УДК 004.021

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ПОТОКОВОЕ ВИДЕО. ОБЗОР

***А. К. Григорьян*[1],**
аспирант
***Н. Г. Аветисова*[1],**
соискатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Дан обзор методов внедрения цифровых водяных знаков в потоковое видео, используемых российскими и зарубежными специалистами. Подробно описаны такие алгоритмы внедрения, как аддитивные алгоритмы, алгоритмы слияния, приведен пример использования консилограмм. Сделаны выводы об эффективности описанных алгоритмов.

Ключевые слова *— аддитивные алгоритмы, цифровой водяной знак, потоковое видео, робастность, консилограммы, вейвлет-преобразование.*

Введение

Информация является одной из ценнейших областей современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. В то же время легкость и скорость такого доступа значительно повысили и угрозу нарушения безопасности данных при отсутствии мер их защиты, а именно угрозу неавторизированного доступа к информации.

Задача надежной защиты авторских прав, прав интеллектуальной собственности или конфиденциальных данных (которые в большинстве случаев имеют цифровой формат) от несанкционированного доступа является одной из старейших и почти не решенных сегодня проблем. В связи с интенсивным развитием и распространением технологий, которые позволяют с помощью компьютера интегрировать, обрабатывать и синхронно воспроизводить различные типы сигналов (так называемые мультимедийные технологии), вопрос защиты информации, представленной в цифровом виде, является чрезвычайно актуальным. Поэтому во всем мире назрел вопрос разработки методов по защите информации организационного, методологического и технического характера, среди них — методы криптографии и стеганографии.

Стеганографирование осуществляется различными способами. Общей же чертой таких способов является то, что скрываемое сообщение встраивается в некий не привлекающий внимание объект, который затем открыто транспортируется (пересылается) адресату.

В данной статье рассмотрены различные методы сокрытия информации в графических носителях (аддитивные алгоритмы, алгоритмы слияния, консилограммы), проведен сравнительный анализ возможности использования известных методов и алгоритмов для внедрения цифрового водяного знака (ЦВЗ) в такой специфический контейнер, как потоковое видео, формируемое автономными видеоустройствами; определены критерии оценки методов. В конце сделаны выводы о возможности применять некоторые алгоритмы, основанные на вейвлет-преобразованиях, для встраивания ЦВЗ в видеопоток, а также определен круг задач по модернизации отобранных алгоритмов.

Стеганография и ЦВЗ

Стеганография — это метод организации связи, который, собственно, скрывает само наличие связи. В отличие от криптографии, где злоумышленник точно может определить, является ли передаваемое сообщение зашифрованным текстом,

[1] Научный руководитель — доктор технических наук, профессор, заведующий кафедрой вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения *М. Б. Сергеев*.

методы стеганографии позволяют встраивать кодированные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного послания [1].

Слово «стеганография» в переводе с греческого буквально означает «тайнопись» («στεγανος» (steganos) — секрет, тайна; «γραφω» (graphy) — запись). К ней относится огромное множество специальных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, «закрытые» каналы и средства связи на плавающих частотах и т. д.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях. Это дает возможность говорить о становлении нового направления — компьютерной стеганографии.

История развития науки стеганографии описана в работе [1].

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки и заголовки [1].

Жизненный цикл и основные свойства цифровых водяных знаков также подробно рассмотрены [1].

Если рассуждать о применении ЦВЗ на практике, то можно выделить следующие аспекты:

– защита авторских прав;

– получение цифрового отпечатка (различные люди получают копии, помеченные разными водяными знаками);

– отслеживание трансляций (телевизионные новости часто содержат водяные знаки, оставленные международными информационными агентствами);

– сокрытие факта обмена информации (стеганография).

Методы сокрытия информации в графических носителях

Все методы, предназначенные для сокрытия данных в графических изображениях, можно разделить по принципам, лежащим в их основе, на форматные и неформатные.

