ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056

О МЕТОДЕ СКРЫТНОГО КОДИРОВАНИЯ КОНТРОЛЬНОЙ ИНФОРМАЦИИ В РЕЧЕВЫЕ ДАННЫЕ

Жиляков Е.Г. [1], Пашинцев В.П. [2], Белов С.П. [1], Лихолоб П.Г. [1]
[1]Белгородский государственный национальный исследовательский университет, Белгород, РФ
[2]Северо-Кавказский Федеральный университет, Ставрополь, РФ
E-mail: zhilyakov@bsu.edu.ru

В работе предложен метод скрытного кодирования контрольной информации в речевые данные, учитывающий распределение энергии частотных компонент на частотной оси. Использование для скрытного кодирование субполосных проекций вместо псевдослучайной последовательности, применяемой в методе расширения спектра, позволяет увеличить скрытность в 1012 раз, при уменьшении вероятности ошибки в 6 раз.

Ключевые слова: фрагмент речевого сигнала, речевые данные, распределение энергии, субполосный анализ/синтез, кодирование, стеганография, контрольная информация, метод расширения спектра, субполосная проекция, метод субполосной проекции.

Постановка задачи

Для человека представляется естественным осуществлять информационный обмен, используя устную речь и визуальное отображение предметов, явлений или процессов. Индустрия создания информационного, образовательного и развлекательного контента применяет устную речь для звукового сопровождения информационных справок, фильмов и музыкальных композиций. Это приводит к росту потоков информации, содержащей речь. В связи с этим возникает проблема обеспечения автоматического контроля за использованием речи, и в частности предотвращения несанкционированных действий с ней.

Иными словами, речь стоит рассматривать с двух позиций: не только как объект, в котором осуществляют скрытное кодирование, обеспечивающее хранение и передачу контрольной информации о контенте, но и как объект, который сам представляет собой контрольную информацию. Контрольная информация может представлять собой сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в цифровой форме.

Исходя из этого для обеспечения автоматического контроля речевых данных необходимо решение ряда задач: подтверждение идентичности полученной информации; идентификация личности; распознавание; определение целостности речи; защита речи от несанкционированного доступа; хранение, при котором невозможно обнаружить контрольную информацию, если не знать о ее существовании. Со многих точек зрения для речевых данных это целесообразно осуществлять в скрытном режиме, когда информация о процессах скрытного кодирования и соответствующих действиях доступна только определенному кругу лиц. Мера скрытности характеризует способность информации не быть обнаруженной в процессе информационного обмена.

Для решения задач, приведенных выше, можно воспользоваться принципом стеганографии, а в случаях аудиоданных – цифровой стеганографией, когда контент и информация контроля представляются в цифровой форме. В основе не очень широкого круга существующих алгоритмов стеганографии используются различные приемы кодирования контрольной информации, среди которых можно выделить: использование наименьшего значащего разряда [1], кодирование на основе расширения спектра [2-3] и некоторые другие.

Отметим, что развитие методов цифровой стеганогорафии направлено на повышение скрытности контрольной информации, выражаемое например через степень искажения, с сохранением стойкости кодирования внедряемой информации к внешним разрушающим воздействиями.

Авторами для решения указанной проблемы предлагается метод адаптивного скрытного кодирования контрольной информации, обеспечивающий при заданной вероятности ошибки высокую скрытность. Суть метода заключается в использовании энергетических свойств речевых данных, математической основой которого является применение в качестве ортогонального базиса собственных векторов субполосной матрицы [4] вме-

сто псевдослучайной последовательности (ПСП), широко применяемой в настоящее время при скрытном кодирования контрольной инфомации.

Математические основы

Пусть $\vec{x} = (x_1, x_2, \ldots, x_n, \ldots, x_N)^T$ – отрезок речевых данных, являющийся цифровым представлением фрагмента устной речи, зафиксированной в дискретные моменты времени на выходе микрофона. На рисунке 1 представлена огибающая отрезка речевых данных, порожденных звуком «о», в количестве $N = 256$ отчетов, взятых с частотой дискретизации $f_д$ = 8 кГц.

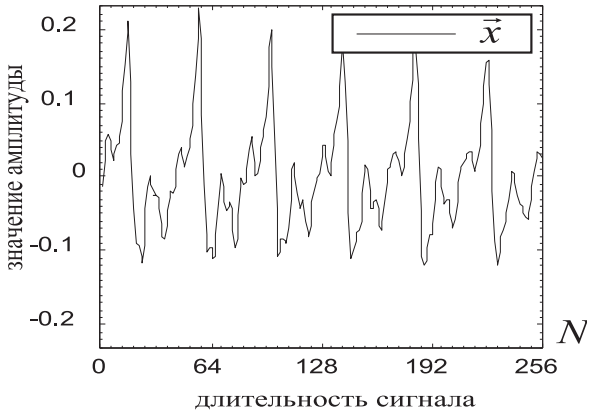

Рис. 1. Отрезок речевых данных, порожденных звуком «о»

Известно, что у большинства звуков русской речи энергия частотных компонент содержится в малой доле частотной полосы [5]. Это энергетическое свойство можно положить в основу модели восприятия речи человеком. Отметим, что процедуры анализа и синтеза сигналов в соответствии с некоторым разбиением области частот (см. рис. 2) на совокупность интервалов принято называть субполосными.

