УДК 621.327:681.5

МЕТОД СУМІЩЕННЯ КОДОВОЇ КОНСТРУКЦІЇ ЕНЕРГЕТИЧНО ЗНАЧУЩОЇ СТРУКТУРНОЇ ОДИНИЦІ З ВИМОГОЮ МЕТОДУ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ ЗАКРИТТЯ ПОТОКОВИХ ВІДЕОДАНИХ НА ОСНОВІ ТЕХНОЛОГІЇ ВНУТРІКАДРОВОЇ СЕЛЕКЦІЇ

В. В. Бараннік, д-р техн. наук, проф., ***Д. І. Комолов***

Харківський національний університет радіоелектроніки

Barannik_V_V@mail.ru

У статті розроблено метод сумісності кодової конструкції енергетично значущої структурної одиниці з вимогою методу блочного симетричного шифрування алгоритмом шифрування для закриття потокових відеоданих на основі технології внутрікадрової селекції базового відеокадра. Розроблено методологічну базу для розрахунку бітової швидкості зашифрованої структурної одиниці базового відеокадра. Подано схеми формування бітових матриць для поєднання з матрицями ключа шифрування. Також представлена схема шифрування значущої структурної одиниці базового кадру. Проведено порівняльний аналіз бітового потоку зашифрованої структурної одиниці з бітовим потоком початкового фрагмента відеозображення.

Ключові слова: відеокадр, група кадрів, шифрування, «Калина», структурна одиниця, бітова матриця, ключ шифрування, селективне шифрування.

This paper developed a method compatibility code construction energetically significant structural unit with the requirement of the method of block symmetric encryption algorithm encryption to close the streaming video technology-based intra-breeding base of the video frame. The methodological basis for calculating the bit rate of the basic structural unit of the encrypted video frame. Schemes of forming bitmap to match the encryption key matrices. Also, encryption is a diagram of a significant structural unit of the base frame. A comparative analysis of the bitstream encoded structural unit in the bit stream of the original video fragment.

Keywords: video frame, the frame group, encryption, «Kalina», structural unit, bitmap, encryption key, selective encryption.

Вступ

З розвитком технологій, поліпшенням характеристик каналів передачі даних і збільшенням кількості кінцевих користувачів у сучасному світі гостро стоїть питання конфіденційності інформації. До такої інформації відносять і відеодані, які формуються в результаті появи різних відеосервісів. До відеосервісів відносять системи зберігання персональних відеоданих, платні відеосервіси з обмеженим доступом, системи відеоспостереження, системи відеоконференцзв'язку і т.д. Для забезпечення конфіденційності відеодані необхідно шифрувати. Так зване повне шифрування, за якого шифрується вся передана відеоінформація, має низку істотних недоліків: великий час шифрування, навантаження на обчислювальні системи, втрата всієї інформації при помилках, що виникають у процесі передавання по каналах зв'язку. Тому актуальним є використання селективних методів шифрування. Робота селективного методу приховування відеоданих базується на шифруванні не всього відеопотоку, а певних його складових. Такими складовими можуть бути: група кадрів, кадр, макроблок, блок. При такому підході закриття основним недоліком є збільшення інтенсивності (зниження пропускної здатності відеоданих до 70 %). Тому для підвищення пропускної здатності пропонується розглядати метод, заснований на шифруванні найбільш значущих структурних одиниць. Під значущою складовою розуміють таку складову базового видеокадра, яка несе найбільшу семантичну і структурну інформативність. Під структурною одиницею розуміють конструкцію макроблоків трьох складових, що описують фрагмент видеокадра. Складністю в селективному методі шифрування є процесі суміщення алгоритму шифрування з двійковим потоком значущої структурної одиниці. Бітова конструкція структурної одиниці має плаваючу довжину, а ключ шифрування — фіксовану. Під час накладення шифроключа на бітове представлення

фрагментів зображення, може утворюватися надмірність. Відповідно, чим більше фрагментів зображення закривається, тим більше зростає надмірність.

