

ТЕХНОЛОГИЯ ЛОКАЛИЗАЦИИ ОШИБКИ ПУТЕМ ПОЗИЦИОНИРОВАНИЯ КОДА ПЕРЕМЕННОЙ ДЛИНЫ

Обосновывается проблематичность обеспечения безопасности видеoinформационного ресурса в системах аэромониторинга и видеоконференцсвязи. Формируются основные недостатки применения статистического кодирования при обработке видео. Обосновывается необходимость позиционирования кодов переменной длины в видеопотоке. Разрабатывается технология распределения кодов в существующем методе. В результате этого формируется механизм локализации действия битовой ошибки на видеопоток. Рассматривается особенность влияния ошибки на компоненты трансформанты, которые относятся к разным частотным областям.

1. Введение

Стремительное развитие информационных технологий создало возможность использовать видеoinформационный ресурс при однонаправленной передаче в системах видеонаблюдения и двухсторонний обмен в системах видеосвязи. Эти системы широко распространены в государственных ведомственных учреждениях, особенно в Министерстве обороны Украины. Этому способствовало улучшение качества системы управления при использовании видеoinформационного ресурса [1], что в свою очередь вызвало необходимость защиты видеoinформационного ресурса, которая обусловлена важностью его содержания. Данная необходимость подтверждается ростом кибернетических угроз государственным учреждениям, возникающих в результате кибератак [2]. Чаще всего применяются атаки типа DDoS-атака [3], что обусловлено простотой осуществления данного вида атак и эффективностью использования. Внешнее проявление применения кибератак выражается в искажении, пропадании и полной недоступности видеoinформационного ресурса. При этом современные методы предотвращения киберугроз [4] реагируют при соответствии параметров сетевой активности. Результатом этого является недостаточная оперативность существующих методов защиты, что приводит к потере данных. Это вызывает необходимость улучшения информационной безопасности видеoinформационного ресурса путем разработки технологии кодирования с учетом воздействия кибератак на ресурс. Актуальность работы связана с важностью видеoinформационного ресурса и необходимостью увеличения его устойчивости к ошибкам. Для обоснования варианта решения поставленной задачи необходимо рассмотреть существующие технологии обработки видеoinформационного ресурса. Данные технологии (JPEG, MPEG-4, H.264) используют сжатие на базе статистического кодирования (кодов переменной длины) [5]. Особенностью данной технологии является использование корреляции между кадрами в группе кадров. Данная группа кадров состоит из опорного кадра и последовательности разностных и обратных кадров. При этом длительность опорного кадра видео значительно меньше длительности всей группы кадров. Применение опорных кадров в процессе обработки обуславливает высокую степень сжатия потока и в то же время создает уязвимость целостности потока к искажениям [6]. Результатом искажения небольшого участка опорного кадра при применении указанных кибератак является потеря содержимого всей группы кадров для потока видеoinформационного ресурса. Это приводит к нарушению таких характеристик информационной безопасности ресурса, как целостность и доступность. Так как для существующих систем киберзащиты характерно некоторое запаздывание реакции, то при наличии краткосрочных атак (медленная DDoS-атака) возможно отсутствие идентификации угрозы при фактической недоступности видеoinформационного ресурса. Для динамических условий использования видеoinформационного ресурса это считается недопустимым, так как приводит к проблеме недостаточной оперативности противодействия киберугрозам для существующих методов защиты. Для локализации действия кибератак предлагается разработать соответствующий метод обработки видеoinформационного ресурса. Поэтому возник-

кает необходимость рассмотреть недостатки современных технологий кодирования видеоданных. В существующей схеме обработки видеоинформационного ресурса применяется статистическое кодирование компонент линейаризованной трансформанты, которая образовалась после дискретно-косинусного преобразования сегментов исходного изображения. В силу префиксности статистического кода переменной длины требование к использованию символов-разделителей в процессе декодирования компонент трансформанты изображения будет отсутствовать. Из этого вытекает условие последовательности осуществления декодирования каждого кода. Последовательность осуществления декодирования обуславливает присутствие уязвимости к наличию ошибки в разряде кода. Результатом битовой ошибки в коде является неверная идентификация кода и его длины, что приводит к дальнейшей неверной идентификации всех последующих VLC кодов, которая выражается в разрушении всего изображения.