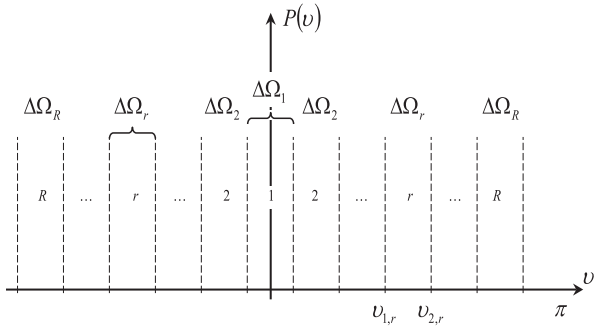

Рис. 2. Разбиение частотной полосы

Характеристику, оценивающую часть энергии $P_r(\vec{x})$, сосредоточенной в частотной субполосе $\Delta\Omega_r$ (рис. 2) возможно определить из соотношения [4]:

$$P_r(\vec{x}) = \int_{\upsilon \in \Delta\Omega_r} |X(\upsilon)|^2 d\upsilon \Big/ 2\pi , \qquad (1)$$

где P_r – приходящаяся на частотную полосу часть энергии отрезка речевых данных; r – индекс, обозначающий порядковый номер частотной субполосы из R возможных; $X(\upsilon)$ – трансформанта Фурье:

$$X(\upsilon) = \sum_{n=1}^{N/2} x_n e^{-j\cdot\upsilon\cdot(n-1)} , \qquad (2)$$

где x_n – отсчеты анализируемого отрезка речевых данных; N – длительность отрезка речевых данных. В качестве инструмента, позволяющего производить вычисления энергии, не переходя в частотную область, предлагается использовать математический аппарат субполосных матриц [4; 6]:

$$P_r(\vec{x}\ ) = \vec{x}^T A_r \vec{x}\ , \qquad (3)$$

где A_r – субполосная матрица, определяемая элементами:

$$A_r = \{a_{i,k}(r)\},\ i,k = 1,\ldots,N ; \qquad (4)$$

$$a_{ik}^r = \frac{\sin(\upsilon_{2,r}(i-k)) - \sin(\upsilon_{1,r}(i-k))}{\pi(i-k)},\ \ i \neq k ; \qquad (5)$$

$$a_{i,k}^r = (\upsilon_{2,r} - \upsilon_{1,r})/\pi ,\ \ i = k , \qquad (6)$$

где i – позиция элемента в строке матрицы; k – позиция элемента в столбце матрицы; υ_{1r} – левая граница субполосы $\Delta\Omega_r$; υ_{2r} – правая граница субполосы $\Delta\Omega_r$.

Исследования показали, что речевые данные, порожденные устной речью, – это цифровое представление нестационарного, сложномодулированного сигнала, порождаемого последовательностью звуков языка или их отсутствием. В ходе экспериментов было выявлено, что с течением времени у речевых данных не только изменяются временное представление, но и распределение энергии по частотной полосе. При этом существуют моменты, когда соотношение долей энергии, содержащейся в частотной полосе, практически не изменяется.

Эта закономерность выполняется, если отрезки речевых данных получены в одних и тех же условиях: для одного и того же звука при длительности отрезков анализа до 20 мс; для фрагмента, где речевой сигнал стационарен; при одинаковом

разбиении полосы частот (см. рис. 2). Эти свойства изменения частотного распределения энергии необходимо учитывать при скрытном кодировании контрольной информации в отрезках речевых данных.

Оптимальными, с позиции учета свойств речевых данных, являются решающие правила с адаптивным определением порога по энергии отрезка данных и учитывающие распределение энергии по частотной полосе. Для определения частотной субполосы $\Delta\Omega_r$ в которой можно осуществить скрытное кодирование, предлагается решающее правило (7), зависящее от энергии анализируемого отрезка и от распределения энергии по частотной полосе:

$$\left| \frac{\Delta\Omega_r}{\pi} \cdot \left\| \vec{x} \right\|^2 - \frac{1}{2\pi} \int\limits_{\upsilon \in \Delta\Omega_r} \left| X\left(\upsilon\right) \right|^2 d\upsilon \right| = \min\limits_{\Delta\Omega_r \in [0,\pi]}, \quad (7)$$

где $\left\| \vec{x} \right\|^2$ – энергия отрезка речевых данных.