Таким чином, **метою** статті є розробка методу поєднання кодової конструкції енергетично значущої структурної одиниці з вимогою методу блочного симетричного шифрування для закриття потокових відеоданих на основі технології внутрікадрової селекції базового видеокадра без утворення надлишкової інформації.

Основна частина

Для реалізації селективного методу шифрування базового видеокадра пропонується використовувати алгоритм симетричного блокового шифрування «Калина». Алгоритм шифрування «Калина» з довжиною ключа в 128 біт є одним з найшвидших за швидкістю шифрування. Показник швидкості шифрування даного алгоритму перевищує 2500 Мбіт/с. Тому для шифрування значущих структурних одиниць пропонується використання алгоритма «Калина» з довжиною ключа в 128 біт. Такий ключ обраний тому, що його довжини досить для забезпечення необхідного рівня конфіденційності для відомчих систем відеоконференцзв'язку.

Сумісність кодової конструкції енергетично значущої структурної одиниці з алгоритмом шифрування «Калина» полягає в створенні механізму накладення кріптоключа на кодову конструкцію, що підлягає шифруванню, без утворення надлишкової інформації.

Значення DC-компоненти трансформанти ДКП розміром 8*8 елементів може змінюватися від 0 до 2047 (–1024 до 1023, оскільки в JPEG проводиться віднімання 128 з усіх вихідних значень, що відповідає відніманню 1024 з DC).

Тому на кодування кожного значення компоненти $y_{\mu,\eta}$ трансформанти $T_{\varphi}^{(\xi,\gamma)}$ ДКП буде виділятися по 11 біт. Це визначається виразом:

$$v(\varphi)_{\mu,\eta}^{(\xi,\gamma)} = \max_{\substack{1\le\mu\le 8\\ 1\le\eta\le 8}} (\log_2 y_{\mu,\eta}) = 11 \text{ бит},$$

де $v(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ — довжина бітового подання значення компоненти $y_{\mu,\eta}$ трансформанти $T_{\varphi}^{(\xi,\gamma)}$ ДКП-го блоку $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці $S_{зн}^{(\xi,\gamma)}$ зображення.

Однак тут потрібно враховувати такі умови:

1. Довжина ключа шифрування є парним числом. Тому для забезпечення сумісності бітового подання значення компоненти трансформанти ДКП з ключем шифрування, необхідно, щоб довжина коду значення компоненти теж була парною.

2. Значення компоненти трансформанти ДКП може бути як позитивним, так і негативним.

Тому для забезпечення цих умов пропонується використовувати додатковий покажчик знака компоненти трансформанти ДКП.

Довжина його кодового представлення дорівнює 1 біт. Даний покажчик буде використовуватися безпосередньо в бітової послідовності значення компоненти трансформанти ДКП для забезпечення парної довжини коду значення компоненти. Тоді за розміром трансформанти $T_{\varphi}^{(\xi,\gamma)} = \{8,8\}$ довжина кодового представлення компонента в довічним описі буде дорівнює 12 бітам, що показано на рис. 1.