Форматные методы сокрытия (форматные стеганографические системы) — это такие методы (системы), в которых принципы, положенные в основу сокрытия, основываются на особенностях формата хранения графических данных. Разработка таких методов сводится к анализу формата в целях поиска полей формата, изменение которых в конкретных условиях не скажется на работе с графическим изображением.

Однако все форматные методы обладают общим недостатком — для них возможно построение полностью автоматического алгоритма, направленного на обнаружение факта сокрытия (с учетом принципа общеизвестности стеганографической системы). Поэтому их стойкость к атакам пассивных злоумышленников крайне низка.

Неформатные методы, напротив, используют не формат хранения графического изображения, а непосредственно сами данные, которыми изображение представлено в этом формате. Применение неформатных методов неизбежно приводит к появлению искажений, вносимых стеганографической системой, однако при этом они являются более стойкими к атакам как пассивных, так и активных злоумышленников.

Поскольку в статье принят в качестве контейнера видеопоток, то рассматривать форматные методы внедрения ЦВЗ нецелесообразно. Ниже описаны некоторые неформатные методы и алгоритмы внедрения ЦВЗ.

Одним из распространенных методов встраивания ЦВЗ является метод модификации наименьших значимых бит (LSB) областей изображения, к которым глаз человека менее чувствителен. Реализация данного метода имеет низкую вычислительную сложность (высокая скорость таких методов обусловливается отсутствием дополнительных преобразований). Поскольку робастность такого ЦВЗ сравнительно низка, обычные LSB-методы невозможно применять для вышеописанных целей. Однако важно отметить, что использование самого принципа LSB, как инструмента внедрения, очень ценно.

По способу встраивания информации стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером либо «вплавляется» (fusion) в него. В нелинейных методах встраивания информации используется скалярное либо векторное квантование. Определенный интерес среди других представляют методы, использующие идеи фрактального кодирования изображений.

Аддитивные алгоритмы

В аддитивных методах внедрения ЦВЗ представляет собой последовательность чисел w_i длиной N, которая внедряется в выбранное подмножество отсчетов исходного изображения f. Основное и наиболее часто используемое выражение для встраивания информации в этом случае

$$f'(m, n) = f(m, n)(1 + \alpha w_i), \quad (1)$$

где f' — модифицированный пиксель изображения; α — весовой коэффициент.

Другой способ встраивания водяного знака был предложен И. Коксом [2]:

$$f'(m, n) = f(m, n) + \alpha w_i \quad (2)$$

или, при использовании логарифмов коэффициентов:

$$f'(m, n) = f(m, n)e^{\alpha w_i}. \quad (3)$$

При встраивании в соответствии с (1) ЦВЗ в декодере находится следующим образом:

$$w_i^* = \frac{f^*(m, n) - f(m, n)}{\alpha\, f(m, n)}. \quad (4)$$

Здесь под f^* понимаются отсчеты полученного изображения, содержащего или не содержащего ЦВЗ w. После извлечения w_i^* сравнивается с подлинным ЦВЗ. Причем, в качестве меры идентичности водяных знаков используется значение коэффициента корреляции последовательностей

$$\delta = \frac{w^* w}{\|w\|^* \|w\|}. \quad (5)$$

Эта величина варьируется в интервале [–1; 1]. Значения, близкие к единице, свидетельствуют о том, что извлеченная последовательность с большой вероятностью может соответствовать встроенному ЦВЗ. Следовательно, в этом случае делается заключение, что анализируемое изображение содержит водяной знак.

В декодере может быть установлен некоторый порог $\tau = \frac{\alpha}{SN}\sum|f'|$ (здесь S — стандартное среднее квадратическое отклонение), который определяет вероятности ошибок первого и второго рода при обнаружении ЦВЗ. При этом коэффициент α может не быть постоянным, а адаптивно изменяться в соответствии с локальными свойствами исходного изображения. Это позволяет сделать водяной знак более робастным (стойким к удалению).

Для увеличения робастности внедрения во многих алгоритмах применяются широкополосные сигналы. При этом информационные биты могут быть многократно повторены, закодированы с применением корректирующего кода либо к ним может быть применено какое-либо другое преобразование.