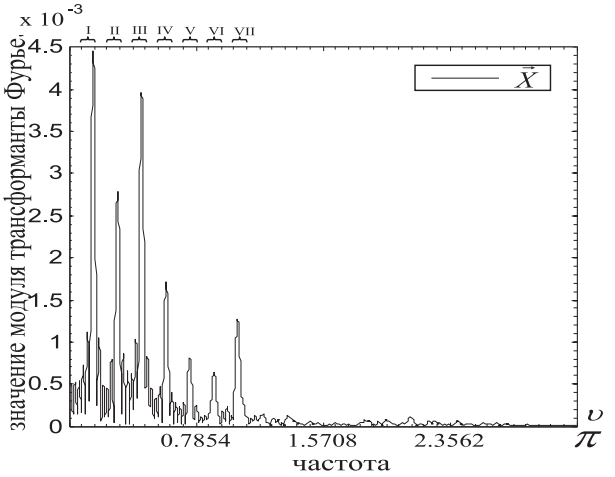

Рис. 3. Спектр отрезка речевых данных, порожденных звуком «о»

В равенстве (7) предлагается использовать близость энергии субполосы к среднему значению, приходящейся на частотную полосу отрезка данных. Также стоит отметить, что доля энергии любого из отрезков, принадлежащего звуку русской речи, сосредоточена в изменяющейся от звука к звуку малой части частотной полосы. На рис. 3 представлена огибающая спектра, являющаяся результатом оценки трансформант Фурье отрезка данных (см. рис. 1).

Анализ рис. 3 показывает, что трансформанты Фурье с большей энергией сосредоточены в частотной полосе $\Delta\Omega_r \in \left(0, 3\pi/8\right]$, при этом распределение энергии трансформант Фурье неоднородно. В данном диапазоне присутствуют узкие субполосы (см. рис. 3, полосы I-VII), энергия которых превышает среднее значение энергии, приходящееся на частотный интервал).

Следовательно, для синтеза в малой части частотной полосы необходимо использовать сигнал, обладающий высокой частотной концентрацией. Для решения этой задачи воспользуемся собственными векторами субполосной матрицы, соответствующими единичным собственным числам. Субполосная матрица A_r симметрична и положительно определенна, поэтому для нее можно найти N собственных векторов и соответствующих им собственных чисел [4]:

$$\lambda_k^r \vec{q}_k^{\,r} = A_r \vec{q}_k^{\,r}, \;\; i,k = 1,\ldots,N, \quad (8)$$

также справедливо

$$A_r = \sum_{i=1}^{N} \lambda_i(r) \cdot \vec{q}_i(r) \vec{q}_i^{\,T}(r) \;\; i,k = 1,\ldots,N, \quad (9)$$

где $q_{k,i} - k$-ый элемент собственного вектора $\vec{q}_i$ субполосной матрицы A_r; λ_i – собственное число, соответствующее $\vec{q}_i$ собственному вектору субполосной матрицы, принимающее значение: $0 < \lambda_i \le 1$. Использование собственных векторов, энергия которых сконцентрирована в заданной частотной полосе, позволяет повысить избирательность в частотной области при реализации задач анализа/синтеза. Для обеспечения избирательности целесообразно использовать собственные вектора, собственные числа которых близки к единице ($\lambda_J \cong \ldots \cong \lambda_2 \cong \lambda_1 \approx 1$).

Свойство соответствия собственных чисел собственным векторам как критерия, применяемого при отборе векторов, обладающих заданной концентрацией энергии, вытекает из следствия равенства Парсеваля (1). Следствие определяет пропорциональность доли энергии собственного вектора значению собственного числа ему соответствующего. Спектр одного из множества векторов, собственное число которого близко к единице, приведен на рис. 4.

Заметим, что количество собственных чисел близких к единице зависит от ширины субполосы (6), то есть от способа разбиения частотной оси (10). Для реализации метода скрытного кодирования предлагается использовать разбиение вида

$$\Delta\Omega_r = 2\Delta\Omega_1; \;\; r = 2; 3 \;\ldots R; \qquad \Delta\Omega_1 = \pi/\left(2\left(R-1\right)+1\right); \;\; R = \left(N-2\right)/4. \quad (10)$$

Следует также отметить, что для разбиения (10) во всех частотных субполосах имеется пара собственных векторов субполосной матрицы, собственные числа которых близки к единице.

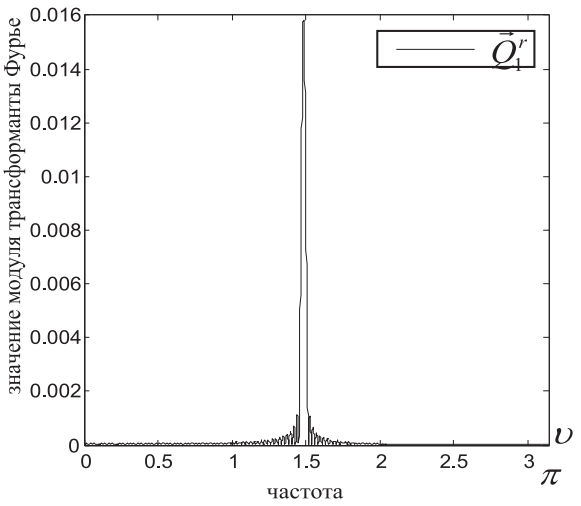

Рис. 4. Спектр собственного вектора $\vec{q}_1^r$ субполосной матрицы A_r, в области трансформант Фурье

К еще одному важному свойству собственных векторов субполосной матрицы, найденных для одной субполосы, можно отнести условие ортонормальности:

$$\left\langle \vec{q}_l^r, \vec{q}_k^r \right\rangle = \begin{cases} 1, & l = k \\ 0, & l \neq k \end{cases} \quad l,k = 1,\ldots,N\,. \quad (11)$$

Это свойство позволяет решить еще одну важную проблему анализа речевых сигналов, а именно: оценить вклад энергии вектора в отрезок данных. Такую операцию естественно называть частотной фильтрацией, а значение скалярного произведения собственного вектора на отрезок данных – субполосной проекцией:

$$\alpha_i^r = \left\langle \vec{q}_i^r, \vec{x} \right\rangle \; i = 1,\ldots,N\,. \quad (12)$$

Субполосную проекцию можно использовать в задачах анализа и синтеза.

