УДК 681.4

Р.Ю. Мартимов

ЭЛЕКТРОННАЯ СТЕГАНОГРАФИЧЕСКАЯ ПОДПИСЬ ВИДЕОДАННЫХ

Мартимов Руслан Юрьевич, *закончил Санкт-Петербургский университет информационных технологий механики и оптики, факультет информационных технологий и программирования. Старший научный сотрудник Санкт-Петербургского филиала ОАО «Концерн Вега». Имеет публикации, также подана заявка на патент РФ в области цифровых водяных знаков. Область интересов: цифровая стеганография, криптография, компьютерное зрение. [e-mail: Ruslan.Martimov@gmail.com].*

Аннотация

Рассматриваются принципы построения асимметричной системы аутентификации видеоданных. Предлагаемая схема использует технологию цифровых водяных знаков (ЦВЗ), для обеспечения подлинности используется робастная функция хэширования, и криптографической основой является схема на базе абсолютной стойкой схемы электронной подписи Йохансона с побитным формированием и проверкой. В результате удается обеспечить защиту как от внешних, так и от потенциальных внутренних нарушителей в условиях высокого уровня ошибок при сжатии видеоданных. В статье приводятся экспериментальные результаты для видеоданных, сжатых кодеком H.264 при различной скорости потока. Экспериментальное сравнение проводится с одной из перспективных схем асимметричной аутентификации с использованием цифровых водяных знаков (ЦВЗ), криптографической основой которой являются хрупкая электронная цифровая подпись (ЭЦП), а также хрупкая имитовставка. На качественном уровне приводится краткий обзор потенциальных угроз подлинности (аутентичности) для видеопоследовательности и анализ того, как данная схема может им противостоять.

Ключевые слова: стеганография, цифровые водяные знаки, электронная подпись, видеопоток.

ELECTRONIC STEGANOGRAPHY SIGNATURE OF VIDEO DATA

Ruslan Yurievich Martimov, *graduated from the Faculty of Information Technologies and Programming of St. Petersburg National Research State University of Information Technologies, Mechanics, and Optics; Senior Staff Scientist at St. Petersburg Branch of OJSC 'Vega' Concern'; an author of articles in the field of digital watermark and stenography; is interested in digital steganography, cryptography, computer vision. e-mail: Ruslan.Martimov@gmail.com.*

Abstract

The article examines principles for building of an asymmetric system of video data authentication. The suggested scheme applies a method of digital watermarks. To provide for the authenticity, we have used the robust hashing function. The cryptographic basis is the scheme based on the Johansson electronic signature absolute stable scheme with the bit generation and verification. As a result, we ensure protection against external and potential internal intruders under conditions of the high error level at video compression. The article gives the experimental results of video data compressed with H.264 codec at variable stream speed. The experimental comparison is performed with one of the advanced asymmetric authentication schemes using digital watermarks based on the fragile electronic digital signature and fragile simulation plug. It is qualitatively discussed potential threats to the authenticity for the video sequence and analyzed how this scheme can face these threats.

Key words: steganography, digital watermarks, electronic signature, video stream.

Введение

С повышением пропускной способности каналов передачи интернет-трафика заметно выросли и коммуникационные услуги, особенно в части видеотелефонии и других сервисов передачи видеопотока по сетям общего пользования. Широкое распространение получили такие сервисы, как видеосвязь по Skype и использование роботов телеприсутствия. В отдельную группу выделяются спутниковые сети распространения видео, различные сервисы Video on Demand и т. п. Все это обостряет проблему защиты видеоинформации от различного рода атак нарушителей.

В связи с широким распространением различного рода видеозаписывающих устройств, таких как, напри-

мер, видеорегистраторы и смартфоны, записанное видео все чаще используется как доказательство произошедших событий. В связи с этим возникает задача юридического установления подлинности таких видеоматериалов. Современные средства формирования фальсифицированных видеоданных становятся настолько совершенными, что существующими методами криминалистического анализа достаточно сложно установить отсутствие в них преднамеренных искажений. Таким образом, защита авторства и подлинности видеоданных является актуальным направлением защиты информации, и его актуальность будет только повышаться, как и требования к защищенности от различных атак нарушителей. При этом в практических приложениях все чаще востребованы такие схемы защиты, в которых получатель-проверяющий не имеет возможности за отправителя-автора действия по формированию аутентификатора, что достигается путем использования асимметричных схем.

