УДК: 621.396 DOI: 10.53816/23061456_2022_7–8_22

АЛГОРИТМ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ДОСТАВКИ ДАННЫХ ПО СПУТНИКОВОМУ СТЕГОКАНАЛУ С УЧЕТОМ ПОТЕРЬ В СРЕДЕ ПЕРЕДАЧИ

ALGORITHM OF THE ENSURING RELIABILITY HIDDEN DATA VIA SATELLITE CHANNELS ACCOUNTING LOSSES

Канд. техн. наук Е.С. Абазина, канд. техн. наук В.Е. Федосеев, Д.В. Леванов

Ph.D. E.S. Abazina, Ph.D. V.E. Fedoseev, D.V. Levanov

ВКА им. А.Ф. Можайского

Статья посвящена вопросам обеспечения требуемой достоверности приема данных, передаваемых скрытно в структуре видеопотока по спутниковым радиолиниям с использованием методов цифровой стеганографии. Рассмотрены технологии, применяемые в стандарте MPEG-2 для борьбы с ошибками на физическом, канальном и транспортном уровнях модели OSI, предложен алгоритм оценивания достоверности приема данных стегоканалов, организованных в видеопотоке спутниковых радиолиний с учетом логики декодирования и восстановления качества видеоданных, передаваемых открыто и используемых для сокрытия.

Ключевые слова: достоверность приема, стегоканал, сокрытие данных, видеоконтейнер, MPEG-2.

The paper is devoted to the issues of ensuring the required reliability of receiving data transmitted covertly in the structure of the video stream over satellite radio lines using digital steganography methods. The technologies used in the MPEG-2 standard to combat errors at the physical, channel and transport levels of the OSI model are considered, an algorithm is proposed to ensure the reliability of receiving data from stegochannels organized in the video stream of satellite radio lines, taking into account the logic of decoding and restoring the quality of video data used as a stegocontainer.

Keywords: reception reliability, stegochannel, data concealment, video container, MPEG-2.

Введение

Анализ тенденций развития современного вооружения и военной техники позволяет в качестве одного из наиболее актуальных направлений совершенствования выделить модернизацию систем управления. В подавляющем большинстве случаев к управлению средствами вооружения и военной техники предъявляется требование обеспечения возможности удаленного управления, а для мобильных средств наличие системы дистанционного управления является обязательным. При этом успешное выполнение функций любой системой управления определяется качественным состоянием телекоммуникационной инфраструктуры, которое выражается в достоверности, своевременности и безопасности связи. В случаях, когда объекты управления размещены и выполняют задачи по предназначению на значительном удалении от пункта управления, в труднодоступных

районах, в территориальных водах, воздушной или космической сферах, спутниковая связь становится основным родом, используемым для обеспечения управления. Основной недостаток спутниковых радиолиний заключается в их высокой разведдоступности, в то время как трафик управления вооружением и военной техникой является критически важным. Устранение указанного недостатка возможно благодаря применению способов и методов цифровой стеганографии, позволяющих скрыть сам факт передачи информации за счет модификации малозначащих элементов данных, передаваемых открыто, элементами скрываемых данных. Модифицируемые данные принято называть стегоконтейнерами. Чем большей избыточностью обладает стегоконтейнер, тем больший объем информации можно в нем скрыть. Видеоданные имеют наибольшую избыточность. Кроме того, в общем объеме телекоммуникационного трафика как сетей общего пользования, так и сетей специального назначения доля видеотрафика возрастает. Это является определяющим при их выборе в качестве стегоконтейнеров. В работах [1–3] установлено, что встраивание данных стегоканала в видеопоток до его компрессии характеризуется большими потерями, однако обладает и большей скрытностью встраивания. Очевидно, что при передаче данных в скрытых каналах, встраиваемых до компрессии стегоконтейнера, потери больше по сравнению с передачей по открытым каналам. Компенсация потерь скрываемых данных на приемной стороне осуществляется за счет свойства устойчивости к децимации двумерных широкополосных сигнальных конструкций Франка–Уолша и Франка–Крестенсена, используемых при формировании матрицы скрытых каналов [1–3]. Дополнительные потери в скрытых каналах обусловлены распространением сигналов открытых видеоданных в спутниковых радиолиниях, а также переполнением буферной памяти коммутационного оборудования шлюзовых станций спутниковых сетей, приводящим к отказам обработки пакетов. Однако оценивания этих потерь и определения их влияния на достоверность приема скрываемых данных в видеопотоках, передаваемых по спутниковым радиолиниям, ранее не осуществлялось. В этой связи задача разработки алгоритма оценивания достоверности приема данных стегоканалов, организованных в видеопотоке с учетом потерь в спутниковых радиолиниях, является актуальной.

