УДК 621.396.01

О ПРИМЕНЕНИИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ АУТЕНТИФИКАЦИИ СИГНАЛОВ, СОДЕРЖАЩИХ РЕЧЕВОЕ СООБЩЕНИЕ

ABOUT THE APPLICATION OF STEGANOGRAPHIC METHODS FOR AUTHENTICATION OF SIGNALS CONTAINING VOICE MESSAGE

Е.Г. Жиляков, П.Г. Лихолоб, Я.В. Цыбина, Е.С. Лихогодина
E.G. Zhilyakov, P.G. Likholob, Ya.V. Cybina, E.S. Likhologodina

Белгородский государственный национальный исследовательский университет,
Россия, 308015, Белгород, ул. Победы, 85

Belgorod State National Research University, 85 Pobeda St, Belgorod, 308015, Russia

e-mail: Zhilyakov@bsu.edu.ru, Likholob@bsu.edu.ru, BakaJana@rambler.ru

Аннотация
В статье приведена обобщенная аддитивная модель стеганографического кодирования дополнительной информации и способ её декодирования. Описаны параметры кодирования, влияющие на обеспечение скрытности и достоверности декодирования информации. Рассмотрено применение стеганографической аддитивной модели кодирования для методов расширения спектра (SSp), дискретно-косинусной трансформации (DCT), оптимального субполосного внедрения (SubBand). При помощи результатов экспериментов показана зависимость скрытности кодируемой информации и достоверность её декодирования от выбора сигнально-кодовой конструкции (ССК). Даны рекомендации, описывающие возможность применения стеганографических алгоритмов для аутентификации сигналов, содержащих речевое сообщение.

Abstract
The article presents a generalized additive model of steganographic encoding of additional information and its method of decoding. The encoding options that effect on the providing of secrecy and the reliability of the decoding information is described. The use of additive steganography model of the encoding techniques spread spectrum (SSp), discrete-cosine transformation (DCT), optimal subband implementation (Subband) is considered. Using the results of the experiments shows the dependence of secrecy of the encoded information and the reliability of its decoding from a selection of signal-code constructions (SCC). Given recommendations, describes the possibility of applying steganographic algorithms for authentication signal that contains a voice message.

Ключевые слова: речь, кодирование, стеганография, метод расширения спектра, дискретно-косинусная трансформация, оптимальный субполосный метод, скрытность, достоверность, корреляция, среднеквадратическое отклонение, вероятность ошибки.
Keywords: speech, encoding, steganography, spread-spectrum method, discrete-cosine transformation, optimal subband implementation, secrecy, reliability, correlation, the standard deviation, the probability of error.

Введение

В настоящее время наблюдается интенсификация потоков, связанных с информационным обменом. Так как устная речь является одной из наиболее естественных для человека форм информационного обмена, то следует ожидать дальнейшего возрастания объемов хранимых и передаваемых речевых сообщений. В связи с этим возникает проблема обеспечения контроля за их использованием, и, в частности, обнаружение несанкционированных действий с речевыми сообщениями.

Под речевыми сообщениями в работе будем понимать фрагменты речевого сигнала, которые представляют собой результаты регистрации в дискретные моменты времени колебаний электрического тока на выходе микрофона $\vec{x}$ [Zhilyakov E.G., 2015].

Со многих точек зрения контроль за использованием информационных потоков речевых данных целесообразно осуществлять в скрытном режиме, когда информация об этих процессах и соответствующих действиях доступна только определенному кругу лиц.

Иными словами, целесообразно воспользоваться принципом стеганографии, а в случае аудиоданных – цифровой стеганографией, когда исходные данные и информация контроля представляются в цифровой форме.

Контрольная информация может представлять собой сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Стеганографическое кодирование/декодирование дополнительной информации

Известно большое количество методов и алгоритмов, позволяющих скрытно кодировать дополнительную информацию в аудио-сигнал [Bender W., 1996; Fridrich, J., 2012; Cox I., 1997; Swanson M.D., et al., 1998; Ozer H., 2000; Iser B., 2008; Hicsonmez S., 2013; Жиляков Е.Г., 2015]. Наиболее широкое распространение получили стеганографические методы, основанные на суммировании исходного сигнала с взвешенной базисной функцией (в дискретном случае вектором):

$$\vec{y} = \vec{x} + e \cdot K \cdot \vec{\phi}, \tag{1}$$

где $\vec{y}$ – вектор синтезированного сигнала $\vec{y} = (y_1, y_2, ..., y_i, ..., y_N)^T$; $\vec{x}$ – вектор исходного сигнала $\vec{x} = (x_1, x_2, ..., x_i, ..., x_N)^T$; e – кодируемая информации $e \in (-\infty, \infty)$; K – весовой коэффициент; $\vec{\varphi}$ – функция $\vec{\varphi} = (\varphi_1, \varphi_2, ..., \varphi_i, ..., \varphi_N)^T$.

Схема стеганографического кодирования (1), предполагает, что известны все параметры и свойства внедряемой базисной функции, представленной вектором – $\vec{\varphi}$. Подразумевается, что внедряемый вектор $\vec{\varphi}$ той же размерности, что и исходный $\vec{x}$. Надо отметить необходимость удовлетворения ряда требований, предъявляемых к базисной функции, первые два из которых являются обязательными:

Требование 1. Все значения $\vec{\varphi}$ известны как при внедрении, так и при восстановлении, в некотором смысле его можно считать табличным, либо известна схема его формирования.

