

УДК 621.3

В.В. Бараннік¹, Р.В. Тарнополов¹, Г.В. Хаханова², Д.В. Бараннік²¹ Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків² Харківський національний університет радіоелектроніки, Харків

МЕТОД ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ТА КОНФІДЕНЦІЙНОСТІ ВІДЕОДАНИХ В ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Пропонується розробити метод закриття відеопотоку з застосуванням двійкового структурного кодування, який базується на виявленні та закритті значущих структурних одиниць, застосовуючи структурне кодування до шифрограми, після використання гарантованого алгоритму шифрування.

Ключові слова: відеопоток, двійкове структурне кодування, значущі структурні одиниці, алгоритм шифрування.

Вступ

Виконання вимог до відеоінформації у відомчих системах за допомогою відеообладнання та передача закритих відеоінформаційних потоків, по існуючим низькошвидкісним каналам зв'язку, не забезпечує необхідний рівень конфіденційності при заданій оперативності та достовірності [1–2].

Отже, існує протиріччя, зумовлене наявністю дисбалансу між відомчими вимогами до відеоінформаційних сервісів і характеристиками системи від'єконоференцзв'язку. Можна забезпечити конфіденційність відеоресурсу, але програти в оперативності доставки відеоданих. Тому підвищення конфіденційності відеоінформації в умовах забезпечення заданої якості відеосервісу є задачею на дослідження.

Виклад основного матеріалу

Розробка загального методу підвищення оперативності та конфіденційності відеоданих на основі двійкового структурного кодування.

Пропонується закрити базовий відеокадр K_1 з урахуванням селекції значущих $S_{zn}^{(\xi, \gamma)}$ структурних одиниць.

Метод закриття відеопотоку з урахуванням селекції значущих $S_{zn}^{(\xi, \gamma)}$ структурних одиниць базового відеокадру K_1 і застосування двійкового структурного кодування включає в себе такі базові етапи [3–6]:

1. Виділення групи кадрів G з потоку відеоданих J .
2. Встановлення базового відеокадру K_1 в групі кадрів.
3. Переведення базового відеокадру з кольорового формату RGB у кольорний формат YCrCb і формування трьох цифрових площин відеозображення (цифрова площина яскравісної складової Y , цифрова площина складової червоного кольору Cr , цифрова площина складової синього кольору Cb).
4. Композиція структурних одиниць $S^{(\xi, \gamma)}$ базового відеокадру K_1 включає в себе такі етапи:
 - 4.1. Сегментизація зображення, яка спрощує буфери-

зацію відеоданих для їх передачі по каналах зв'язку. В результаті цього формуються блоки $V(Y)_\phi^{(\xi, \gamma)}$,

$V(Cr)_\phi^{(\xi, \gamma)}$ і $V(Cb)_\phi^{(\xi, \gamma)}$ розміром $k \times l$ пікселів.

4.2. Побудова композицій макроблоків $M(Y)^{(\xi, \gamma)}$, $M(Cr)^{(\xi, \gamma)}$ та $M(Cb)^{(\xi, \gamma)}$ на основі об'єднання блоків.

4.3. Складання структурних одиниць $S^{(\xi, \gamma)}$ з макроблоків $M(Y)^{(\xi, \gamma)}$, $M(Cr)^{(\xi, \gamma)}$ та $M(Cb)^{(\xi, \gamma)}$.

5. Дискретне косинусне перетворення блоків $V(Y)_\phi^{(\xi, \gamma)}$, $V(Cr)_\phi^{(\xi, \gamma)}$ та $V(Cb)_\phi^{(\xi, \gamma)}$ відеозображення.

6. Селекція значущих структурних одиниць, яка складається з таких дій: 6.1. Для виявлення значущих блоків встановлюються порогові значення δ_{\min_n} , δ_{\max_n} і δ_v .

Визначення значущості структурної одиниці відбувається в результаті порівняння порогових значень з показниками $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю значень низькочастотних компонент і показниками $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю високочастотних значень компонент трансформанти ДКП.

6.2. Визначення показника $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю низькочастотних значень компонент трансформанти ДКП в блоках $V(Y)_\phi^{(\xi, \gamma)}$ яскравісної складової.

6.3. Визначення показника $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю високочастотних значень компонент трансформанти ДКП в блоках $V(Y)_\phi^{(\xi, \gamma)}$ яскравісної складової.