Наиболее ярким представителем алгоритмов внедрения ЦВЗ на основе использования широкополосных сигналов является алгоритм Кокса и другие, в частности усовершенствованные, алгоритмы [3–9].

Алгоритмы слияния

Если вместо последовательности псевдослучайных чисел в изображение встраивается другое изображение (например, логотип фирмы), то соответствующие алгоритмы внедрения называются алгоритмами слияния. Размер внедряемого сообщения намного меньше размера исходного изображения. Перед встраиванием оно может быть зашифровано или преобразовано каким-нибудь иным способом.

У таких алгоритмов есть два преимущества. Во-первых, можно допустить некоторое искажение скрытого сообщения, так как человек все равно сможет распознать его. Во-вторых, наличие внедренного логотипа является более убедительным доказательством прав собственности, чем наличие некоторого псевдослучайного числа.

Распространенные алгоритмы внедрения изображений в изображения описаны в работах [4, 9].

Консилограммы

В последнее время появился еще один стеганографический способ защиты документов. Разработанный профессором Розеном совместно с профессором Коннектикутского университета Бахрамом Явиди (Bahram Javidi) новый метод стеганографии получил название «concealogram» или «консилограмма» (от conceal — «скрывать» и «голограмма»), поскольку секретная часть документа встраивается в обычное изображение методами, родственными голографическим [10].

Постановка задачи и определение модели решения

Необходимо разработать технологию защиты потоковой видеоинформации от возможных преднамеренных атак в процессе передачи по каналам общего пользования, а также оригинальный метод, осуществляющий защиту такого рода для потока видеоинформации, формируемого в режиме реального времени на устройствах автономного класса.

Вначале следует описать принципы функционирования изучаемой системы.

Аппаратной составляющей такой системы является автономная видеосистема с сигнальным процессором типа ADSP-BF537 с частотой 600 МГц и памятью объемом 32 МБ SDRAM. В обычном режиме работы процессор и ОЗУ имеют загруженность ЦП и ОЗУ порядка 50–60 %.

Данная система работает в режиме реального времени по следующему принципиальному алгоритму. Производится захват видеокадров, их обработка на сигнальном процессоре типа ADSP-BF537 (Blackfin), сжатие, накопление последовательности (пакета) кадров для передачи на ло-

кальном запоминающем устройстве и последующая передача информации по открытым каналам связи на удаленный сервер. Поскольку передача осуществляется по незащищенным открытым каналам связи, существует вероятность ее перехвата и намеренного искажения или подмены какой-либо последовательности кадров. Поэтому необходимо подтвердить подлинность видеопотока путем внедрения ЦВЗ на стадии формирования потока. Причем ЦВЗ следует внедрять до процесса сжатия видео, и, следовательно, знак должен быть устойчив к сжатию.

Цифровой водяной знак может представлять собой цветное или черно-белое растровое изображение небольшого размера (например, логотип). Предельный размер внедряемого ЦВЗ рассчитывается исходя из характеристик контейнера и метода внедрения. Поскольку внедрение происходит на уровне бит, в роли ЦВЗ может выступить любая цифровая последовательность, однако наличие извлеченного из кадра осмысленного изображения проще использовать для доказательства подлинности принятого видеопотока.

Если в ходе передачи совершится так называемая «активная» атака на передаваемую информацию, вследствие чего будет произведена подмена кадров целиком или их частичная модификация, то ЦВЗ, внедренный в атакованные кадры, частично или полностью разрушится.

При извлечении водяного знака из принятой видеопоследовательности можно будет однозначно определить, имело ли место вмешательство, и если имело, то каковы его масштабы.

Поскольку передача производится по обычным каналам связи, существует вероятность искажения передаваемой информации (и, как следствие, ЦВЗ) из-за существующих в канале помех. Необходимо установить обоснованный коэффициент достоверности, позволяющий отделить случайные искажения от преднамеренных.

