УДК 621.327:681.5

В.В. Баранник[1], Д.И. Комолов[2]

[1] *Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков*
[2] *Харьковский национальный университет радиоэлектроники, Харьков*

МЕТОД СЕЛЕКТИВНОЙ ОБРАБОТКИ БАЗОВОГО КАДРА ДЛЯ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ЗАКРЫТОГО ВИДЕОКАНАЛА В ВЕДОМСТВЕННЫХ СИСТЕМАХ

В данной статье разработан метод селективной обработки базового видеокадра, основанный на совместимости кодовой конструкции энергетически значимой структурной единицы с требованием метода блочного симметричного шифрования алгоритмом шифрования для закрытия потоковых видеоданных на основе технологии внутрикадровой селекции базового видеокадра. Данный метод позволяет повысить пропускную способность закрытого канала видеосвязи в ведомственных системах передачи данных. Разработана методологическая база для расчета битовой скорости зашифрованной структурной единицы базового видеокадра. Представлены схемы формирования битовых матриц для совмещения с матрицами ключа шифрования. Также представлена схема шифрования и расшифровывания значимой структурной единицы базового кадра. Проведен сравнительный анализ битового потока зашифрованной структурной единицы с битовым потоком исходного фрагмента видеоизображения. Представлен пример закрытого базового видеокадра на основе шифрования значимых структурных единиц.

Ключевые слова: *видеокадр, группа кадров, шифрование, калина, структурная единица, битовая матрица, ключ шифрования, селективное шифрование.*

Введение

С развитием технологий, улучшением характеристик каналов передачи данных и увеличением количества конечных пользователей в современном мире остро стоит вопрос конфиденциальности информации. К такой информации относятся и видеоданные, которые формируются в результате появления различных видеосервисов. К видеосервисам относятся системы хранения персональных видеоданных, платные видеосервисы с ограниченным доступом, системы видеонаблюдения, публичные и ведомственные системы видеоконференцсвязи, специальные системы хранения и передачи видеоданных. К специальным системам хранения и передачи видеоданных относятся системы, применяемые в проведении оперативных и следственных мероприятий. Для обеспечения конфиденциальности видеоданные необходимо шифровать. Так называемое полное шифрование, при котором шифруется вся передаваемая видеоинформация, обладает рядом существенных недостатков: большое время шифрования, нагрузка на вычислительные системы, потеря всей информации при ошибках, возникающих в процессе передачи по каналам связи. Поэтому актуальным направлением научно-прикладных исследований является использование селективных методов шифрования.

Работа селективного метода скрытия видеоданных базируется на шифровании не всего видеопотока, а определенных его составляющих. Такими составляющими могут быть: группа кадров, кадр, макроблок, блок. В таком подходе закрытия основным недостатком является увеличение интенсивности (снижение пропускной способности видеоданных до 70%). Поэтому для повышения пропускной способности предлагается рассматривать метод, основанный на шифровании наиболее значимых структурных единиц. Под значимой составляющей понимается такая составляющая базового видеокадра, которая несет в себе наибольшую семантическую и структурную информативность. Под структурной единицей понимается конструкция макроблоков трех составляющих, описывающих фрагмент видеокадра. Сложностью в селективном методе шифрования является процесс совмещения алгоритма шифрования с битовым потоком значимой структурной единицы. А также процесс декодирования зашифрованной значимой структурной единицы. Битовая конструкция структурной единицы имеет плавающую длину, а ключ шифрования – фиксированную. При наложении шифроключа на битовое представление фрагментов изображения может образовываться избыточность. Соответственно, чем больше фрагментов изображения закрывается, тем больше возрастает избыточность. В процессе декодирования сложность вызывает процедура определения зашифрованных фрагментов изображения из всего потока видеоданных [4].

Таким образом, **целью статьи** является разработка селективного метода обработки базового кадра для повышения пропускной способности закрытого видеоканала в ведомственных системах. А также создание метода кодирования и декодирования закрытого видеопотока на основе технологии внутрикадровой селекции.

Основная часть

Для реализации селективного метода шифрования базового видеокадра предлагается использовать алгоритм симметричного блочного шифрования «Калина». Данный алгоритм был принят в национальном стандарте Украины ДСТУ 7624:2014 «Информационные технологии. Криптографическая защита информации. Алгоритм симметричного блочного преобразования» (введен в действие 1 июля 2015 г.). Это позволяет применять его в ведомственных телекоммуникационных системах Украины. Криптографические преобразования, применяемые в алгоритме, соответствуют современным требованиям к уровню криптографической стойкости и быстродействию. Алгоритм разработан с учетом существующих и потенциальных угроз, дальнейшего интенсивного развития информационных технологий и необходимости активного использования в течение нескольких следующих десятилетий [1].

Алгоритм шифрования «Калина» с длиной ключа в 128 бит является одним из самых быстрых по скорости шифрования. Показатель скорости шифрования данного алгоритма превышает 2500 Мбит/с. Поэтому для шифрования значимых структурных единиц предлагается использование алгоритм «Калина» с длиной ключа в 128 бит. Такой ключ выбран потому, что его длины достаточно для обеспечения требуемого уровня конфиденциальности для ведомственных систем видеоконференцсвязи.