6.4. Визначення енергетичної значущості за низькочастотною складовою. Це дає змогу виявити яскравісні та контрастні переходи в блоці відеозображення. Визначення енергетично значущих блоків відбувається в результаті порівняння показника $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю низькочастотних значень компонент трансформанти ДКП з пороговими значеннями δ_{\min_n} та δ_{\max_n} .

Якщо показник $Z(B_n)_\phi^{(\xi, \gamma)}$ за сукупністю низькочастотних

значень компонент більший за порогові значення або знаходиться між δ_{\min} та δ_{\max} , то блок вважається відповідно сильнонасиченим або середньонасиченим. Порівняння відбувається з усіма блоками $V(Y)_{\phi}^{(\xi, \gamma)}$ яскравісної складової структурної одиниці. 6.5. Визначення енергетичної значущості за високочастотною складовою відбувається тільки для блоків, які вважаються енергетично насиченими за низькочастотною складовою. Це відбувається шляхом порівняння показника $Z(B_v)_{\phi}^{(\xi, \gamma)}$ за сукупністю високочастотних значень компонент трансформанти з пороговим значенням δ_v . Таким чином, визначається наявність текстурних переходів і дрібних деталей в блоці $V(Y)_{\phi}^{(\xi, \gamma)}$ яскравісної складової відеокадру, крім наявних у ньому яскравих і контрастних переходів. 6.6. Якщо виконуються умови (п.п. 6.4, 6.5) щодо визначення структурної та семантичної значущості для блока $V(Y)_{\phi}^{(\xi, \gamma)}$ яскравісної складової, то мітка для визначення енергетичної значущості макроблока набуває значення $M=1$. У цьому випадку структурна одиниця, до складу якої входять макроблоки яскравості та кольоровості, вважається енергетично значущою $S_{\text{зн}}^{(\xi, \gamma)} = S^{(\xi, \gamma)}$. 6.7. Обробка значущих структурних одиниць $S_{\text{зн}}^{(\xi, \gamma)}$. Всі значення компонент ДКП блоків яскравості і кольоровості $V(Y)_{\phi}^{(\xi, \gamma)}$, $V(Cr)_{\phi}^{(\xi, \gamma)}$ та $V(Cb)_{\phi}^{(\xi, \gamma)}$ зашифровуються гарантованим алгоритмом шифрування. 6.8. Застосування структурного кодування до отриманих блоків.

7. Обробка незначущих структурних одиниць $S_{\text{незн}}^{(\xi, \gamma)}$. Якщо в макроблоці $M(Y)_{\phi}^{(\xi, \gamma)}$ яскравісної складової немає блоків $V(Y)_{\phi}^{(\xi, \gamma)}$, що володіють структурною і семантичною насиченістю, то мітка набуває значення $M=0$. Тоді така структурна одиниця вважається незначущою $S_{\text{незн}}^{(\xi, \gamma)} = S^{(\xi, \gamma)}$. Кодування незначущої структурної одиниці $S_{\text{незн}}^{(\xi, \gamma)}$ відбувається за стандартним алгоритмом компресії відеозображення JPEG, який складається з таких етапів: 7.1. Квантування компонент трансформанти ДКП за допомогою таблиць квантування, що задаються. На цьому етапі здійснюється управління ступенем стиснення і відбуваються найбільші втрати. 7.2. Лінеаризація трансформанти ДКП у вектор шляхом зигзаг-сканування всіх компонент трансформанти ДКП. 7.3. Згортання вектора за допомогою алгоритму групового кодування (RLE). Відбувається заміна однакових символів, які йдуть підряд, числом, що характеризує їх кількість. 7.4. Кодування одержаних пар із застосуванням фіксованих таблиць Хаффмана.

8. Формування стиснутого представлення закритої базового відеокадру шляхом формування єдиного кодового потоку зашифрованих і закодова-

них структурних одиниць.

9. Обробка Р-кадру, яка включає в себе: 9.1. Прогнозування вперед за попереднім I- або Р-кадром. Робиться обчислення різниці з відповідним макроблоком в опорному кадрі для формування різницевого кадру або кодування з прогнозуванням, в результаті чого формується різницевий кадр. 9.2. Кодування макроблоків за стандартним алгоритмом компресії відеозображення JPEG.

