримки заданої доступності.

Аналіз існуючих підходів щодо забезпечення конфіденційності зображень показав, що найбільш розповсюджені криптографічні методи захисту на основі скремблювання та шифрування даних.

Вони використовуються в наступних підходах:

– застосування криптографічних перетворень до різних представлень відеоданих [1–5];

– на основі поетапного виконання компресійних та криптографічних перетворень [6];

– на основі стеганографічних методів [7–16].

– технологіях візуальної криптографії на основі об'єднання та розсіювання елементів зображень [17–21];

– схемах скремлювання елементів нестиснених зображень [22–27];

– схемах перцептивного шифрування до виконання компресіного перетворення [28–31];

– застосування криптографічних перетворень на різних етапах технологій компресі [32–42].

Методи скремблювання є менш стійкими з позиції захисту інформації. Найбільш часто вони організовуються на основі операцій перестановок, які змінюють місце розташування даних в межах оброблюваних блоків або всього зображення. Однак перестановки не змінюють самих оброблюваних даних. Організація перестановок в межах блоків вихідних даних малої розмірності взагалі не забезпечує конфіденційності зображень. Через психовізуальні особливості сприйняття відеоданих, великі об'єкти в таких скрембльованих зображеннях можуть бути помітні. Для усунення даного недоліку використовуються перестановки для блоків даних більших розмірів аж до розмірів зображень, а також перестановки самих оброблюваних блоків в межах всього кадру та/або між кадрами. Скремблюючі перетворення на основі таблиць перестановки, застосовувані до відкритих відеоданих, підвищують стійкість візуальної інформації зображення до помилок в фрагментах скрембльованих зображення, що виникають в результаті помилок в каналі зв'язку [43].

Однак, використання скремблюючих перетворень в сучасних технологіях компресії нейтралізує даний виграшний ефект. Це пов'язано з тим, що помилки в стислих даних є дуже суттєвими.

Методи шифрування дозволяють забезпечити більш стійкий захист даних. Вони змінюють самі дані не змінюючи їх розташування. Невеликим винятком з позиції зміни місця розташування при блокової обробці даних є байтові та/або бітові перестановки в межах блоку. Однак при обробці даних в блоках або напівблоках шифрування розмірністю від 32 до 256 біт такі перестановки без використання інших криптографічних примітивів є нікчемними, тому що в них бере участь тільки від 4 до 32 байт інформації (8-бітних елементів даних, що обробляються).

Такі перестановки в алгоритмах шифрування призначені для організації лавинного ефекту при розсіюванні і перемішуванні даних. Методи шифрування

критичні до виникнення помилок в зашифрованих даних.

Навіть одинична помилка в блоці зашифрованих даних призводить до його неправильного розшифрування. А в разі використання схем гамування, неправильно розшифрованими можуть виявитися і всі блоки даних, розташовані за помилковим блоком.

Існуючим підходам забезпечення конфіденційності відеоданих характерні наступні проблемні недоліки:

– забезпечення конфіденційності відеоданих без використання технологій компресії призводить до істотного зниження їх доступності;

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

– в криптографічних перетвореннях відсутні недетерміновані характеристики. Це може вплинути на рівень криптостійкості особливр при використанні скремблюючих перетворень.

Для їх усунення даних проблемних недоліків були розроблені підходи щодо криптокомпресійного кодування зображень, що забезпечують комплексування технологій компресії та шифрування [44–48].

Сформовані криптокомпресійні кодограми зображень складаються з інформаційної та службової складових. Інформаційна складова, яка містить інформацію про вихідні значення елементів в зображенні, являє собою зашифроване представлення, яке неможливо правильно декодувати без наявності службової складової. Службова складова містить інформацію про виявлені структурні характеристики в зображенні.

Вона є ключовим елементом для декодування інформаційної складової. У відритому вигляді з елементів службової складової можна реконструювати образ зображення в зменшеному розмірі.

Тому для забезпечення криптографічної стійкості всієї кріптокомпресійної кодограми потрібно організувати додаткове криптографічне перетворення над елементами службової складової, яке може бути побудовано на основі алгоритмів скремблювання або шифрування даних.

Метою статті є розробка методу скремблювання системи службових складових криптокомпресійних кодограм для забезпечення криптостійкості відеоданих зі збереженням заданої якості інформації без зниження її доступності. Особливість організації криптокомпресійного кодування полягає в тому, що службові складові з одного боку визначають правильну довжину відповідних їм кодів інформаційної складової, а з іншого боку визначають кількість елементів вихідного зображення, які сформували дані коди, і дозволяють правильно декодувати їх значення. Службові складові, що змінені на основі перетворень скремблювання або шифрування даних, в процесі криптокомпресійного декодування не можуть бути правильно зіставлені з кодами інформаційних складових і відповідно є помилковими для них. Крім того, хибні службові складові не дозволяють правильно декодувати зображення.

Причому в процесі криптокомпресійного декодування на основі хибних службових складових помилки накопичуються. Це пов'язано з тим, що хибні службові складові криптокомпресійних кодограм при декодуванні проміжних значень службових складових першого каскаду також формують помилкові значення. Вони в свою чергу неправильно декодують реконструйовані елементи, які не збігаються з вихідними значеннями.

Процес організації криптографічного перетворення службових складових криптокомпресійних кодограм будемо розглядати в загальному вигляді, який залежить від способу представлення даних, що захищаються, та організації їх перетворення без вибору конкретного алгоритму перетворення. Службові складові криптокомпресійних кодограм можуть бути представлені у вихідному динамічному діапазоні та в зниженому динамічному діапазоні за рахунок відкидання молодшого значущого розряду у елементів вихідних зображень в процесі їх криптокомпресійного кодування.

