УДК 004.415.24

Н.В. Кошкина

Определение инварианта к сжатию с потерями для аудиосигналов

Исследован характер воздействия на аудиосигнал кодеков сжатия с потерями качества. Представлены методы определения инварианта к сжатию с потерями и внедрения в аудиоданные цифровых водяных знаков. Доказана возможность блокирования несанкционированного доступа к упомянутым знакам. Описана методика получения оценок качества стеганосистемы.

A character of the influence on the audio signal of compression codecs with the quality loss is studied. .The methods of defining the invariant to the compression with losses and of the of introduction of digital watermarks to the audio data are presented. The possibility of blocking the unauthorized access to these watermarks is proved. The technique of evaluating the quality of the steganosystem is described.

Досліджено характер впливу на аудіосигнал кодеків стиснення зі втратами. Запропоновано методи визначення інваріанту до стиснення зі втратами та вкраплення у аудіодані цифрових водяних знаків. Доведено можливість блокування несанкціонованого доступу до згаданих знаків. Описано методику отримання оцінок якості стеганосистеми.

Введение. Создание систем с цифровыми водяными знаками (ЦВЗ) – одно из направлений компьютерной стеганографии, решающее задачи защиты прав на цифровые объекты и контроля их использования [1–3]. ЦВЗ – это специальная метка, способная функционировать как инструмент идентификации и аутентификации сигнала, его источника, владельца и т.п. Процедуру внедрения ЦВЗ называют маркировкой, а сигнал, содержащий ЦВЗ, – маркированным.

Один из типов сигналов, для которых востребованы технологии ЦВЗ, – это цифровые аудиосигналы, в частности речевые сигналы. Базовые требования при построении эффективных стеганосистем с ЦВЗ – требования неощутимости и стойкости внедренного цифрового водяного знака. Так, необходимо, чтобы внедренный ЦВЗ не ухудшал качество восприятия аудиоданных пользователями, т.е. был неслышим. Кроме того, наличие ЦВЗ не должно прослеживаться при визуальном или статистическом анализе численных значений отсчетов аудиосигнала или его спектра стеганоаналитиком. Поступив в открытый доступ маркированный контейнер может подвергаться различным преобразованиям: смена формата файла, сжатие с потерями качества, низкочастотная фильтрация, цифро-аналоговое (ЦАП) и аналого-цифровое преобразование (АЦП) и т.д. ЦВЗ должен корректно извлекаться из маркированного сигнала после применения к нему подобных искажающих операций.

Отметим, что на практике существенными преимуществами обладают стеганосистемы с ЦВЗ, использующие слепую схему декодирования, т.е. не требующие при извлечении наличия оригинального сигнала и (или) оригинального ЦВЗ. Разработка таких систем, как позволяющих решить более широкий класс практических задач компьютерной стеганографии, наиболее актуальна.

Для оцифровки аналоговых сигналов используется импульсно-кодовая модуляция (ИКМ). Зачастую объем аудиофайла с сигналом, закодированным отсчетами ИКМ с достаточно большой частотой дискретизации и разрядной сеткой, неприемлемо велик для его хранения или передачи «как есть». Поэтому разработаны различные стандарты сжатия аудио. Наиболее распространенные сегодня – стандарты *MPEG*–1 *Layer* 3 (*MP*3), *MPEG*–2/4 (*AAC*), *Ogg Vorbis*, *WMA* (закрытый).

Цифровой водяной знак должен «переживать» вероятные операции обработки аудиосигнала, к которым относится сжатие с потерями. Поэтому прежде чем строить алгоритмы внедрения ЦВЗ в аудиосигналы, необходимо изучить характер искажений, вносимых в них различными кодеками сжатия с потерями, и определить области сигнала, инвариантные к сжатию и позволяющие модификацию без ухудшения качества восприятия аудио данных.

Алгоритмы компрессии звука

Систему человеческого слуха можно промоделировать как частотный анализатор, а именно как банк полосовых фильтров, что и реализовывается в аудиокодерах сжатия с потерями качества. Объем данных аудиосигнала умень-

шается путем устранения их психоакустической и статистической избыточности.

