УДК 004.932.056.55 **doi: 10.32620/reks.2021.2.05**

В. В. БАРАННІК[1], С. О. СІДЧЕНКО[2], Н. В. БАРАННІК[3], А. М. ХІМЕНКО[3]

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

МЕТОД МАСКУВАЛЬНОГО УЩІЛЬНЕННЯ СЛУЖБОВИХ ДАНИХ В СИСТЕМАХ КОМПРЕСІЇ ВІДЕОЗОБРАЖЕНЬ

Попит на забезпечення конфіденційності відеозображень постійно збільшується. При цьому, необхідно вирішити актуальну науково-прикладну проблему, яка полягає в підвищенні конфіденційності відеоінформації в умовах заданої часової затримки на її обробку та доставку при забезпечення її достовірності. Для її вирішення можуть використовуватися криптокомпресійні перетворення. В якості ключа перетворення використовується службова складова, яка безпосередньо формується в процесі перетворення та містить інформацію про виявлені структурні характеристики відеоданих. Тому така інформація потребує забезпечення конфіденційності. Існуючі методи криптографії призначені для обробки універсального потоку даних та не враховують структуру та особливості службових складових. Це призводить до формування надмірних даних, використання надлишкової кількості операцій та збільшення витрат часу на обробку в процесі захисту службової інформації з використанням універсальних методів криптографії. Тому метою статті є розробка методу маскувального ущільнення службових даних для забезпечення їх конфіденційності з урахуванням особливостей їх формування методами криптокомпресії. В режимах з контрольованою втратою якості інформації елементи службової складової формуються в зниженому динамічному діапазоні. Їх довжина становить 7 двійкових розрядів. Для забезпечення конфіденційності таких елементів необхідно розробити метод маскувального ущільнення службових даних в системах компресії відеозображень. З одного боку, блоки службових даних не повинні містити надлишкової інформації. З іншого боку, вони повинні формуватися з двійкових розрядів з різних елементів службових складових. Для цього пропонується організувати укомплектування елементів службових складових. Воно організується за рахунок об'єднання 7-бітних елементів службових складових в 8-бітові укомплектовані послідовності. З 8-бітних послідовностей формуються блоки шифрування. Укомплектування службових складових забезпечує змішування службових даних і зменшення їх кількості. Для порушення структури представлення службових складових пропонується додатково організувати перестановку 8-бітних укомплектованих послідовностей. Це забезпечує значне розсіювання двійкових розрядів 7-бітних елементів службових складових і руйнування кореляції між елементами службових даних. Коефіцієнти кореляції вихідних і реконструйованих відеозображень з використанням зашифрованих службових складових знаходяться в районі 0. Кількість пікселів, що змінюються, знаходиться вище теоретичного порогового значення 99,5341 %.

Ключові слова: *крипто компресійне представлення зображення; службова складова; захист інформації; конфіденційність; шифрування; скремблювання; кодування; компресія; зображення; найменш значущий біт.*

Вступ

Попит на забезпечення конфіденційності зображень дедалі збільшується. Це призвело до того, що навіть в JPEG-технології компактного представлення даних, яка отримала широке розповсюдження, розробляється нова функціональність "JPEG Privacy & Security" [1]. Крім цього ведуться численні дослідження щодо розробки нових підходів і методів забезпечення безпеки відеозображень. В залежності від способу забезпечення конфіденційності їх можна розділити на наступні групи:

– на основі використання стандартних криптографічних алгоритмів до різних варіантів представлення відеоданих, а саме до вихідного формату без стиснення та його компактного представлення [2]. В якості криптографічних алгоритмів виступають симетричні [3-6] та асиметричні [7] стандарти шифрування;

– на основі схем розподілу секрету (візуальна криптографія), які спрямовані на обробку одного [8] або декількох [9-11] зображень;

– на основі скремблювання елементів вихідного зображення [12-15];

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

– на основі перестановочно-розсіюючих алгоритмів [15-18];

– на основі схеми "Encryption-then-Compression", яка полягає у виконанні послідовного шифрування зображень і стиснення зашифрованих даних [19-21];

– на основі перетворень скремблювання та шифрування, які організуються спільно з використанням технологій компресії відеоданих. Так, в [22] запропоновані загальні підходи до послуги Secure JPEG, що реалізує функціонал конфіденційності в технології JPEG, а в [23] – в технології JPEG 2000. Різні підходи щодо скремблювання даних в процесі виконання компресійного перетворення представлені в [24-26]. Підходи відносно скремблювання бітового потоку JPEG запропоновані в [27-30]. Приклади відносно використання перетворень шифрування в різних схемах компресії наведено в [31-33];

– на основі стеганографічних підходів [34-36], які спрямовані на забезпечення конфіденційності всього зображення та окремих його областей з об'єктів кризової інфраструктури.

Однак, їм притаманні проблемні недоліки, серед яких можна відзначити:

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

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

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

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

Тому, необхідно вирішити науково-прикладну проблему, яка полягає в підвищенні конфіденційності відеоінформації в умовах заданої часової затримки та забезпечення її достовірності.

Для усунення даних проблемних недоліків в роботах [37-39] були розроблені основні підходи і базові методи формування криптокомпресійних представлень (ККП) зображень. Під криптокомпресійним представленням зображення розуміється кодограма, яка складається з двох складових, а саме інформаційної та службової складових. Інформаційна складові є компактним представленням вихідних значень елементів в зображенні. Службова складова (СС) містить інформацію про виявлені структурні характеристики відеоданих. Вона використовується для кодування та декодування кодових величин інформаційної складової. Тому така інформація виступає в якості ключа перетворення. Значить в системах криптокомпресійного кодування потрібно забезпечити конфіденційність службових складових. У той же час існуючі методи криптографії призначені для обробки універсального потоку даних. У зв'язку з цим вони не враховують структуру та особливості службових складових, які формуються в процесі криптокомпресійних перетворень. Це призводить до формування надмірних даних, використання надлишкової кількості операцій та збільшення витрат часу на обробку в процесі захисту службової інформації з використанням універсальних методів криптографії.

Тому для забезпечення конфіденційності службових складових з урахуванням особливостей їх формування методами криптокомпресії необхідно розробити метод маскувального ущільнення службових даних в системах компресії відеозображень.