Цель работы – создать технологию локализации ошибки при позиционировании статистических кодов в потоке и рассмотреть изменение устойчивости видеоинформационного ресурса к ошибкам для предложенной технологии.

2. Основной материал

Для устранения уязвимости, связанной с неверным позиционированием кода переменной длины, предлагается применять перераспределение данных кодов в кодовые слова равномерной длины. Это достигается с помощью технологии упругого к ошибкам энтропийного кодирования (Error Resilient Entropy Code – EREC). Данная технология задается функцией преобразования f_{errec} согласно соотношению:

$$L(\theta) \xrightarrow{f_{\text{errec}}} S(\Lambda). \quad (1)$$

Здесь f_{errec} – функция распределения VLC кодов ℓ_ξ по слотам s_λ ; Λ – количество слотов, в которые распределены VLC коды.

Технология EREC характеризуется следующими этапами: размещение содержимого кодовых конструкций ℓ_ξ ; перераспределение содержимого кодовых конструкций ℓ_ξ . Данная технология размещает VLC коды ℓ_ξ в слоты пакета EREC $S(\Lambda)$ на основе перестройки битовой структуры. Здесь учитывается, что слотами являются кодовые слова равномерной длины, т.е.

$$|s_i|_2 = |s_j|_2 = v, \text{ при } i \neq j. \quad (2)$$

В результате преобразования последовательности $L(\theta)$ VLC кодов образуется пакет $S(\Lambda)$ слотов. Вектор слотов (пакет) записывается следующим образом:

$$S(\Lambda) = \{s_1; \dots; s_\lambda; \dots; s_\Lambda\}.$$

Здесь s_1 – начальный слот в пакете; s_Λ – последний слот в пакете. Схематическое распределение VLC кодов ℓ_ξ по слотам s_ξ , т.е: $\ell_\xi \rightarrow s_\xi^{(1)}$, в соответствии с технологией EREC, показано на рис. 1. В данной формуле $s_\xi^{(1)}$ – слот, сформированный при размещении кода ℓ_ξ ; (1) – индекс начального этапа, соответствующий первичному размещению VLC кодов по слотам. На данном рисунке представлено распределение кодового потока $L(\theta)$, состоящего из $\Lambda = 19$ VLC кодов ℓ_ξ по 19 слотам. Различные VLC коды ℓ_ξ представлены схематично в виде разных прямоугольников.

На первичном этапе рассматривается размещение VLC кодов ℓ_ξ по слотам s_ξ без учета их выравнивания по длине v . Порядок заполнения слотов s_ξ определяется следующими правилами:

1) установление порядка расстановки VLC кодов по слотам пакета. Согласно этому правилу 1-я кодовая последовательность ℓ_1 размещается в слоте s_1 (как показано на рис. 1);