Существует приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 г. № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования», в тексте которого среди прочего введены «Технические нормы на показатели функционирования сетей передачи данных». Согласно данному приказу, коэффициент потери пакетов информации не должен превышать 0,1 %, а коэффициент ошибок в пакетах информации — более 0,01 % [11]. Однако реальная ситуация такова, что в сетях общего пользования существуют потери до 5 % передаваемой информации. В связи с этим предлагается установить значение в 95 % для коэффициента достоверности переданного ЦВЗ. Все кадры, содержащие водяной знак, который удовлетворяет этому условию, признаются достоверными.

Учитывая ограниченный временной и вычислительный ресурс на стадии внедрения, планируется защищать цифровым знаком не все кадры подряд, а только некоторую их последовательность (например, 3–5 кадров), причем с определенным интервалом (например, в 15 кадров).

Ввиду того, что предполагаемая атака будет вестись не на отдельный кадр (что является бессмысленным при скорости потока 25 кадров / с), а на значительную их последовательность, декодеру необходимо выбрать группу кадров и проанализировать некоторые кадры из этой группы. Допускается, что в последовательности может присутствовать один или несколько достаточно сильно «зашумленных» кадров, и водяной знак, извлеченный из них, будет сильно разрушен. Однако если после обработки всей группы кадров из определенной доли этих кадров удается извлечь подлинный ЦВЗ, то делается вывод об отсутствии вмешательства в эту группу кадров.

Подобная методика анализа сигнала является допустимой, поскольку он будет выполняться на компьютере, что подразумевает доступ к несравнимо большему вычислительному ресурсу, чем на стадии внедрения.

Анализ существующих методов внедрения ЦВЗ

В отечественной и зарубежной литературе описано множество различных методов и алгоритмов внедрения цифрового водяного знака в неподвижное видеоизображение. Подобную технологию следует использовать и при работе с видеопотоком.

В таблице приведены самые известные и распространенные методы и алгоритмы [1]. Принципы работы прочих алгоритмов можно считать сходными с тем или иным уже описанным алгоритмом.

Авторы [1] использовали в качестве ЦВЗ псевдослучайную последовательность чисел различной длины (в основном, около 1000 Б). Сохранена авторская нумерация алгоритмов [1].

Далее необходимо провести селекцию упомянутых выше методов и выделить те из них, которые наиболее подходят для решения описанной ранее задачи.

В качестве первичного критерия отбора выбрана методика поиска возможного внедренного ЦВЗ при декодировании. В большинстве упомянутых выше алгоритмов декодер «знает» искомый водяной знак. Из соображений эффективности разрабатываемой системы, а также принимая во внимание относительно безграничный вы-