У першому випадку, коли службові складові представлені у вихідному динамічному діапазоні, для зберігання значення яскравості одного елементу виділяється 8 біт (1 байт). У другому випадку для зберігання значення яскравості одного елемента в зниженому динамічному діапазоні потрібно $(8-n_{LSB})$ біт, де $n_{LSB}$ – кількість відкинутих молодших розрядів в елементі зображення. Для забезпечення мінімальної втрати якості реконструкції зображень в криптокомпресійних перетвореннях було запропоновано відкидати один молодший значущий розряд у елементів вихідного зображення. Тому, для зберігання значення яскравості одного елемента службових складових в зниженому динамічному діапазоні виділяється 7 біт.

**Основна частина**

Розглянемо процес організації скремблюючих перетворень службових складових криптокомпресійних кодограм. Перестановки службових складових можуть організовуватися, як без урахування зміни їх динамічного діапазону, так і з урахуванням цієї зміни. У першому варіанті передбачається, що перестановці піддаються дані в їх вихідному динамічному діапазоні, тобто організовується тільки зміна їх розташування в межах

блоку скремблювання або в межах всіх службових складових.

Так, перестановка службових складових у вихідному динамічному діапазоні передбачає організацію звичайних байтових перестановок. Перестановка службових складових в зниженому динамічному діапазоні передбачає організацію перестановок елементів довжиною ($8-n_{LSB}$) біт.

Для службових складових з одним відкинутим молодшим розрядом організовується перестановка 7-бітних елементів. Така організація перестановки забезпечує розрив кореляційних взаємозв'язків між елементами службових складових (хоча самі елементи не змінюються) і розрив відповідності службових складових з кодами інформаційних складових.

Другий варіант організації скремблюючих перетворень передбачає об'єднання службових даних, представлених в зниженому динамічному діапазоні з довжиною ($8-n_{LSB}$) біт кожний при $n_{LSB}>0$ в 8-бітові об'єднані елементи.

Це пов'язано з тим, що, як правило, дані обробляються і зберігаються в 8-бітовому вигляді. Фактично кожен елемент службової складової містить в собі незаповненими (приймаючі нульові значення) старші розряди, кількість яких дорівнює $n_{LSB}$.

Так як для забезпечення мінімальної втрати якості реконструкції зображень в криптокомпресійних перетвореннях було запропоновано відкидати один молодший значущий розряд у елементів вихідного зображення, то організацію процесу об'єднання службових даних в зниженому динамічному діапазоні в 8-бітові дані будемо розглядати з позиції обробки 7-бітних даних.

Об'єднані 8-бітові дані в подальшому піддаються байтовим векторним або матричним перестановкам в межах блоку скремблювання або в межах всіх службових складових.

Нехай необхідно сформувати послідовність з 8-бітних даних $d_{i_d}$, де $i_d$ – порядковий номер в сформованої послідовності, для організації перестановок над ними, $i_d=\overline{1,i_{d_{max}}}$, $i_{d_{max}}$ – максимальний порядковий номер сформованого 8-бітного елемента.

Для цього використовується послідовність 7-бітних службових складових $a_{i_a}$, де $i_a$ – порядковий номер елементів службових складових, $i_a=\overline{1,i_{a_{max}}}$, $i_{a_{max}}$ – максимальний порядковий номер елемента службових складових. Максимальний порядкового номера $i_{a_{max}}$ може бути визначений за допомогою формули:

$$i_{a_{max}}=\frac{M\cdot N}{m\cdot n}, \quad (1)$$

де $M$, $N$ – кількість рядків і стовпців в початковому зображенні, відповідно; $m$, $n$ – кількість рядків і стовпців у сегменті зображення для організації криптокомпресійних кодограм. Останнім буде сформований 8-бітний елемент $d_{i_{d_{max}}}$ з порядковим номером $i_{d_{max}}$, який визначається відповідно до значення максимального порядкового номера $i_{a_{max}}$ (який визначено за допомогою виразу (1)) для службових даних $a_{i_a}$ в зниженому динамічному діапазоні і рівнем зниження динамічного діапазону $n_{LSB}$ на основі формули:

$$i_{d_{max}}=\frac{(8-n_{LSB})\cdot M\cdot N}{8\cdot m\cdot n}=\frac{(8-n_{LSB})}{8}\cdot i_{a_{max}}. \quad (2)$$

При об'єднанні 7-бітних значень службових складових криптокомпресійних кодограм, коли відкидається одні молодший розряд $n_{LSB}=1$, вираз (2) прийме наступний вигляд:

$$i_{d_{max}}=\frac{7\cdot M\cdot N}{8\cdot m\cdot n}=\frac{7}{8}\cdot i_{a_{max}}. \quad (3)$$

Дане значення буде відповідати:

– загальної кількості сформованих 8-бітних елементів, що піддаються подальшому криптографічному перетворенню;

– розмірності необхідної таблиці для організації векторної перестановки або відповідної їй матричної форми;

– загального обсягу службових даних в байтах для оброблюваної колірної площині.

Останній сформований 8-бітний елемент $d_{i_{d_{max}}}$ повинен бути повністю заповненим, тобто відповідно до виразу (3) повинна виконуватися умова:

$$i_{d_{max}}=[\frac{7}{8}\cdot i_{a_{max}}], \quad \frac{7}{8}\cdot i_{a_{max}}=[\frac{7}{8}\cdot i_{a_{max}}]. \quad (4)$$

Якщо умова (4) не виконується, то біти, що залишилися, заповнюються випадковим чином нульовими та/або одиничними бітовими значеннями.

Умова (4) виконується при мінімальному значенні $i_{a_{max}}=8$. У цьому випадку значення $i_{d_{max}}$ на основі виразу (3) дорівнюватиме 7. Умова (4) буде виконуватися для всіх значень $i_{a_{max}}$ кратних восьми.

Відповідно, можна зробити висновок про те, що кожні 7 послідовних 8-бітних об'єднаних даних будуть сформовані з 8 послідовних 7-бітних значень службових складових. Схема об'єднання 7-бітних значень $a_{i_a}$ службових складових криптокомпресійних кодограм в

8-бітові дані для подальшого їх криптографічного перетворення представлена на рис. 1 для перших семи варіантів об'єднання. Надалі вони будуть циклічно повторюватися. На схемі в блоках даних записана змінна $a_{i_a}$, яка бере участь в об'єднанні, а через кому кількість її розрядів. Об'єднання бітових розрядів може бути організовано на основі математичних операцій ділення та множення значень на 2 або використанні бітових операцій циклічного зсуву вліво $\mathrm{shl}$ і вправо $\mathrm{shr}$.