Обобщенная схема аудиокодеров, реализующих основные стандарты сжатия с потерями качества, представлена на рис. 1. Как правило, при сжатии входной сигнал пропускается через банк полосовых фильтров. А так как удаление статистической избыточности более эффективно выполнять для частотного представления сигнала, то для субполос полученного разложения вычисляются коэффициенты модифицированного дискретного косинусного преобразования (МДКП) [4]. Параллельно с этим сигнал анализируется психоакустической моделью кодера (ПАМ) с целью определения порогов психоакустического маскирования. Далее спектральные коэффициенты сигнала квантуются так, чтобы спектр шума по возможности (если позволяет битрейт) оказался ниже порогов маскировки и не был слышен. Удаляются компоненты сигнала, лежащие ниже вычисленных порогов. На последнем этапе сжатия к квантованным коэффициентам применяется неравномерное кодирование, удаляющее статистическую избыточность данных.

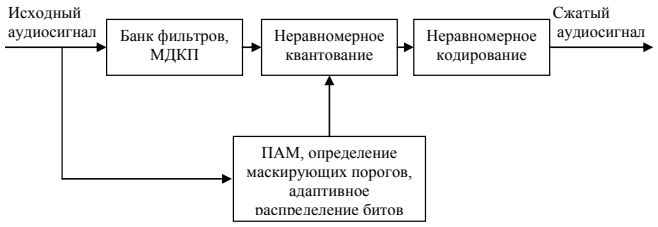


Рис. 1. Обобщенная схема кодеров сжатия аудиосигналов с потерями качества

Для неравномерного кодирования используют код Хаффмана, на этом этапе происходит сжатие информации без потерь. Таким образом, критичны для стеганографии – этапы субполосного кодирования и квантования с учетом ПАМ.

Отметим, что кодек, реализовывающий тот или иной стандарт сжатия, обычно имеет несколько альтернативных режимов – сжатие с постоянным, переменным или усредненным битрейтом. Выбор постоянного битрейта дает возможность точно предсказать размер сжатого файла, переменный битрейт дает наилучшее качество звучания, а усредненный – это гибрид первых двух режимов.

Субполосное кодирование

Субполосное кодирование реализуется путем свертки сигнала с несколькими полосовыми фильтрами и децимацией результата. Совокупность набора фильтров с дециматорами называют банком фильтров. Каждый получившийся в результате преобразования сигнал несет в себе информацию о спектральной составляющей исходного сигнала при некотором временном масштабе. Для обратного синтеза сигнала, т.е. его реконструкции, в декодере выполняется операция интерполяции субполосных сигналов, фильтрация и их сложение.

На рис. 2 изображена обобщенная (L-канальная) схема банка фильтров анализа–синтеза, где

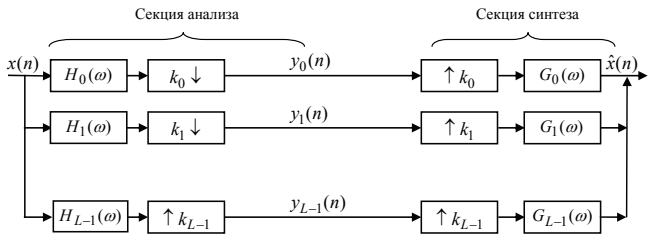


Рис. 2. Обобщенная схема банка фильтров анализа–синтеза

где $H_i(\omega) = \sum_n h_i(n) e^{-j\omega n}$ – частотная характеристика (ЧХ) i-го полосового КИХ-фильтра анализа, $G_i(\omega) = \sum_n g_i(n) e^{-j\omega n}$ – ЧХ i-го полосового КИХ-фильтра синтеза. Во временной области фильтрация соответствует операции круговой свертки входного сигнала $x(n)$ длиной N с импульсной характеристикой КИХ-фильтра ($h_i(n)$ или $g_i(n)$), в частотной области фильтрация соответствует умножению спектра сигнала $X(\omega)$ на $H_i(\omega)$ при разложении сигнала или на $G_i(\omega)$ – при его реконструкции. Длина фильтра меньше размера сигнала. Блоки $k_i\downarrow$ означают децимацию в k_i раз, т.е. оставление лишь каждого k_i отсчета, блоки $k_i\uparrow$ – интерполяцию в k_i раз, т.е. вставку $k_i - 1$ нулей между отсчетами. k_i – целые числа, являющиеся делителями N.

Банк фильтров анализа-синтеза должен минимизировать ошибку реконструкции сигнала $\varepsilon(n) = \hat{x}(n) - x(n)$, в частотной области легко раз-

деляющейся на две части: нежелательную алиасинговую составляющую (алиасинг – эффект наложения спектров, в результате которого в аудиосигнале появляются слышимые помехи [5, 6]) и составляющую, инвариантную к сдвигу.