■ *Сравнительная таблица методов и алгоритмов работы с ЦВЗ*

№	Принцип работы	Преимущества	Недостатки
Аддитивные алгоритмы			
A17	Модификация 1000 самых больших коэффициентов дискретно-косинусного преобразования (ДКП)	Сильная робастность ЦВЗ при сжатии и других видах обработки сигнала	Трудоемкость вычисления двумерного ДКП
A18	Модификация всех коэффициентов детальных поддиапазонов первого подуровня разложения при выполнении четырехуровневого вейвлет-преобразования	Возможность обнаружения ЦВЗ без исходного изображения. Сильная визуальная незаметность ЦВЗ	Для извлечения ЦВЗ необходимо иметь исходное изображение
A19	Модификация всех коэффициентов LL-поддиапазона вейвлет-преобразования изображения	Возможность модификации алгоритма для использования ключа	То же
A20	Модификация наибольших коэффициентов детальных поддиапазонов трехуровневой декомпозиции изображения	Хорошая визуальная маскировка внедренных данных. Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
A21	Модификация перцептуально значимых коэффициентов трехуровневой декомпозиции изображения с использованием биортогональных вейвлет-фильтров	Робастность ЦВЗ ко многим видам атак. Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
A22	Модификация наибольших коэффициентов каждого поддиапазона трехуровневой декомпозиции изображения (за исключением поддиапазонов наивысшего уровня разрешения)	Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
A23	Модификация 1000 наибольших коэффициентов пакетного вейвлет-преобразования (ЦВЗ также подвергается преобразованию)	То же	—
A24	Модификация наибольших коэффициентов трехуровневого вейвлет-преобразования (коэффициенты отбираются в соответствии с заданным порогом)	Высокая робастность ЦВЗ к некоторым видам атак	Для извлечения ЦВЗ необходимо иметь исходное изображение
A25	Модификация коэффициентов четырехуровнего вейвлет-преобразования, отобранных с учетом заданного порога	Высокая робастность внедряемого ЦВЗ	То же
A26	Модификация наибольших коэффициентов из высокочастотного и среднечастотного диапазонов преобразования Хаара	Высокая робастность к атакам с изменением масштаба. Возможность сокращения количества вычислительных операций при обнаружении ЦВЗ	– « –
A27	Модификация значимых коэффициентов всех поддиапазонов пятиуровневого вейвлет-преобразования	Возможность модификации алгоритма для использования стегоключа	– « –
A28	Алгоритм A28 представляет собой модифицированный вариант алгоритма A27, со слепым извлечением ЦВЗ	Для обнаружения ЦВЗ не требуется наличие исходного изображения	Сильно пониженная помехоустойчивость по сравнению с алгоритмом A27
A29	Модификация всех коэффициентов одноуровневой декомпозиции исходного изображения	Большой размер скрываемого ЦВЗ (до четверти размера исходного изображения)	Для извлечения ЦВЗ необходимо иметь исходное изображение

Окончание таблицы

№	Принцип работы	Преимущества	Недостатки
A30	Модификация всех коэффициентов детальных поддиапазонов вейвлет-преобразования исходного изображения (преобразование Хаара)	Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
Алгоритмы на основе слияния ЦВЗ и контейнера			
A31	Модификация высокочастотных коэффициентов голубой компоненты изображения после пятиуровневого целочисленного вейвлет-преобразования	Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
A32	Модификация ВЧ-НЧ и НЧ-ВЧ областей двухуровневого вейвлет-преобразования исходного изображения	Большой размер скрываемого ЦВЗ	Для извлечения ЦВЗ необходимо иметь исходное изображение; низкая стойкость алгоритма по отношению к операциям обработки сигнала
A33	Модификация n-мерного вектора коэффициентов дискретного вейвлет-преобразования исходного изображения	Большой размер скрываемого ЦВЗ. Возможно контролировать робастность, уровень искажений и качество внедряемого изображения	Для извлечения ЦВЗ необходимо иметь исходное изображение
Алгоритмы с использованием фрактальных преобразований			
A34	Формируется из исходного изображения (до 15 различных ЦВЗ)	Для обнаружения ЦВЗ не требуется наличие исходного изображения	—
A35	Использование строки бит	Наличие секретного ключа; устойчивость к сжатию JPEG	—
A36	Использование строки бит	Наличие секретного ключа	Возможно заметное ухудшение качества изображения при встраивании ЦВЗ

числительный и временной ресурс, имеющийся на стороне приема и расшифровки потока, на данной стадии были отобраны только алгоритмы со «слепым» извлечением: алгоритмы A17, A20, A21, A23, A30.

Далее, принимая во внимание особенности используемой аппаратной платформы, при отборе методов необходимо учитывать ограниченную вычислительную мощность используемой аппаратной системы.

Таким образом, необходимо ранжировать имеющиеся алгоритмы по вычислительной сложности используемых в них методов обработки сигнала. В алгоритме A17, основанном на дискретно-косинусном (дискретно-синусном) преобразовании сигнала используются относительно емкостные для процессора формулы вычисления косинусов (синусов) соответствующих величин (даже с использованием численных методов вычисления синуса). Другой тип алгоритмов (A20, A21, A23, A30), основанных на вейвлет-преобразовании сигнала (ДВП, например, преобразование Хаара), можно представить в виде самых простых (и, соответственно, самых быстрых) для вычисления процессором математических операций. Это дает значительную экономию времени по сравнению с ДКП.