Метод расширения спектра. К методам, обладающим высокой скрытностью и устойчивостью к воздействию шума, можно отнести кодирование на основе расширения спектра модулированным гармоническим сигналом [2-3]:

$$\tilde{\vec{x}} = \vec{x} + K_{\text{m}} \cdot e_m \cdot \vec{c}\,, \; m \in M\,; \quad (13)$$

$$e_m = 2b_m - 1, \; m \in M\,, \quad (14)$$

где $\tilde{\vec{x}}$ – отрезок речевых данных с закодированной информацией; K_{m} – коэффициент пропорциональности; e_m – кодируемый символ контрольной информации; b_m – бит контрольной информации; M – объем контрольной информации в битах; $\vec{c}$ – псевдослучайная последовательность, модулируемая гармоническим сигналом:

$$\vec{c} = \vec{u} \cdot \vec{g}\,, \; g_n = \cos\left(n \cdot \omega_r\right), \; n = 1,2,\ldots,N\,, \quad (15)$$

где $\vec{u}$ – псевдослучайная последовательность (ПСП), описываемая нормальным законом распределения $\vec{u} \in \{-1,1\}$; $\vec{g}$ – отрезок данных, соответствующий гармоническому сигналу с центральной частотой $\omega_r \in (0,\pi)$.

Коэффициент пропорциональности, определяющий скрытность контрольной информации и учитывающий энергию шума, в работах [2-3] рекомендовано выбирать как

$$K_m = \left\langle \vec{x}, \vec{c} \right\rangle \Big/ \left\| \vec{c} \right\|^2\,. \quad (16)$$

Декодирование контрольной информации методом расширения спектра осуществляется путем определения знаков проекций для отрезка данных и сохраненного отрезка модулированной случайной последовательности [6-7]:

$$\tilde{e}_m = sign\left(\left\langle \tilde{\vec{x}}, \vec{c} \right\rangle\right); \quad \tilde{b}_m = \left(\tilde{e}_m + 1\right)/2\,, \quad (17)$$

где $\tilde{e}_m$ – символ, декодируемый методом расширения спектра информации; $\tilde{b}_m$ – бит, декодируемый методом расширения спектра.

Основным недостатком метода расширения спектра является вероятность ошибки, возникающей при декодировании бит контрольной информации. Как будет показано далее, вероятность ошибки $P_{ош}$ на бит (BER) может достигать 0,3. Появление такой высокой вероятности ошибки вызвано корреляцией отрезка речевых данных с ПСП. Одним из способов уменьшения вероятности ошибки является использование модуляции гармонического сигнала ПСП для формирования сигнально-кодовой конструкции (СКК). Модуляция частично концентрирует энергию относительно центральной частоты ω_r. Но использование модуляции не позволяет полность сконцентрировать всю энергию ПСП в заданной полосе частот (см. рис. 5), что все равно приводит к изменению отрезка речевых данных во всей частотной области.

Также к недостатку метода можно отнести необходимость хранения ПСП, которая отвечает за передаваемый символ, или правила, по которому ПСП будет сформирована, а также хранение центральной частоты ω_r.

Метод субполосных проекций. Исходя из приведенных выше соотношений (3)-(8) предлагается модель, осуществляющая скрытное кодирова-

ние бит контрольной информации b_m в отрезок речевых данных $\vec{x}$:

$$\hat{\vec{x}} = \vec{x} + \sum_{j=1}^{J} \left(sign(e_m) \cdot \left| \alpha_j^r \right| - \alpha_j^r \right) \cdot \vec{q}_j^r ; \quad e_m = 2b_m - 1, \; m \in M , \tag{18}$$

где $sign(\cdot)$ – операция выделения знака; J – количество собственных векторов, собственные числа которых близки к единице.