В настоящей работе рассматривается задача защиты видеоданных от действий не только внешних, но и потенциальных внутренних нарушителей, в условиях передачи по зашумленному каналу. С этой целью предложена асимметричная робастная схема защиты видеоданных, которая реализована в системе электронной стеганографической подписи видеоданных. Приводятся результаты экспериментального исследования, подтверждающие эффективность предложенного решения.

Целью статьи является разработка стеганографической системы электронной подписи видеоданных, устойчивой к операциям обработки видео, типа сжатие с потерями, и обеспечивающей высокую стойкость к атакам внешних и потенциальных внутренних нарушителей на подлинность защищаемых видеоданных.

Требования к системе электронной стеганографической подписи видеоданных

В зависимости от сферы применения видеоданных выбираются и соответствующие способы их защиты. Системы защиты авторства и подлинности видеоданных можно условно разделить на 3 группы:

1. Симметричные системы, в которых ключ отправителя и ключ получателя одинаковы;
2. Несимметричные системы, в которых ключ отправителя и ключ получателя различны;
3. Гибридные системы, в которых комбинируются симметричные и несимметричные системы.

В научно-технической литературе представлены различные варианты использования симметричных и несимметричных систем для обеспечения защиты подлинности и авторства видеоданных, передаваемых по каналам с ошибками [1, 2]. Например, в работе [3] предлагается использовать симметричную или несимметричную систему, такую как криптографическая система формирования имитовставки или ЭЦП, а для повышения помехоустойчивости они дополняются известными методами помехоустойчивого кодирования. В работе [4] предлагается формировать криптографический хэш-код из заверяемых видеоданных и встраивать его в эти же данные с использованием стеганографической технологии ЦВЗ.

В целом симметричные системы характеризуются высокой устойчивостью к воздействию ошибок канала передачи на заверенные видеоданные, однако они обеспечивают защиту только от атак внешних нарушителей.

Для защиты не только от внешних, но и от потенциальных внутренних нарушителей применяются асимметричные системы. Однако эти системы сложны в реализации, обладают более низкой помехоустойчивостью и стойкостью, а также требуют дополнительных расходов от канала связи. В таблице 1 [5] представлены зависимости вероятности доставки сообщений от длины сообщения L_x и длины аутентификатора L при различной вероятности ошибки на 1 бит доставляемой информации.

Заметим, что длина аутентификатора $L = 32$ бита соответствует длине имитовставки, а $L = 512$ бит – длине ЭЦП. С учетом этого можно сделать вывод, что для стабильного функционирования системы с использованием имитовставок нижним пределом вероятности ошибки в канале связи является значение 10^{-4}, а для ЭЦП – 10^{-5}–10^{-6}. Для аутентификатора с допустимой погрешностью сообщения (т. е. $L \geq 512$ бит) ситуация выглядит несколь-

Таблица 1

Вероятности доставки сообщения в зависимости от его длины L_x [бит], длины аутентификатора L [бит] и вероятности ошибок на 1 бит в канале связи

	10^{-7}	10^{-6}	10^{-5}	10^{-4}	$5*10^{-4}$	10^{-3}	10^{-2}
$L_x =$ 500, $L =$ 32	0,9999	0,9995	0,995	0,948	0,766	0,587	$4,76*10^{-3}$
$L_x =$ 1000 $L =$ 32	0,9998	0,9990	0,990	0,902	0,597	0,356	$3,13*10^{-5}$
$L_x =$ 1000 $L =$ 512	0,9998	0,9985	0,985	0,860	0,469	0,220	$2,51*10^{-7}$
$L_x =$ 10000 $L =$ 1024	0,9989	0,9896	0,900	0,349	$5,2*10^{-3}$	$2,7*10^{-5}$	10^{-11}

ко лучше: допустимая вероятность ошибок составляет порядка 10^{-4} [5]. Также автор [5] приводит теоретическую и практическую оценки устойчивости аутентификатора и показывает, что, исходя из теоретических границ, наиболее перспективным является построение систем аутентификации с допустимой погрешностью.

В соответствии с требованиями ФЗ РФ «Об электронной подписи» система электронной стеганографической подписи видеоданных должна обеспечивать защиту от следующих типов атак внешнего нарушителя:

- имитация (атака I) – отправитель ничего не отправлял, нарушитель имитирует сообщение;
- подмена (атака S) – перехваченное нарушителем сообщение меняется на другое;
- повтор (атака Q) – перехваченное сообщение отправляется повторно в другое время;
- переадресация (атака A) – нарушитель пересылает сообщение, посланное одному получателю, другому получателю.