Выходной сигнал банка фильтров анализа в частотной области имеет вид:

$$Y_i(\omega) = \frac{1}{k}\sum_{j=0}^{k-1} H_i(\frac{\omega}{k} + \frac{2\pi j}{k}) X(\frac{\omega}{k} + \frac{2\pi j}{k}).$$

Выходной сигнал всей схемы с учетом децимации и интерполяции:

$$\hat{X}(\omega) = \sum_{i=0}^{L-1} Y_i(k\omega) G_i(\omega).$$

Объединив эти выражения, получаем:

$$\hat{X}(\omega) = \frac{1}{k}\sum_{i=0}^{L-1}\left[\sum_{j=0}^{k-1} H_i(\omega + \frac{2\pi j}{k}) X(\omega + \frac{2\pi j}{k})\right] G_i(\omega) =$$

$$= \sum_{i=0}^{L-1} H_i(\omega) G_i(\omega) X(\omega) +$$

$$+ \frac{1}{k}\sum_{j=1}^{k-1} X(\omega + \frac{2\pi j}{k}) \sum_{i=0}^{L-1} H_i(\omega + \frac{2\pi j}{k}) G_i(\omega).$$

Таким бразом, первое слагаемое соответствует отклику линейной независимой системы, а второе – алиансигу системы.

Субполоса $y_i(n)$, полученная при помощи банка фильтров анализа, может быть еще раз разложена некоторым банком фильтров анализа, субполосы полученного разложения опять могут подаваться на вход банка фильтров анализа. В результате получается иерархическая каскадно-соединенная система. Причем, если первоначальный банк фильтров обладал свойством полного восстановления, то и получившаяся двухуровневая, трехуровневая и т.д. система обладает этим свойством.

Решить проблему алиасинга помогает применение квадратурных зеркальных фильтров (КЗФ), впервые предложенных для кодирования речи [5]. Так, выход двухканального банка фильтров анализа–синтеза, построенного на КЗФ, свободен от алиасинга. Для такого банка фильтров сигнал на каждом уровне делится на субполосы с помощью одного низкочастотного и одного высокочастотного фильтра. Свое название КЗФ получили потому, что ЧХ низкочастотного фильтра есть зеркальным отображением ЧХ соответствующего ему высокочастотного относительно половины частоты дискретизации. Чем более близки ЧХ выбранных фильтров к ЧХ идеального фильтра, тем меньшая погрешность привносится в сигнал при его обработке банком фильтров анализа-синтеза.

Частный случай КИХ-фильтров – КИХ-фильтры, построенные на базе вейвлетов. Разложение сигнала на субполосы с целью дальнейшего анализа или модификации можно выполнить при помощи ортогональных или биортогональных вейвлетов, для которых вычисляются две пары КЗФ-фильтров банка фильтров анализа-синтеза. Алгоритм быстрого вейвлет-преобразования также использует банки фильтров.

Кодирование с преобразованием

После разложения аудиосигнала на субполосы дальшейшему квантованию и кодированию подвергаются частотные коэффициенты этих субполос. Теоретически получить спектр можно при помощи дискретного преобразования Фурье (ДПФ), дискретного косинусного преобразования (ДКП), модифицированного дискретного косинусного преобразования (МДКП). Как правило, стандарты сжатия с потерями предполагают на этом этапе использование МДКП, как наиболее учитывающее специфику аудио.

Перед преобразованием сигнал делится на кадры, коэффициенты МДКП вычисляются с 50%-ным наложением двух последовательных кадров. Такое перекрытие в сочетании с синусоидальным окном преобразования (MP3) или окном Кайзера–Бесселя (AAC) позволяет получить полную реконструкцию сигнала. Так, например, в MP3 коэффициенты МДКП определяются согласно следующим формулам:

$$X_i(r) = \frac{2}{M}\sum_{n=0}^{2M-1} \psi(n) c(r,n) x(n + iM),$$

$$\psi(n) = \sin\left[\frac{\pi(2n-1)}{4M}\right],\ 0 \le r \le M-1\ ,\ 0 \le n \le 2M-1$$

$$c(r,n) = \cos\left[\frac{\pi(2r+1)(2n+M+1)}{4M}\right],$$

где i – индекс кадра, r – индексы частотных коэффициентов в каждом кадре, M – общее ко-

личество коэффициентов в кадре, $\psi(n)$ – оконная функция, компенсирующая эффект искажений на границах кадра, индекс $(n + iM)$ – индекс выборки перед синхронизацией кадров.