Совместимость кодовой конструкции энергетически значимой структурной единицы с алгоритмом шифрования «Калина» заключается в создании механизма наложения криптоключа на кодовую конструкцию, подлежащую шифрованию, без образования избыточной информации.

Значения DC-компоненты трансформанты ДКП размером 8*8 элементов может меняться от 0 до 2047 (-1024 до 1023, так как в JPEG производится вычитание 128 из всех исходных значений, что соответствует вычитанию 1024 из DC). Поэтому на кодирование каждого значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП будет выделяться по 11 бит. Это определяется следующим выражением:

$$v(\varphi)_{\mu,\eta}^{(\xi,\gamma)} = \max_{\substack{1\le\mu\le8\\1\le\eta\le8}}(\log_2 y_{\mu,\eta}) = 11 \text{ бит},$$

где $v(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ – длина битового представления значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП φ-го блока $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы $S_{\text{зн}}^{(\xi,\gamma)}$ изображения.

Однако здесь требуется учитывать следующие условия:

1. Длина ключа шифрования является четным числом. Поэтому для обеспечения совместимости битового представления значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП с ключом шифрования, необходимо, чтобы длина кода значение компоненты $y_{\mu,\eta}$ тоже была четной.

2. Значение компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП может быть как положительным, так и отрицательным.

Поэтому для обеспечения этих условий предлагается использовать дополнительный указатель знака компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Длина его кодового представления равна 1 бит. Данный указатель будет использоваться непосредственно в битовой последовательности значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП для обеспечения четной длины кода значение компоненты $y_{\mu,\eta}$. Тогда при размере трансформанты $T_{\varphi}^{(\xi,\gamma)} = \{8,8\}$ длина кодового представления компонента в двоичном описании будет равна 12 битам. Это представлено на рис. 1.

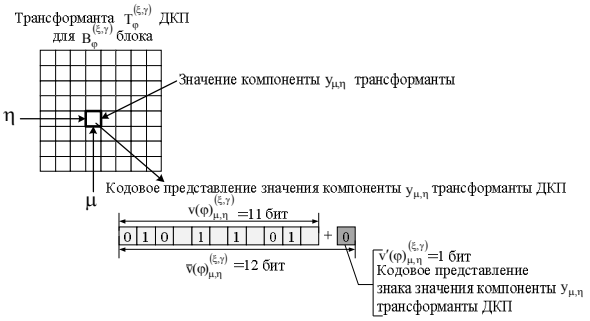

Рис. 1. Схема формирования кодового представления $\bar{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП для блока $B_{\varphi}^{(\xi,\gamma)}$ изображения

На рис. 1 изображено сформированное кодовое представление компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП длиной $\bar{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ в 12 бит для дальней-

шего шифрования. В первых 11 битах длины $v(\varphi)^{(\xi,\gamma)}_{\mu,\eta}$ кода записано значение компоненты трансформанты ДКП $y_{\mu,\eta} = 754$. В 12-й бит записывается значение 0 или 1, которое учитывает знак компоненты. Это представлено в следующем выражении:

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

Тогда интенсивность $V(\varphi)^{(\xi,\gamma)}_{скр}$ битового потока трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП рассчитывается так:

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

где $\overline{v}(\varphi)^{(\xi,\gamma)}$ – длина кодового представления (μ,η)-й компоненты трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП φ-го блока $B^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-й структурной единицы $S^{(\xi,\gamma)}_{зн}$ изображения.

Таким образом, длина $V(\varphi)^{(\xi,\gamma)}_{скр}$ кодового слова трансформанты ДКП из 64 компонент $T^{(\xi,\gamma)}_{\varphi} = \{y1,...,y64\}$ будет занимать 768 бит = 96 байт (рис. 2).

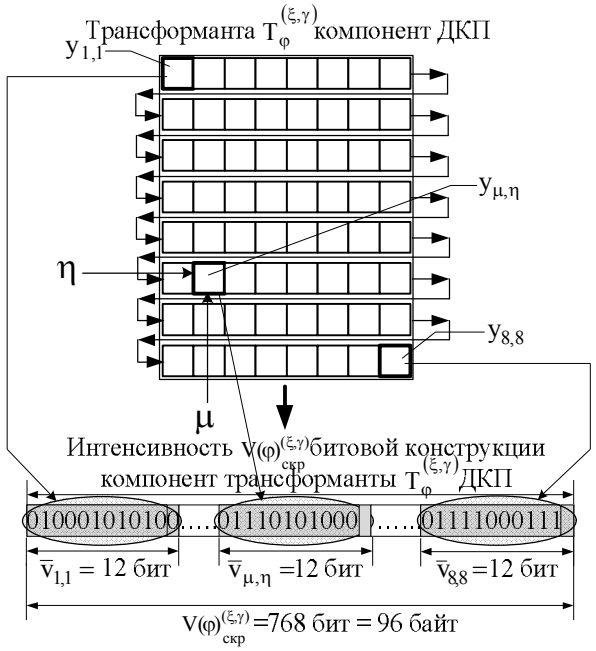

Рис. 2. Схема формирования кодового представления $\tilde{V}(\varphi)^{(\xi,\gamma)}_{скр}$ значений компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП блока $B^{(\xi,\gamma)}_{\varphi}$ изображения