Предлагаемая система также должна обеспечивать защиту от атак потенциального внутреннего нарушителя:

- ренегатство (атака T) – отказ отправителя от отправленного им сообщения, мотивируемый атакой имитации внешнего нарушителя;
- фальсификация приема (атака R_0) – отправитель ничего не передает, получатель формирует выгодное ему сообщение и утверждает, что получил его от отправителя;
- переделка (атака R_1) – при получении сообщение модифицируется к виду, выгодному получателю.

Если обозначить вероятности успеха каждой из перечисленных атак через P_I, P_S, P_Q, P_A, P_T, P_{R_0} и P_{R_1} соответственно, то вероятность успеха нарушителя (вероятность имитонавязывания по группе атак) P_D определяется как:

$$P_D = max\,(P_I, P_S, P_Q, P_A, P_T, P_{R_0}, P_{R_1}).$$

В современных системах защиты подлинности и авторства информации значение допустимой вероятности успеха нарушителя, как правило, должно быть $P_D \le 10^{-9}$.

Оценка параметров асимметричной робастной схемы защиты видеоданных

Для повышения робастности ЭЦП предлагается ее построение на базе схемы, отличной от схем построения криптографических электронных подписей на основе однонаправленной функции.

Для обеспечения защиты от описанных выше атак, подпись должна содержать не только заверенные биты авторства и подлинности, но и время, и идентификаторы отправителя. Предлагается построение алгоритма на базе схемы, предложенной Йохансоном [6, 7].

Подпись состоит из частей Y, B и A, причем часть Y отвечает за защиту от внешнего нарушителя, а части B и A – за защиту от внутреннего и частично от внешнего нарушителя. В части Y подписи содержатся зашифрованные идентификаторы, а также дата и время подписания. Основная задача данной части – обеспечить защиту от атаки повтора (Q), переадресации (A), а также частично атаки имитации (I) и подмены (S).

Результирующая вероятность подделки оценивается по формуле [5]:

$$P \ge \frac{\sum_{v=0}^{k} C_n^v - L}{\sum_{v=0}^{k} C_n^k + \sum_{v=k+1}^{n} C_n^v - L}, \qquad (1)$$

где n – общее число бит, L – число перехваченных сообщений при атаке подмены, k – число несовпавших бит. Значение k в (1) содержательно связано с механизмом проверки подписи, а именно, части A и B подписи проверяются через сравнение соответствующих элементов сигнатур, что соответствует прохождению либо непрохождению проверки частного двухбитового аутентификатора, в то же время при проверке части Y значение k связывается с расстоянием Хэмминга между тем, что извлекли и что должно быть.

В таблице 2 приведены значения допустимого количества несовпавших частных аутентификаторов для обеспечения вероятности подделки $P \le 10^{-9}$, рассчитанные в предположении, что каждый частный аутентификатор состоит из 2 бит. Если же длина частных аутентификаторов составляет 1 бит, то длина аутентификатора в битах будет в 2 раза меньше соответственно.

Таблица 2

Допустимое количество несовпавших аутентификаторов для обеспечения вероятности подделки не выше 10^{-9}

Длина аутентификатора, бит	Допустимое число несовпавших частных аутентификаторов
64	0
72	2
104	6
160	14
200	22
260	30
512	79
600	97

Таким образом, если ключ V_T формирования подписи состоит из l_{V_T} независимых элементов:

$$V_T = \left(v_{T_1}, v_{T_2}, ..., v_{T_i}, ...\right), \qquad 1 \le i \le l_{V_T},$$

каждый элемент ключа формирования подписи содержит 4 бита:

$$v_{T_i} = \left(v_{T1_i}, v_{T2_i}, v_{T3_i}, v_{T4_i}\right),$$

а ключ проверки V_R подписи видеоданных состоит из l_{V_R} независимых элементов:

$$V_R = \left(v_{R_1}, v_{R_2}, \ldots, v_{R_i}, \ldots\right),$$

где каждый элемент содержит 3 бита,

$$v_{R_i} = \left(v_{R1_i}, v_{R2_i}, v_{R3_i}\right),\ 1 \le i \le l_{V_R},$$

то для подписи однобитового аутентификатора требуется 7 бит ключа. В то же время для шифрования посредством гаммирования одного бита информации потребуется всего 1 бит.