Психоакустика

Шаг квантования коэффициентов МДКП устанавливается пропорционально психоакустическим порогам маскирования. Среди существующих психоакустических моделей наибольшее распространение получила модель *NMR* (*Noise to Mask Ratio* – отношение сигнал/маска), учитывающая абсолютный порог слышимости и маскировку в частотной области.

Абсолютный порог слышимости. При одном и том же уровне звукового давления ощущение громкости чистых тонов разной частоты оказывается различным, как и минимальное звуковое давление, при котором еще существует слуховое ощущение, или порог слышимости чистых тонов разной частоты. Порог слышимости зависит и от условий эксперимента. Минимальный уровень звукового давления, при котором обнаруживается звуковая волна гармонической формы в отсутствие других звуков, называется абсолютным порогом слышимости или порогом слышимости в тишине (рис. 3). Очевидно, что те спектральные компоненты полезного сигнала, лежащие ниже абсолютного порога слышимости, кодировать и передавать не следует.

Маскировка в частотной области. Порог слышимости одного сигнала изменяется в присутствии другого сигнал. Порог слышимости одних звуковых компонент в присутствии других называется относительным порогом слышимости.

Слабое, но слышимое звуковое колебание становится неслышимым при наличии более громкого, т.е. маскируется им. Эффект маскирования зависит от спектральных и временных характеристик маскируемого сигнала и сигнала маскирования. Маскировка в частотной области проявляется по-разному в зависимости от особенностей спектров звуковых сигналов. При разработке алгоритмов компрессии учитывается различие маскировки внутри частотной группы слуха и вне ее [7]. Маскирующий порог зависит от частоты, уровня подавления сигнала, тональной или шумовой характеристик маскируемого сигнала и сигнала маскирования. Например, широкополостным шумовым сигналом маскировать тональное колебание легче, чем чистым тоном маскировать шум.

Рис. 3. Пример определения порогов маскирования для одной из психоакустических моделей стандарта *MP*3 (ПАМ1)

Спектральные компоненты, лежащие ниже относительного порога слышимости, слухом не воспринимаются, поэтому их также можно не передавать на приемную сторону системы при кодировании (см. рис. 3).

Маскировка во временной области. При восприятии аудиосигналов системой человеческого слуха, кроме частотной маскировки, происходит и временная. Это явление характеризует динамические свойства слуха, показывая изменение во времени относительного порога слышимости, когда маскирующий и маскируемый сигналы звучат не одновременно. При этом следует различать явления послемаскировки (изменение порога слышимости после сигнала высокого уровня) и предмаскировки (изменение порога слышимости перед приходом сигнала максимального уровня).

Послемаскировка проявляется на интервале времени, равном 100...200 мс. Предмаскировка проявляется на значительно более коротком временном интервале. Он обычно составляет около 10 мс. Длительность предмаскировки в большой степени зависит от особенностей индивидуума. Чаще всего именно по этим двум причинам явление предмаскировки не учитывается.

Визуальный анализ характера воздействия на аудиосигнал кодеков сжатия с потерями

Так как каждый из кодеров эксплуатирует свою ПАМ, то, решая задачу поиска инварианта для всех распространенных стандартов сжатия с потерями, целесообразно отталкиваться от общих оценок. В частности от оценок, полученных при помощи визуального анализа спектрограмм оригинального и сжатого сигналов.

Спектрограмма – это диаграмма, на которой по оси абсцисс откладывается время, по оси ординат – частота, а амплитуда соответствующей частотной составляющей отмечается интенсивностью цвета в данной точке графика. При ее построении необходимо для каждого момента времени посчитать спектр сигнала в блоке вокруг этой точки времени, амплитуды спектра (рис. 4) в логарифмическом масштабе есть значениями одного столбца графика (рис. 5).