Структурная единица базового видеокадра состоит из 6 блоков (4 блока яркости и 2 цветности). Длины кодового представления блоков яркости и цветности, подлежащих шифрованию, равны. Это представлено следующим выражением:

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

где $V^{(\xi,\gamma)}_{B(Y)_{скр}}$ – длина кодового представления трансформанты ДКП блока яркости; $V^{(\xi,\gamma)}_{B(Cr)_{скр}}$ – длина кодового представления трансформанты ДКП блока красного цвета; $V^{(\xi,\gamma)}_{B(Cb)_{скр}}$ – длина кодового представления трансформанты ДКП блока синего цвета.

Интенсивность $V''^{(\xi,\gamma)}_{S_{Iскр}}$ структурной единицы, подлежащей шифрованию, определяется так:

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

где N_b – количество блоков в структурной единице.

Тогда интенсивность $V_{S_{скр}}$ битового потока закрытой структурной $S^{(\xi,\gamma)}_{зн}$ единицы рассчитывается как:

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

Таким образом, структура кодовой конструкции закрытой структурной единицы будет иметь вид, представленный на рис 3.

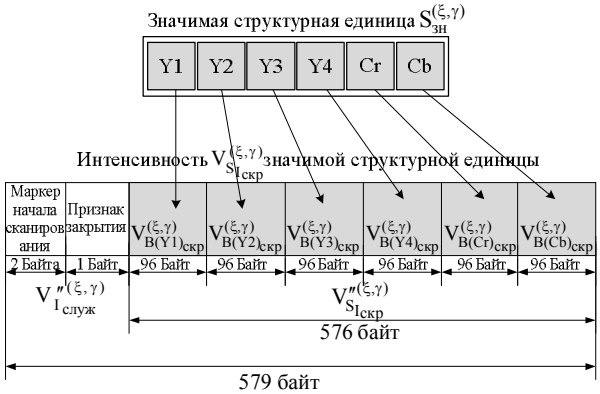

Рис. 3. Структура кодовой конструкции закрытой структурной единицы базового видеокадра

Из рис. 3 видно, что структурная единица, подлежащая шифрованию, имеет длину $V^{(\xi,\gamma)}_{S_{Iскр}}$ 576 байт (96 байт*6=576 байт) при условии, что размер блока $B^{(\xi,\gamma)}_{\varphi}$ видеоизображения равен 64 пикселям ($\mu = 8$, $\eta = 8$). Длина кода $V_{S_{Iисх}}$ исходного изображения размером в 256 пикселей ($m = 16, n = 16$), где раз-

мер одного пикселя равен 1 байту, представленного в трех плоскостях (YCrCb) будет равна 768 байт:

$$V_{S_{I_{исх}}} = V_{B(Y_{m,n})_{исх}} + V_{B(Cr_{m,n})_{исх}} + V_{B(Cb_{m,n})_{исх}} =$$
$$= 16 \cdot 16 \text{ бит} + 16 \cdot 16 \text{ бит} + 16 \cdot 16 \text{ бит} = 786 \text{ байт},$$

где $V_{B(Y_{m,n})_{исх}}$ – битовая интенсивность кода яркостной составляющей исходного изображения; $V_{B(Cr_{m,n})_{исх}}$ – битовая интенсивность составляющей красного цвета исходного изображения; $V_{B(Cb_{m,n})_{исх}}$ – битовая интенсивность составляющей синего цвета исходного изображения [2].

Отсюда следует, что в результате применения внутрикадрового метода селективного шифрования за счет использования формата цветового представления 4:2:0 интенсивность битового потока структурной единицы после шифрования снизится на 25% по сравнению с битовым потоком исходного видеоизображения.

Ключ алгоритма шифрования «Калина» длиной в 128 бит (16 байт) представлен в виде матрицы К, которая состоит из 16 элементов по 8 бит (1 байт) каждый:

$$K = \begin{bmatrix} k1 & k2 & k3 & k4 \\ k5 & k6 & k7 & k8 \\ k9 & k10 & k11 & k12 \\ k13 & k14 & k15 & k16 \end{bmatrix},$$

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

где k_i – 8-битный элемент матрицы шифрования К; i – номер 8-битного элемента в матрице шифрования К [3].

Для битового согласования элементов матрицы шифрования $K = \{k1,...k16\}$ с битовым потоком компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ предлагается битовый поток $V(\varphi)_{скр}^{(\xi,\gamma)}$ поделить на элементы такой же длины как элементы матрицы шифрования К. Таким образом, весь битовый поток $V_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы разделяется на 96 элементов по 8 бит. Это выражено следующей формулой:

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

где b_i – 8-битный элемент переформатированного потока компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы; i – номер 8-битного элемента переформатированного потока компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы.

Схема формирования элементов по 8 бит из битового потока компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы базового видеокадра представлена на рис. 4.