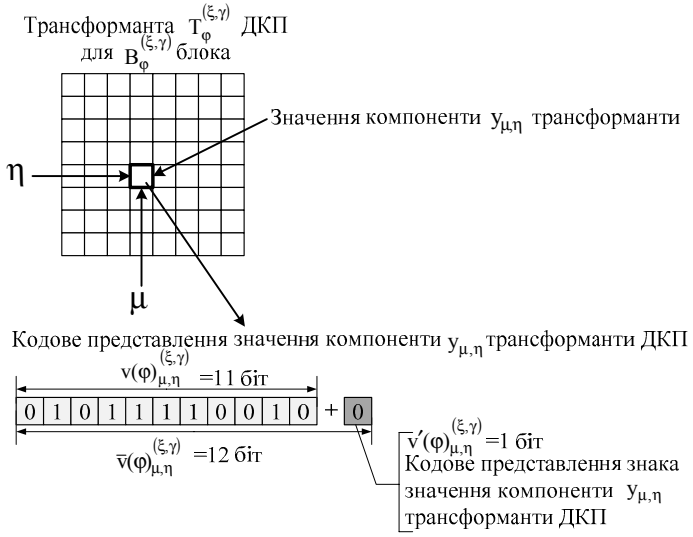

Рис. 1. Схема формування кодового подання значення компоненти трансформанти ДКП для блоку зображення

У перших 11 бітах довжини $v(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ коду записано значення компоненти трансформанти ДКП $y_{\mu,\eta} = 754$. В 12-й біт записується значення 0 або 1, яке враховує знак компоненти. Це представлено в такому виразі:

$$\overline{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)} = v(\varphi)_{\mu,\eta}^{(\xi,\gamma)} + v'(\varphi)_{\mu,\eta}^{(\xi,\gamma)}.$$

Тоді інтенсивність $V(\varphi)_{скр}^{(\xi,\gamma)}$ бітового потоку трансформанти $T_{\varphi}^{(\xi,\gamma)}$ ДКП розраховується так:

$$V(\varphi)_{скр}^{(\xi,\gamma)} = \sum_{i=1}^{\mu\cdot\eta} \overline{v}(\varphi)_i^{(\xi,\gamma)} = 768 \text{ бит} = 96 \text{ байт},$$

де $\overline{v}(\varphi)^{(\xi,\gamma)}$ — довжина кодового представлення (μ,η)-ї компоненти трансформанти ДКП φ-го блоку (ξ,γ)-ї структурної одиниці зображення.

Таким чином, довжина $V(\varphi)_{скр}^{(\xi,\gamma)}$ кодового слова трансформанти ДКП з 64 компонент $T_{\varphi}^{(\xi,\gamma)} = \{y1,..., y64\}$ буде займати 768 біт = 96 байт.

Довжини кодового представлення блоків яскравості і кольоровості, що підлягають шифруванню, рівні. Це представлено таким виразом:

$$V_{B(Y)скр}^{(\xi,\gamma)} = V_{B(Cr)скр}^{(\xi,\gamma)} = V_{B(Cb)скр}^{(\xi,\gamma)} = V(\varphi)_{скр}^{(\xi,\gamma)} =$$
$$= 768 \text{ бит} = 96 \text{ байт},$$

де $V_{B(Y)скр}^{(\xi,\gamma)}$ — довжина кодового представлення трансформанти ДКП блоку яскравості; $V_{B(Cr)скр}^{(\xi,\gamma)}$ — довжина кодового представлення трансформанти ДКП блоку червоного кольору; $V_{B(Cb)скр}^{(\xi,\gamma)}$ — довжина кодового представлення трансформанти ДКП блоку синього кольору.

Інтенсивність $V_{S_{Iскр}}^{''(\xi,\gamma)}$ структурної одиниці, що підлягає шифрування, визначаються так:

$$V_{S_{Iскр}}^{''(\xi,\gamma)} = \sum_{\varphi=1}^{N_b} V(\varphi)_{скр}^{(\xi,\gamma)} = 4608 \text{ бит} = 576 \text{ байт},$$

де N_b — кількість блоків у структурній одиниці.

Інтенсивність $V_{S_{скр}}$ бітового потоку закритої структурної одиниці $S_{зн}^{(\xi,\gamma)}$ розраховуються так:

$$V_{S_{Iскр}} = V_{I_{служ}}^{''(\xi,\gamma)} + V_{S_{Iскр}}^{''(\xi,\gamma)} = V_{I_{служ}}^{''(\xi,\gamma)} + \sum_{\varphi=1}^{N_b} V(\varphi)_{скр}^{(\xi,\gamma)} =$$
$$= 24 \text{ біта} + 4608 \text{ біт} = 4632 \text{ біта} =$$
$$= 3 \text{ байти} + 576 \text{ байт} = 579 \text{ байт}.$$

Таким чином, структура кодової конструкції закритої структурної одиниці матиме вигляд, представлений на рис. 2.