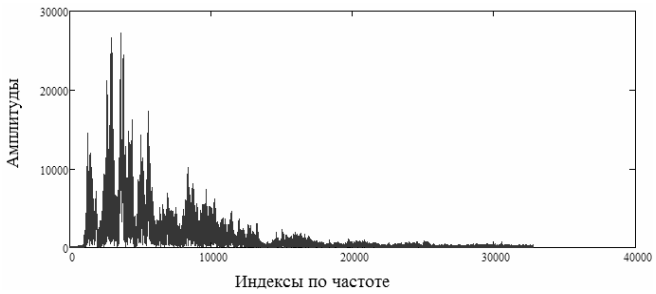
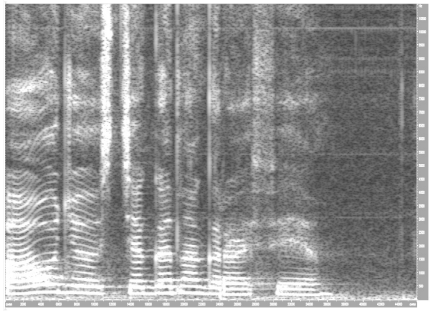
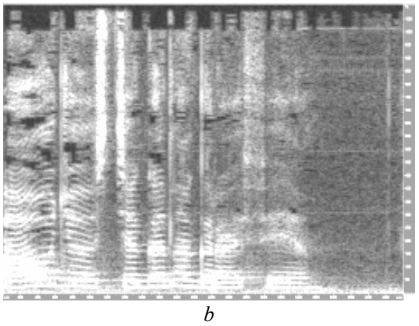


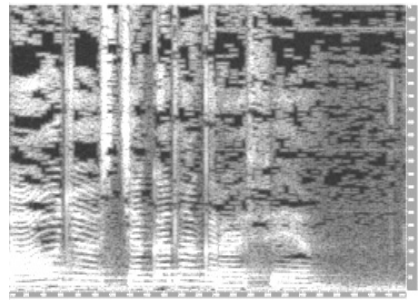
Рис. 4. Амплитудный спектр аудиосигнала для фиксированного момента времени



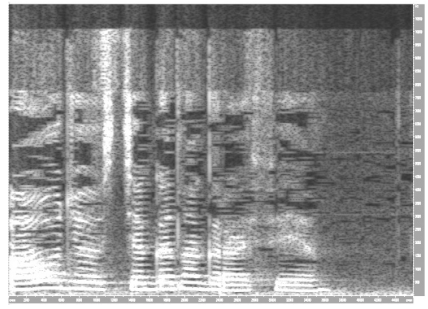
a



b



c



d

Рис. 5. Характер искажений, вносимых операцией сжатия с потерями: *a* – исходный речевой сигнал в формате *WAV* (ИКМ), оцифрованный с частотой 22 КГц и разрядностью 16 бит; *b* – сигнал, закодированный в формате *mp*3 с битрейтом 64 кбит/с; *c* – сигнал, закодированный в формате *ogg* с битретом 32 кбит/с; *d* – сигнал, закодированный в формате *wma* с битретом 20 кбит/с

Чтобы гарантированно сохранить внедренный ЦВЗ, целесообразно рассмотреть спектрограммы аудиосигналов, сжатых разными кодерами с низким битрейтом (рис. 5). Так, на примерах спектрограмм видно, в каких областях происходят существенные изменения сигнала (более темные участки в сравнении с исходными). Кодер, реализовывающий *MPEG*–1 *Layer* 3, в основном обрезал высокие частоты исходного файла (*b*), кодер *Ogg Vorbis* сильнее всего обрезал часть средних и высоких частот (*c*), кодер *WMA* внес существенные изменения в средние и высокие частоты (*d*).

Таким образом, согласно итогам визуального анализа инвариант к сжатию разными алгоритмами целесообразно искать в низких частотах аудиосигналов.

Отметим, что спектральный анализ выполняется на основе индексов временных $n=0\ldots$ $\ldots N-1$ и спектральных $r=0\ldots N-1$ отсчетов без учета частоты дискретизации аудисигналов. Это позволяет использовать алгоритмы вычисления спектра при любой частоте дискретиза-

ции не меняя вычислительную программу. Если необходимо привязать индексы к частоте дискретизации (реальной оси частот), то нужно учесть, что частотный спектр дискретизировался с шагом $\Delta\omega\frac{2\pi}{N\cdot\Delta t}$ рад/сек или $\Delta f\frac{1}{N\cdot\Delta t}$ Гц, где $\Delta t\frac{1}{F_d}$, F_d – частота дискретизации в Гц. Таким образом, если известна частота дискретизации, то r-й спектральный отсчет соответствует частоте $\omega = r\cdot\Delta\omega$ рад/сек или $f = r\cdot\Delta f$ Гц. На рис. 3 и 4 приведена половина отсчетов амплитуд спектра, так как спектр вещественных сигналов, к которым относятся и аудиосигналы, симметричен относительно $\frac{N}{2}$.