В рамках цієї статті будимо використовувати бітову арифметику. Формування 8-бітних об'єднаних даних $d_{i_d}$ на основі бітових операцій циклічного зсуву вліво $\mathrm{shl}$ і вправо $\mathrm{shr}$ в поєднанні з операцією бітового складання по модулю 2 з 7-бітних значень службових складових для перших семи варіантів об'єднання, представлених на рис. 1, організовується за допомогою виразів:

$$d_1 = \mathrm{shl}_1 a_1 \oplus \mathrm{shr}_6 a_2, \quad (5)$$

$$d_2 = \mathrm{shl}_2 a_2 \oplus \mathrm{shr}_5 a_3, \quad (6)$$

$$d_3 = \mathrm{shl}_3 a_3 \oplus \mathrm{shr}_4 a_4, \quad (7)$$

$$d_4 = \mathrm{shl}_4 a_4 \oplus \mathrm{shr}_3 a_5, \quad (8)$$

$$d_5 = \mathrm{shl}_5 a_5 \oplus \mathrm{shr}_2 a_6, \quad (9)$$

$$d_6 = \mathrm{shl}_6 a_6 \oplus \mathrm{shr}_1 a_7, \quad (10)$$

$$d_7 = \mathrm{shl}_7 a_7 \oplus a_8. \quad (11)$$

Тут $\oplus$ – бітова операція "виключає АБО" (додавання по модулю 2). Роботу бітових операцій циклічного зсуву вліво $\mathrm{shl}$ і вправо $\mathrm{shr}$ описує наступний приклад. Число $204 = 11001100_2$ в результаті операцій циклічного зсуву на 2 біта вліво $\mathrm{shl}_2 204$ перетворюється в значення $48 = 00110000_2$.

А результатом операцій циклічного зсуву на 2 біти вправо $\mathrm{shr}_2 204$ буде число $51 = 00110011_2$.

Вирази (5)–(11) для формування 8-бітних об'єднаних даних на основі бітових операцій в загальному випадку приймуть вид:

$$d_{i_d} = \begin{cases} \mathrm{shl}_{i_d - [\frac{i_d}{7}]\cdot 7} a_{i_d + [\frac{i_d}{7}]} \oplus \mathrm{shr}_{7-\left(i_d - [\frac{i_d}{7}]\cdot 7\right)} a_{i_d + [\frac{i_d}{7}]+1}, & [\frac{i_d}{7}] \neq \frac{i_d}{7}; \\ \mathrm{shl}_7 a_{i_d + [\frac{i_d}{7}]-1} \oplus a_{i_d + [\frac{i_d}{7}]}, & [\frac{i_d}{7}] = \frac{i_d}{7}. \end{cases} \quad (12)$$

З аналізу схеми формування 8-бітних об'єднаних даних $d_{i_d}$ з 7-бітних службових складових $a_{i_a}$, представленої на рис. 1 і описаної виразами (5)–(12), видно, що:

– кожних байт об'єднаних даних $d_{i_d}$ для подальшого криптографічного перетворення складається з бітів, що належать двом 7-бітовим елементів службової складової, що стоять поруч, $a_{i_a}$ і $a_{i_a+1}$;

– у формуванні тільки кожного першого і кожного сьомого 8-бітного об'єднаного елемента $d_{i_d}$ приймають участь всі бітові розряди, відповідно, кожного першого і кожного восьмого 7-бітного елемента $a_{i_a}$ службових складових. У формуванні всіх інших 8-бітних об'єднаних елементів $d_{i_d}$ (а саме, з другого по шостий) беруть участь окремі бітові розряди 7-бітних елементів службової складової, що стоять поруч, $a_{i_a}$ і $a_{i_a+1}$;

– формування кожних 7 послідовних 8-бітових об'єднаних даних $d_{i_d}$, що використовуються для подальшого криптографічного перетворення, з повністю заповненими бітовими розрядами організовується на основі 8 послідовних елементів $a_{i_a}$ службової складової, з яких використовуються всі бітові значення;

– загальна довжина 7 послідовних 8-бітових об'єднаних даних $d_{i_d}$ з повністю заповненими бітовими розрядами становить 56 біт.

Після об'єднання всіх $i_{a_{max}}$ 7-бітних службових складових $a_{i_a}$ в 8-бітові об'єднані дані $d_{i_d}$, останні піддаються криптографічному перетворенню на основі векторної або матричної перестановки.

В результаті виконання перестановочного перетворення організовується зміна місця розташування 8-бітних об'єднаних даних $d_{i_d}$.

А так як вони складаються з бітових значень двох поруч стоять 7-бітних елементів службової складової $a_{i_a}$ і $a_{i_a+1}$, то дана перестановка фактично призводить до поділу 7-бітних елементів на частини і має свої особливості:

– при формуванні кожного першого і сьомого елемента 8-бітних об'єднаних даних $d_{i_d}$ спостерігаються ситуації, коли всі розряди 7-бітного елемента службових складових $a_{i_a}$ потрапляють в один 8-бітний елемент $d_{i_d}$ (це кожен перший і кожен восьмий 7-бітний елемент $a_{i_a}$ службових складових при розбитті їх в групи по 8 елементів). Перестановка таких даних призводить тільки до зміни їх розташування;

– розряди кожного другого - сьомого 7-бітного елемента $a_{i_a}$ службових складових з груп по 8 елементів, що стоять поруч, потрапляють в два різних сусідніх 8-бітних об'єднаних елемента $d_{i_d}$.

Саме ці 7-бітові елементи $a_{i_a}$ службових складових за рахунок зміни місця розташування 8-бітних об'єднаних даних $d_{i_d}$ поділяються і координати їх окремих бітових підпослідовностей віддаляються одна від одної.