На этапе генерации ключей должно выполняться условие зависимости ключей формирования и проверки подписи:

$$\begin{cases} v_{T3_i} = v_{R1_i} \oplus v_{T1_i} \cdot v_{R2_i}, \\ v_{T4_i} = v_{R3_i} \oplus v_{T2_i} \cdot v_{R2_i}, \end{cases} \quad (2)$$

$$1 \le i \le l_{V_T} = l_{V_R},$$

в котором операции сложения и умножения выполняются по модулю 2. Данное условие позволяет часть битов элементов обоих ключей генерировать независимо друг от друга и равновероятно, а другую часть бит вычислять в зависимости от ранее случайно выбранных бит элементов обоих ключей.

Каждый заверяемый фрагмент кадра X'видео отправитель хэширует по хэш-функции с двоичным выходом:

$$x_i' = h\left(X_i\right).$$

Функцию генерации хэш-кода предлагается [8] строить на базе discrete wavelet transform (DWT) non-negative matrix factorization (NMF) разложения. Затем от хэш-кода каждого фрагмента видеоданных отправитель вычисляет элемент сигнатуры A, состоящий из массива бит α:

$$\alpha_i = f_{\text{форм}\,\alpha}\left(x_i, v_{T_i}\right) = v_{T1_i} \oplus x_i \cdot v_{T2_i}, \quad (3)$$

используя i-й элемент ключа формирования подписи кадра:

$$\alpha = (\alpha_1, \alpha_2, \ldots \alpha_i, \ldots, \alpha_n), \quad 1 \le i \le n.$$

Очередной элемент сигнатуры B, состоящий из массива бит β_i, отправитель определяет по правилу:

$$\beta_i = f_{\text{форм}\,\beta}\left(x_i, \alpha_i, v_{T_i}'\right) = v_{T3_i} \oplus x_i \cdot v_{T4_i},$$

где $\beta = (\beta_1, \beta_2, \ldots, \beta_i, \ldots, \beta_n),\ 1 \le i \le n.$

Вычисленные элементы сигнатур встраиваются в соответствующие фрагменты кадров на передаче и извлекаются на приеме для проверки. Получатель хэширует каждый принятый фрагмент изображения $\hat{X}_i$,

$$\hat{x}_i = h\left(\hat{X}_i\right),$$

и вычисляет элемент проверочной сигнатуры:

$$\beta_i = f_{\text{пров}\,\beta}\left(\hat{x}_i, \hat{\alpha}_i, v_{R_i}\right) = v_{R1_i} \oplus \hat{\alpha}_i \cdot v_{R2_i} \oplus \hat{x}_i \cdot v_{R3_i}. \quad (4)$$

Выполнение равенства $\beta_i = \hat{\alpha}_i$ в i-й проверке гарантирует, что вероятность нарушения подлинности принятого фрагмента кадра не более ½.

Таким образом, уравнение (2) показывает, что отправитель, зная свои биты, не может определить с вероятностью больше 0,5 биты получателя, а получатель, зная свои биты, не может однозначно определить биты подписи с вероятностью больше 0,25.

Предлагаемый алгоритм построения асимметричной робастной схемы защиты видеоданных

Для генерации ключей предлагается использовать доверенный для отправителя и получателя центр сертификации. Центр сертификации формирует множество наборов соответствий из бит ключей проверки и подписи. При этом в каждом j-м наборе 4 битам ключа формирования электронной подписи (ЭП) соответствуют 3 бита ключа проверки. Затем для j-го набора биты ключа формирования подписи передаются подписывающему, а биты ключа проверки – получателю.

В схеме используется генератор гаммы для случайного выбора набора бит, удовлетворяющего требованиям уравнений (2). После этого непосредственно осуществляется встраивание бит с использованием схемы расщепления спектра сигнала [4]. Таким образом, ключи формирования и проверки подписи имеют общий ключ для генератора гаммы и разнесенные, но попарно синхронизированные наборы бит ключей проверки и формирования подписи, а также идентификатор отправителя. Последний при сложении по модулю 2 со временем может образовывать часть Y в явном виде, что позволит точнее идентифицировать тип атаки внешнего нарушителя. С целью уменьшения нагрузки на канал связи целесообразно часть Y складывать с общим ключом генератора гаммы и использовать в качестве ключа генератора гаммы.