Метод маркировки аудиосигналов

Ранее определено, что носителем ЦВЗ целесообразно выбрать низкочастотную субполосу аудиосигнала как наименее искажаемую при сжатии. Кроме того, согласно ппсихоакустике человеческое ухо наиболее чувствительно к искажениям, возникающим на частотах 1–6 Кгц (см. абсолютный порог слышимости на рис. 3, с учетом того, что его график приведен при $N = 512$ и $F_d = 44010$ Гц). Следовательно, в низкие частоты до 1 кГц можно привнести больше неслышимых модификаций, чем в частоты 1–6 кГц, и вместе с тем эти модификации будут более стойкими к сжатию модификаций частот свыше 6 кГц.

Для выделения субполосы внедрения используем многоуровневый вейвлет-анализ. При выборе количества уровней разложения следует учесть следующие зависимости.

С увеличением количества уровней разложения увеличивается:

- неощутимость внедренного ЦВЗ;
- вычислительная сложность алгоритма маркировки (что критично для систем с ЦВЗ, работающих в реальном режиме времени);

кроме того,

- уменьшается пропускная способность стеганоканала, т.е. в аудиосигнал можно будет внедрить меньшее количество дополнительных данных.

На рис. 6 представлен Z-уровневый банк фильтров анализа, используемый для выделения субполосы–носителя ЦВЗ.

Кодирование битов ЦВЗ осуществляется методом относительной замены значений амплитудного спектра выбранной субполосы. Пары значений соседних амплитуд будут носителем одного бита ЦВЗ. При внедрении нуля значение парной амплитуды уменьшается (вплоть до обнуления) так, чтобы выполнялось условие $\left|X'_{2r}+P\right| < \left|X'_{2r+1}\right|$. При внедрении единицы уменьшается значение непарной амплитуды так, чтобы $\left|X'_{2r+1}+P\right| < \left|X'_{2r}\right|$, $P>0$.

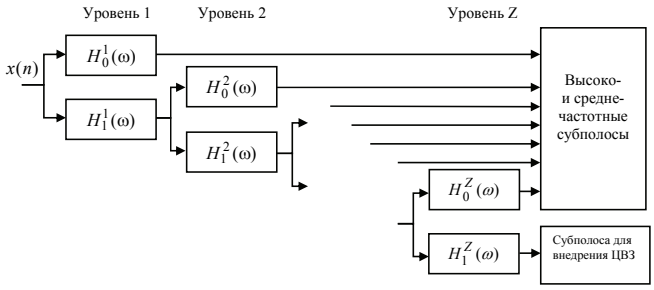


Рис. 6. Схема Z-уровневого ассиметричного банка фильтров анализа, построенного на вейвлет-фильтрах (КЗФ)

Для того чтобы внедрение не отразилось на качестве восприятия аудиосигнала, т.е. внедренный ЦВЗ был неслышим, следует избегать существенной модификации пиков амплитудного спектра субполосы. В декодере ЦВЗ сравниваются те же пары значений амплитуд. Если парная амплитуда меньше непарной – извлекается нулевой бит, если наоборот – единичный. Такой ЦВЗ сохранится в отсутствие преобразований аудиосигнала. Вместе с тем в силу воздействия ПАМ он может быть искажен сжатием с потерями качества.

Получить инвариант к сжатию возможно путем дублирования внедряемой информации, т.е. если рассматривать не пары значений амплитуд, а, например, пары троек значений. Тогда носителем одного бита ЦВЗ становится не две, а шесть амплитуд субполосы. Стеганокодеру при внедрении нуля необходимо обеспечить выполнение соотношений:

$$\left|X'(6r)+P\right| < \min\left(\left|X'(6r+3)\right|,\left|X'(6r+4)\right|,\left|X'(6r+5)\right|\right),$$

$$\left|X'(6r+1)+P\right|<\min\left(\left|X'(6r+3)\right|,\left|X'(6r+4)\right|,\left|X'(6r+5)\right|\right),$$

$$\left|X'(6r+2)+P\right|<\min\left(\left|X'(6r+3)\right|,\left|X'(6r+4)\right|,\left|X'(6r+5)\right|\right).$$