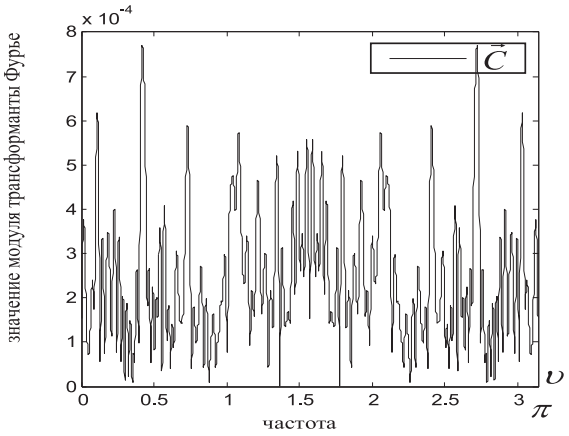

Рис. 5. Спектр СКК в области трансформант Фурье для метода расширения спектра

Декодирование контрольной информации осуществляется путем определения знаков проекций α_i^r для собственных векторов $\vec{q}_i^r$ субполосной матрицы A_r, найденных для пространства $r \in \mathbf{R}_1$:

$$\hat{e}_m = sign\left(\left\langle \hat{\vec{x}}, \vec{q}_i^r \right\rangle \right), \; m \in M ; \quad \hat{b}_m = \left(\hat{e}_m + 1 \right) / 2 , \tag{19}$$

где $\hat{e}_m$ – символ, декодируемый методом субполосных проекций; $\hat{b}_m$ – бит, декодируемый методом субполосных проекций.

Кодирование, осуществляемое путем изменения знака субполосной проекции, позволяет использовать для скрытного кодирования энергетические свойства отрезка речевых данных. Использование субполосных проекций, полученных для векторов, собственные числа которых близки к единице, минимизирует их влияние на частотную полосу в тех местах, где скрытное кодирование не осуществляется.

Результаты компьютерного моделирования

Исходные данные. Компьютерное моделирование метода субполосных проекций и метода расширения спектра реализовывалось в системе Matlab. Для этого была сформирована следующая база:

- для формирования контрольной информации генерировалась бинарная случайная последовательность b_m, содержащая 10^6 элементов с одинаковым количеством нулевых и единичных бит [7]. Из полученной бинарной последовательности формировались символы e_m (14);
- была сформирована база отрезков речевых данных, соответствующая буквам русского языка, обладающая характеристиками: количество значений N = 256; разрядностью B = 16; частотой дискретизации f_∂ = 8 кГц; всего количество тестовых отрезков речевых данных составило $Z = 6400$;
- при помощи генератора Фибоначчи [7] была сформирована ПСП ($\vec{u} \in \{0,1\}$), применяемая в методе расширения спектра. Последовательность разделена на 10^6 некоррелированных отрезков длиной в N = 256 значений;
- в качестве модели шума используется белый гауссов шум, энергия которого равномерно распределена в частотной области с нулевым математическим ожиданием. Последовательность разделена на 10^6 некоррелированных отрезков длиной в N = 256 значений.

Оценка скрытности. Для оценки скрытности δ контрольной информации, закодированной в отрезке речевых данных, использовалось выражение

$$\delta = \sqrt{\frac{1}{Z} \sum_{z=1}^{Z} \left(\left\| \vec{x} \right\| - \left\| \hat{\vec{x}} \right\| \right)^2 \Big/ \left\| \vec{x} \right\|^2} , \tag{20}$$

где $\boldsymbol{Z}$ – число проанализированных отрезков речевых данных. Моделирование осуществлялось следующим образом:

- согласно разбиению частотной оси (10) анализировался каждый отрезок данных с целью выбора субполосы $\Delta\Omega_r$, удовлетворяющей решающему правилу (7);
- осуществлялось скрытное кодирование в субполосе $\Delta\Omega_r$ символа e_m методом субполосных проекций (20);
- оценивалась энергия, вносимая методом субполосных проекций при кодировании символа e_m:

$$K_m = \sqrt{(\alpha_m)^2} , \tag{21}$$

- оценивалась скрытность метода субполосных проекций (20);
- осуществлялось скрытное кодирование на центральной частоте субполосы $\Delta\Omega_r$ символа

e_m методом расширения спектра (13), с коэффициентом пропорциональности (21);

- оценивалась скрытность метода расширения спектра (20).

Степень искажения контролируемой информации (отрезка речевых данных), усредненная для каждого звука, соответствующего букве русского алфавита, сведена в таблицу 1.

Моделирование показало, что у метода расширения спектра степень искажения достигает $7{,}1\cdot10^{-3}$, а для метода субполосной проекции данный параметр не превышает $2{,}69\cdot10^{-16}$. Иными словами, при использовании метода субполосных проекций изменения в энергии речевых данных практически равны нулю. Таким образом, для уменьшения степени искажения контролируемой информации для скрытного кодирования целесообразно использовать метод субполосных проекций.

Оценка стойкости контрольной информации к воздействию шума. Значение вероятности ошибки $P_{ош}$ на бит (BER) вычислялось согласно выражению:

$$P_{ош} = M_{ош}/M\,, \qquad (22)$$

где $M_{ош}$ – количество ошибочно принятых бит из всего объема контрольной информации; M – объем контрольной информации. Оценивалась ошибка, возникающая в результате воздействия шума:

$$\vec{y} = \hat{\vec{x}} + \sqrt{h_0^2}\cdot\vec{u}\,, \qquad (23)$$

где: h_0 – соотношение «шум/сигнал» в разах; $\hat{\vec{x}}$ – отрезок речевых данных, содержащий контрольную информацию; $\vec{y}$ – отрезок речевых данных, содержащий контрольную информацию, после воздействия шума.