Метою дослідження є розробка методу маскувального ущільнення службових даних в системах криптокомпресії відеозображень для усунення кодової надмірності в них.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз підходів відносно забезпечення конфіденційності інформації, які можуть бути використані для забезпечення маскування службових складових в криптокомпресійних кодограмах;

– розробити схему укомплектування елементів службових даних, яка враховує їх структуру та усуває кодову надмірність в них;

– розробити схему усунення кодової надмірності для блоків службових складових, що формують блоки шифрування;

– розробити спосіб попереднього скремблювання елементів службових даних для модифікації їх структури;

– провести експериментальну оцінку якості забезпечення конфіденційності відеоданих в технології криптокомпресійного кодування зображень за умови організації шифрування СС за допомогою розробленого методу маскувального ущільнення.

Підходи відносно забезпечення маскування службових складових

Існуючі підходи відносно забезпечення конфіденційності інформації базуються в основному на скремблюванні та шифруванні даних.

Методи скремблювання найбільш часто організовуються на основі операцій перестановок. В осно-

вному це стосується модифікації позиціонування оброблюваних послідовностей в структурних блоках. Вони є менш стійкими з позиції захисту інформації. Навпаки, методи шифрування модифікують вміст самих даних, але не змінюють їх структурне позиціонування. Найбільш відомими стандартами шифрування є AES, "Калина", DES, ГОСТ 28147-89 [3-6]. Вони дозволяють забезпечити більш стійкий захист даних.

Тому, метод маскувального ущільнення службових даних криптокомпресійних кодограм відеозображень пропонується будувати в системі криптографічного шифрування.

З огляду на особливості криптокомпресійного перетворення організація шифрування СС проводитися для даних, представлених в зниженому динамічному діапазоні. Для кожного елемента СС виділяється $(8-n_{LSB})$ бітових розрядів, де n_{LSB} – кількість відкинутих молодших бітових розрядів в оброблюваних даних. В криптокомпресійних перетвореннях з контрольованою втратою якості інформації оптимальним є відкидання одного молодшого значущого розряду $n_{LSB}=1$. Тому, при зниженому динамічному діапазоні для зберігання кожного елементу СС буде виділятися 7 бітових розрядів.

У той же час в блокових алгоритмах шифрування криптографічні перетворення організовуються над даними, що мають рівномірну довжину L_{ev}. При цьому розмір таких рівномірних блоків вибирається кратним ступеня 2, а саме 64, 128, 192 і 256 біт [3-6]. Тому в процесі посилення процесу захисту СС ККП відеозображень потрібно забезпечити узгодження їх структури та розмірності шифрованих блоків в системах криптографічного перетворення. Це дозволить з одного боку підвищити рівень конфіденційності, а з іншого боку знизити обсяг оброблюваних даних.

Послідовності службових складових необхідно представляти у вигляді байтових структур.

Укомплектування елементів службових даних

Для зберігання елементів службових складових виділяється 7 бітових розрядів. Тому перед організацією шифрування службові складові криптокомпресійних кодограм об'єднуються в 8-бітові послідовності d_ϑ. Приклади таких об'єднань представлені на рис. 1. На схемі в блоках даних записана змінна a_ς, яка бере участь в об'єднанні, а через кому кількість її бітових розрядів.

Для об'єднання використовується наступна система виразів:

$$d_\vartheta=\begin{cases}\left(a_{\vartheta+[\frac{\vartheta}{7}]}-[\frac{a_{\vartheta+[\frac{\vartheta}{7}]}}{2^{8-\left(\vartheta-[\frac{\vartheta}{7}]\cdot 7\right)}}]\cdot 2^{8-\left(\vartheta-[\frac{\vartheta}{7}]\cdot 7\right)}\right)\times & \\ \times 2^{\vartheta-[\frac{\vartheta}{7}]\cdot 7}+[\frac{a_{\vartheta+[\frac{\vartheta}{7}]+1}}{2^{7-\left(\vartheta-[\frac{\vartheta}{7}]\cdot 7\right)}}], & \rightarrow [\frac{\vartheta}{7}]\neq\frac{\vartheta}{7}; \\ \left(a_{\vartheta+[\frac{\vartheta}{7}]-1}-[\frac{a_{\vartheta+[\frac{\vartheta}{7}]-1}}{2}]\cdot 2\right)\cdot 2^7+a_{\vartheta+[\frac{\vartheta}{7}]}, & \\ & \rightarrow [\frac{\vartheta}{7}]=\frac{\vartheta}{7}.\end{cases} \quad (1)$$

де ϑ – координатна змінна 8-бітної послідовності d_ϑ, $\vartheta=\overline{1,[\frac{7\cdot Q_{SC\_CCP}-1}{8}]+1}$;

$a_{\vartheta+[\frac{\vartheta}{7}]}$ – значення елемента СС ККП зображення в зниженому динамічному діапазоні на 1 бітовий розряд з векторною координатою ($\vartheta+[\frac{\vartheta}{7}]$);

$[\bullet]$ – ціла частина числа.

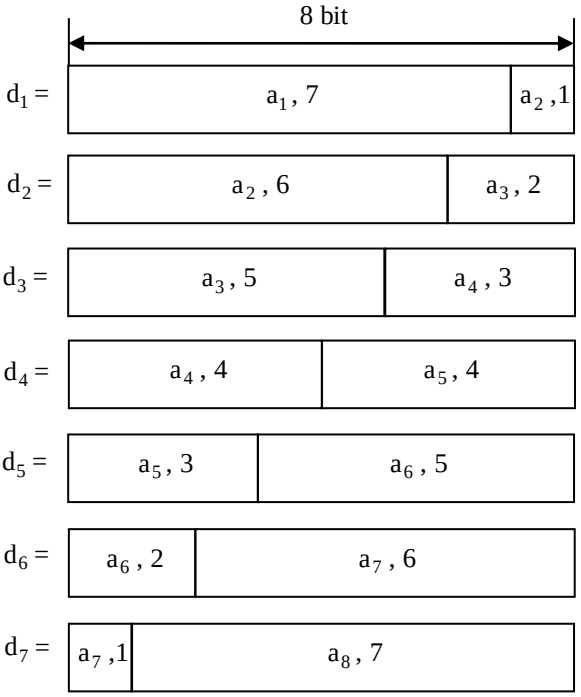


Рис. 1. Схема об'єднання 7-бітних послідовностей a_ς СС ККП в 8-бітові послідовності d_ϑ

Формування 8-бітних послідовностей d_ϑ на основі системи формул (1) організовується на основі виконання умов, коли:

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

– формуються з першого по шостий елемент d_{ϑ} з групи по сім елементів. Координатна змінна ϑ повинна задовольняти умові $[\frac{\vartheta}{7}] \neq \frac{\vartheta}{7}$;

– формується сьомий елемент d_{ϑ} з групи по сім елементів. Координатна змінна ϑ повинна задовольняти умові $[\frac{\vartheta}{7}] = \frac{\vartheta}{7}$.