А при внедрении единицы:

$$\left|X'(6r+3)+P\right|<\min\left(\left|X'(6r)\right|,\left|X'(6r+1)\right|,\left|X'(6r+2)\right|\right),$$

$$\left|X'(6r+4)+P\right|<\min\left(\left|X'(6r)\right|,\left|X'(6r+1)\right|,\left|X'(6r+2)\right|\right),$$

$$\left|X'(6r+5)+P\right|<\min\left(\left|X'(6r)\right|,\left|X'(6r+1)\right|,\left|X'(6r+2)\right|\right).$$

При извлечении в декодере проверяется соотношение сумм амплитуд. Если

$$\left|X''(6r)\right|+\left|X''(6r+1)\right|+\left|X''(6r+2)\right|<$$
$$<\left|X''(6r+3)\right|+\left|X''(6r+4)\right|+\left|X''(6r+5)\right|,$$

то извлекается нулевой бит. А если

$$\left|X''(6r)\right|+\left|X''(6r+1)\right|+\left|X''(6r+2)\right|>$$
$$>\left|X''(6r+3)\right|+\left|X''(6r+4)\right|+\left|X''(6r+5)\right| -$$

извлекается единичный.

Механизм легального доступа к ЦВЗ

При эксплуатировании стеганосистем с ЦВЗ объектом информационного интереса может выступать как маркированный сигнал, так и водяной знак. Поэтому система должна предусматривать механизм легального доступа к ЦВЗ. Такой механизм обеспечивается путем введения в систему ключа, используемого в алгоритмах внедрения и извлечения ЦВЗ. Извлечение, выполненное с ключом, отличным от того, который использован при внедрении, приводит к невозможности восстановления ЦВЗ.

Для организации доступа к ЦВЗ по ключу перед внедрением спектр низкочастотной субполосы расширяют ключевой последовательностью, генерирующей как псевдослучайный набор битов, в котором все нули преобразовываются в –1. При прямом расширении спектра последовательность, состоящая из 1 и –1, умножается на входной сигнал. Так как 1*1 = 1 и $(1)*(-1)=1$, то исходный сигнал может быть восстановлен путем умножения расширенного сигнала на ту же псевдослучайную последовательность. Простой пример прямого и инверсного расширения ключом приведен на рис. 7.

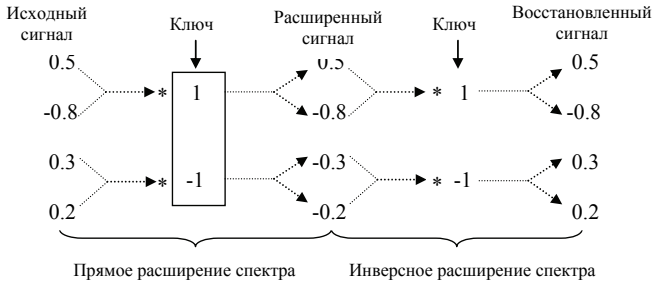


Рис. 7. Расширение спектра сигнала ключевой последовательностью

Оценка качества

Оценка стеганографического метода и алгоритма включает в себя оценку неощутимости, стойкости, пропускной способности и вычислительной сложности реализации.

Неощутимость ЦВЗ оценивается при помощи тестов на прослушивание, визуального анализа спектрограмм и сонограмм сигналов, а также определив отношение «сигнал/шум»:

$$SNR=10\cdot\log_{10}\left(\frac{\sum_{n=0}^{N-1}x^2(n)}{\sum_{n=0}^{N-1}\left[x'(n)-x(n)\right]^2}\right).$$

Численный показатель стойкости – коэффициент битовых ошибок (*BER – Bit error rate*) после типичных операций обработки и атак, представляющий собой процент корректно извлеченных битов ЦВЗ в сравнении с внедренными битами.

Пропускная способность или емкость – это количество битов ЦВЗ в сравнении с количеством битов данных исходного сигнала. При фиксированном количестве уровней разложения пропускная способность предложенного метода прямо пропорционально зависит от частоты дискретизации аудиосигнала и обратно пропорционально – от разрядности квантования. При добавлении каждого нового уровня разложения пропускная способность уменьшается в два раза.