Стоит отметить, что в качестве модели использовался белый гауссов шум, энергия которого равномерно распределена в частотной области с нулевым математическим ожиданием. Для каждого соотношения «шум/сигнал» h_0^2 осуществлялось усреднение результатов по каждой букве. Также в ходе моделирования проводилась проверка, направленная на то, чтобы шум, применяемый в методе расширения спектра, максимально отличался (имел корреляцию близкую к нулю) от шума, участвующего в оценке стойкости.

Результаты компьютерного моделирования, представленные в виде кривых помехоустойчивости (см. рис. 6) с номерами I (метод расширения спектра) и II (метод субполосных проекций), показывают вероятности ошибок на бит при различных соотношениях «шум/сигнал».

Таблица 1. Степень искажения контролируемой информации

Буква	δ	
	метод субполосных проекций	метод расширения спектра
1	2	3
а	$1{,}91\cdot10^{-16}$	$3{,}0\cdot10^{-3}$
б	$1{,}85\cdot10^{-16}$	$2{,}8\cdot10^{-3}$
в	$1{,}97\cdot10^{-16}$	$1{,}9\cdot10^{-3}$
г	$1{,}69\cdot10^{-16}$	$1{,}8\cdot10^{-3}$
д	$2{,}08\cdot10^{-16}$	$2{,}4\cdot10^{-3}$
е	$2{,}11\cdot10^{-16}$	$2{,}2\cdot10^{-3}$
ж	$2{,}36\cdot10^{-16}$	$5{,}0\cdot10^{-3}$
з	$2{,}34\cdot10^{-16}$	$3{,}0\cdot10^{-3}$
и	$1{,}94\cdot10^{-16}$	$1{,}9\cdot10^{-3}$
й	$1{,}55\cdot10^{-16}$	$1{,}9\cdot10^{-3}$
к	$2{,}69\cdot10^{-16}$	$7{,}1\cdot10^{-3}$
л	$1{,}35\cdot10^{-16}$	$2{,}0\cdot10^{-3}$
м	$1{,}76\cdot10^{-16}$	$2{,}3\cdot10^{-3}$
н	$1{,}65\cdot10^{-16}$	$1{,}8\cdot10^{-3}$
о	$1{,}81\cdot10^{-16}$	$3{,}2\cdot10^{-3}$
п	$1{,}24\cdot10^{-16}$	$4{,}2\cdot10^{-3}$
р	$1{,}70\cdot10^{-16}$	$4{,}9\cdot10^{-3}$
с	$1{,}80\cdot10^{-16}$	$5{,}6\cdot10^{-3}$
т	$1{,}94\cdot10^{-16}$	$6{,}0\cdot10^{-3}$
у	$1{,}85\cdot10^{-16}$	$2{,}1\cdot10^{-3}$
ф	$2{,}28\cdot10^{-16}$	$6{,}6\cdot10^{-3}$
х	$1{,}22\cdot10^{-16}$	$5{,}6\cdot10^{-3}$
ц	$2{,}48\cdot10^{-16}$	$5{,}4\cdot10^{-3}$
ч	$1{,}98\cdot10^{-16}$	$5{,}7\cdot10^{-3}$
ш	$1{,}97\cdot10^{-16}$	$4{,}3\cdot10^{-3}$
щ	$2{,}04\cdot10^{-16}$	$6{,}9\cdot10^{-3}$
ы	$1{,}31\cdot10^{-16}$	$2{,}5\cdot10^{-3}$
э	$2{,}05\cdot10^{-16}$	$2{,}0\cdot10^{-3}$
ю	≈ 0	$4{,}7\cdot10^{-3}$
я	$2{,}41\cdot10^{-16}$	$2{,}5\cdot10^{-3}$
Среднее значение	$1{,}78\cdot10^{-16}$	$3{,}8\cdot10^{-3}$

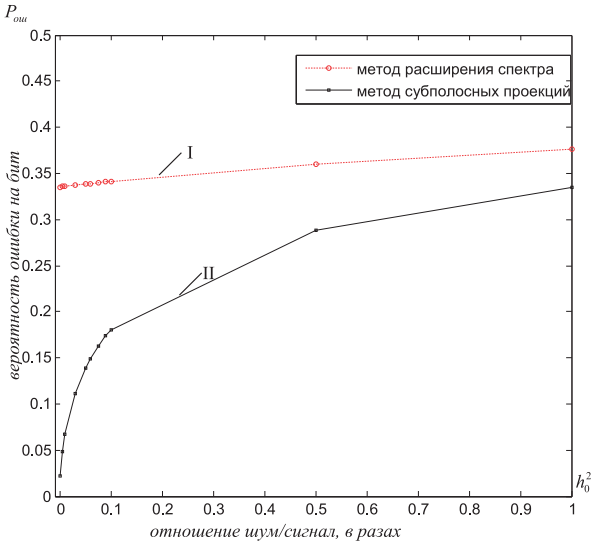

Рис. 6. Графики зависимостей вероятности ошибки на бит (BER) от отношения «шум/сигнал» для метода расширения спектра и метода субполосных проекций

Численные результаты оценки появления ошибочного бита при декодировании контрольной информации в условии воздействия шума представлены в таблице 2.