Отримані 8-бітові послідовності d_{ϑ} будемо називати укомплектованими послідовностями СС ККП зображення в системі криптографічного перетворення.

Зворотне перетворення з 8-бітних укомплектованих послідовностей d_{ϑ} в 7-бітові елементи a_{ς} СС криптокомпресійних кодограм організовується на основі системи формул:

$$a^{\bullet}_{\varsigma} = \begin{cases} d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7+1}[\frac{}{2}], & \rightarrow [\frac{\varsigma}{8}] \neq \frac{\varsigma}{8}, \varsigma - [\frac{\varsigma}{8}]\cdot 8 = 1; \\ \left(d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7+(\varsigma-[\frac{\varsigma}{7}]\cdot 8)-1} - [\frac{d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7+(\varsigma-[\frac{\varsigma}{7}]\cdot 8)-1}}{2^{\varsigma-[\frac{\varsigma}{8}]\cdot 8-1}}] \cdot 2^{\varsigma-[\frac{\varsigma}{8}]\cdot 8-1} \right) \times \\ \times 2^{8-\left(\varsigma-[\frac{\varsigma}{8}]\cdot 8\right)} + [\frac{d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7+(\varsigma-[\frac{\varsigma}{7}]\cdot 8)}}{2^{\varsigma-[\frac{\varsigma}{8}]\cdot 8}}], \\ \qquad \rightarrow [\frac{\varsigma}{8}] \neq \frac{\varsigma}{8}, \varsigma - [\frac{\varsigma}{8}]\cdot 8 \neq 1; \\ d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7} - [\frac{d^{\bullet}_{[\frac{\varsigma}{8}]\cdot 7}}{2^{7}}] \cdot 2^{7}, & \rightarrow [\frac{\varsigma}{8}] = \frac{\varsigma}{8}; \end{cases} \quad (2)$$

де ς – координатна змінна 7-бітного елемента a_{ς} СС криптокомпресійних кодограм, $\varsigma = \overline{1, Q_{SC\_CCP}}$.

Відновлення 7-бітного елемента a_{ς} СС криптокомпресійних кодограм на основі системи формул (2) організовується на основі виконання умов, коли:

– відновлюється перший елемент a_{ς} з групи по вісім елементів. Координатна змінна ς повинна задовольняти умові $[\frac{\varsigma}{8}] \neq \frac{\varsigma}{8}$ та $\varsigma - [\frac{\varsigma}{8}]\cdot 8 = 1$;

– відновлюються елементи a_{ς} з другого по сьомий з групи по вісім елементів. Координатна змінна ς повинна задовольняти умові $[\frac{\varsigma}{8}] \neq \frac{\varsigma}{8}$ та $\varsigma - [\frac{\varsigma}{8}]\cdot 8 \neq 1$;

– відновлюється восьмий елемент a_{ς} з групи по вісім елементів. Координатна змінна ς повинна задовольняти умові $[\frac{\varsigma}{8}] = \frac{\varsigma}{8}$.

Усунення кодової надмірності для блоків службових даних

Сім послідовно розташованих 8-бітних укомплектованих послідовності d_{ϑ} СС ККП зображення формують структурні послідовності

$$D^{(\upsilon)} = \{d_{\vartheta}\} = \{a_{\varsigma}\}, \ \upsilon = \overline{1, [\frac{7 \cdot Q_{SC\_CCP}}{56 \cdot 8}]},$$
$$\vartheta = \overline{((\upsilon-1)\cdot 7+1), (7\cdot\upsilon)}, \ \varsigma = \overline{((\upsilon-1)\cdot 8+1), (8\cdot\upsilon)}.$$

Їх будемо називати множиною укомплектованих послідовностей.

Довжина множини укомплектованих послідовностей $L_{dr} = 56$ біт. Вона менше розміру блоку шифрування L_{ev} та не кратна йому, тобто $\frac{L_{ev}}{L_{dr}} \neq [\frac{L_{ev}}{L_{dr}}]$ при L_{ev} = 64, 128, 192 і 256. Тому блок шифрування буде формуватися на основі більш однієї множини $D^{(\upsilon)}$ укомплектованих послідовностей. Отже, кожен блок шифрування буде сформований не тільки з цілого кількості вихідних 7-бітних елементів a_{ς} СС ККП, а також з бітових розрядів окремих елементів a_{ς}.

Схема об'єднання 56-бітних множин $D^{(\upsilon)}$ укомплектованих послідовностей в 128-бітові фрейми

$$B^{(\omega)} = \{d_{\vartheta}\}, \ \omega = \overline{1, [\frac{7 \cdot Q_{SC\_CCP}}{128 \cdot 8}]},$$
$$\vartheta = \overline{((\omega-1)\cdot 16+1), (16\cdot\omega)},$$

для шифрування представлена на рис. 2 для перших семи варіантів об'єднання. На схемі в блоках даних записані 56-бітові множини $D^{(\upsilon)}$ укомплектованих послідовностей, а через кому кількість її бітових розрядів.

У загальному вигляді 56-бітові множини $D^{(\upsilon)}$ укомплектованих послідовності можуть бути об'єднані в L_{ev}-бітний фрейми $B^{(\omega)} = \{d_{\vartheta}\}$, $\omega = \overline{1, [\frac{7 \cdot Q_{SC\_CCP}}{L_{ev} \cdot 8}]}$, $\vartheta = \overline{((\omega-1)\cdot \frac{L_{ev}}{8}+1), (\frac{L_{ev}}{8}\cdot\omega)}$, $\frac{L_{ev}}{8} = [\frac{L_{ev}}{8}]$. Якщо останній фрейм укомплектова-

них послідовності для шифрування є незаповненим, то він заповнюється нульовими, одиничними або випадковими бітовими розрядами до розміру L_{ev} блоку шифрування. На етапі розшифрування ці додаткові бітові розряди будуть відкинуті, виходячи із загального обсягу одного типу службових даних ККП в площині відеозображення, який дорівнює $(8-n_{LSB})\cdot Q_{SC\_CCP}$ біт, і довжини L_{ev} блоку шифрування за допомогою формули:

$$n_{add\_bit} = (8-n_{LSB})\cdot Q_{SC\_CCP} - \\ -[\frac{(8-n_{LSB})\cdot Q_{SC\_CCP}}{L_{ev}}]\cdot L_{ev}\ [bit],$$

де n_{add_bit} – кількість доданих в останній блок шифрування бітових розрядів.