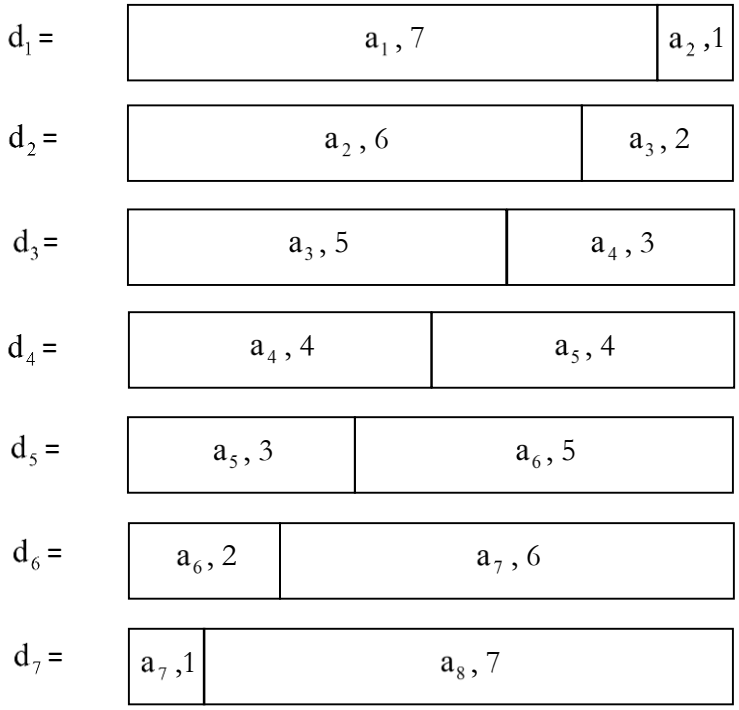



Рис. 1. Схема об'єднання 7-бітних значень службових складових в 8-бітові об'єднані дані

При цьому положення окремих розрядів 7-бітних елементів $a_{i_a}$ службових складових всередині 8-бітних об'єднаних даних $d_{i_d}$ не змінюється. Приклади поділу 7-бітних елементів $a_{i_a}$ службових складових за рахунок зміни місця розташування 8-бітних об'єднаних даних $d_{i_d}$ в процесі векторної та матричної перестановки представлені на рис. 2.

З позиції криптографії даний підхід до об'єднання 7-бітних елементів в 8-бітові даний з подальшою організацією байтової перестановки виконує функції розсіювання і змішування службових складових в криптокомпресійних кодограмах.

На етапі реконструкції 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових без організації зворотного скремблюючого перетворення або його організація на основі не автентичної перестановки відбувається не тільки не правильне відновлення розташування 8-бітних даних $d_{i_d}^{\bullet} \neq d_{i_d}$, але і самі елементи службових складових не можуть бути відновлені, тобто $a_{i_a}^{\bullet} \neq a_{i_a}$.

Даний варіант організації скремблювання службових складових криптокомпресійних кодограм на основі перестановки елементів за умови об'єднання 7-бітних службових даних в 8-бітові об'єднані представлення є більш виграшним, ніж використання варіанту без об'єднання даних.

Виграш полягає в наступному:

– забезпечується підвищення криптостійкості скремльованих службових складових за рахунок змішування і розсіювання даних на етапі їх об'єднання в 8-бітові представлення з подальшою організацією байтової векторної або матричної перестановки. На відміну від стандартного підходу, організуючого зміну місця розташування елементів, забезпечується додаткове зміна їх значень. Причому, при використанні стандартного підходу на основі перестановок елементів у вихідному динамічному діапазоні криптостійкість криптокомпресійних кодограм визначається тільки криптостійкістю використовуваного скремблюючого перетворення (не вище даного перетворення). Другий варіант, коли перестановка організується спільно з об'єднанням 7-бітних елементів в 8-бітові представлення, фактично забезпечується підвищення криптостійкості;

– для організації скремблюючих перетворень в межах всієї множини елементів службових складових потрібно формування таблиць перестановки меншої розмірності.

Це призведе до підвищення оперативності формування таблиць перестановки при збереженні їх криптостійкості (ключові параметри і алгоритм формування таблиць перестановки залишаються незмінними), а так само підвищиться оперативність виконання самого перестановочного перетворення за рахунок обробки меншої кількості даних.

Все це також сприяє підвищенню доступності відеоінформації.

Розмірність матриці перестановок для випадку її організації для елементів у вихідному динамічному діапазоні перевершує варіант її організації для 7-бітних службових складових, об'єднаних в 8-бітові дані, на 12,5%.

Реконструкція 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових з об'єднаних 8-бітних даних $d_{i_d}^{\bullet}$ (які можуть бути, як автентифікованими так і ні) організовується на основі зворотних перетворень з використанням операцій бітової арифметики в загальному випадку за допомогою виразу:

$$a_{i_a}^{\bullet} = \begin{cases} \mathrm{shl}_1 d_{[\frac{i_a}{8}]\cdot 7+1}^{\bullet}, & [\frac{i_a}{8}] \neq \frac{i_a}{8}, i_a - [\frac{i_a}{8}]\cdot 8 = 1; \\ \mathrm{shl}_{8-\left(i_a-[\frac{i_a}{8}]\cdot 8\right)} d_{[\frac{i_a}{8}]\cdot 7+(i_a-[\frac{i_a}{7}]\cdot 8)-1}^{\bullet} \oplus \mathrm{shr}_{i_a-[\frac{i_a}{8}]\cdot 8} d_{[\frac{i_a}{8}]\cdot 7+(i_a-[\frac{i_a}{7}]\cdot 8)}^{\bullet}, & [\frac{i_a}{8}] \neq \frac{i_a}{8}, i_a - [\frac{i_a}{8}]\cdot 8 \neq 1; \\ \mathrm{shr}_1\left(\mathrm{shl}_1 d_{[\frac{i_a}{8}]\cdot 7}^{\bullet}\right), & [\frac{i_a}{8}] = \frac{i_a}{8}. \end{cases}$$

У разі, якщо на етапі реконструкції 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових була організована автентифікована схема дескремблюючого перетворення (використовувався автентифікований ключ) і об'єднані 8-бітові дані $d_{i_d}^{\bullet}$ не піддавалися модифікації, тобто $d_{i_d}^{\bullet} = d_{i_d}$, то реконструйовані значення $a_{i_a}^{\bullet}$ службових складових співпадуть з вихідними $a_{i_a}$, тобто буде виконуватися рівність $a_{i_a}^{\bullet} = a_{i_a}$.