Показателем качества так же является вычислительная сложность алгоритмов, реализующих метод, которая напрямую связана со скоростью работы системы. Вычислительная сложность зависит от выбранных базисных вейвле-

тов (их порядка), количества уровней разложения сигнала, алгоритма вычисления амплитудного спектра субполосы внедрения, формата представления численных значений и т.п.

Заключение. На основе разработанного метода в дальнейшем предполагается построение адаптивных алгоритмов внедрения ЦВЗ, учитывающих специфику реального применения, а также получение численных оценок качества стеганоалгоритмов в применении к аудиосигналам с различными параметрами и при сжатии разными кодеками с варьируемыми режимом/битрейтом.

1. *Грибунин В.Г.*, *Оков И.Н.*, *Туринцев И.В.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 261 с.
2. *Хорошко В.А.*, *Шелест М.Е.* Введение в компьютерную стеганографию. – К.: Національний авіаційний ун-т, 2002. – 152 с.
3. *Конахович Г.Ф.*, *Пузыренко А.Ю.* Компьютерная стеганография. – К.: МК-ПРЕСС, 2006. – 283 с.
4. *Pan D.A* Tutorial on MPEG/Audio Compression // IEEE Multimedia, – 1995. – **2**. – N. 2. – P. 60–74.
5. *Воробьев В.И.*, *Грибунин В.Г.* Теория и практика вейвлет-преобразования. – СПб.: Военный ун-т связи, 1999. – 203 с.
6. *Лукин А.* Введение в цифровую обработку сигналов (Математические основы). – М.: МГУ, Лаборатория компьютерной графики и мультимедиа, 2002. – 44 с.
7. *Алдошина И.А.* Основы психоакустики (цикл статей, Ч. 1–17) // Звукорежиссер, 1999–2002 гг. – http://rus.625-net.ru/audioproducer/1999

Поступила 30.03.2010

Тел. для справок: (044) 526-4569 (Киев)
E-mail:*k-n_v@ukr.net*

Окончание статьи В.Е. Мухина и др.

Таким образом, предложенная модель позволяет формально определить правила доступа субъектов к объектам РКС, описать угрозы безопасности РКС и определить принципы и условия безопасного администрирования РКС.

Заключение. Наличие научно-обоснованной и формализованной политики безопасности – обязательное условие комплексной защиты распределенных компьютерных систем.

Предложенный элемент политики безопасности – модель безопасного администрирования доступа субъектов к объектам РКС – позволяет формализовать важный компонент системы защиты информации. Для эффективного внедрения разработанной политики информационной безопасности на основе предложенной модели дополнительно выполняются следующие мероприятия: корректировка стратегии и основных положений политики безопасности на всех ее уровнях; постоянное совершенствование системы реагирования на инциденты; повышение эффективности методов и средств аудита информационной безопасности.

1. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей. – М.: ФОРУМ: ИНФРА–М, 2008. – 416 с.
2. *Barman S.* Writing Information Security Policies. – Boston: New Riders, 2002. – 342 p.
3. *Девянин П.Н.* Модели безопасности компьютерных систем. – М.: Академия, 2005. – 143 с.
4. *Галатенко В.А.* Основы информационной безопасности. – М.: УИТ, 2003. – 277 с.
5. *ISO*/*IEC* 27001:2005. «Information technology. Security techniques. Information security management systems. Requirements», 18 Oct. 2005. – 44 p.
6. *Peltier T.R.*. Information Security Policies. Procedures and Standards: Guideline for Effective Information Security Management. – Boca Raton: Auerbach Publ., 2002. – 176 p.
7. *Wood C.C.* Information Security Policies Made Easy. – Houston, Texas, USA: Pentasafe Security Technologies Inc., 2002. – 84 p.
8. *Application* of formal methods to the analysis of web-services security / L. Tobarra, D. Cazorle, F. Cuartero et al. // 2nd Intern. Workshop on Web Services and Formal Methods (WS-FM'05), Versailles, France, Sept. 2005. – P. 215–229.
9. *An Advisor* for Web Services Security Policies / K. Bhagavan, C. Fournet, A.D. Gordon et al. // Proc. of ACM Workshop on Secure Web Services (SWS'05), Fairfax, Virginia, USA, Nov. 2005. – P. 197–206.

Поступила 15.01.2010

Тел. для справок: (044) 406-8650 (Киев)
E-mail: *mukhin@comsys.ntu-kpi.kiev.ua*, *drang@ukr.net*