В результате ключ для подписи состоит из ключа генератора гаммы, идентификатора отправителя, а также списка наборов бит, используемых при формировании подписи. В свою очередь, ключ проверки состоит из симметричного ключа для гамма-генератора, идентификатора отправителя (формирователя) и набора проверочных бит. При этом каждый из наборов бит V_T (4 бита) и V_R (3 бита) отвечает требованиям уравнения (2).

Возможны различные варианты построения защиты. Как было предложено выше, можно перед началом сеанса текущее время начала сеанса складывать с ключом генератора гаммы и идентификаторами отправителя. Это позволяет сформировать гамму, зависящую от времени, идентификатора отправителя и общего ключа, и, как следствие, подпись, зависящую от всех этих параметров.

Для защиты подлинности видеокадров целесообразно использовать робастную хэш-функцию [8]. При этом формируется 64-битный аутентификатор подлинности, для которого подпись имеет длину 128 бит, что соответствует частям A и B; часть Y используется для сложения с ключом генератора гаммы и присутствует косвенно.

На рисунке 1 представлена схема формирования ЭП для отдельного кадра. На вход схемы подается изображение A, над которым выполняется дискретное вейвлет-

преобразование. Над полученной матрицей (обозначим ее V) выполняется NMF-разложение:

$$V \approx WH,\ W \in R^{m \times r},\ H \in R^{r \times n},\quad (5)$$
$$r < m * n/(m+n),\ r << \min(n, m),$$

и формируется список C устойчивых коэффициентов из матрицы W [8]. В блоке хэширования с использованием криптографической хэш-функции H формируется набор однобитовых аутентификаторов X на основе ранее сформированного списка коэффициентов. В формирователе ЭП для каждого однобитового аутентификатора формируется двухбитовый аутентификатор ЭП S на основе подаваемой псевдослучайно бинарной последовательности G от генератора гаммы $G0$. После этого в блоке встраивания ЭП выполняется встраивание полученных бит посредством технологии IDA [4]. После встраивания заверенное изображение попадает на вход видеокодека и передается в видеопоток AC (Рис. 1).

На рисунке 2 представлена схема проверки ЭП. На вход схемы подается заверенное сжатое изображение AC, которое извлекается из потока видеоданных и разжимается посредством видеодекодера. На данном этапе работа делится на два потока выполнения: один извлекает (ЭП), другой выполняет формирование набора однобитовых аутентификаторов на основе коэффициентов DWT NMF. Блок проверки выполняет сравнение полученных результатов и выдает значение вероятности подлинности входного изображения на основе формулы (1).

Предложенная стеганографическая схема ЭП видеопотока позволяет выполнять аутентификацию поэлементно для видеопотока, что существенно повышает устойчивость к внешним искажениям, а также устраняет дополнительную нагрузку на канал связи за счет полухрупкой структуры [9]. Для подписи однобитового аутентификатора необходимо встраивать 2 бита подписи, соответствующие вычисленным значениям α_i по формуле (3) и β_i по формуле (4). Что же касается ключей подписи и проверки, они содержат 256-битный ключ генератора гаммы, идентификатор отправителя и наборы ключей подписи или проверки.