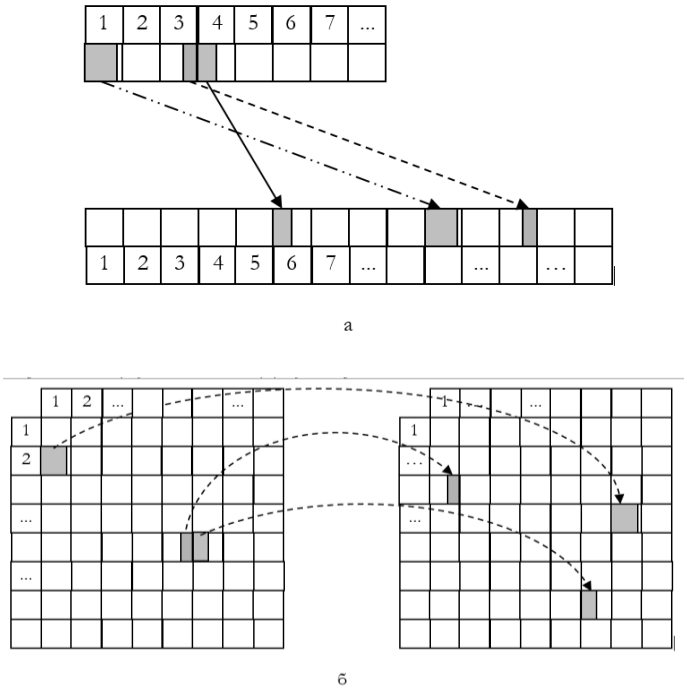



Рис. 2. Приклади поділу елементів службових складових за рахунок зміни місця розташування об'єднаних даних в процесі перестановки: а – векторна перестановка, б – матрична перестановка

**Експериментальна частина**

Були проведені експериментальні дослідження щодо оцінки якості забезпечення конфіденційності в схемі криптокомпресійного кодування зображень в просторі RGB за умови зниження динамічного діапазону вихідних значень за рахунок відкидання одного молодшого значущого розряду з подальшим скремблюванням службових складових, об'єднаних в 8-бітові дані.

Оцінка проводилася на основі порівняння вихідних зображень з реконструйованими зображеннями, відновленими з криптокомпресійних кодограм зі скремльованими службовими складовими.

Для прикладу в статті представлені результати обробки тільки декількох тестових зображень різного ступеня насиченості.

При цьому отримані результати характерні для більшості з оброблюваних відеоданих. Для оцінки якості використовувалися такі підходи:

– візуальна оцінка якості вихідних та відповідних їм скрембльованих зображень;

– кількісна оцінка якості обробки зображень за допомогою показників якості середньоквадратичного відхилення RSME (mean squared error), пікового відношення сигналу до шуму PSNR (Peak Signal-to-Noise Ratio) та коефіцієнта кореляції;

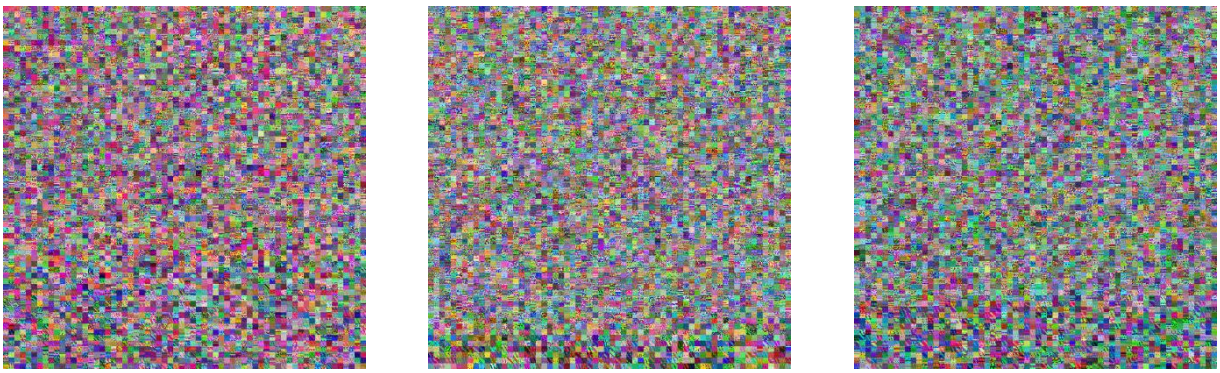
– оцінка кількості пікселів, що змінюються, NPCR (Number of Changing Pixel Rate), яка найбільш часто використовується для оцінки якості шифрування зображень;

– оцінка якості розсіювання та перемішування пікселів в скрембльованих даних за допомогою побудови гістограм кореляції між елементами в скрембльованих зображеннях та гістограм розподілу елементів в скрембльованих зображеннях;

– оцінка можливості додаткової компресії даних на основі використання архіваторів ZIP і RAR.

В експерименті в якості базового скремблюючого перетворення було використано логістичне відображення [49].

Результати оцінки якості забезпечення конфіденційності відеоданих за основі використання запропонованих рішень представлені на рис. 3, 4 і в табл. 1.