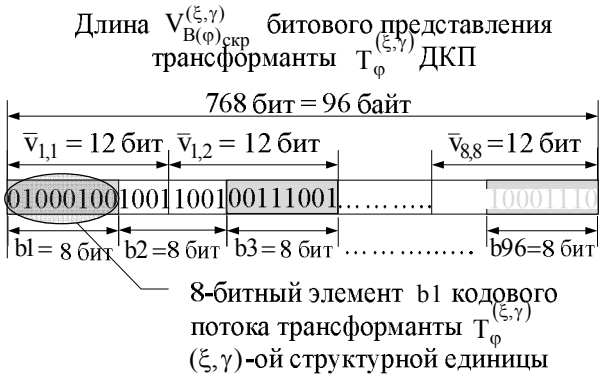

Рис. 4. Схема формирования элементов по 8 бит из битового потока компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы базового видеокадра

Так как длина ключа алгоритма шифрования «Калина» представлена в виде матрицы из 16 элементов (4*4) длиной в 128 бит, то для ее согласования с битовым потоком компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ необходимо этот битовый поток разделить на фрагменты по 128 бит. Для этого предлагается разделить битовый поток компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ на 8 равных частей (d1…d8), длина каждой из них равна 96 битам (12 байтам). Полученные фрагменты (d1,…,d8) по 12 байт располагаются по очереди сверху вниз. В результате чего формируется матрица $\overline{T}_{\varphi}^{(\xi,\gamma)} = \{b1,...,b96\}$ 8-битных элементов машинного кода компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Таким образом, матрица $\overline{T}_{\varphi}^{(\xi,\gamma)}$ будет иметь 12 элементов по горизонтали и 8 элементов по вертикали. Это представлено на рис. 5.

Далее предлагается полученную матрицу $\overline{T}_{\varphi}^{(\xi,\gamma)}$ двоичного кода φ-го блока $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы $S_{зн}^{(\xi,\gamma)}$ разделить на 6 матриц (T1,…,T6) по 128 бит (16 байт). Это выражено следующей формулой:

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

Формирование матриц происходит путем деления строк d1, d2, d3 d4 и d5, d6, d7, d8 на три равные части по 4 байта (16 бит). Это представлено на рис. 6.

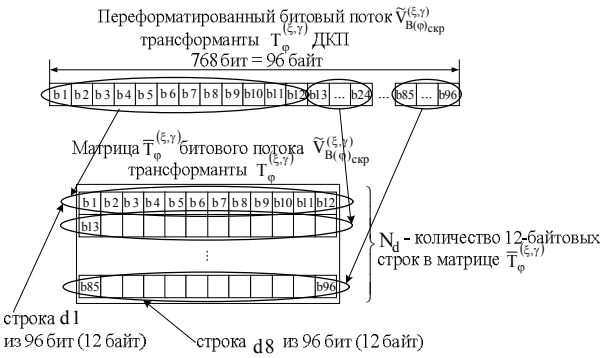

Рис. 5. Формирование матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ двоичного кода, состоящей из 8 строк по 12 байт

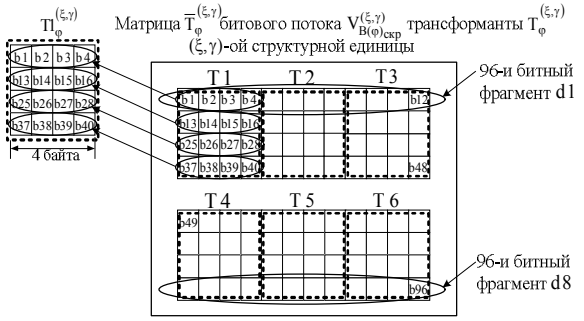

Рис. 6. Формирование матриц T1,…,T6 двоичного кода для наложения на них шифроключа К

Из рис. 6 видно, что в результате скремблирования 8-ми битных элементов (b1,…,b96) матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ битового кода дополнительно повышается помехоустойчивость и степень защиты передаваемых закрытых видеоданных.

Таким образом для шифрования битового потока трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП блока $B^{(\xi,\gamma)}_{\varphi}$ изображения (ξ,γ)-й структурной единицы базового видеокадра сформировано 6 матриц (T1,…,T6) такого же размера, как шифроключ (128 бит).

Ключ шифрования К длиной в 128-бит накладывается на каждую матрицу (T1,…,T6) битового кода отдельно. Это представлено в следующих выражениях:

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

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

где E_K – функция шифрования матриц $T_i = T1,...,T6$ матрицей ключей К.

Функция шифрования E_K с помощью матрицы $K = \{k1,...k16\}$ проводит шифрование матрицы T_i. Алгоритм шифрования «Калина» выполняет шифрование каждого из 16 элементов матрицы T_i с помощью 16 элементов матрицы ключей $K = \{k1,...k16\}$. Длина каждого элемента в матрице шифрования К и матрице T_i равна 8 битам. В результате чего формируются 6 матриц ($T'1,...,T'6$) битовых зашифрованных компонент трансформанты ДКП блока видеокадра. $c1,...,c96$ – 8-битные элементы зашифрованного потока компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-й структурной единицы.

Процесс наложения шифроключа К на матрицу T1 представлен на рис. 7.