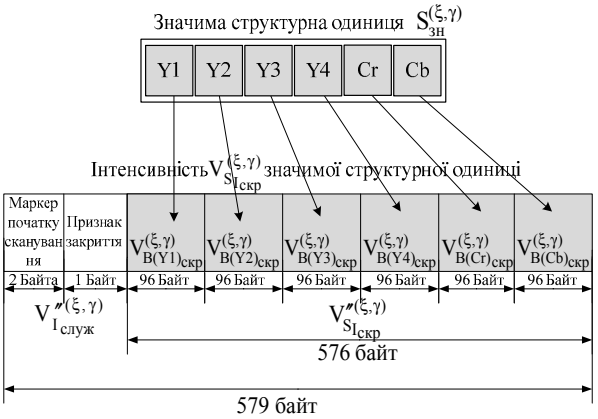

Рис. 2. Структура кодової конструкції закритої структурної одиниці базового видеокадра

Довжина коду вихідного зображення розміром в 256 пікселів ($m = 16, n = 16$), де розмір одного пікселя дорівнює 1 байту, представленого в трьох площинах (YCrCb) буде дорівнює 768 байт:

$$V_{S_{Iисх}} = V_{B(Y_{m,n})исх} + V_{B(Cr_{m,n})исх} + V_{B(Cb_{m,n})исх} =$$
$$= 16\cdot16 \text{ біт} + 16\cdot16 \text{ біт} + 16\cdot16 \text{ біт} = 786 \text{ байт},$$

де $V_{B(Y_{m,n})исх}$ — бітова інтенсивність коду складової яскравості вихідного зображення; $V_{B(Cr_{m,n})исх}$ — бітова інтенсивність складової червоного кольору вихідного зображення; $V_{B(Cb_{m,n})исх}$ — бітова інтенсивність складової синього кольору вихідного зображення.

Звідси випливає, що в результаті застосування внутрикадрового методу селективного шифрування за рахунок використання формату колірного уявлення 4:2:0 інтенсивність бітового потоку структурної одиниці після шифрування знизиться на 25 % порівняно з двійковим потоком вихідного відеозображення.

Ключ алгоритму шифрування «Калина» довжиною в 128 біт (16 байт) представлений у вигляді матриці К, яка складається з 16 елементів по 8 біт (1 байт) кожний:

$$K = \{k_i\}, \text{ де } i = \overline{1,16},$$

де k_i — 8-бітовий елемент матриці шифрування К; i — номер 8-бітового елемента в матриці шифрування К.

Для бітового узгодження елементів матриці шифрування $K = \{k1,...k16\}$ з двійкового потоком компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ пропонується потік $V(\varphi)_{скр}^{(\xi,\gamma)}$ бітів поділити на елементи такої самої довжини як елементи матриці шифрування К. Отже, увесь потік $V_{B(\varphi)скр}^{(\xi,\gamma)}$ бітів компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці поділяється на 96 елементів по 8 біт. Це показано такою формулою:

$$b_i = \frac{V_{B(\varphi)скр}^{(\xi,\gamma)}}{8 \text{ бит}} = \frac{768 \text{ бит}}{8 \text{ бит}} = 96, \text{ де } i = \overline{1,96},$$

де b_i — 8-бітовий елемент переформатованого потоку компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці; i — номер 8-бітового елемента переформатованого потоку компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці.

Схема формування елементів по 8 біт з бітового потоку компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці базового видеокадра представлена на рис. 3.