Обеспечение достоверности приема видеоданных, передаваемых открыто в спутниковых радиолиниях

Организация передачи видеотрафика, представленного неподвижными видеоданными, потоковыми видеоданными, реального и нереального времени, трансляцией телевизионных программ подразумевает в большинстве случаев применение технологий доставки данных в соответствии со стандартами MPEG-2, MPEG-4, а для IP-сетей — протокола UDP, либо совместное использование этих технологий. Основными мероприятиями обеспечения требуемой достоверности приема видеоданных, передаваемых по открытым спутниковым радиолиниям, являются [1, 2]:

– контроль достоверности принимаемых видеоданных на различных уровнях эталонной модели взаимодействия открытых систем по следующим параметрам: отношение сигнал/шум на входе приемника Signal-to-Noise Ratio (SNR), коэффициент ошибок модуляции MER (Modulation Error Ratio), коэффициент битовых ошибок BER (Bit Error Ratio), идентификатор потока PID (Program Identifier), коэффициент непрерывности видеопотока CC (Continuity Counter);

– формирование структуры транспортного потока MPEG-TS (Transport Stream), которая обеспечивает возможность мультиплексирования элементарных потоков в магистральный и обратные действия для их верного демультиплексирования на приемной стороне [4];

– применение алгоритмов помехоустойчивого кодирования с упреждающим исправлением ошибок Forward Error Correction (FEC).

Использование перечисленных технологий позволяет достичь достоверности приема данных в видеопотоке, передаваемом открыто по спутниковым радиолиниям, значений BER не хуже 10^{-6}–10^{-12} [5].

Алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных

Достоверность скрываемых данных в стегоканале оценивается по показателю коэффициента битовых ошибок для скрываемых данных $BER^{стг}$, требования к значениям которого определяются видом скрываемых данных: для речевых

сообщений $BER^{стг} > 10^{-3}$, для команд и сигналов $BER^{стг} > 10^{-9}$. Реализация оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных, передаваемых в спутниковых радиоканалах, предполагает разрешение следующих основных задач:

– оценивание достоверности скрываемых данных с учетом потерь, вносимых в результате компрессии открытого видеотрафика при встраивании, потерь, возникающих при распространении сигнала в среде передачи, а также при обслуживании сетевыми устройствами;

– порядок мониторинга состояния стегоконтейнера на приемной стороне и оповещения стегопередатчика для осуществления адаптивного перехода при встраивании скрываемых данных на методы, обеспечивающие большую достоверность.

Разрешение указанных задач требует, с одной стороны, разработки алгоритма оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных, с другой стороны — организации мониторинга качества функционирования спутниковой радиолинии, используемой для передачи видеоданных со встроенным стегоканалом. Решение второй задачи может быть получено благодаря применению анализаторов, размещаемых в одной или нескольких точках сети спутниковой связи или интегрированных в терминальное оборудование для оценивания параметров качества обслуживания видеотрафика, в том числе параметров достоверности. Качество принимаемых видеоданных открытого трафика напрямую определяет качество приема скрываемых данных. Таким образом, очевидна прямая корреляционная зависимость между параметрами достоверности приема открытых видеоданных и параметрами достоверности скрываемых в этих данных стегосообщений. Оценка достоверности скрываемых данных формируется в результате сравнения коэффициента битовой ошибки стегоданных $BER^{стг}$ с требованиями, предъявляемыми к достоверности конкретного вида сообщений, встраиваемых в стегоконтейнер. Алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных, представлен на рисунке.

Оценивание начинается с измерения значений SNR для сигнала из спутниковой радиолинии, несущего информацию открытого видеотрафика. SNR является безразмерной величиной, равной отношению мощности полезного сигнала к мощности шума на входе приемника, значение которого сравнивается с величиной чувствительности приемника, и составляет суть условия приема сигнала из спутниковой радиолинии.