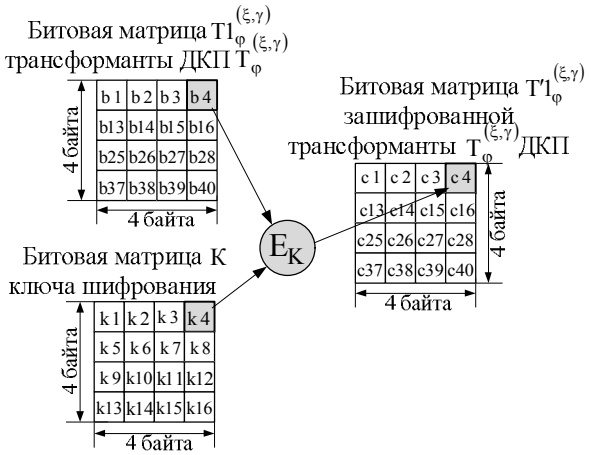

Рис. 7. Схема шифрования двоичных данных матрицы T1 из матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ битового кода компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП блока $B^{(\xi,\gamma)}_{\varphi}$ изображения

Из рис. 7 видно, что в результате наложения 16-байтового ключа К на 16-байтовую матрицу T1 двоичных данных формируется 16-байтовая матрица $T'1$ зашифрованных компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП. Таким образом, происходит шифрование всех битовых матриц значимой структурной единицы без образования избыточных битов данных [4].

На рис. 8 представлена схема формирования битового потока из матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ зашифрованного двоичного кода.

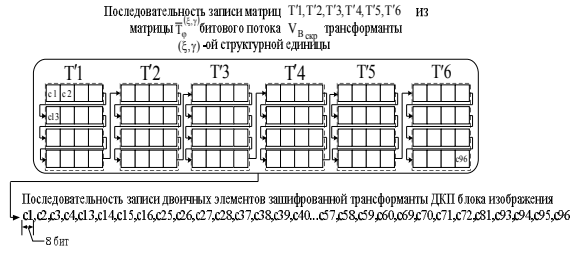

Рис. 8. Схема формирования битового потока из матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ зашифрованного двоичного кода

На рис. 8 представлен процесс шифрования алгоритмом «Калина» и схема формирования машинного кода зашифрованной энергетически значимой структурной единицы $S_{зн}^{(\xi,\gamma)}$ видеокадра.

В результате чего происходит шифрование всего битового потока энергетически значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ видеоизображения без остатка и избытка битовых последовательностей.

Метод декодирования закрытого видеопотока включает в себя следующие базовые этапы:

1. Выделение кодовой конструкции группы кадров из двоичной последовательности потока видеоданных.

2. Определение типа видеокадров в группе кадров.

3. Выделение цифрового представления закрытого базового видеокадра K_I из цифрового представления группы кадров.

4. Определение закрытых $S_{зн}^{(\xi,\gamma)}$ и не закрытых $S_{незн}^{(\xi,\gamma)}$ структурных единиц. Это происходит в результате анализа метки М, значение которой хранится в дополнительных данных цифровом описании структурной единицы. Если значение метки М=1, то структурная единица определяется как значимая $S^{(\xi,\gamma)} = S_{зн}^{(\xi,\gamma)}$. Если значение метки М=0, то структурная единица определяется как незначимая $S^{(\xi,\gamma)} = S_{незн}^{(\xi,\gamma)}$.

5. Дешифровка закрытых значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц, при которой расшифровываются значения компонент трансформант ДКП следующих блоков:

$$B(Y)_{m,n}^{(\xi,\gamma)},\ B(Cr)_{m,n}^{(\xi,\gamma)} \text{ и } B(Cb)_{m,n}^{(\xi,\gamma)}.$$

6. Декодирование незначимых $S_{незн}^{(\xi,\gamma)}$ структурных единиц, которое включает в себя такие этапы:

6.1. Обратная линеаризация трансформант ДКП блоков составляющей яркости и цветности $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$ незначимых структурных единиц.

6.2. Деквантование трансформант ДКП незначимых блоков.

7. Обратное ДКП значимых и незначимых блоков составляющей яркости и цветности $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$.

8. Построение композиции структурных единиц $S^{(\xi,\gamma)}$ базового видеокадра K_I, которое включает в себя следующие этапы:

8.1. Декодирование служебной информации для формирования структурных единиц $S^{(\xi,\gamma)}$.

8.2. Формирование композиций макроблоков $M(Y)^{(\xi,\gamma)}$, $M(C_r)^{(\xi,\gamma)}$ и $M(C_b)^{(\xi,\gamma)}$.

8.3. Формирование видеоизображения из блоков $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$.

9. Преобразование цифровых плоскостей видеоизображения I-кадра из формата YUV в формат RGB (формирование одного видеоизображения из 3-х цифровых плоскостей YCrCb).

10. Обратная дифференциальная импульсно-кодовая модуляция для восстановления P-кадров.

11. Обратное интерполирование для восстановления B-кадров.

12. Преобразование цифровых плоскостей видеоизображений P и B-кадров из формата YUV в формат RGB.

13. Формирование группы видеокадров из восстановленных I, P и B-кадров.