Рис. 3. Схема формування елементів по 8 біт з бітового потоку компонент трансформанти $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці базового видеокадра

Оскільки довжина ключа алгоритму шифрування «Калина» представлена у вигляді матриці з 16 елементом (4 * 4) довжиною в 128 біт, то для її узгодження з двійкового потоком компонент трансформанти необхідно цей потік бітів поділити на фрагменти по 128 біт. Для цього пропонується поділити потік бітів компонент трансформанти на 8 рівних частин (d1,...,d8), довжина кожної з них дорівнює 96 бітам (12 байтам). Отримані фрагменти (d1,…,d8) по 12 байт розташовуються по черзі зверху вниз.

У результаті формується матриця $\overline{T}_{\varphi}^{(\xi,\gamma)} = \{b1,...,b96\}$ 8-бітових елементів машинного коду компонент трансформанти ДКП.

Таким чином, матриця $\overline{T}_{\varphi}^{(\xi,\gamma)}$ буде мати 12 елементів по горизонталі і 8 елементів по вертикалі. Далі пропонується отриману матрицю $\overline{T}_{\varphi}^{(\xi,\gamma)}$ двійкового коду φ-го блоку $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ї структурної одиниці поділити на 6 матриць (T1, ..., T6) по 128 біт (16 байт). Це виражено такою формулою:

$$\overline{T}_{\varphi}^{(\xi,\gamma)} = T1 \cup T2 \cup T3 \cup T \cup T5 \cup T6$$

Формування матриць відбувається діленням рядків d1, d2, d3 d4 і d5, d6, d7, d8 на три рівні частини по 4 байта (16 біт) що показано на рис. 4.

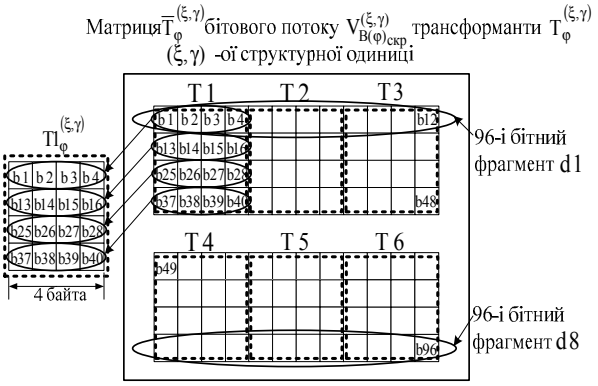

Рис. 4. Формування матриць T1,...,T6 двійкового коду для накладення на них шифроключа К

На рис. 4 видно, що в результаті скремблювання 8-ми бітових елементів (b1,...,b96) матриці $\overline{T}_{\varphi}^{(\xi,\gamma)}$ бітового коду додатково підвищуються стійкість і ступінь захисту закритих відеоданих.

Таким чином, для шифрування бітового потоку трансформанти ДКП блоку зображення (ξ,γ) -ї структурної одиниці базового видеокадра сформовано 6 матриць (T1, ..., T6) такого самого розміру, як і шифроключ (128 біт).

Ключ шифрування К довжиною в 128 біт накладається на кожну матрицю (T1,...,T6) бітового коду окремо. Це представлено в таких висловлюваннях:

$$T'1 = E_K(T1);\ T'2 = E_K(T2);\ T'3 = E_K(T3);$$

$$T'4 = E_K(T4);\ T'5 = E_K(T5);\ T'6 = E_K(T6),$$

де E_K — функція шифрування матриць $T_i = T1,...,T6$ матрицею ключів К.

Функція шифрування E_K за допомогою матриці $K = \{k1,...k16\}$ проводить шифрування матриці T_i. Алгоритм шифрування «Калина» виконує шифрування кожного з 16 елементів матриці T_i за допомогою 16 елементів матриці ключів $K = \{k1,...k16\}$.