Lena Baboon Зона аеропорту

Рис. 3. Приклади візуалізації скрембльованих зображень

Таблиця 1

Результати оцінки якості скрембльованих зображень

| Тестове зображення | Показники якості обробки | | | |
|---|---|---|---|---|
| | RSME | PSNR, dB | коефіцієнт кореляції | NPCR, % |
| Baboon | 88,94 | 9,15 | -0,0030 | 99,5832 |
| Lena | 87,02 | 9,34 | 0,0760 | 99,5519 |
| Зона аеропорту | 82,20 | 9,83 | 0,0029 | 99,5518 |

З аналізу отриманих результатів можна зробити наступні висновки:

– візуальна оцінка якості зображень (рис. 3) показує повне їх руйнування. Скрембльовані представлення різних зображень практично стали схожі один на одного. Домінуючий фон окремих вихідних зображень повністю зруйнований;

– значення показників RSME, PSNR і коефіцієнта кореляції між скрембльованими та вихідними зображеннями (табл. 1) повністю підтверджують дані візуальної оцінки про повне руйнування відеоданих.

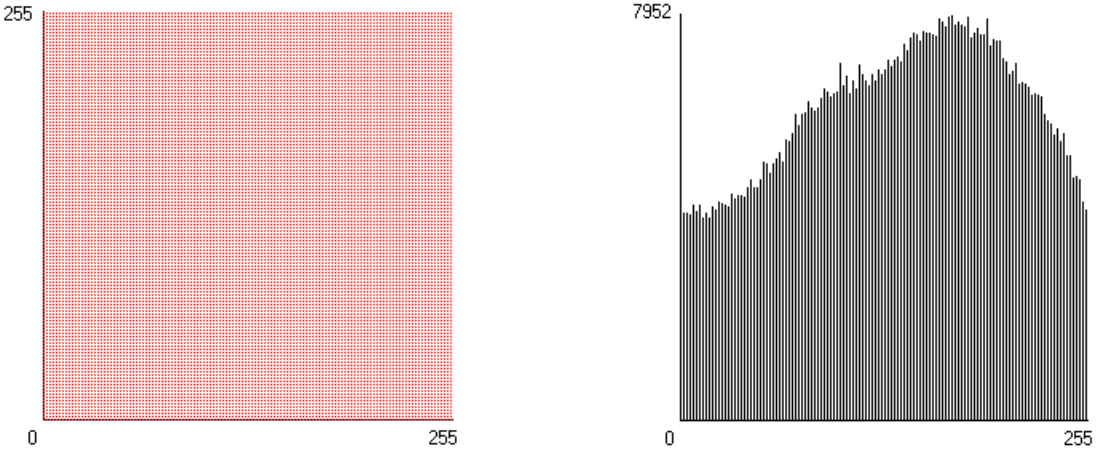
Для всіх типів зображень значення RSME знаходиться вище 80, PSNR – нижче 10 dB. Значення коефіцієнтів кореляції для більшості зображень знаходиться в

районі 0, хоча для деяких відеоданих значення коефіцієнта кореляції можуть спостерігатися в районі до 0,1;

– кількості пікселів, що змінюється, NPCR (табл. 1) для всіх зображень знаходиться вище теоретичного порогового значення 99.5341% [50 – 52], що свідчить про високу стійкість зашифрованих даних до диференціальних атак;

– гістограми кореляції між елементами для різних зображень збігаються незалежно від їх вмісту (рис. 4,а). На гістограмах сформувалося зображення у вигляді квадрата, що істотно змінило гістограми вихідних відеоданих. Через те що дані реконструюються в зниженому діапазоні за рахунок відкидання молодшого розряду, як і в вихідних відеоданих, на гістограмі на рис. 4,а в квадраті пікселі розташовані через один у вертикальному і горизонтальному напрямках. Гістограма у вигляді квадрата свідчить про повністю зруйновану кореляція між сусідніми елементами;

– гістограми розподілу елементів для різних зображень щодо вихідних відеоданих сильно змінилися, відбулося значне вирівнювання кількості елементів (рис. 4,б). Через те що дані обробляються з урахуванням зниження їх динамічного діапазону, на гістограмах відліки розташовуються через один. Фактично присутні тільки елементи з парними значеннями. На гістограмах спостерігаються зміни кількості елементів і відсутні варіанти, коли немає якогось парного значення яскравості або кількість даних значень є малою.




а б

Рис. 4. Приклад гістограм оцінки вмісту скрембльованих тестового зображення:
а – кореляція між елементами; б – розподіл елементів

На гістограмах розподілу елементів не організовується повного вирівнювання їх кількості, з одного боку, через те, що в процесі скремблювання об'єднаних 8-бітних даних змінюються значення тільки кожних шості 7-бітних значень службових складових з восьми, тоді як два значення (перше і восьме) залишаються без зміни.

З іншого боку, в процесі скремблювання не використовувалися спеціальні перетворення, що усувають надмірність. Оцінка додаткової компресії криптокомпресійоних кодограм відеоданих за допомогою архіваторів ZIP і RAR показав, що розміри кодограм додатково не зменшуються.

Для більшості даних навпаки спостерігається незначне збільшення їх обсягу за рахунок формування архіваторами ZIP і RAR своєї службової інформації на початку сформованого архіву. Це свідчить про відсутність надмірності в сформованих криптокомпресійоних кодограмах та про усунення кореляції між елементами.

Відкидання одного молодшого незначущого розряду, що організоване в схемі криптокомпресійного перетворення без втрати якості інформації, з одного боку, призводить до зниження якості реконструйованих даних.

Хоча, данє зниження якості є незначним.

Для всіх зображення значення показника RSME знаходиться на рівні 0,71, PSNR – вище 51 dB, а коефіцієнт кореляції становить 0,9999. З іншого боку забезпечується:

– підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення;

– підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів.

**Висновки**

**Наукова новизна отриманих результатів.**

Розроблено метод скремблювання системи службових складових в криптокомпресійних кодограмах, сформованих за умови відкидання найменшого значущого розряду в значеннях яскравості пікселів в просторі RGB. Відмінність даного методу від відомих полягає в що, перед виконанням скремблюючих перетворень організовується об'єднання службових даних, представлених в зниженому динамічному діапазоні, в 8-бітові об'єднані елементи.