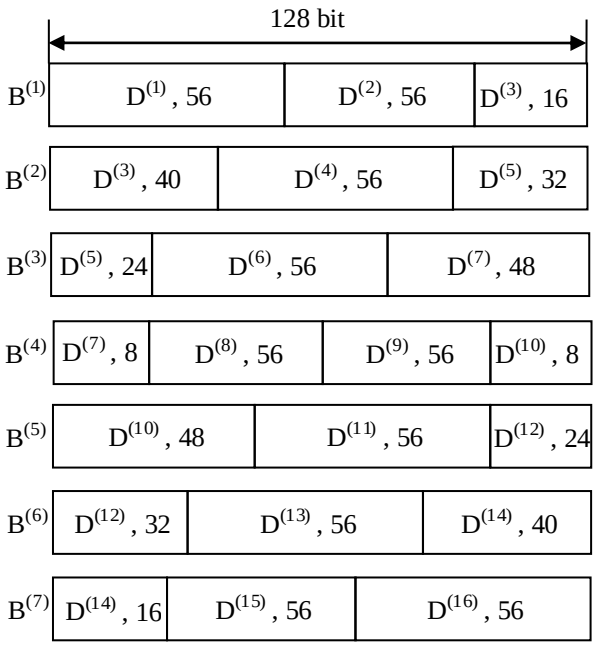


Рис. 2. Схема об'єднання 56-бітних множин $D^{(\upsilon)}$ укомплектованих послідовностей в 128-бітові фрейми $B^{(\omega)}$

Фрейми $B^{(\omega)}$ укомплектованих послідовностей мають наступні характеристики:

– формування кожних 7-і послідовних L_{ev}-бітних фреймів $B^{(\omega)}$ для шифрування організовується на основі $\frac{7\cdot L_{ev}}{56}$ послідовних 56-бітних множин $D^{(\upsilon)}$ елементів службових складових a_{ς};

– кожен L_{ev}-бітний фрейм $B^{(\omega)}$ для шифрування складається з бітових розрядів $[\frac{L_{ev}}{56}]+1$ або $[\frac{L_{ev}}{56}]+2$ поруч стоячих 56-бітних множин $D^{(\upsilon)}$ укомплектованих послідовностей службової складової a_{ς}. Це відповідає $\frac{L_{ev}}{8}$ поруч стоячих 8-бітних укомплектованих послідовностей d_{ϑ}, а також $[\frac{L_{ev}}{7}]+1$ або $[\frac{L_{ev}}{7}]+2$ поруч стоячих 7-бітних елементів a_{ς} СС ККП.

Запропонована технологія укомплектування 7-бітних елементів a_{ς} СС ККП забезпечує змішування даних на основі зсуву бітових розрядів. Це підсилює лавинний ефект в процесі подальшого шифрування. Крім того, технологія укомплектування забезпечує шифрування більшої кількості елементів a_{ς} в одному блоці шифрування. Це досягається за рахунок усунення кодової надмірності в процесі шифрування цих елементів a_{ς}. Кодова надмірність усувається за рахунок відкидання незначущих бітових розрядів в процесі укомплектування елементів a_{ς} службових складових.

Розробка способу скремблювання службових даних

Для модифікації структури представлення СС ККП пропонується додатково організувати їх попереднє скремблювання. Воно базується на виконанні перестановочного перетворення. Для цього може використовуватися таблиця перестановок з відомими параметрами. Ця таблиця виступає в якості довгострокового ключового елемента. Вона призначена для руйнування кореляційних взаємозв'язків між елементами в оброблюваних службових даних.

Перестановки елементів СС ККП зображень можуть бути організовані в двох варіантах:

1) в вихідному динамічному діапазоні оброблюваних даних;

2) з урахуванням об'єднання службових складових в 8-бітові укомплектовані послідовності.

Перший варіант перестановки елементів СС у вихідному динамічному діапазоні змінить їхнє місце розташування (порушить кореляційні взаємозв'язки між ними). Блоки шифрування будуть формуватися з $[\frac{L_{ev}}{8-n_{LSB}}]+1$ елементів СС. Нехай відкидається одні молодший розряд $n_{LSB}=1$ у елементів службових складових. Тоді в формуванні блоку шифрування довжиною $L_{ev}=64$ біта братимуть участь бітові розряди 10-и елементів СС. При цьому будуть спостерігатися такі об'єднання:

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

– все бітові розряди дев'яти 7-бітних елементів службових складових та додаткові бітові розряду з одного неповного 7-бітного елемента;

– все бітові розряди восьми 7-бітних елементів службових складових та додаткові бітові розряду з двох неповних 7-бітних елементів.

Другий варіант перестановки елементів службових складових з урахуванням їх об'єднання в 8-бітові укомплектовані дані:

– модифікує розташування $(8-n_{LSB})$-бітних службових даних (порушить кореляційні взаємозв'язки між ними);

– модифікує значення більшості з $(8-n_{LSB})$-бітних службових даних.

В цьому варіанті блоки шифрування формуються з 8-бітних укомплектованих послідовностей, які модифікували своє місце розташування. Причому кожна 8-бітна укомплектована послідовність складається з бітових розрядів декількох $(8-n_{LSB})$-бітних службових даних. У варіанті відкидання одного молодшого розряду $n_{LSB}=1$ в результаті перестановки 8-бітних укомплектованих послідовностей кожні 6 з 8 елементів 7-бітних службових даних поділяються на дві частини, які віддаляються одна від одної. Кожна з 8-бітних укомплектованих послідовностей буде складатися з бітових розрядів двох різних елементів 7-бітних службових даних. Формування фрейму шифрування довжиною L_{ev} біта із 8-бітний укомплектованих послідовностей фактично призведе до випадку, коли фрейм буде формуватися з окремих бітових розрядів $\frac{L_{ev}}{4}$ елементів. Так, у 64-бітному фреймі шифрування братиме участь в середньому 2-3 цілих 7-бітних елемента СС і окремі бітові розряди з 13-14 не повних елементів.