Довжина кожного елемента в матриці шифрування К і матриці T_i дорівнює 8 бітам. У результаті формуються 6 матриць $(T'1,...,T'6)$ бітових зашифрованих компонент трансформанти ДКП блоку видеокадра.

Процес накладення шифроключа на матрицю T1 показано на рис. 5.

Із рис. 5 видно, що в результаті накладення 16-байтового ключа К на 16-байтову матрицю T1 довічних даних формується 16-байтова матриця $T'1$ зашифрованих компонент трансформанти ДКП. Таким чином, відбувається шифрування всіх бітових матриць значущої структурної одиниці без утворення надлишкових бітів даних.

На рис. 6 представлена схема формування бітового потоку з матриці $\overline{T}_{\varphi}^{(\xi,\gamma)}$ зашифрованого двійкового коду, де показано процес шифрування алгоритмом «Калина» і схема формування машинного коду зашифрованою енергетично значущою структурною одиницею $S_{зн}^{(\xi,\gamma)}$ видеокадра. В результаті відбувається шифрування всього бітового потоку енергетично значущих структурних одиниць $S_{зн}^{(\xi,\gamma)}$ відеозображення без залишку і надлишку бітових послідовностей.

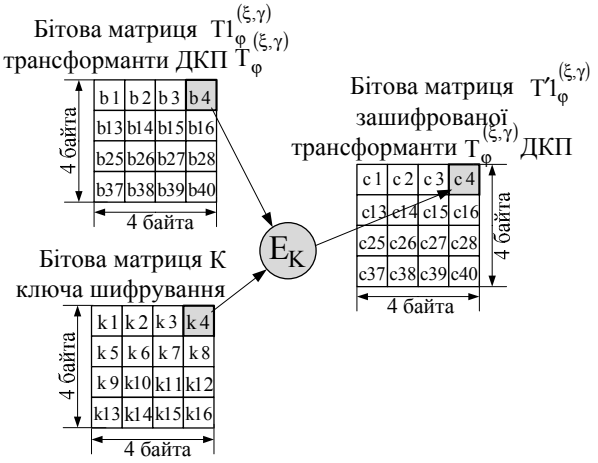

Рис. 5. Схема шифрування довічних даних матриці T1 з матриці бітового коду компонент трансформанти ДКП блоку зображення

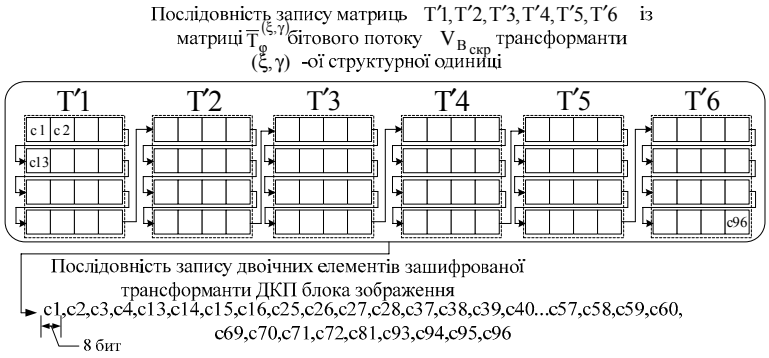

Рис. 6. Схема формування бітового потоку з матриці зашифрованого двійкового коду

Висновки

Розроблено метод сумісності кодової конструкції енергетично значущої структурної одиниці і ключової послідовності алгоритму шифрування «Калина», що базується на таких технологічних складових:

1. Формування 12-бітового кодового подання значення компоненти трансформанти ДКП з 11-бітового значення компоненти трансформанти ДКП і 1-бітового елемента, який визначає знак значення цієї компоненти. В результаті утворюється машинне слово парної довжини. Таким чином, досягається подальша сумісність бітового потоку енергетично значущої структурної одиниці з 128-бітовим ключем шифрування.

2. Формування кодової конструкції значущої структурної одиниці базового видеокадра, що підлягає шифруванню.