10. Обробка В-кадру, яка включає в себе такі етапи: 10.1. Прогнозування вперед або назад за попереднім I- або Р-кадром. Робиться обчислення різниці з відповідним макроблоком в наступному або попередньому кадрі для формування проміжного кадру або кодування з прогнозуванням. 10.2. Кодування макроблоків за стандартним алгоритмом компресії відеозображення JPEG.

11. Формування стиснутого представлення закритої групи кадрів шляхом кодування і зберігання інформації про черговий кадр, що відрізняється від інших наявністю або відсутністю залежностей цього кадру від попереднього і наступного.

Структура відеопотоку складається з таких рівнів [7–9]:

1. Рівень відеопотоку Stream. Цей рівень формується з послідовності груп відеокадрів GOP.

2. Рівень груп відеокадрів GOP. Цей рівень складається з послідовності відеокадрів. Кожна група кадрів формується з визначеної кодером кількості кадрів I, В і Р типів, де I-кадр є основним, а решта відеокадрів посилаються на I-кадр. У стандартних режимах кодування група відеокадрів зазвичай складається з 8, 12, 15 кадрів.

3. Рівень відеокадрів. На цьому рівні кожний базовий кадр K_1 переводиться з формату кольорового представлення RGB у формат YCrCb, в результаті чого він представляється у вигляді трьох площин по одній від кожного кольорового формату. Ці площини розбиваються на безліч структурних одиниць $S^{(\xi, \gamma)}$.

4. Рівень структурних одиниць $S^{(\xi, \gamma)}$. На відміну від стандартного алгоритму JPEG, селективний метод обробки відеокадру не передбачає використання трьох макроблоків $M(Y)_{\phi}^{(\xi, \gamma)}$, $M(Cr)_{\phi}^{(\xi, \gamma)}$ та $M(Cb)_{\phi}^{(\xi, \gamma)}$ – по одному від кожної кольорової складової. На цьому рівні відбувається формування структурних одиниць $S^{(\xi, \gamma)}$ з блоків яскравості $V(Y)_{\phi}^{(\xi, \gamma)}$ та кольоровості $V(Cr)_{\phi}^{(\xi, \gamma)}$,

$V(Cb)_{\phi}^{(\xi, \gamma)}$. Селективний метод обробки відеоданих припускає наявність як значущих $S_{\text{зн}}^{(\xi, \gamma)}$, так і незначущих $S_{\text{незн}}^{(\xi, \gamma)}$ структурних одиниць. Енергетична значущість структурних одиниць визначається на основі структурної та семантичної насиченості блоків $V(Y)_{\phi}^{(\xi, \gamma)}$ яскравісної складовою, що входять до складу цих структурних одиниць $S^{(\xi, \gamma)}$. Кількість блоків,

що входять до складу структурної одиниці, може змінюватися залежно від колірного формату представлення відеокадру.

5. Рівень блоків $V(Y)_{\phi}^{(\xi,\gamma)}$, $V(Cr)_{\phi}^{(\xi,\gamma)}$, $V(Cb)_{\phi}^{(\xi,\gamma)}$.

На цьому рівні відбувається формування послідовності блоків для їх подальшого кодування або шифрування. Алгоритм селективної обробки визначає енергетичну значущість структурних одиниць $S^{(\xi,\gamma)}$ за структурною та семантичною значущістю блоків яскравісної складової. Енергетично значущі блоки обробляються за розробленим алгоритмом селективного шифрування. Так, після формування трансформант ДКП блоків енергетично значущих структурних одиниць $S_{\text{зн}}^{(\xi,\gamma)}$ відбувається шифрування значень компонент цих трансформант. Всі незначущі блоки зображення кодуються за стандартним алгоритмом JPEG [3].

6. Рівень кодового представлення відеоданих. На цьому рівні здійснюється цифровий опис блоків у певному порядку. Спочатку записується службова інформація про блоки і характеристики їх кодування. Після чого проводиться запис інформаційної частини кодової конструкції блоків. Цифрове представлення блоків здійснюється у певному порядку: спочатку по черзі записуються кодограми блоків яскравісної складової, потім блоків червоного кольору, після чого – синього. Приклад такого опису виглядає наступним чином: Y1Y2Y3Y4CrCb.

Висновки

1. Обґрунтовано необхідну службу інформацію, яка потрібна для взаємно-однозначного відновлення двійкових даних.