На следующем этапе осуществляется оценивание коэффициента MER, отражающего значение величины вектора ошибки [5]. В результате его сравнения с требуемыми значениями формируется запрос передатчику открытого видеотрафика на изменение значности используемой модуляции в сторону ее увеличения при хорошем состоянии среды передачи, и, наоборот, снижения — при значениях ниже максимально допустимых. Результаты оценки MER открытых видеоданных передаются также и стегопередатчику, который принимает решение об изменении периода используемой двумерной шумоподобной конструкции при формировании стегоканала и изменении числа строк матриц видеоданных для встраивания дублируемой скрываемой информации [1–3].

Затем выполняется оценивание коэффициента ошибок BER, контролируемого в двух точках — до декодера FEC (preBER) и после него (postBER). Технология FEC предусматривает внесение избыточности путем формирования специальных пакетов FEC. Дополнительная информация (пакеты FEC) передается не постоянно, а лишь при ухудшении качества передаваемого видеопотока. Применение FEC предполагает клиент-серверную организацию передатчика и приемника, использующих анализаторы, называемые контроллерами с функциями защиты от потерь и контроля состояния, которые информируют передающую сторону о возникающих проблемах.

После выполнения указанных процедур начинается распаковка транспортного потока MPEG-TS, имеющего длину в 188 байт, из которых 4 байта выделяются на заголовок и 184 байта — на полезные данные. Каждый пакет переносит данные только одного вида. При оценивании потерь в структуре заголовка видеоданных предлагаемый алгоритм анализирует лишь значения двух полей заголовка: поле 13-битового идентификатора типа пакета PID (Packet Identifier или