Збільшення розмірності фрейму шифрування збільшує кількість елементів СС, окремі бітові розряди яких його формують. Це забезпечує підвищення криптостійкості в процесі організації шифрування. Кількість елементів СС, що беруть участь у формуванні фрейму шифрування, представлено в табл. 1. Вона залежить від розміру фрейму шифрування і кількості бітових розрядів, виділених для зберігання одного елементу службових даних.

З аналізу даних в табл. 1 видно наступне. У разі 8-бітного представлення службових даних a_ς фрейми $B^{(\omega)}$ шифрування формуються з цілої їх кількості. Це кількість не залежить від умов організації попередньої перестановки. При 7-бітному представленні службових даних a_ς без урахування організації попередньої перестановки формуються фрейми $B^{(\omega)}$ шифрування переважно з цілої кількості службових даних a_ς. Для 7-бітного представлення елементів a_ς СС за умови організації попередньої перестановки їх 8-бітних укомплектованих представлень d_ϑ формуються фрейми $B^{(\omega)}$ шифрування переважно з окремих бітових розрядів службових даних a_ς.

Таблиця 1

Кількість елементів службових складових, що беруть участь у формуванні фрейму шифрування

Розмір фрейму (блоку) шифрування, біт	Кількість бітових розрядів для зберігання одного елемента		
	8 біт	7 біт	
		без організації перестановки	з організацією перестановки
L_{ev}, $\frac{L_{ev}}{8}=[\frac{L_{ev}}{8}]$	$\frac{L_{ev}}{8}$	$[\frac{L_{ev}}{7}]+1$	$\frac{L_{ev}}{4}$
64	8	10	16
128	16	19	32
192	24	28	48
256	32	37	64

Організація попередньої перестановки 8-бітних укомплектованих елементів d_υ перед формуванням фрейму $B^{(\omega)}$ шифрування забезпечує значне розсіювання бітових розрядів 7-бітних елементів a_ς службових складових з частковим їх перемішуванням. Крім цього порушуються кореляційні взаємозв'язки між сусідніми 8-бітними елементами в фреймах шифрування. Це дає можливість використовувати більш швидкодіючі алгоритми шифрування або відомі стандарти шифрування зі зменшеною кількістю раундів перетворення.

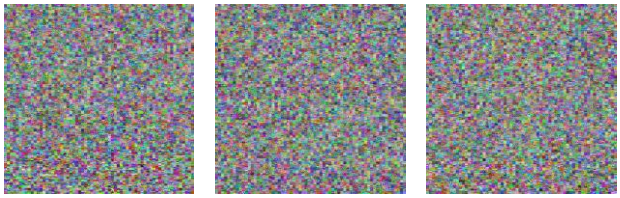
Оцінка ефективності

Існує багато метрік оцінки візуальної якості зображень [40, 41]. В цієї роботі ми обмежимося лише тими, що частіше застосовуються при оцінки ефективності методів забезпечення їх конфіденційності.

Результати оцінки якості забезпечення конфіденційності відеоданих на основі використання схеми криптокомпресійного кодування зображень з зашифрованими СС представлені на рис. 3-5 і в табл. 2. На рис. 4, *а* і 5, *а* представлені гістограми для вихідних незашифрованих СС, на рис. 4, *б* і 5, *б* – для зашифрованих СС в зниженому динамічному діапазоні.

З аналізу отриманих результатів видно, що:

– реконструйовані на основі зашифрованих СС зображення (рис. 3) повністю зруйновані. Вони стали схожі один на одного та не залежать від ступеня насиченості та кольоровості вихідних відеоданих;



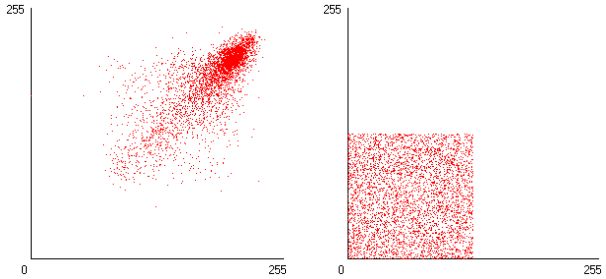
Lena Baboon Airport

Рис. 3. Приклади візуалізації реконструкції тестових зображень з зашифрованими СС

Таблиця 2

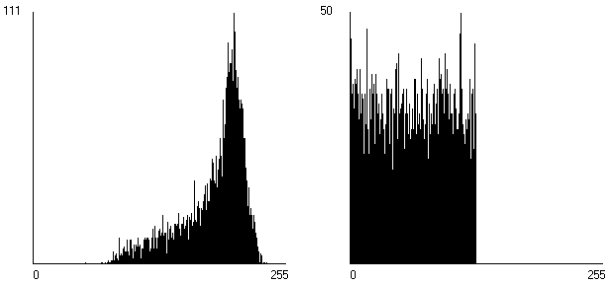
Результати оцінки якості зашифрованих тестових зображень

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



а б

Рис. 4. Приклад гістограм кореляції між елементами службових складових: а – вихідний стан елементів; б – зашифровані елементи в зниженому динамічному діапазоні



а б

Рис. 5. Приклад гістограми розподілу елементів службових складових: а – вихідний стан елементів; б – зашифровані елементи в зниженому динамічному діапазоні

– значення показників якості (див. табл. 2) повністю підтверджують результати візуальної оцінки про повне зруйнування відеоданих. Для всіх типів зображень значення RSME знаходиться вище 80, PSNR – нижче 10 dB, а коефіцієнта кореляції – в районі 0;

– кількість пікселів, що змінилися, NPCR (див. табл. 2) для всіх зображень знаходиться вище теоретичного порогового значення 99,5341 % [42]. Це свідчить про високу стійкість зашифрованих відеоданих до диференціальних атак;

– гістограми кореляції між елементами зашифрованих СС для різних відеозображень збігаються незалежно від вмісту вихідних відеоданих (див. рис. 4, *б*). На гістограмах формується зображення у вигляді квадрата. Вони суттєво відрізняються від гістограм кореляції між вихідними елементами службових складових, на яких формується чіткий малюнок (див. рис. 4, *а*). Квадрат не повністю заповнений одним кольором через малу кількість елементів СС. Їх кількість становить 6,25 % від загальної кількості пікселів у вихідному відеозображенні. Квадрат на гістограмі свідчить про повне порушення кореляції між сусідніми елементами в СС;

– гістограми розподілу елементів зашифрованих СС (див. рис. 5, *б*) сильно змінилися відносно незашифрованого представлення (див. рис. 5, *а*). На гістограмі для незашифрованих даних характерні істотні перепади між кількістю елементів. Так, кількість окремих елементів домінує, а деякі з елементів взагалі можуть не зустрічатися в відеоданих. На гістограмах для зашифрованих СС відсутні випадки, коли кількість елементів дорівнює нулю. Значення щодо кількостей всіх елементів значно вирівняні.