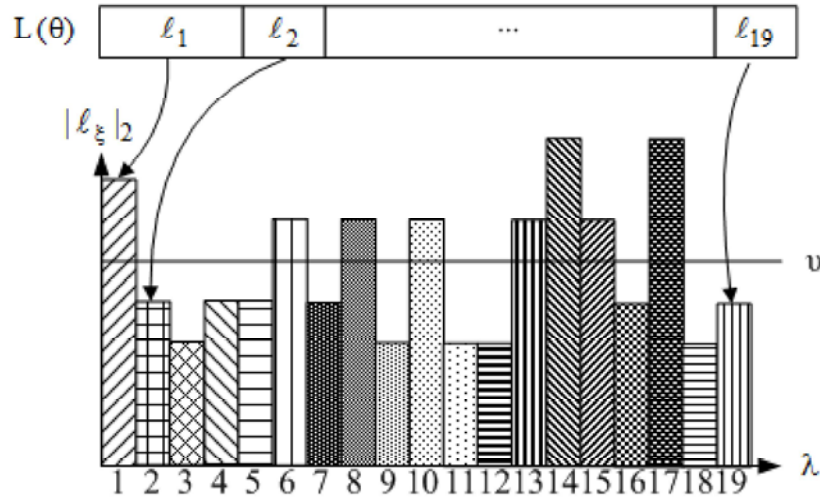


Рис. 1. Первичный этап размещения битовых составляющих кодовых конструкций при формировании пакета слотов

2) установка порядка заполнения слотов разрядами VLC кодов. Согласно этому правилу старшие разряды $q_{\xi,\gamma}; \gamma \rightarrow 1$ кодовой конструкции ℓ_ξ размещаются в нижних битовых позициях слота s_ξ . Наоборот, младшие разряды $q_{\xi,\gamma}; \gamma \rightarrow |\ell_\xi|_2$ кодовой конструкции ℓ_ξ размещаются в верхних битовых позициях слота s_ξ .

Следующим этапом формирования пакета слота является выравнивание длин кодовых слов s_ξ для выполнения условия (2) в случае, когда известно количество Λ слотов в пакете. Для этого сначала требуется определить длину v слота. Она определяется как отношение суммарной длины $|L(\theta)|_2$ последовательности $L(\theta)$ кодов к количеству Λ слотов. Формула расчета длины указана в следующем выражении:

$$v = \frac{|L(\theta)|_2}{\Lambda} = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\theta} |\ell_i|_2 \right\rceil. \quad (3)$$

Здесь $\lceil x \rceil$ – оператор округления значения x до большего натурального числа.

Для повышения эффективности заполнения слотов в соответствии с технологией EREC происходит перераспределение избыточных составляющих $\Delta\ell_\xi$ VLC кодов ℓ_ξ по избыточным составляющим $\Delta s_i, i \neq \xi$ слотов $s_i, i \neq \xi$, что задается формулой:

$$\Delta L(\theta) \xrightarrow{f_p} \Delta S(\Lambda), \quad (4)$$

где $\Delta L(\theta) = \{\Delta\ell_1; \dots; \Delta\ell_\xi; \dots; \Delta\ell_\theta\}$ – совокупность избыточных составляющих $\Delta\ell_\xi$ VLC кодов ℓ_ξ ; $\Delta S(\Lambda) = \{\Delta s_1; \dots; \Delta s_\xi; \dots; \Delta s_\Lambda\}$ – совокупность избыточных составляющих Δs_ξ слота s_ξ .

Это позволит: 1) сохранить информацию VLC кодов ℓ_ξ на основе заполнения пустот слотов s_ξ ; 2) сократить избыточность, вызванную недогрузкой слота. В общем случае избыточная составляющая $\Delta\ell_\xi$ VLC кода ℓ_ξ будет размещена по нескольким слотам s_i (рис. 2).

В процессе декодирования при поразрядной сборке VLC кодов ℓ_ξ происходит обращение к содержимому избыточных составляющих Δs_i других слотов $s_i, i \neq \xi$. Это обращение производится только после идентификации других VLC кодов ℓ_i .

При этом внесения двоичных разрядов $h_{\xi+d_g,\mu}$ избыточных составляющих $\Delta s_{\xi+d_g}^{(\gamma)}$ слота $s_{\xi+d_g}$ в содержимое части кода $\partial\ell_\xi$ продолжают до идентификации окончания ξ -й кодовой комбинации ℓ_ξ . Следует заметить, что каждый этап сборки VLC кодов ℓ_ξ должен происходить после завершения предыдущего на позициях всех слотов s_i . Результат формирования кода ℓ_ξ при обращении к битовым составляющим нескольких слотов представлен на рис. 3.