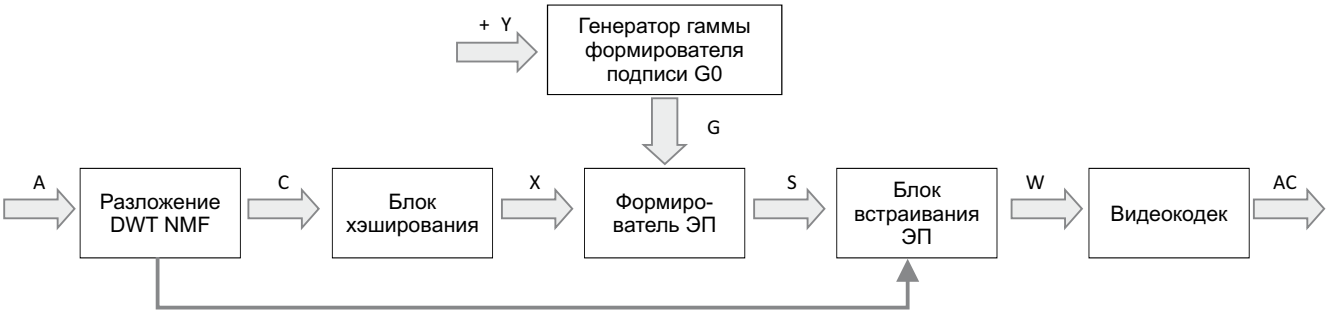

Рис. 1. Формирование ЭП для кадров: A – входное изображение; C – список NMF-коэффициентов; X – список однобитовых аутентификаторов; S – список двухбитовых аутентификаторов ЭП; W – заверенное изображение; AC – заверенное изображение, сжатое и помещенное в поток видеоданных; G – шифрующая гамма для формирователя ЭП; $K + Y$ – ключ генератора гаммы, сложенный по модулю 2 с Y частью подписи

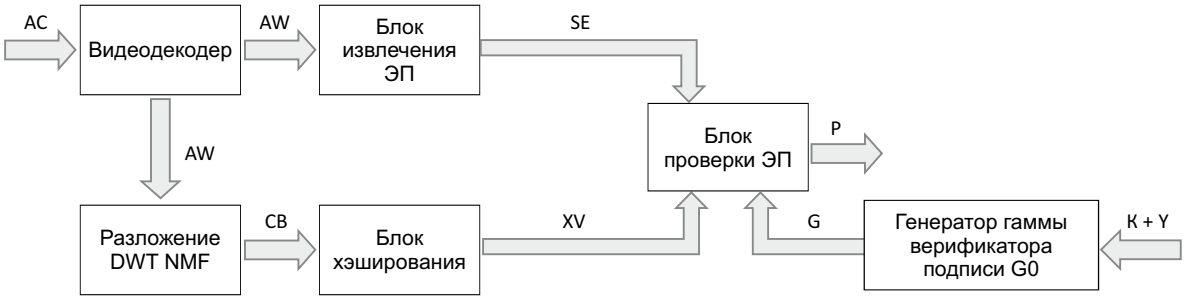

Рис. 2. Проверка ЭП: AC – сжатое заверенное изображение в видеопотоке; AW – заверенное разжатое изображение; SE – извлеченный набор двухбитовых аутентификаторов ЭП; CB – проверяемый набор коэффициентов DWT NMF; XV – сформированный набор однобитовых аутентификаторов; P – выходная вероятность подлинности и авторства; G – шифрующая гамма для формирователя ЭП; $K + Y$ – ключ генератора гаммы, сложенный по модулю 2 с Y частью подписи

Результаты экспериментов

Для оценки эффективности предложенного алгоритма были проведены оценки робастности, формируемой ЭП при сжатии кодеком H.264. Для сравнения использовался алгоритм [4]. В качестве тестовых данных были выбраны 4 стандартные видеопоследовательности: Forman, Highway, Flower, Coastguard, представленные на рисунке 3. Полученные результаты представлены в таблицах 3–6. В экспериментах кадр классифицировался как изображение с неподтвержденными подлинностью и авторством, если вероятность имитонавязывания превышала 10^{-9}. В качестве метрики качества было выбрано пиковое соотношение сигнала к шуму (peak signal-to-noise ratio (PSNR)).

Coastguard	Flower	Forman	Highway

Рис. 3. Стандартные видеопоследовательности

Таблица 3

Результаты экспериментов для видеопоследовательности Highway

Скорость потока Кб/с	PSNR без встраивания dB		PSNR после встраивания dB		Доля изображений с неподтвержденными авторством и подлинностью (%)
	min.	ср.	min.	ср.	
3078	38,8497	43,3752	37,3	39,4	0
2048	37,7002	41,7677	36,8	39,1	6,5
1536	35,8934	40,8681	36,4	39,0	63,95 %

Таблица 4

Результаты экспериментов для видеопоследовательности Forman

Скорость потока Кб/с	PSNR без встраивания dB		PSNR после встраивания dB		Доля изображений с неподтвержденными авторством и подлинностью (%)
	min.	ср.	min.	ср.	
3078	39	41	32,7	36,7	0,06
2048	34	39	31,0	35,8	8,02
1536	32	37	30,0	35,0	45,00

Таблица 5

Результаты экспериментов для видеопоследовательности Flower

Скорость потока Кб/с	PSNR без встраивания dB		PSNR после встраивания dB		Доля изображений с неподтвержденными авторством и подлинностью (%)
	min.	ср.	min.	ср.	
3078	31,9	35,5	27,4	28,3	0
2048	28,4	31,7	26,2	27,5	10,80
1536	26,5	29,5	25,2	27,2	79,90