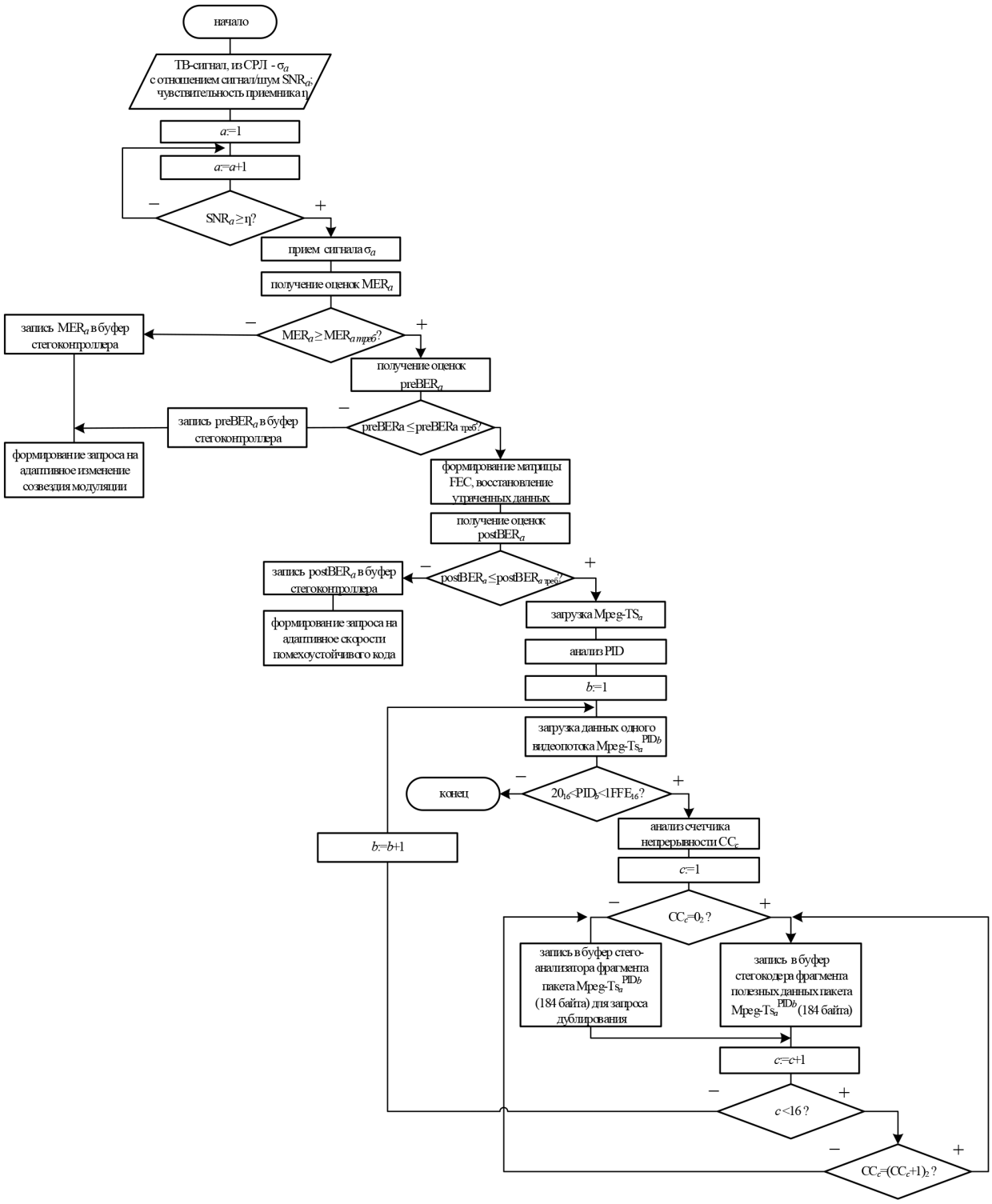

Рис. Алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных

Program Identification Number) и поле 4-битового счетчика непрерывности (CC — Continuity Counter). Идентификатор программ PID указывает на принадлежность пакета тому или иному элементарному PES-потоку и позволяет выделить в магистральном потоке единственный видеоканал. Стегокодер, анализируя PID, принимает решение о записи полезной нагрузки каждого из пакетов транспортного потока MPEG-TS, содержащей скрываемые данные. Для канала с видеоданными PID может принимать значения от 20 до 1FFF в 16-тиричной системе счисления.

На следующем этапе осуществляется оценивание значений счетчика непрерывности пакетов транспортного потока CC, являющегося циклическим. Первоначальное значение CC соответствует нулю, которое с получением каждого нового пакета последовательно увеличивается на единицу до 15, после чего счетчик обнуляется и цикл повторяется. Оценивание числа пропущенных значений счетчика непрерывности позволяет определить элементы потерянных открытых видеоданных, а соответственно и определить какие строки матрицы стегоданных не были получены в результате потерь в открытом транспортном потоке. Извещение передатчика стегоканала о том, какие элементы стегоматрицы не были получены, позволяет выполнить их дублирование и обеспечить требуемую достоверность на приемной стороне.

На завершающем этапе выполняется оценивание коэффициента битовых ошибок для скрываемых данных $BER^{стг}$, сведения о котором также передаются стегокодеру. При потере не более 20 % восстановление потерянных стегоданных возможно благодаря свойству устойчивости к децимации двумерных шумоподобных сигналов Франка–Уолша и Франка–Крестонсона, используемых при формировании стегоканала [3–11]. В противном случае стегокодером принимается решение об увеличении периода используемой двумерной шумоподобной конструкции для обеспечения требуемых значений показателя коэффициента битовых ошибок для скрываемых данных $BER^{стг}$ не хуже значений, установленных для данного вида трафика.

Таким образом, представленный алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных, отличается от известных учетом потерь открытых видеоданных, выбранных для встраивания, при их передаче по каналам спутниковой сети связи путем оценивания достоверности их приема по показателям SNR, MER, PID, CC, BER и $BER^{стг}$ с последующим оповещением передающей стороны стегосистемы, реализуя адаптивный выбор периода двумерной шумоподобной сигнальной конструкции для формирования стегоканала и кратность повторной передачи скрываемых данных.

Заключение

Вопросы обеспечения достоверности скрываемых данных требуют разработки алгоритма оценивания и мониторинга как открытого трафика, выступающего в качестве стегоконтейнера, так и трафика, передаваемого в стегоканалах. Одна из очевидных задач состоит в интеграции сведений о состоянии стегоданных во множество параметров качества открытого трафика с последующей передачей по служебным каналам открытой связи на передающую сторону для реализации адаптивной подстройки. Представленные предложения формирования канала обратной связи в интересах адаптации стегокодера к условиям передачи являются элементом новизны. Учет особенностей современных технологий, применяемых при восстановлении качества видеоданных, в части, касающейся значений оцениваемых параметров, мониторинг которых предусмотрен при организации транспортных видеотрансляций по стандарту MPEG-2, необходим ввиду их прямой корреляции с достоверностью скрываемых данных.