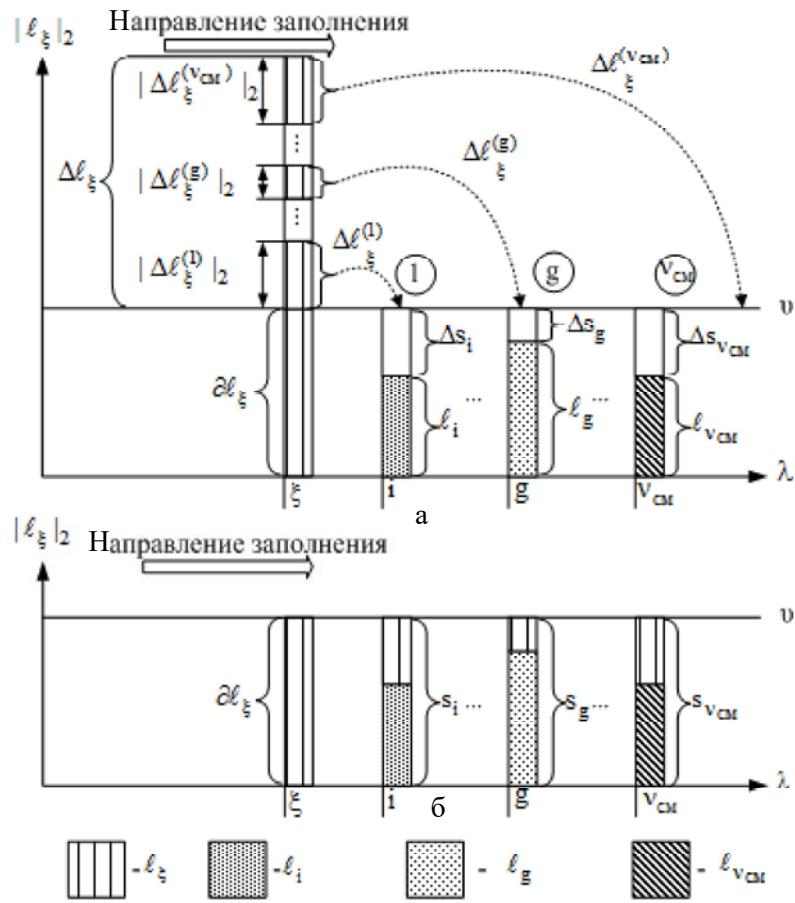


Рис. 2. Структурная схема многослотового распределения VLC: а – до распределения; б – после распределения