14. Формирование восстановленной видеопоследовательности из групп видеокадров.

После выделения базового кадра из битового потока группы видеокадров происходит определение значимых $S_{зн}^{(\xi,\gamma)}$ и незначимых $S_{незн}^{(\xi,\gamma)}$ структурных единиц. Выявление значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц заключается в определении значения бита признака закрытия М, который находится в служебной части кодовой конструкции всех структурных единиц базового видеокадра. Если значение бита признака закрытия М=1, то осуществляется стандартное декодирование структурной единицы. Если значение бита признака закрытия М=0, то такая структурная единица определяется как значимая, и она подлежит расшифровке.

Процесс расшифровывания $S_{зн}^{(\xi,\gamma)}$ структурных единиц происходит следующим образом:

1. Информационная часть битовой последовательности значимой $S_{зн}^{(\xi,\gamma)}$ структурной единицы делится на 6 равных фрагментов кода. Таким образом формируются 6 битовых потоков $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ трансформант $T_{\varphi}^{(\xi,\gamma)}$ ДКП блоков $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-й структурной единицы $S_{зн}^{(\xi,\gamma)}$.

2. Формирование битовых матриц $T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$ из битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ трансформант $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит делением битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ на строки длиной 4 байта. Каждые 4 строки битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ формируют матрицу из 16 элементов. Это представлено на рис. 9.

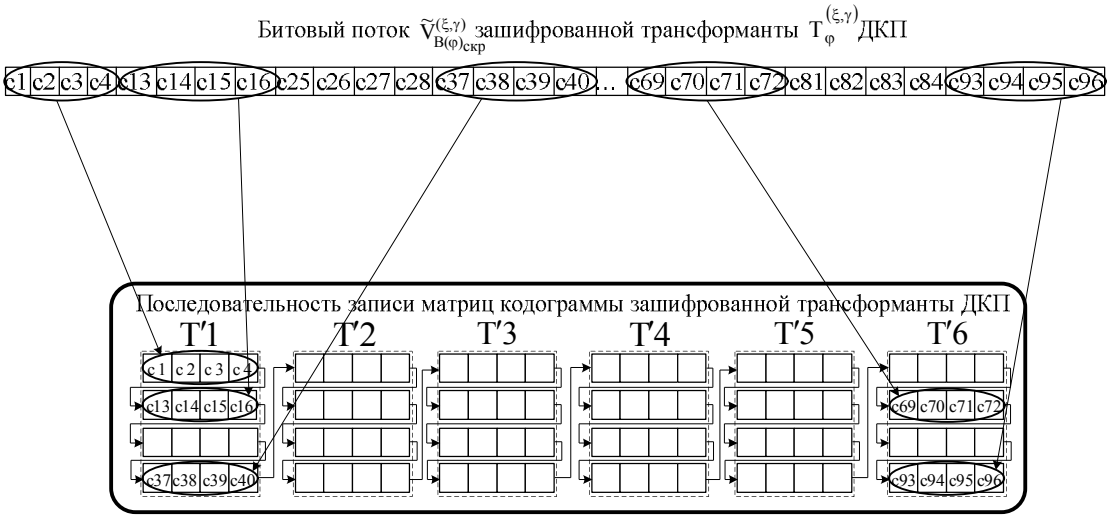

Рис. 9. Схема формирования 6 матриц

$(T'1^{(\xi,\gamma)}_{\varphi},...,T'6^{(\xi,\gamma)}_{\varphi})$ по 16 байт из битового потока $\tilde{V}^{(\xi,\gamma)}_{B(\varphi)скр}$ зашифрованной трансформанты ДКП

На рис. 9 представлен процесс формирования 6 матриц $(T'1^{(\xi,\gamma)}_{\varphi},...,T'6^{(\xi,\gamma)}_{\varphi})$ из битового потока $\tilde{V}^{(\xi,\gamma)}_{B(\varphi)скр}$ зашифрованной трансформанты ДКП. В результате чего сформированы матрицы такого же размера (16 байт), что и матрица ключей дешифрования K'.

3. Расшифровывание битового представления значений компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП. Это происходит путем наложения матрицы ключей K' длиной в 128-бит на каждую матрицу $(T'1^{(\xi,\gamma)}_{\varphi},...,T'6^{(\xi,\gamma)}_{\varphi})$ битового потока.

Процесс расшифровывания матриц $T'1^{(\xi,\gamma)}_{\varphi},...,T'6^{(\xi,\gamma)}_{\varphi}$ битового кода $\tilde{V}^{(\xi,\gamma)}_{B(\varphi)скр}$ компонент зашифрованной трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП представлен в следующих выражениях:

$$T1 = D_{K'}(T'1);\ T2 = D_{K'}(T'2);T3 = D_{K'}(T'3);$$

$$T4 = D_{K'}(T'4);T5 = D_{K'}(T'5);T6 = D_{K'}(T'6),$$

где $D_{K'}$ – функция расшифровывания матриц $T'1,...,T'6$ матрицей ключей K'.