Литература

1. ISO/IEC 13818-1 (ITU-T H.222.0), «Information technology — Generic coding of moving pictures and associated audio information: systems». 2002. 15 p.

2. Локшин Б.А. Цифровое вещание. От студии к телезрителю // Учебное пособие. — Москва: Компания Сайрус системс. 2001. 316 с.

3. Цветков К.Ю. Теория оптимальных систем сложных дискретных сигналов и ее приложения. — СПб.: ВКА, 2005. 160 с.

4. Абазина Е.С. Формирование стеганографического канала с кодовым уплотнением на ос-

нове двумерных нелинейных сигналов // Вопросы радиоэлектроники в сфере техники телевидения. 2015. № 1. С. 15–26.

5. Абазина Е.С. Модель кодера скрытого канала с кодовым уплотнением с использованием сигнальных последовательностей Франка–Уолша, Франка–Крестенсона / К.Ю. Цветков, В.Е. Федосеев, В.М. Коровин и др. // Журнал НИИ Радио. 2014. № 2. С. 28–35.

6. Абазина Е.С. Метод скрытой передачи информации с кодовым уплотнением в видеоданных // Информация и космос. 2014. № 1. С. 33–38.

7. Цветков К.Ю., Ерунов А.А. и др. Алгоритм кодового уплотнения скрытых каналов с учетом приоритетов абонентов // Известия Института инженерной физики. 2016. № 4 (42). С. 25–31.

8. Стеганография, цифровые водяные знаки и стегоанализ: монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин и др. — М.: Вузовская книга, 2009. 220 с.

9. Ерунов А.А., Коровин В.М. и др. Вычислительная сложность алгоритмов формирования стегоканала с кодовым уплотнением в видеопотоке // Труды Военно-космической академии им. А.Ф. Можайского. 2018. Вып. 665. С. 35–45.

10. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: Солон-Пресс, 2009. 272 с.

11. Абазина Е.С., Цветков К.Ю. Концептуальная модель взаимодействия стегосистем передачи данных в составе эталонной модели взаимодействия открытых систем // Труды Военно-космической академии им. А.Ф. Можайского. 2019. Вып. 668. С. 70–80.

References

1. ISO/IEC 13818-1 (ITU-T H.222.0), «Information technology — Generic coding of moving pictures and associated audio information: systems», 2002. 15 p.

2. Lokshin B.A. Digital broadcasting. From the studio to the viewer. — Moscow: Company Sirus systems, 2001. 316 p.

3. Tsvetkov K.Yu. Theory of optimal systems of complex discrete signals and its applications. — Saint-Petersburg: Mozhaisky Military Space Academy, 2005. 160 p.

4. Abazina E.S. Formation of the steganographic channel with a code seal based on two-dimensional nonlinear signals // Radio engineering issues in the field of television technology. № 1. 2015. P. 15–26.

5. Abazina E.S. A model of the hidden channel encoder with a code seal using Frank–Walsh, Frank–Krestenson signal sequences // Journal of the Radio Research Institute. № 2. 2014. P. 28–35.

6. Abazina E.S. Formation of the steganographic channel with a code seal based on two-dimensional nonlinear signals // Information and space. 2014. № 1. P. 33–38.

7. Tsvetkov K.Yu., Yerunov A.A., et al. Algorithm of code sealing of hidden channels taking into account the priorities of subscribers // News of Engineering Physics Institute. 2016. № 4 (42). P. 25–31.

8. Steganography, digital watermarks and steganalysis: monograph / A.V. Agranovsky, A.V. Balakin, V.G. Gribunin et al. — M.: University Book, 2009. 220 p.

9.Erunov A.A., Korovin V.M. et al. Computational complexity of algorithms for the formation of a code-compacted stegocanal in a video stream // Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2018. Issue 665. P. 35–45.

10. Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography. — Moscow: Solon-Press, 2009. 272 p.

11. Abazina E.S., Tsvetkov K.Yu. Conceptual model of interaction of stegosystems of data transmission as part of the reference model of interaction of open systems // Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2019. Issue 668. P. 70–80.