Оцінка додаткової компресії криптокомпресійних кодограм відеоданих за допомогою архіваторів ZIP та RAR без втрати якості інформації показала, що розмір кодограм додатково не зменшився. Це свідчить про відсутність надмірності в криптокомпресійних кодограмах і про усунення кореляції між елементами.

Запропонований підхід щодо об'єднання 7-бітних значень a_ς службових складових в L_{ev}-бітні фрейми $B^{(\omega)}$ шифрування може бути застосований при забезпечення безпеки незжатих зображень. При цьому для вихідних даних організується зниження глибини кольоровості до 7 біт за рахунок відкидання найменшого значущого біта. Це незначно знижує якість відеоданих. Показники якості знаходяться на рівні: RSME – 0,71; PSNR – 51,13 dB; коефіцієнт кореляції – 0,9999. Вони знаходяться на рівні показників якості при організації перетворення з колірного простору RGB в колірний простір YCbCr. Дане зниження якості відеоданих не відчутно, для людського ока. При цьому додатково забезпечується коефіцієнт компресії зображення в 1,14 рази (зменшення обсягу зображення на 12,5 %).

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

Висновки

1. Вперше розроблено метод маскувального ущільнення службових даних в системах компресії відеозображень. Його відмінність від відомих полягає в наступному:

– організовується об'єднання елементів службових складових, представлених в зниженому динамічному діапазоні, в 8-бітові укомплектовані елементи. Це забезпечує усунення шифрування незначущих бітових розрядів в елементах службових складових і змішування даних на основі зсуву бітових розрядів;

– об'єднання елементів службових складових складається з двох каскадів укомплектування та залежить від довжини блоку шифрування. Це збільшує кількість елементів службових складових, що беруть участь у формуванні блоку шифрування;

– перед виконанням шифрування може додатково організовуватися перестановка 8-бітних укомплектованих елементів в межах всіх службових даних. Фактично виконується повноцінне скремблювання даних, що забезпечує їх розсіювання. В результаті у формуванні блоку шифрування беруть участь окремі бітові розряди даних в кількості до 2-х разів більшому, ніж в стандартних підходах без організації попереднього скремблювання;

– за рахунок організації попереднього скремблювання службових даних забезпечується можливість організації шифрування з використанням швидких алгоритмів криптографічного перетворення або з використанням стандартних криптоперетворень зі зменшеними параметрами.

2. Розроблений метод забезпечує:

– підвищення криптостійкості відеоданих за рахунок:

1) змішування даних на основі зсуву бітових розрядів в процесі двохкаскадного укомплектування елементів службових складових криптокомпресійних кодограм;

2) організації попереднього скремблювання та формування блоку шифрування з бітових розрядів різних елементів СС ККП. Їх кількість до 2-х разів більше, ніж в стандартних підходах без організації попереднього скремблювання;

– підвищення доступності відеоданих за рахунок:

1) зменшення кількості даних, які піддаються криптографічному перетворенню. Це досягається шляхом відкидання незначущих бітових розрядів і укомплектування значущих бітових послідовностей у фрейми шифрування;

2) використання швидкодіючих криптографічних перетворень або відомих стандартів шифрування зі зменшеною кількістю раундів перетворення.

3. Практичне значення отриманих результатів:

– формуються криптокомпресійні кодові конструкції з зашифрованими службовими складовими. Зашифровані зображення візуально не відрізняються один від одного і не можуть бути реконструйовані неавтентифікованими користувачами;

– для всіх зашифрованих зображень забезпечується їх руйнування в порівнянні з вихідними відеоданими. Показники якості для таких зображень приймають наступні значення: RSME знаходиться вище 80, PSNR – нижче 10 dB, а коефіцієнт кореляції – в районі 0. Кількість пікселів, що змінюються, для всіх зображень знаходиться вище теоретичного порогового значення 99,5341 %.

4. Розвиток цього дослідження можливий за двома напрямами. По-перше, це вдосконалення існуючих перетворень шифрування для підвищення оперативності їх виконання. По-друге, це вдосконалення методу з позиції обробки динамічних відеоданих.

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. 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.

3. Announcing the ADVANCED ENCRYPTION STANDARD (AES) [Text]. – Federal Information Processing Standards Publication 197, 2001. – 51 p.

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. Naor, M. Visual Cryptography [Text] / M. Naor, A. Shamir // Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science. – 1995. – Vol. 950. – P. 1–12. DOI: 10.1007/bfb0053419.

9. Chen, Ch.-Ch. A secure Boolean-based multi-secret image sharing scheme [Text] / Ch.-Ch. Chen, W.-J. Wu // Journal of Systems and Software. – 2014. – Vol. 92. – P. 107–114. DOI: 10.1016/j.jss.2014.01.001.

10. Deshmukh, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic [Text] / M. Deshmukh, N. Nain, M. Ahmed // IEEE 30 th International Conference on Advanced Information Networking and Applications (AINA). – 2016. – P. 690–697. DOI: 10.1109/aina.2016.56.

11. Yang, Ch.-N. Enhanced Boolean-based multi secret image sharing scheme [Text] / Ch.-N. Yang, Ch.-H. Chen, S.-R. Cai // Journal of Systems and Software. – 2016. – Vol. 116. – P. 22–34. DOI: 10.1016/j.jss.2015.01.031.

12. 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. – 7.04.2021.

13. 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.

14. Wong, K.-W. Image encryption using chaotic maps [Text] / K.-W. Wong // Intelligent Computing Based on Chaos. – 2009. – Vol. 184. – P. 333–354. DOI: 10.1007/978-3-540-95972-4_16.