Функция шифрования $D_{K'}$ с помощью матрицы расшифровывания $K' = \{k1,...k16\}$ проводит расшифровывание шифрование матриц $T'1,...,T'6$. Алгоритм шифрования «Калина» выполняет шифрование каждого из 16 элементов матриц $T'1,...,T'6$ с помощью 16 элементов матрицы ключей K'. Длина каждого элемента в матрице шифрования K' и матриц $T'1,...,T'6$ равна 8 битам. В результате чего формируются 6 битовых матриц $(T1,...,T6)$ расшифрованных компонент трансформанты ДКП блока видеокадра.

4. Формирование битовой матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП. Это происходит путем слияния матриц-аргументов элементов битовых матриц T1, T2, T3 слева направо. Процесс слияния матриц-аргументов элементов битовых матриц T1, T2, T3 представлен на рис. 10.

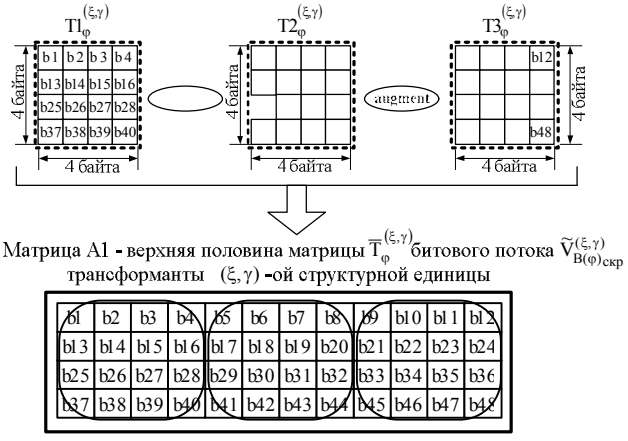

Рис. 10. Схема слияния двоичных матриц $T1^{(\xi,\gamma)}_{\varphi}$, $T2^{(\xi,\gamma)}_{\varphi}$ и $T3^{(\xi,\gamma)}_{\varphi}$ из битового кода $\tilde{V}^{(\xi,\gamma)}_{B(\varphi)скр}$ компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП в матрицу A1

В результате слияния битовых матриц T1, T2, T3 образуется матрица A1, которая состоит из 4 строк длиной в 12 бит.

Матрица A1 является верхней половиной матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$. Нижняя часть матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ форми-

руется таким же образом как и матрица A1, из слияния битовых матриц T4, T5, T6 слева направо.

В результате формируется матрица A2, которая состоит из 4 строк длиной в 12 бит. Она является нижней частью битовой матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$. Далее выполняется слияние матриц A1 и A2 сверху вниз. В результате чего формируется матрица $\overline{T}_{\varphi}^{(\xi,\gamma)}$.

Таким образом, формируется битовая матрица $\overline{T}_{\varphi}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП из 8 строк. Каждая строка матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ состоит из 12 элементов по 8 бит.

5. Преобразование битовой матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ в матрицу значений компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит следующим образом:

– каждая строка битовой матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ длиной в 12 байт (96 бит) делится на 8 элементов по 12 бит. Таким образом, формируются битовые представления компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП;

– первые 11 бит двоичного представления значения компоненты трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП переводятся в десятичную систему исчисления, а 12-й бит определяет знак компоненты.

6. Далее сформированная трансформанта $T_{\varphi}^{(\xi,\gamma)}$ ДКП блока $B_{\varphi}^{(\xi,\gamma)}$ изображения (ξ,γ)-й структурной единицы базового видеокадра обрабатывается по стандартному методу декодирования.

На рис. 11 изображен исходный базовый видеокадр «Видеодокументирование задержания», который подлежит закрытию.

Рис. 11. Исходный видеокадр «Видеодокументирование задержания»

Результат по закрытию базового видеокадра на основе шифрования значимых структурных единиц представлен на рис. 12.

Рис. 12. Результат закрытия видеокадра «Видеодокументирование задержания» с применением метода селекции значимых структурных единиц

Выводы

Разработан метод совместимости кодовой конструкции энергетически значимой структурной единицы и ключевой последовательности алгоритма шифрования «Калина». Он базируется на следующих технологических составляющих:

1. Формирование 12-битового кодового представления значения компоненты трансформанты ДКП из 11-битового значения компоненты трансформанты ДКП и 1-битового элемента, который определяет знак значения этой компоненты. В результате чего образуется машинное слово четной длины. Таким образом, достигается дальнейшая совместимость битового потока энергетически значимой структурной единицы со 128-битным ключом шифрования.

2. Формирование кодовой конструкции значимой структурной единицы базового видеокадра, подлежащей шифрованию. В результате чего записывается определенным образом 579-битная последовательность служебных данных и цифровых описаний блоков яркости и цветности структурной единицы.

3. Формирование матриц двоичного кода значимой структурной единицы такого же размера, что и ключ шифрования. В результате чего происходит скремблирование битового потока, что дополнительно повышает степень защиты и помехоустойчивости передаваемых закрытых видеоданных.

В результате применения метода совместимости кодовой конструкции энергетически значимой структурной единицы и ключевой последовательности алгоритма шифрования «Калина» при использовании внутрикадровой селективной обработке базового видеокадра происходит увеличение интенсивности закрытого базового видеокадра на 20-45% по сравнению с компрессионным базовым видеокадром. При этом достигается уменьшение интенсивности зашифрованной структурной единицы по сравнению с исходной на 25% за счет использования формата цветового представления 4:2:0.