Таким образом, на следующем этапе отсева был исключен алгоритм A17, в основе которого лежит ДКП.

Рассматривая оставшиеся алгоритмы, выделим 2 семейства алгоритмов ДВП: быстрое вейвлет-преобразование (БВП) (A20, A21, A30) и преобразование с использованием вейвлет-пакетов (A23).

Согласно работе [12], при использовании модифицированного алгоритма Малла (БВП) для преобразования сигнала длиной $N = 2^n$ до k-го уровня потребуется $2^{n-1}(2^{k-1} - 1)$ операций сложения (нормирующие множители не учитываются, умножение на единицу также игнорируется [12]). После этого высокочастотную последова-

тельность k-го уровня необходимо обработать в соответствии с выбранным алгоритмом. Число таких операций будет равно сумме элементов геометрической прогрессии со знаменателем 2, начинающейся с 2^{n-k} и заканчивающейся числом 2^{n-1}, т. е. $2^n\left(1-\frac{1}{2^k}\right)$ операций. Поскольку при больших k множитель $\left(1-\frac{1}{2^k}\right)\to 1$, то обработка будет занимать 2^n операций. Затем необходимо произвести синтез сигнала по инверсным формулам, поэтому число операций синтеза также будет $2^{n-1}(2^{k-1}-1)$. Итого, сложность операции внедрения ЦВЗ с использованием алгоритма БВП сигнала будет $2^n + 2^{k-1}$ операций. Хранить в памяти нужно 2^{n-k} низкочастотных и $2^n\left(1-\frac{1}{2^k}\right)$ высокочастотных коэффициентов всех уровней, т. е. 2^n чисел.

При использовании же пакетных вейвлетов преобразование также выполняется для всех низко- и высокочастотных диапазонов каждого уровня с использованием, например, алгоритма одиночного дерева. Для сигнала длиной $N = 2^n$ при применении двухканального блока фильтров число базисов S_k, перебираемых алгоритмом одиночного дерева, вычисляется рекурсивно [13]:

$$S_k = S_{k-1}^2 + 1, \text{ где } k \in [2, 3, ..., n], \text{ а } S_1 = 2.$$

Для сигнала длиной $N = 2^n$ и дерева максимальной высотой k вычислительная сложность алгоритма одиночного дерева будет $O(Nk)$. Число операций для декомпозиции сигнала до k-го уровня составляет $3(2^n - 2^{k-1})$. Обработка всех высокочастотных коэффициентов (собственно внедрение ЦВЗ) не будет превышать $3 \cdot 2^{n-1}$ операций. Итого $3(5 \cdot 2^{n-1} - 2^k)$ операций. Объем памяти для хранения коэффициентов всех уровней равен $3 \cdot 2^{n-1} + 2^{n-k}$.

Исходя из вышеописанного делаем следующие выводы.

Использование пакетного вейвлет-преобразования позволит получить разложение, адаптированное к сигналу, хотя адаптивность достигается за счет увеличения вычислительной стоимости. Поскольку в результате внедрения ЦВЗ будут изменены небольшие коэффициенты преобразования, то добиться большей незаметности внедрения позволит именно пакетное вейвлет-преобразование.

Использование сигнально-независимого вейвлет-преобразования несет меньшую вычислительную нагрузку, но, возможно, внедрение ЦВЗ будет более заметным.

Таким образом, в результате анализа известных алгоритмов был отобран алгоритм, имеющий самую низкую вычислительную мощность (и соответственно, наименьшее время выполнения), т. е. алгоритм БВП Хаара (А30).

Однако для решения конкретной поставленной задачи (внедрение ЦВЗ в видеопоток, формируемый при помощи сигнального процессора), отобранный алгоритм необходимо модернизировать и оптимизировать по следующим параметрам:

1) необходимо решение для внедрения цветного изображения;

2) необходимо решение в целых числах, поскольку перевод процессора в режим работы с плавающей точкой увеличит временные затраты и затраты по памяти;

3) внедряемый ЦВЗ должен быть устойчив к сжатию и помехам;

4) необходимо определить наиболее эффективные параметры ДВП (уровень декомпозиции и т. д.) для решения поставленной задачи.