15. Cryptographic and Information Security Approaches for Images and Videos [Text] / S. Ramakrishnan, et al. – CRC Press, 2018. – 962 p. DOI: 10.1201/9780429435461.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. Dufaux, F. Toward a Secure JPEG [Text] / F. Dufaux, T. Ebrahimi // Applications of Digital Image Processing XXIX. – 2006. – Vol. 6312. – P. 1–8. DOI: 10.1117/12.686963.

23. 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.

24. Hierarchical image-scrambling method with scramble-level controllability for privacy protection [Text] / T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, T. Fujino // IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS). – 2013. – P. 1371–1374. DOI: 10.1109/MWSCAS.2013.6674911.

25. 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.

26. 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.

27. Bitstream-based JPEG Encryption in Real-time [Text] / S. Auer, A. Bliem, D. Engel, A. Uhl, A. Unterweger // International Journal of Digital Crime and Forensics. – 2013. – Vol. 5, Iss. 3. – P. 1–14. DOI: 10.4018/jdcf.2013070101.

28. Kobayashi, H. Bitstream-Based JPEG Image Encryption with File-Size Preserving [Text] / H. Kobayashi, H. Kiya // IEEE 7 th Global Conference on Consumer Electronics (GCCE). – 2018. – P. 1–4. DOI: 10.1109/gcce.2018.8574605.

29. 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.

30. 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.

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

31. 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.

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

33. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability [Text] / Y. Yang, B. B. Zhu, S. Li, N. Yu1 // EURASIP Journal on Information Security. 2008. – Vol. 2007. – Article ID 56365. – 13 p. DOI: 10.1155/2007/56365.

34. 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.

35. Barannik, V. V. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems [Text] / V. V. Barannik, Yu. N. Ryabukha, O. S. Kulitsa // Telecommunications and Radio Engineering. – 2017. - Vol. 76 No. 9. – P. 785–797. DOI: 10.1615/TelecomRadEng.v76.i9.40.

36. 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.

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

38. 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.

39. 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, No. 9(111). – P. 103–115. DOI: 10.15587/1729-4061.2021.235521.

40. Li, F. Two-step providing of desired quality in lossy image compression by SPIHT / F. Li, S. Krivenko, V. Lukin // Radioelectronic and computer systems. – 2020. – No. 2. – P. 22-32. DOI: 10.32620/reks.2020.2.02.

41. Ieremeiev, O. Combined visual quality metric of remote sensing images based on neural network / O. Ieremeiev, V. Lukin, K. Okarma // Radioelectronic and computer systems. – 2020. – No. 4. – P. 4-15. DOI: 10.32620/reks.2020.4.01.

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. 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.

3. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication 197, 2001, 51 p.

4. DSTU 7624:2014: *Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia* [Information Technology. 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. Naor, M., Shamir, A. Visual Cryptography. *Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science*, 1995, vol. 950, pp. 1-12. DOI: 10.1007/bfb0053419.

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. Deshmukh, M., Nain, N., Ahmed, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. *IEEE 30 th International*

Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 690-697. DOI: 10.1109/aina.2016.56.

11. Yang, Ch.-N., Chen, Ch.-H., Cai, S.-R. Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*, 2016, vol. 116, pp. 22-34. DOI: 10.1016/j.jss.2015.01.031.

12. 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 7.04.2021).

13. 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).

14. Wong, K.-W. Image encryption using chaotic maps. *Intelligent Computing Based on Chaos*, 2009, vol. 184, pp. 333–354. DOI: 10.1007/978-3-540-95972-4_16.

15. Ramakrishnan, S. et al. *Cryptographic and Information Security Approaches for Images and Videos*, CRC Press, 2018. 962 p. DOI: 10.1201/9780429435461.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. Dufaux, F., Ebrahimi, T. Toward a Secure JPEG. *Applications of Digital Image Processing XXIX*, 2006, vol. 6312, pp. 1-8. DOI: 10.1117/12.686963.

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

24. 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. DOI: 10.1109/MWSCAS.2013.6674911.

25. 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.

26. 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.

27. Auer, S., Bliem, A., Engel, D., Uhl, A., Unterweger, A. Bitstream-based JPEG Encryption in Real-time. *International Journal of Digital Crime and Forensics*, 2013, vol. 5, iss. 3, pp. 1-14. DOI: 10.4018/jdcf.2013070101.

28. Kobayashi, H., Kiya, H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. *IEEE 7 th Global Conference on Consumer Electronics (GCCE)*, 2018, pp. 1-4. DOI: 10.1109/gcce.2018.8574605.

29. 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.

30. 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.

31. 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).

32. Phatak, A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. International Journal of Image. *Graphics and Signal Processing*, 2016, vol. 8, no. 6, pp 64-71. DOI: 10.5815/ijigsp.2016.06.08.

33. Yang, Y., Zhu, B. B., Li, S., Yu1, N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, 2008, Article ID 56365, 13 p. DOI: 10.1155/2007/56365.

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

34. 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.

35. Barannik, V. V., Ryabukha, Yu. N., Kulitsa, O. S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. *Telecommunications and Radio Engineering*, 2017, vol. 76, no. 9, pp. 785-797. DOI: 10.1615/TelecomRadEng.v76.i9.40.

36. 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.

37. Alimpiev, A. N., Barannik, V. V., Sidchenko, S. A. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. *Telecommunications and Radio Engineering*, 2017, vol. 76, no. 6, pp. 521-534. DOI: 10.1615/TelecomRadEng.v76.i6.60.

38. 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.

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

40. Li, F., Krivenko, S., Lukin, V. Two-step providing of desired quality in lossy image compression by SPIHT. *Radioelectronic and computer systems*, 2020, no. 2, pp. 22-32. DOI: 10.32620/reks.2020.2.02.

41. Ieremeiev, O., Lukin, V., Okarma, K. Combined visual quality metric of remote sensing images based on neural network. *Radioelectronic and computer systems*, 2020, no. 4, pp. 4-15. DOI: 10.32620/reks.2020.4.01.

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.