В результате вычислительных экспериментов удалось установить, что контрольная информация, закодированная предлагаемым метод субполосных проекций, обладает в 18 раз большей стойкостью по сравнению с методом расширения спектра при наиболее распространенном воздействии шума с соотношении «шум/сигнал» 0,001.

Исследования частично финансировались в рамках грантов РФФИ №15-07-01463 и №15-07-01570

Таблица 2. Значения вероятности ошибки $P_{ош}$

Характеристика	Вероятность ошибки $P_{ош}$	
Отношение «шум/сигнал», h_0^2	метода расширения спектра	метод субполосных проекций
1	2	3
0,0010	0,370828	0,021937
0,0100	0,370966	0,067710
0,1000	0,374175	0,180317
1,0000	0,394746	0,334562

Выводы

В результате проведенных исследований установлено, что предлагаемый метод субполосных проекций обладает высоким уровнем скрытности контрольной информации по сравнению с методом расширения спектра, так как вызывает меньшие изменения в доле энергии отрезка речевых данных. Минимизация изменения в энергии той части полосы, где кодирование не осуществлялось, достигается за счет использования субполосных проекций, найденных для собственных векторов, собственные числа которых близки к единице. В предложенном методе изменения энергии близки к нулю, в методе расширения спектра не превышают 1%. Сравнение проводилось при учете равенства энергии добавляемых сигналов (энергии их проекций).

Метод субполосных проекций обладает на порядок меньшей вероятностью ошибки декодирования контрольной информации. Этот показатель достигается за счет скрытного кодирования контрольной информации в узкой полосе, а следовательно, и воздействие шума с равномерным распределением в частотной области меньше. Стоит отметить, что энергия шума с равномерным распределением, воздействующая на СКК в методе субполосных проекций, обратно пропорциональна ширине субполосы. Иными словами: чем уже субполоса, тем меньшая энергия шума оказывает влияние на СКК. Также важно для повышения помехоустойчивости отбирать для скрытного кодирования СКК, обладающие большей энергией.

Исследования показали, что применение субполосных проекций для скрытного кодирования контрольной информации позволяет обеспечить высокую скрытность при небольшой вероятности ошибки, возникающей в результате воздействия шума. Также отличительным свойством метода является безошибочное декодирование контрольной информации, в случае если речевые данные не подвергались изменению.

Литература

1. Алексеев А.П., Аленин А.А. Скрытая передача данных в звуковых файлах формата WAV // ИКТ. Т.8, №3, 2010. – С.101-106.
2. Vercoe B.L. Csound: A Manual for the Audio-Processing System. MIT Media Lab, Cambridge 1995.
3. Dutoit T., Marques F. Applied Signal Processing A MATLAB TM-Based Proof of Concept 2009.
4. Жиляков Е.Г. Вариационные метода анализа и построения функций по эмпирическим данным. Белгород: Изд-во БелГУ, 2007.
5. Жиляков Е. Г., Девицина С.Н., Лихолоб П.Г. Определение возможного объема внедряемой информации при скрытой передаче меток в речевых данных // Научные ведомости БелГУ.

Серия «Информатика». Вып. 23/1, №13 (132), 2012. – С. 222-227.
6. Жиляков Е.Г. Белов С.П., Черноморец А.А. Вариационные методы анализа сигналов на основе частотных представлений // Вопросы радиоэлектроники. Серия ЭВТ. Вып. 1, 2010. – С. 10-26.
7. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей // Вопросы радиоэлектроники. Серия ЭВТ. Вып. 1, 2003. – 240 с.

Получено 20.05.2015

Жиляков Евгений Георгиевич, д.т.н., профессор, заведующий Кафедрой информационно-телекоммуникационных систем и технологий (ИТСТ) Белгородского государственного национального исследовательского университета (НИУ «БелГУ»). Тел. (8-472) 230-13-92. E-mail: zhilyakov@bsu.edu.ru

Пашинцев Владимир Петрович, д.т.н., профессор Кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. Тел. 8-918-741-33-16. E-mail: pashintsevp@mail.ru

Белов Сергей Павлович, д.т.н, профессор Кафедры ИТСТ НИУ «БелГУ». Тел. 8-980-323-61-04. E-mail: belov@bsu.edu.ru

Лихолоб Петр Георгиевич, ассистент Кафедры ИТСТ НИУ «БелГУ». E-mail: likho-lob@bsu.edu.ru.