Заключение

Как показывает практика, за последние несколько лет актуальность проблемы информационной безопасности неуклонно возрастала, постоянно стимулируя при этом поиск новых методов защиты информации.

Сделать заметный вклад в общее дело наряду с другими призваны и стеганографические методы защиты информации, в частности, методы компьютерной стеганографии. Эта технология имеет юридическую силу и применяется для подтверждения подлинности цифровой информации, позволяя определить факт несанкционированного в нее вмешательства и ее искажения.

Поскольку целью данной работы был анализ алгоритмов внедрения ЦВЗ в изображения и оценка возможности использовать эти алгоритмы для защиты потокового видео в рамках аппаратной платформы с использованием процессора ADSP-BF537 (или подобного ему), были определены критерии оценки:

– независимость от внедренного ЦВЗ («слепые» методы);

– низкая вычислительная сложность алгоритма;

– сравнительно малый объем ОЗУ.

Были исследованы известные алгоритмы внедрения ЦВЗ, такие как А17 (Cox), А18 (Barni), А21 (J. Kim), А25 (C. Podilchuk) и др.

В ходе многоуровневой селекции был отобран алгоритм (А30), использующий БВП Хаара. Следующим этапом исследований планируется оптимизация выбранного алгоритма по указанным параметрам для защиты реального видеопотока.

Литература

1. **Грибунин В. Г., Оков И. Н., Туринцев И. В.** Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.
2. **Cox I. J., Kilian J., Leighton T., Shamoon T. G.** Secure spread spectrum watermarking for images, audio and video // Proc. of the IEEE Intern. Conf. on Image Processing. 1996. Vol. 3. P. 243–246.
3. **Barni M. et al.** DWT-based technique for spatio-frequency masking of digital signatures // Proc. of the 11th SPIE Annual Symp. Electronic Imaging '99: Security and Watermarking of Multimedia Contents. San Jose, CA, 1999. Vol. 3657. P. 31–39.
4. **Dugad R., Ratakonda K., Ahuja N.** A new wavelet-based scheme for watermarking images // Proc. of the IEEE Intern. Conf. on Image Processing. 1998. Vol. 1. P. 419–423.
5. **Kim Y.-S., Kwon O.-H., Park R.-H.** Wavelet based watermarking method for digital images using the human visual system // Electronic Letters. 1999. N 35(6). P. 466–467.
6. **Nicchiotti G., Ottaviano E.** Non-invertible statistical wavelet watermarking // Proc. of the 9th European Signal Processing Conf. European Association for Signal Processing. Island of Rhodes, Greece. Sept. 1998. P. 2289–2292.
7. **Podilchuk C. I., Zeng W.** Digital image watermarking using visual models // IEEE J. on Selected Areas in Communications. 1998. Vol. 16. P. 525–539.
8. **Wang Houng-Jyh, Lu C., Kuo C.-C. Jay.** Image protection via watermarking on perceptually significant wavelet coefficients // Proc. of the IEEE Workshop on Multimedia Signal Processing. Redondo Beach, CA, 1998. Vol. 1. P. 279–284.
9. **Xia X.-G., Boncelet C. G., Arce G. R.** Wavelet transform based watermark for digital images // Optics Express. 1998. N 3. P. 497–502.
10. **Смирнов М. В.** Голографический подход во встраивании скрытых ЦВЗ в фотографические изображения // Оптические технологии. 2005. Т. 72. № 6. С. 464–468.
11. **Об утверждении Требований** к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования: Приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 г. № 113 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. 26 нояб. № 48. С. 165–169.
12. **Копенков В. Н.** Эффективные алгоритмы локального дискретного вейвлет-преобразования с базисом Хаара // Компьютерная оптика. 2008. Т. 32. № 1. С. 78–84.
13. **Воробьев В. И., Грибунин В. Г.** Теория и практика вейвлет-преобразования / ВУС. — СПб., 1999. — 204 с.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (80x@mail.ru).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.