На етапі перестановки об'єднаних 8-бітових даних організовується не лише зміна місця розташування значень вихідних 7-бітних елементів службових складових, але також і зміна їх значень. Це дозволяє підвищити криптографічні характеристики відомих перестановочних перетворень. Розроблений метод забезпечує:

– підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення;

– підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів.

**Практичне значення отриманих результатів.** Створена програмна реалізація методу скремблювання системи службових складових в криптокомпресійних кодограмах, яка забезпечує:

– формування захищених криптокомпресійних кодових конструкцій зі скремблюваними службовими складовими. Реконструйовані неавтентифікованими користувачаими зображення є повністю зруйнованими і все скремблювані зображення візуально не відрізняються одне від одного;

– для всіх скремблюваних зображень забезпечується значне зниження їх якості в порівнянні з вихідними відеоданими. Показники якості для таких зображень приймають наступні значення: RSME знаходиться вище 80, PSNR – нижче 10 dB. Значення коефіцієнтів кореляції для більшості зображень знаходиться в районі 0, хоча для деяких відеоданих значення коефіцієнта кореляції можуть спостерігатися в районі до 0,1. Кількість пікселів, що змінюється, NPCR для всіх зображень знаходиться вище теоретичного порогового значення 99.5341%.

Скремблюючі перетворення на основі таблиць перестановки, застосовувані до системи службових складових в криптокомпресійних кодограмах, забезпечують стійкість візуальної інформації зображення до помилок в кодограмах, що виникають в каналі зв'язку. Це при тому, що криптокомпресійні кодограми представляють собою стисле представлення вихідних зображень.

## Література

[1] Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York City, United States: Wiley, 2015. – 784 p.

[2] Announcing the ADVANCED ENCRYPTION STANDARD (AES*) // Federal Information Processing Standards Publication* [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[3] DSTU 7624:2014: *Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm.* Order of the Ministry of Economic Development of Ukraine № 1484, 2014.

[4] DSTU GOST 28147:2009: *Information processing system. Cryptographic protection. Cryptographic transformation algorithm* GOST 28147-89, 2008.

[5] Rivest R.L., Shamir A., Adleman L.M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, Vol. 2, Iss. 21, 1978. - pp. 120–126.

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

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

[8] Barannik V., Barannik D., Fustii V., Parkhomenko M. Evaluation of Effectiveness of Masking Methods of Aerial Photographs // *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019. - pp. 415-418.

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

[10] 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.

[11] Barannik V.V., Ryabukha Yu. N., Tverdokhleb V.V., Barannik D.V. Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding // *2nd International Conference on Advanced Information and Communication Technologies (AICT)*, 2017. - pp.188-192.

[12] Barannik V., Krasnoruckiy A., Hahanova A. The positional structural-weight coding of the binary view of transformants // *East-West Design & Test Symposium (EWDTS)*, 2013. – pp 1-4.

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

[14] 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.

[15] Barannik V., Shulgin S. The method of increasing accessibility of the dynamic video information resource // *13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016. - pp. 621-623.

[16] Barannik V., Tarasenko D. Method coding efficiency segments for information technology processing video // *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2017. - pp. 551-555.

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

[18] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, Vol. 91, Iss. 1, 2011. - pp. 90-97.

[19] Deshmukh M., Nain N., Ahmed M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic // *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016. - pp. 690-697.

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

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

[22] 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 (ATIT 2020)*, 2020, - pp. 52 – 56.

[23] Ramakrishnan S. *Cryptographic and Information Security Approaches for Images and Videos.* CRC Press, 2018. - 962 p.

[24] Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. Multi-morphological image data hiding based on the application of Rubik's cubic algorithm // *IEEE International Carnahan Conference on Security Technology (ICCST0),* 2012. - pp. 135-139.

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

[26] Wu Yu., Agaian S., Noonan J. Sudoku Associated Two Dimensional Bijections for Image Scrambling // *IEEE Transactions on multimedia* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv:1207.5856v1.

[27] Zhou Y., Panetta K., Agaian S., Chen C.L.P. Image encryption using P-Fibonacci transform and decomposition. *Optics Communications*, Vol. 285, Iss. 5, 2012. - pp. 594-608.

[28] Kurihara K., Shiota S., Kiya H. An encryption-then-compression system for JPEG standard // *Picture Coding Symposium (PCS)*, 2015. - pp. 119–123.

[29] 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.

[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.

[31] 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*, Vol. 9, Iss. 1, 2014. - pp. 39–50.

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

[33] Dufaux F., Ebrahimi T. Toward a Secure JPEG. *Applications of Digital Image Processing* XXIX, Vol. 6312, 2006.

[34] Honda T., Murakami Y., Yanagihara Y., Kumaki T., Fujino T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection // *IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013. - pp. 1371-1374.

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

[36] Ji Sh., Tong X., Zhang M. *Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv: 1208.0999.

[37] Kobayashi H., Kiya H. Bitstream-Based JPEG Image Encryption with File-Size Preserving //*IEEE 7th Global Conference on Consumer Electronics*, 2018. - pp. 1-8.

[38] Minemura K., Moayed Z., Wong K., Qi, X., Tanaka, K. JPEG image scrambling without expansion in bitstream size // *19th IEEE International Conference on Image Processing*, 2012. - pp. 261-264.

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

[40] 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.

[41] Yang Y., Zhu B.B., Li S., Yu N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, Article ID 56365, 2008. – pp. 1-13.

[42] Yuan L., Korshunov. P., Ebrahimi T. Secure JPEG Scrambling enabling Privacy in Photo Sharing //

*11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2015. – pp. 1-6.

[43] Gschwandtner M., Uhl A., Wild P. Transmission error and compression robustness of 2D chaotic map image encryption schemes. *EURASIP Journal on Information Security*, 2007. – pp. 1-16.