2. Побудовано рекурентне відновлення елементів двійкових масивів, що ґрунтується на одновимірному плаваючому структурному декодуванні двійкових послідовностей. Це декодування відрізняється від інших підходів тим, що: декодування проводиться для кодових конструкцій, сформованих для змінної кількості двійкових елементів; вагові коефіцієнти знаходяться за рекурентними виразами на основі відомих значень двох попередніх відновлених елементів і вагового коефіцієнта попереднього елемента.

Список літератури

1. Комолов Д.І. Метод захисту низькочастотних складових в алгоритмі кодування JPEG / Д.І. Комолов, В.В. Ларін, Д.С. Гаврилов, К. Ялівець // Системи обробки інформації. – 2015. – №9. – С. 121-123.
2. Баранник В.В. Методология селективной защиты видеопотока по базовым кадрам для ведомственных систем / В.В. Баранник, Д.И. Комолов, Р.В. Тарнополов, О.Ю. Отман Шади // Інформаційна безпека України: наук.-техн. конф., (Київ, 12–13 берез. 2015 р.). – Київ. нац. ун-т імені Тараса Шевченка. – С. 25.
3. Алімпієв А.М. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні / А.М. Алімпієв, В.В. Баранник, Т.В. Белікова, С.О. Сідченко // Системи обробки інформації. – 2017. – № 4(150). – С. 113-121.
4. Баранник В.В. Метод эффективного кодирования разделенных по комбинированной схеме аэрофотоснимков / В.В. Баранник, С.Ю. Стасев, Р.В. Тарнополов // Радиоэлектроника и информатика. – 2016. – №2 (73). – С. 33-37.
5. Barannik V.V. The model of avalanche-relating effect in the process of images reconstruction in the combined cryptosemantic systems on the polyadic presentation / V.V. Barannik V.V. Larin, S.A. Sidchenko // Наукоємні технології. – 2010. – № 1(5). – С. 68-70.
6. Barannik V.V. Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component / V.V. Barannik, Dm. Komolov, A.P. Musienko, R.V. Tarnopolov // Modern problems of radio engineering, telecommunications and computer science (TCSET'2016): the XIV International Conference, (Lviv –Slavske, Ukraine, February 22-26, 2016). P. 572-574.
7. Barannik V.V. The Method Of Controlling The Rationing Component Of Transformants Based On The Structural Richness Of Aerial Photographs Fragments / V.V. Barannik, S.A. Podlesny, S.Yu. Stasev // Science-based technologies. – 2016. – Vol. 31. – No 3. – Pp. 261-264.
8. Barannik V. The methods of intellectual processing of video frames to enhance their semantic integrity and efficiency of delivery in aeromonitor systems / V.V. Barannik, Yu.N. Ryabukha, A.V. Hahanova, A.P. Musienko // International Symposium [«IEEE Design & Test»], (Batumi, Georgia, September 26-29, 2015). – Batumi, 2015. – Pp. 379-382.
9. Barannik V. Synthesis of Combined Crypto-compressed Systems for Providing Safety Video Information in Infocommunications / Vladimir Barannik, Sergey Sidchenko, Ivan Tupitsya, Sergey Stasev // International Symposium [«IEEE East-West Design & Test»], (Batumi, Georgia, September 26–29, 2015). – Batumi, 2015. – P. 421-423.

Надійшла до редколегії 29.06.2017

Рецензент: д-р техн. наук проф. В.М. Безрук, Харківський національний університет радіоелектроніки, Харків.

МЕТОД ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ВИДЕОДАНЫХ В ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

В.В. Баранник, Р.В. Тарнополов, А.В. Хаханова, Д.В. Баранник

Разрабатывается метод закрытия видеопотока с применением двоичного структурного кодирования, который основан на выявлении и закрытии значимых структурных единиц, применяя структурное кодирование в шифрограммы, после использования гарантированного алгоритма шифрования.

Ключевые слова: видеопоток, двоичное структурное кодирование, значимые структурные единицы, алгоритм шифрования.

METHOD OF IMPROVING OPERATIONAL PRIVACY AND CONFIDENTIALITY OF VIDEOINFORMATION BASED IN INFOCOMMUNICATION TECHNOLOGIES

V. Barannik, R. Tarnopolov, A. Khakhanova, D. Barannik

A method for closing a video stream using binary structured coding is developed, which is based on the identification and closing of significant structural units, applying structural coding to the ciphertexts, after using the guaranteed encryption algorithm.

Keywords: video stream, binary structural coding, significant structural units, encryption algorithm.