Надійшла до редакції 16.04.2021, розглянута на редколегії 20.05.2021

МЕТОД МАСКИРОВОЧНОГО УПЛОТНЕНИЯ СЛУЖЕБНЫХ ДАННЫХ В СИСТЕМАХ КОМПРЕССИИ ВИДЕОИЗОБРАЖЕНИЙ

В. В. Баранник, С. А. Сидченко, Н. В. Баранник, А. М. Хименко

Спрос на обеспечение конфиденциальности видеоизображений постоянно увеличивается. При этом необходимо решить актуальную научно-прикладную проблему, которая заключается в повышении конфиденциальности видеоинформации в условиях заданной временной задержки на ее обработку и доставку при обеспечении ее достоверности. Для ее решения могут использоваться криптокомпрессионные преобразования. В качестве ключа преобразования используется служебная составляющая, которая непосредственно формируется в процессе преобразования и содержит информацию о выявленных структурные характеристики видеоданных. Поэтому такая информация требует обеспечения конфиденциальности. Существующие методы криптографии предназначены для обработки универсального потока данных и не учитывают структуру и особенности служебных составляющих. Это приводит к формированию избыточных данных, использования избыточного количества операций и увеличения временных затрат на обработку в процессе защиты служебной информации с использованием универсальных методов криптографии. Поэтому целью статьи является разработка метода маскировочного уплотнения служебных данных для обеспечения их конфиденциальности с учетом особенностей их формирования методами криптокомпрессии. В режимах с контролированной потерей качества информации элементы служебной составляющей формируются в пониженном динамическом диапазоне. Их длина составляет 7 битовых разрядов. Для обеспечения конфиденциальности таких элементов необходимо разработать метод маскировочного уплотнения служебных данных в системах компрессии видеоизображений. С одной стороны, блоки служебных данных не должны содержать избыточной информации. С другой стороны, они должны формироваться из битовых разрядов из разных элементов служебных составляющих. Для этого предлагается организовать укомплектацию элементов служебных составляющих. Она организуется за счет объединения 7-битных элементов служебных составляющих в 8-битные укомплектованные последовательности. Из 8-битных последовательностей формируются блоки шифрования. Укомплектация служебных составляющих обеспечивает смешивание служебных данных и уменьшение их количества. Для нарушения структуры представления служебных составляющих предлагается дополнительно организовать перестановку 8-битных укомплектованных последовательностей. Это обеспечивает значительное рассеивание битовых разрядов 7-битных элементов служебных составляющих и разрушение корреляцию между элементами служебных данных. Коэффициенты корреляции исходных и реконструированных изображений с использованием зашифрованных служебных составляющих находятся

в районе 0. Количество изменяющихся пикселей находится выше теоретического порогового значения 99,5341 %.

Ключевые слова: криптокомпрессионное представление изображения; служебная составляющая; защита информации; конфиденциальность; шифрование; скремблирование; кодирование; компрессия; изображение; наименее значащий бит.

THE METHOD OF MASKING OVERHEAD COMPACTION IN VIDEO COMPRESSION SYSTEMS

V. Barannik, S. Sidchenko, N. Barannik, A. Khimenko

The demand for video privacy is constantly increasing. Simultaneously, it is necessary to solve an urgent scientific and applied problem, which consists in increasing the confidentiality of video information under conditions of a given time delay for its processing and delivery, while ensuring its reliability. The crypto compression transformations can be used to solve it. A service component is used as a conversion key, which is directly formed in the conversion process and contains information about the identified structural characteristics of the video data. Therefore, such information requires confidentiality. The existing methods of cryptography are designed to process a universal data stream and do not consider the structure and features of service components. It leads to the formation of redundant data, the use of an excessive number of operations, and an increase in processing time in the process of protecting service information using universal cryptography methods. Therefore, the article aims to develop a method for masking service data compression to ensure their confidentiality, considering the peculiarities of their formation by crypto compression methods. In modes with controlled loss of information quality, the elements of the service component are formed in a reduced dynamic range. Their length is 7 bits. To ensure the confidentiality of such elements, it is necessary to develop a method for masking overhead compression in video compression systems. On the one hand, overhead blocks should not contain redundant information. On the other hand, they must be formed from bit positions from different elements of the service components. On the other hand, they should be formed from bit positions from different elements of the service components. For that, it is proposed to organize the assembly of the elements of the service components. It is organized by combining 7-bit elements of service components into 8-bit complete sequences. Encryption blocks are formed from 8-bit sequences. The assembly of service components ensures the mixing of service data and reducing their quantity. To violate the structure of the representation of service components, it is proposed to additionally organize the permutation of 8-bit completed sequences. It provides a significant dispersion of the bit positions of the 7-bit overhead elements and the destruction of the correlation between the overhead elements. The correlation coefficients of the original and reconstructed images using encrypted service components are in the region of 0. The number of changing pixels is above the theoretical threshold value of 99.5341%.

Keywords: crypto compression image presentation; service component; information protection; confidentiality; encryption; scrambling; encoding; compression; image; the least significant bit.

Бараннік Володимир Вікторович – д-р техн. наук, проф., проф. кафедри штучного інтелекту та програмного забезпечення, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

Сідченко Сергій Олександрович – канд. техн. наук, старш. наук. співроб., докторант науково-організаційного відділу, Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна.

Бараннік Наталія Вячеславівна – здобувач, Харківський національний університет радіоелектроніки, Харків, Україна.

Хіменко Андрій Михайлович – здобувач, Харківський національний університет радіоелектроніки, Харків, Україна.

Vladimir Barannik – doctor of technical sciences, professor, professor of artificial intelligence and software department, V. N. Karazin Kharkiv National University, Kharkov, Ukraine,
e-mail vvbar.off@gmail.com, ORCID: 0000-0002-2848-4524, Scopus Author ID: 27867503300, https://scholar.google.com/citations?user=3xZFPUQAAAAJ&hl.

Serhii Sidchenko – PhD, senior scientific researcher, doctoral student of scientific organizing department, Ivan Kozhedub National Air Force University, Kharkov, Ukraine,
e-mail sidserg72@gmail.com, ORCID: 0000-0002-1319-6263, Scopus Author ID: 35796112800, https://scholar.google.com/citations?hl=ru&user=MNLC_ckAAAAJ.

Natalia Barannik – PhD student, Kharkov National University of Radio Electronics, Kharkov, Ukraine,
e-mail barannik11121972@gmail.com, ORCID: 0000-0001-6420-1838, Scopus Author ID: 57207757558, https://scholar.google.com.ua/citations?hl=ru&user=6rGhQ5EAAAAJ.

Andrii Khimenko – PhD student, Kharkov National University of Radio Electronics, Kharkov, Ukraine,
e-mail: ahimenko@ukr.net.