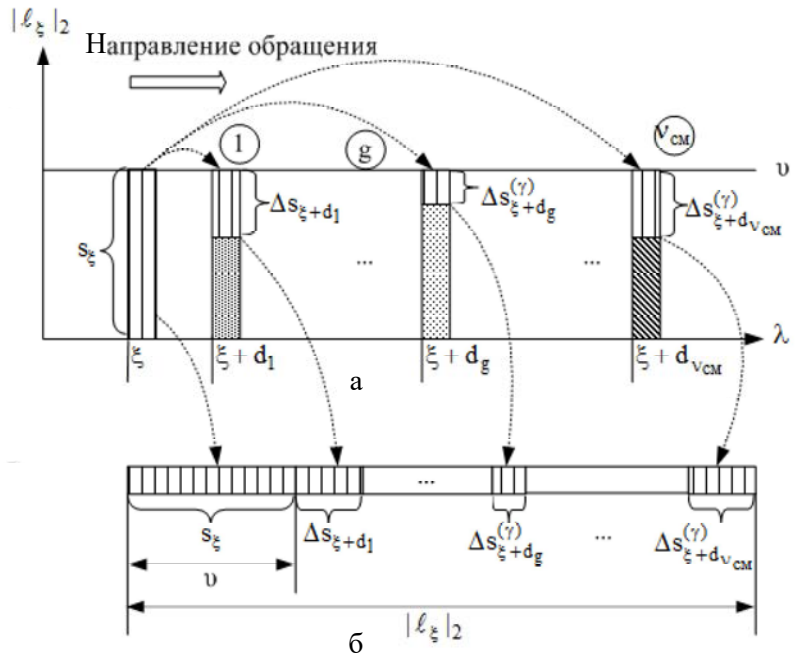


Рис. 3. Сборка VLC кода ℓ_ξ по подпоследовательности $\Delta S(v_{cm})$ до идентификации окончания кодовой комбинации ℓ_ξ : а – изъятие битовых составляющих других слотов $S_\xi + d_g$; б – результат формирования кода ℓ_ξ

Очевидно, что в силу последовательности этапов обращения к содержимому слотов, при идентификации λ -й кодовой комбинации ℓ_λ ошибка затрагивает избыточную составляющую $\Delta s_\lambda^{(\gamma)}$ слота s_λ , к которой идет обращение при сборке на g -м этапе ξ -го кода ℓ_ξ , $\xi = \lambda - d_g$. При этом также возможна неверная идентификация окончания ξ -й кодовой комбинации ℓ'_ξ . Идентификация кода ℓ_λ и ℓ_i кодов ℓ_i , избыточные составляющие которых входят в избыточные составляющие $\Delta s_\lambda^{(j)}$, $j < \gamma$ слота s_λ , будет произведена верно. В связи с особенностью построения статистического кода, которая заключается в обратной пропорциональности длины кода частоте его появления, применение технологии перераспределения защищает от битовой ошибки ВЧ компоненты трансформанты [7]. В то же время сохраняется лавинный эффект ошибки для НЧ компонент изображения. Для устранения лавинного эффекта предлагается использовать изменяющуюся избыточность распределения с механизмом обратной связи между кодером и декодером.

Выводы

Разработана технология локализации ошибки путем позиционирования кода переменной длины при незначительном увеличении длины пакета, который необходим для кодирования компонент. Создана технология, которая учитывает применение кибератак на видеoinформационный ресурс. Для локализации ошибки декодирования для НЧ компонент впервые предложено использовать динамическую избыточность технологии распределения с механизмом обратной связи между кодером и декодером.

Список литературы: 1. *Анализ действия кибератак на видеoinформационный ресурс в информационно-телекоммуникационных сетях* / В.В. Баранник, С.А. Подлесный // АСУ и приборы автоматики. 2014. Вып. 164. С. 16-22. 2. *Захист інформаційних мереж є питанням державної безпеки - голова Держспецзв'язку Геннадій Резніков* [Електронний ресурс] http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712, 2012. 3. *Звіт CERT-UA за 2014 рік* [Електронний ресурс]. <http://cert.gov.ua/?p=2019>, 2015. 4. *Мартынчук И.* Материалы технического тренинга «Построение безопасных сетей на оборудовании D-Link», [Електронний ресурс], <http://service.d-link.ua/sites/default/files/files/Security.zip>, Киев, 2012. 190 с. 5. *Richardson E.* "H.264 and MPEG-4 video compression". Chichester, UK: Wiley and Sons, 2003. 306 p. 6. *Wang Y. and Zhu Q.F.* Error control and concealment for video communication: A review. Proceedings of the IEEE, 1998. Vol. 86, no. 5. P. 974-997. 7. *Обґрунтування підходу щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі дії кібератаки на відеоінформаційний ресурс в інформаційно-телекомунікаційних мережах* / В.В. Баранник, С.А. Підлісний // Радіoeлектроніка та інформатика. 2015. №3. С.62-66.

Поступила в редколлегию 12.01.2016

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79. E-mail: barannik_v_v@mail.ru.

Подлесный Сергей Анатольевич, начальник отделения Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61023, Харьков, ул. Сумская 77/79. E-mail: serg380638472732@gmail.com.

Туренко Сергей Викторович, преподаватель ХНУРЭ. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61000, Харьков, ул. Сумская 77/79. E-mail: barannik_v_v@mail.ru.