Таблица 6

Результаты экспериментов для видеопоследовательности Coastguard

Скорость потока Кб/с	PSNR без встраивания dB		PSNR после встраивания dB		Доля изображений с неподтвержденными авторством и подлинностью (%)
	min.	ср.	min.	ср.	
3078	37,4	38,7	33,6	34,4	0
2048	33,9	35,3	32,9	32,9	4,30
1536	31,9	35,3	30,8	31,7	36,30

Сравнительный анализ результатов показывает, что для указанного кодека при генерации только кадров I-типа наиболее приемлемой является скорость порядка 3 Мб/с, что для данных тестовых видеопоследовательностей соответствует средней степени сжатия в 5,7 раз. При использовании алгоритма встраивания на основе IDA [4] применение разработанного алгоритма наиболее выгодно для низкочастотных изображений. В то же время на высокочастотных видеопоследовательностях (Flower) наблюдается некоторое снижение робастности, поскольку алгоритм встраивания работает именно с высокочастотными коэффициентами.

Пути повышения стойкости схемы к атакам внешнего нарушителя на видеоданные

Выше были описаны и показаны количественные и качественные характеристики устойчивости схемы к сжатию и возможным внешним помехам. Существенной характеристикой системы аутентификации является также стойкость к имитонавязыванию. В этом случае для характерного значения $P_D \le 10^{-9}$ внешний или потенциальный внутренний нарушитель не сможет подменить более 1 кадра на миллиард кадров видеопоследовательности без обнаружения. В данном разделе речь пойдет о качественной оценке защищенности видеопотока от разного рода атак.

Типовыми атаками внешнего нарушителя на видеоданные являются:

1. Искажение значимой информации в кадре – атака V;
2. Изменение порядка следования кадров (повтор группы кадров) – атака T;
3. Полная замена кадров на произвольные – атака C.

Существуют разные подходы для решения данного типа задач как на базе робастных функций [10], так и на базе только полухрупкого ЦВЗ [9]. Для защиты от атаки класса V применяется робастная хэш-функция. Причем, если хэш-код встраивается в тот же самый кадр, требуется робастность не только к сжатию, но и к искажениям, вносимым ЦВЗ. Ключевым параметром в этом случае является минимальный размер (в пикселях) искаженной области видеокадра. Результат атаки в этом случае напрямую зависит от контента видеокадра – от типа и содержания видеоданных, а также от качества и разрешения видео. Интегрирующим параметром здесь является восприятие человека. Например, искажение размером 200×200 пикселей на 1–2 кадрах будет намного менее заметным и существенным, чем искажение размером 50×50 пикселей, но на протяжении нескольких секунд видеопотока.

Таким образом, при конструировании робастных хэш-функций, автор видит в качестве основной проблемы достижение достаточно малого размера искажений с одновременной минимизацией ложных срабатываний при типовых искажениях в процессе сжатия и наложения ЦВЗ (если аутентификатор встраивается в тот же кадр). Подробное рассмотрение этой проблемы выходит за рамки настоящей статьи.

Для защиты от атак классов T и C может быть применена взаимная синхронизация приемника и источника, например, посредством генератора гаммы, ключ формирования которой неизвестен внешнему нарушителю. Аутентификатор, встраиваемый в кадр, зависит от некоторого числа бит из гаммы. При этом требуется достаточно большой период генератора гаммы, чтобы не допустить повтора кадра с той же ключевой последовательностью.

Заключение

Таким образом, предложен подход к построению стеганографической ЭП видеоданных в условиях воздействия помех, состоящий из следующих компонентов:

- алгоритм встраивания и извлечение битов, данных ЦВЗ,
- криптосхема с побитовым формирование ЭП, которая обеспечивает побитовую аутентификацию по асимметричной схеме;
- хэш-функция для фрагмента кадра, формирующая робастный хэш-код, который при разрешенных операциях обработки видео изменяется незначительно, а при умышленной модификации – лавинообразно.

В отличие от традиционных подходов к формированию ЭП видеоданных, здесь не требуется дополнительной безошибочной передачи криптографической электронной подписи и заверяемого сообщения. Предложенный подход реализует защиту видеоданных от атак как внешних, так и потенциальных внутренних нарушителей, причем без построения дополнительных каналов передачи, что является его существенным преимуществом. Таким образом, поставленная цель разработки стеганографической системы ЭП видеоданных была достигнута. Данная система обеспечивает защиту от атак внешних и потенциальных внутренних нарушителей на подлинность видеоданных.