У результаті певним чином записується 579-бітова послідовність службових даних і цифрових описів блоків яскравості і кольоровості структурної одиниці.

3. Формування матриць двійкового коду значущою структурною одиницею такого самого розміру, що і ключ шифрування.

У результаті відбувається скремблирование бітового потоку, що додатково підвищує ступінь захисту і завадостійкості переданих закритих відеоданих.

При шифруванні сформованих матриць кодового представлення структурної одиниці за допомогою алгоритму «Калина» досягається повна сумісність 128-бітового шіфроключа зі 128-бітовими фрагментами потоку структурної одиниці без утворення надлишкових бітів даних. Потім із отриманих матриць двійкового коду зашифрованою структурною одиницею формується битовая послідовність закритих відеоданих.

У результаті застосування методу сумісності кодової конструкції енергетично значущої структурної одиниці і ключовій послідовності алгоритму шифрування «Калина» при використанні внутрікадрової селективної обробки базового видеокадра відбувається збільшення інтенсивності закритого базового видеокадра на 20–45 % порівняно з компресійним базовим відеокадром. При цьому досягається зменшення інтенсивності зашифрованої структурної одиниці порівняно з початковою на 25 % за рахунок використання формату колірного уявлення 4: 2: 0.

Уперше розроблено метод сумісності кодової конструкції енергетично значущої структурної одиниці за методом блочного симетричного шифрування для закриття потокових відеоданих на основі технології внутрікадрової селекції базового видеокадра. Відмінні риси даного методу від інших методів сумісності полягають у:

– формуванні парної довжини двійкового коду компонент трансформанти ДКП для блока зображення за рахунок використання максимального (фіксованого) значення компоненти трансформанти ДКП і її знака;

– формування матриць з двійкового коду значущої структурної одиниці такого самого розміру, що й матриця ключа шифрування для їх повної сумісності.

У результаті застосування даного методу інтенсивність двійкового коду зашифрованого відеозображення збільшується на 20–45 % порівняно з бітової інтенсивністю компресійного кадру і зменшується на 25 % порівняно з інтенсивністю вихідного видеокадра. Це відбувається за рахунок використання формату колірного уявлення 4: 2: 0 і формування матриць з двійкового коду значущої структурної одиниці такого самого розміру, що й матриця ключа шифрування без внесення додаткової надмірності. Так само, за рахунок формування матриць машинного коду необхідного розміру відбувається скрембліювання елементів у матрицях зашифрованих компонент трансформанти ДКП. Це додатково підвищує конфіденційність закритого відеоінформаційні ресурсу. За рахунок шифрування тільки найбільш значущих структурних одиниць, а не всього бітового потоку базового видеокадра, підвищується стійкість переданих відеоданих.

ЛІТЕРАТУРА

1. *Rate* Control and H.264. Режим доступу: http://www.pixeltools.com/rate_control_paper.html.

2. *Гонсалес Р*. Цифрова обробка зображень / Р. Гонсалес, Р. Вудс // М. : Техносфера, 2006. — 1072 с.

3. *Кирилов С. Н*. Алгоритм стиснення цифрових зображень з використанням синтезованого базиса на кожній ступені вейвлет-пакетного розкладення / С. Н. Кирилов, И. В. Косткин // Доклади 10-й Международної конференції «Цифрова обробка сигналів та її використання». — М., 2008. — Т.2. — С. 480–483.

4. *Горбенко І. Д.* Перспективний блоковий шифр «Калина»: основні положення та специфікації / І. Д. Горбенко, В. І. Долгов, Р. В. Олейніков // Прикладна радіотехніка, 2007, частина 6, № 2. — С. 195–208.

5. *Долгов В. І.* Подстановочні конструкції сучасних симетричних блочних шифрів / В. І. Долгов // Радіоелектронні і комп'ютерні системи, 2009, № 6. — С. 65—93.