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

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

[46] Barannik V.V., Tupitsya I.M., Sidchenko S.A., Tarnopolov R.V. The Method of Crypto-Semantic Presentation of Images Based on the Floating Scheme in the Basis of the Upper Boundaries // 2th International Scientific-Practical Conference *Problems of Infocommunications. Science and Technology* (PIC S&T'2015), 2015. - pp. 248 – 250.

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

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

[49] Barannik V., Sidchenko S., Barannik D. Technology for Protecting Video Information Resources in the Info-Communication Space // *2nd IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, 2020. – pp. 415-418.

[50] 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*, Vol. 3, № 9 (111), 2021. – pp. 112-124.

[51] May R. Simple mathematical models with very complicated dynamics. *Nature*, Vol. 261 (5560), 1976. – pp. 459–467.

[52] Y. Wu, J.P. Noonan, S. Agaian, "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, 2011. – pp. 31–38.

**УДК 621.327:681.5**

***Баранник В.В, Сидченко С.А., Баранник В.В., Игнатьев А.А. Метод скремблирования системы служебных составляющих криптокомпрессионных кодограмм***

***Аннотация.*** *В системах кризисного управления требуется обеспечение конфиденциальности передаваемых видеоданных с сохранением заданного качества информации без снижения ее доступности. Однако, существует проблема связанная с тем, что обеспечение конфиденциальности видеоданных может быть организовано либо за счет увеличения временных затрат на их обработку и доставку при сохранении заданного качества видеоданных, либо за счет снижения объема полезной информации для поддержания заданной доступности. Разработан метод скремблирования системы служебных составляющих в криптокомпрессионных кодограммах, сформированных при условии отбрасывания наименьшего значащего разряда в яркостных значениях пикселей в пространстве RGB. Отличие данного метода от известных заключается в что, перед выполнением скремблирующих преобразований организуется объединение служебных данных, представленных в пониженном динамическом диапазоне, в 8-битные объединенные элементы. На этапе перестановки объединенных 8-битных данных организуется не только изменение местоположения значений исходных 7-битных элементов служебных составляющих, но также и изменение их значений. Это позволяет повысить криптографические характеристики известных перестановочных преобразований. Разработанный метод обеспечивает: повышение доступности видеоданных за счет дополнительного уменьшения объема криптокомпрессионного представления изображения; повышение криптостойкости за счет изменения значений элементов системы служебных данных, нарушения корреляции между элементами и изменения частоты появления точек. Скремблирующие преобразования на основе таблиц перестановки, применяемые к системе служебных составляющих в криптокомпрессионных кодограммах, обеспечивают устойчивость визуальной информации изображения к ошибкам в кодограммах, возникающим в канале связи. Это при том, криптокомпрессионные кодограммах представляют собой сжатое представление исходных изображений.*

***Ключевые слова:*** *криптокомпресионное кодирования, защита информации, скремблирование, шифрование, кодирование, перестановка, компрессия, конфиденциальность, изображение.*

***Barannik V., Sidchenko S., Barannik V., Ignatyev O. The method for scrambling the system of service components in the cryptocompression codograms***

***Annotation.*** *Crisis management systems require the confidentiality of transmitted video data while maintaining the specified quality of information and without reducing its availability. However, there is a problem associated with the fact that ensuring the confidentiality of video data can be organized either by the availability of video data while maintaining a given quality, or by reducing the amount of useful information to maintain a given availability. The method for scrambling a system of service components in the cryptocompression codograms, formed under the condition of*

*discarding the least significant bit in the values of pixel brightness in RGB space, has been developed. The difference between this method and the known ones is that, before performing scrambling transformations, the integration of service components in a reduced dynamic range into 8-bit combined elements is organized. At the stage of permutation of the combined 8-bit data, not only the change of the location of the values of the original 7-bit elements of the service components is organized, but also the change of their values. This improves the cryptographic characteristics of the known permutation transformations. The developed method provides: increase of availability of video data due to additional reduction of volume of cryptocompression image presentation; increasing cryptographic stability by changing the values of the elements of the system of service components, breaking the correlation between the elements and changing the frequency of pixels. Scrambling transformations based on permutation tables applied to the system of service components in cryptocompression codograms, ensure the stability of the visual image information to errors in codograms that arise in the communication channel. Moreover, cryptocompression codograms are a compressed representation of the original images.*
***Key words:*** *cryptocompression coding, information protection, scrambling, encryption, encoding, permutation, compression, confidentiality, image.*

**Бараннік Володимир Вікторович**, д.техн.,наук, професор, професор кафедри штучного інтелекту і програмування, Харківський національний університет імені В.Н. Каразіна.
**Баранник Владимир Викторович**, д.техн.наук, профессор, профессор кафедры искусственного интеллекта и программирования, Харьковский национальный университет имени В.Н. Каразина.
**Volodymyr V. Barannik**, Doctor of Technical Sciences, Professor, Professor Department, V.N. Karazin Kharkiv National University.

**Сідченко Сергій Олександрович**, к. техн. наук, старший науковий співробітник, докторант, Харківський національний університет Повітряних Сил імені І. Кожедуба.
**Сидченко Сергей Александрович**, к. техн. наук, старший научный сотрудник, докторант Харьковский национальный университет Воздушных Сил шимени И. Кожедуба.
**Serhii Sidchenko**, PhD, Senior Scientific Researcher, Doctoral Student, Ivan Kozhedub Kharkiv National Air Force University.

**Бараннік Валерій Володимирович**, студент, Харківський національний університет радіоелектроніки.
**Баранник Валерий Владимирович**, студент, Харьковский национальный университет радиоэлектроники.
**Valery Barannik**, student, Kharkov National University of Radio Electronics.

**Ігнатьєв Олександр Олексійович**, студент Харківського національного університету радіоелектроніки.
**Игнатьев Александр Алексеевич**, студент Харьковского национального университета радиоэлектроники.
**Ignatyev Oleksandr**, student, Kharkov National University of Radio Electronics, Kharkiv.

Отримано 26 *липня 2021 року,* затверджено редколегією *27 серпня 2021 року*