Впервые разработан метод селективной обработки базового кадра для повышения пропускной способ-

ности закрытого видеоканала в ведомственных системах. Отличительные особенности данного метода от других методов совместимости заключаются в:

– формировании четной длины двоичного кода компонент трансформанты ДКП для блока изображения за счет использования максимального (фиксированного) значения компоненты трансформанты ДКП и ее знака;

– формировании матриц из двоичного кода значимой структурной единицы такого же размера, что и матрица ключа шифрования для их полной совместимости.

Получил дальнейшее развитие метод реконструкции закрытого видеопотока на основе технологии дифференцированной обработки кадров. Отличительными характеристиками данного метода являются дифференцированный процесс декодирования базового кадра в зависимости от значимости его структурных составляющих с последующим обратным криптографическим преобразованием информативных структурных единиц. Это позволяет обеспечить требуемый уровень конфиденциальности видеопотока для несанкционированного пользователя и наоборот, обеспечивать достоверное восстановление видеоинформации для авторизированного пользователя.

В результате применения данного метода интенсивность двоичного кода зашифрованного видеоизображения увеличивается на 20-45% по сравнению с битовой интенсивностью компрессионного кадра и уменьшается на 25% по сравнению с интенсивностью исходного видеокадра. Это происходит за счет использования формата цветового представления 4:2:0 и формирования матриц из двоичного кода значимой структурной единицы такого же размера, что и матрица ключа шифрования без внесения дополнительной избыточности. Так же, за счет формирования матриц машинного кода необходимого размера происходит скремблирование элементов в матрицах зашифрованных компонент трансформанты ДКП. Это дополнительно повышает конфиденциальность закрытого видеоинформационного ресурса. За счет шифрования только наиболее значимых структурных единиц, а не всего битового потока базового видеокадра, повышается помехоустойчивость передаваемых видеоданных.

Список литературы

1. Rate Control and H.264. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.pixeltools.com/rate_control_paper.html.

2. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2006. – 1072 с.

3. Горбенко И.Д. Перспективный блочный шифр «Калина»: основные положения и спецификации / И.Д. Горбенко, В.И. Долгов, Р.В. Олейников // Прикладная радиотехника. – 2007. – Часть 6, №2. – С. 195-208.

4. Подстановочные конструкции современных симметричных блочных шифров / В.И. Долгов, И.Д. Горбенко, Р.В. Олейников, И.В. Лисицкая, Р.В. Сергиенко // Радиоэлектронные и компьютерные системы. – 2009. – №6. – С. 65-93.

Поступила в редколлегию 1.03.2016

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД СЕЛЕКТИВНОЇ ОБРОБКИ БАЗОВОГО КАДРУ ДЛЯ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ ЗАКРИТОГО ВІДЕОКАНАЛУ У ВІДОМЧИХ СИСТЕМАХ

В.В. Баранник, Д.І. Комолов

У статті розроблено метод селективної обробки базового відеокадра, заснований на сумісності кодової конструкції енергетично значущою структурної одиниці з вимогою методу блочного симетричного шифрування алгоритмом шифрування для закриття потокових відеоданих на основі технології внутрішньокадрової селекції базового відеокадра. Даний метод дозволяє підвищити пропускну здатність закритого каналу відеозв'язку в відомчих системах передачі даних. Розроблено методологічну базу для розрахунку бітової швидкості зашифрованої структурної одиниці базового відеокадра. Представлені схеми формування бітових матриць для суміщення з матрицями ключа шифрування. Також представлена схема шифрування і розшифрування значущої структурної одиниці базового кадру. Проведено порівняльний аналіз бітового потоку зашифрованої структурної одиниці з двійковим потоком вихідного фрагмента відеозображення. Представлений приклад закритого базового відеокадра на основі шифрування значущих структурних одиниць.

Ключові слова: *відеокадр, група кадрів, шифрування, калина, структурна одиниця, бітова матриця, ключ шифрування, селективне шифрування.*

METHOD OF SELECTIVE TREATMENT BASE FRAME FOR INCREASING CAPACITY CLOSED VIDEO CHANNEL IN DEPARTMENTAL SYSTEMS

V.V. Barannik, D.I. Komolov

This paper developed a method for the selective treatment of the underlying video frame, based on the compatibility of the code structure is energetically meaningful structural unit with the requirement of the method of block symmetric encryption algorithm to encrypt the closing streaming video technology-based intra-breeding base of the video frame. This method allows to increase the capacity of the closed channel video data in departmental systems. A methodological framework for the calculation of the bit rate of encoded structural unit of the base of the video frame. Schemes formation bitmap to match the encryption key matrices. Also featuring encryption and decryption scheme is a significant structural unit of the base frame. A comparative analysis of the bitstream encoded structural unit in the bit stream of the original fragment the video. The example of the closed base of the video frame based on the encryption of significant structural units.

Keywords: *video frame, the frame group, encryption, kalina, structural unit, bitmap, encryption key, selective encryption.*