СПИСОК ЛИТЕРАТУРЫ

1. Weiwei Zhang, Ru Zhang, Xianyi Liu, Chunhua Wu, Xinxin Niu. A Video Watermarking Algorithm of H.264/AVC for Content Authentication Journal of Networks, 2012, no. 8, part 7.

2. Zhenjun Tang, Shuozhong Wang, Xinpeng Zhang, Weimin Wei, and Shengjun Su. Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization Journal of Ubiquitous Convergence and Technology, 2008, no. 7, part 1.

3. Habib, A. and Xu, D. and Atallah, M. and Bhargava, B., and Chuang, J. A Tree-Based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming Cerias Tech Report, 2005.

4. Mohamed Hefeeda, Kianoosh Mokhtarian. AuthenticationSchemesforMultimediaStreams:Quantitative Analysis and Comparison. Simon Fraser University, 2010.

5. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи / Военная академия свя-

зи. – СПб. : Издательство Политехнического университета, 2006. – 300 с.

6. Оков И.Н., Головачев В.Ю. Обеспечение подлинности переговоров: стеганографические технологии // Управление безопасностью. – 2004. – № 2.

7. Johansson T. On the construction of perfect authentication codes that permit arbitration // Advance in Cryptology, Proc. Crypto -93. Sprinter-varlag, 1993.

8. Gabriele Oligeri, Stefano Chessa, Roberto Di Pietro, Gaetano Giunta. Robust and Efficient Authentication of Video Stream Broadcasting TISSEC1401-05 ACM-Transaction May 6, 2011.

9. Mohamed Hefeeda and Kianoosh Mokhtarian Analysis jf Authentication Schemes for Nonscalable Video Streams. Simon Fraser University Surrey, BC, Canada, 2009.

10. Brenden Chong Chen. Robust Image hash function using Higher Order Spector. Laboratory Science and Engendering faculty, 2012.

REFERENCES

1. Weiwei Zhang, Ru Zhang, Xianyi Liu, Chunhua Wu, Xinxin Niu. A Video Watermarking Algorithm of H.264/AVC for Content Authentication. *Journal of Networks,* 2012, no. 8, Part 7.

2. Zhenjun Tang, Shuozhong Wang, Xinpeng Zhang, Weimin Wei, and Shengjun Su. Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization. *Journal of Ubiquitous Convergence and Technology,* 2008, no. 7, Part 1.

3. Habib, A. and Xu, D. and Atallah, M. and Bhargava, B., and Chuang, J. *A Tree-Based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming Cerias*. Tech Report. 2005.

4. Mohamed Hefeeda, Kianoosh Mokhtarian. *Authentication Schemes for Multimedia Streams: Quantitative Analysis and Comparison*. Simon Fraser University, 2010.

5. Okov I.N. *Autentifikatsiya rechevykh soobshcheniy i izobrazheniy v kanalakh svyazi* [Authentication of Voice Messages and Images within Communications Channels]. Military Communications Academy. Sankt-Peterburg, Izdatelstvo Politekhnicheskogo Universiteta Publ., 2006. 300 p.

6. Okov I.N., Golovachev V.Yu. Obespecheniye podlinnosti peregovorov: steganograficheskiye tekhnologii [Negotiation Authentication: Steganography Technologies]. *Upravleniye bezopasnostyu* [Journal of Security Management], 2004, no. 2.

7. Johansson T. On the construction of perfect authentication codes that permit arbitration. *Advances in Cryptology, Crypto-93, Proceedings,* Springer-verlag, 1993.

8. Gabriele Oligeri, Stefano Chessa, Roberto Di Pietro, Gaetano Giunta. *Robust and Efficient Authentication of Video Stream Broadcasting*. TISSEC1401-05 ACM-Transaction, May 6, 2011.

9. Mohamed Hefeeda and Kianoosh Mokhtarian. *Analysis of Authentication Schemes for Nonscalable Video Streams*. Simon Fraser University Surrey, BC, Canada. 2009.

10. Brenden Chong Chen. *Robust Image hash function using Higher Order Spector*. Laboratory Science and Engendering faculty, 2012.