ABOUT THE METHOD FOR HIDDEN CODING OF CONTROL INFORMATION TO SPEECH DATA

Zhilyakov E.G. [1], Pashintsev V.P. [2], Belov S.P. [1], Likholob P.G. [1]
[1]Belgorod State National Research University, Belgorod, Russian Federation
[2]North Caucasus Federal University, Stavropol, Russian Federation
E-mail: zhilyakov@bsu.edu.ru

Currently, the industry's creation of information, educational and entertainment content for audio information inquiries, movies and music are widely used spoken language. In this connection there is the problem of providing automatic control of the use of speech and in particular to prevent unauthorized actions with it. In many ways, this control is advantageously carried out in a secretive mode, where information about the processes of encoding and appropriate action avail-able only to a specific group of persons. The authors have to solve this problem, we propose a method of adaptive hidden coding control information, providing for a given error probability of high secrecy. The method is to use the power properties of the voice data, the mathematical basis is used as an orthogonal basis of eigenvectors sub-band matrix instead of a pseudo-random sequence (PRS), which is widely used at present in the hidden coding control information. The studies found that the proposed method of sub-band projections has a higher level of secrecy of information control over the method of spreading since it causes less change in the proportion of the energy of speech segment data. Minimizing variations in energy band of the portion where the coding is not carried out, it is achieved through the use of sub-band projections found for sub-band matrix of eigenvectors whose eigenvalues are close to unity.

Keywords: fragment of speech signal, speech data, energy distribution, sub-band analysis/synthesis, encoding, steganography, control information, method for spectrum spreading, sub-band projection, method of sub-band projection

DOI: 10.18469/ikt.2015.13.3.14

Zhilyakov Evgeny Georgiyevich, Doctor of Technical Science, Professor, the Head of Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russian Federation. Tel.: +74722301392. E-mail: zhilyakov@bsu.edu.ru

Pashintsev Vladimir Petrovich, Doctor of Technical Science, Professor, Professor of the Department of Information Security Automated Systems, North Caucasus Federal University, Stavropol, Russian Federation. Tel.: +79187413316. E-mail: pashintsevp@mail.ru

Belov Sergey Pavlovich, Doctor of Technical Science, Professor, Professor of the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Re-search University, Belgorod, Russian Federation. Tel.: +79803236104. E-mail: belov@bsu.edu.ru

Likholob Petr Georgiyevich, Assistant of the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russian Federation. E-mail: likholob@bsu.edu.ru

References

1. Alekseev A.P., Alenin A.A. Skrytaja peredacha dannyh v zvukovyh failah formata WAV [Hidden data transmission a sound file to wav format]. *Infokommunikacionnye tehnologii*, 2010, vol. 8, no. 3, pp.101-106.
2. Vercoe B.L. *Csound: A Manual for the Audio-Processing System*. MIT Media Lab, Cambridge, 1995.
3. Dutoit T., Marques F. *Applied Signal Processing A MATLAB TM-Based Proof of Concept*, Springer, 2009. 456 p.
4. Zhiljakov E.G. *Variacionnye metody analiza i postroenija funkcii po yempiricheskim dannym* [Variational methods of analysis and features from empirical data]. Belgorod, BelGU Publ., 2007. 160 p.
5. Zhiljakov E. G., Devicina C.N., Liholob P.G. Opredelenie vozmozhnogo ob''ema vnedrjaemoi informacii pri skrytoi peredache metok v rechevyh dannyh [Definition possible volume introduces information in secure communication tags in voice data]. *Nauchnye vedomosti BelGU. Serija «Informatika»,* 2012, no. 13, pp. 222-227.
6. Zhiljakov E.G. Belov S.P., Chernomorec A.A. Variacionnye metody analiza signalov na osnove chastotnyh predstavlenii [Variational methods of signal analysis based on frequency representation]. *Voprosy radioyelektroniki. Serija YeVT*, 2010, no. 1, pp. 10-26.
7. Ivanov M.A., CHugunkov I.V. Teorija, primenenie i ocenka kachestva generatorov psevdosluchainyh posledovatel'nostei [Theory, application and evaluation of the quality of pseudorandom sequence generator]. *Voprosy radioyelektroniki. Serija YeVT*, 2003, no. 1.

Received 20.05.2015

УДК 004.056

ТРЕБОВАНИЯ К УЧЕБНОЙ ЛИТЕРАТУРЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Алексеев А.П., Макаров М.И., Орлов В.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: apa_ivt@rambler.ru

Описываются требования к учебной литературе по криптографии и стеганографии, а также принципы построения современных систем защиты информации. Изучение методов защиты информации должно происходить путем решения большого числа практических задач. Описывается метод скрытого распределения информации по множеству каналов телекоммуникационной сети, причем в каждом канале используется оригинальный алгоритм защиты информации. Рассматривается метод сетевой стеганографии, заключающийся в сокрытии информации в значении длины сетевых пакетов.

Ключевые слова: криптография, стеганография, контейнеры, пространственно-временное распыление.

Введение

Число публикаций, посвященных криптографии и стеганографии, растет экспоненциально. По криптографии издано большое число учебников, задачников, пособий для проведения лабораторных работ и практических занятий [1-2; 12-13], а также проводятся онлайн курсы [10-11]. Применительно к стеганографии заметен дефицит учебной литературы, содержащей описание лабораторных работ и практических задач. Компенсировать это пробел пытаются преподаватели и ученые в различных высших учебных заведениях, в том числе России и Болгарии. В России такими работами являются [3-5], а в Болгарии - книги, написанные профессором С. Станевым и его учениками [6; 14-15].

Требования к учебной литературе

Авторы придерживаются мнения, что современная учебная литература по защите информа-