Требование 2. Для исходного отрезка $\vec{x}$ и $\vec{\varphi}$ должно существовать линейное пространство со скалярным произведением:

$$\alpha = \langle \vec{x}, \vec{\varphi} \rangle = \sum_{i=1}^{N} x_i \cdot \varphi_i . \tag{2}$$

где α – результат скалярного произведения

Требование 3. Энергию функции $\vec{\varphi}$ можно нормировать к единице:

$$\|\vec{\varphi}\|^2 = \sum_{i=1}^{N} \varphi_i^2 = 1, \tag{3}$$

где φ_i – мгновенное значение функции $\vec{\varphi} = (\varphi_1, \varphi_2, .., \varphi_i, .., \varphi_N)^T$.

Естественно заметить, что в случае, когда энергия функции $\vec{\varphi}$ не равна единице, то прибегают к использованию коэффициента, обеспечивающего равенство энергии единице:

$$K_\varphi = 1/\|\vec{\varphi}\| = \left(\sqrt{\sum_{i=1}^{N} \varphi_i^2} \right)^{-1}, \tag{4}$$

где K_φ – нормирующий коэффициент.

Соответственно имеет место равенство:

$$\left\|K_{\varphi}\cdot\bar{\varphi}\right\|^2=\sum_{i=1}^{N}\left(K_{\varphi}\cdot\varphi_i\right)^2=\sum_{i=1}^{N}\left(\frac{1}{\|\bar{\varphi}\|}\cdot\varphi_i\right)^2=1. \quad (5)$$

Для упрощения изложения далее будем считать, что энергия базисной функции равна единице.

Требование 4. Вектор $\bar{\varphi}$ должен быть не коррелирован (ортогонален) с исходным внедряемым, т. е. необходимо выполнение равенства:

$$\beta=\langle\bar{x},\bar{\varphi}\rangle=\sum_{i=1}^{N}x_i\cdot\varphi_i=0, \quad (6)$$

где β – результат скалярного произведения $\alpha\in(-\infty,\infty)$; $\langle\,,\rangle$ – операция скалярного произведения.

Одним из подходов для увеличения степени ортогональности отрезка $\bar{x}$ к базисной функции $\bar{\varphi}$ является фильтрация вида:

$$\bar{c}=\bar{x}-\alpha\cdot\bar{\varphi}, \quad (7)$$

где $\bar{c}$ – синтезированный вектор (контейнер).

Результатом выполнения (6) будет уменьшение корреляции исходного отрезка с базисной функцией:

$$\langle\bar{c},\bar{\varphi}\rangle=0. \quad (8)$$

С учетом выполнения вышеописанного, можно использовать операцию декодирования информации, осуществляемую на основе скалярного произведения синтезированного отрезка и базисной функции $\bar{\varphi}$, т. е. используется соотношение вида:

$$\tilde{\alpha}=\langle\bar{y},\bar{\varphi}\rangle=\sum_{i=1}^{N}y_i\cdot\varphi_i, \quad (9)$$

где $\tilde{\alpha}$ – декодируемая информации $\tilde{\alpha}\in(-\infty,\infty)$.

Из декодируемой информации $\tilde{\alpha}$ возможно восстановить исходную контрольную информацию [Жиляков Е.Г., 2015], путем сопоставления $\tilde{\alpha}$ с областью допустимых значений, учитывая, что выполняется неравенство:

$$(\tilde{\alpha})^2>\varepsilon, \quad (10)$$

где ε – значение порога, определяющего близость к нулю вычисляемых значений.

Ниже на рис. 1 приведена обобщенная модель значений, принимаемых проекцией, на основе которой реализуются процедуры декодирования.

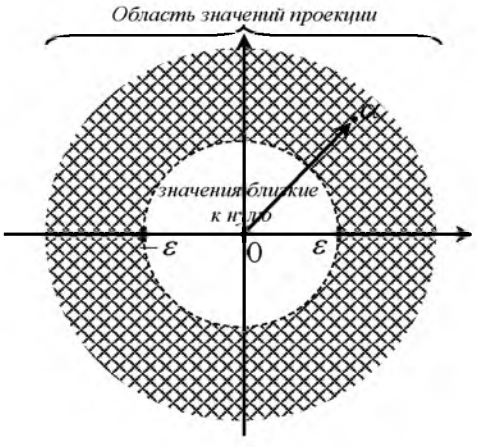

Рис. 1. Модель значений, принимаемых проекцией
Fig. 1. Model of values taken by the projection

Далее для стеганографического кодирования будем рассматривать упрощенную схему, когда кодируется бит информации в соответствующем знаке $\tilde{\alpha}$:

$$\tilde{e} = sign(\tilde{\alpha}) = \begin{cases} \tilde{\alpha} > \varepsilon, & 1 \\ \tilde{\alpha} < -\varepsilon, & -1 \end{cases}, \quad (11)$$

где $sign(\ )$ - операция выделения знака; $\tilde{e}$ – декодируемый бит информации.

Необходимо отметить, что для построения упрощенной схемы стеганографического внедрения, когда знак скалярного произведения определяет кодируемый бит, изменяют подход к кодированию (1), соответственно:

$$\bar{y} = \bar{c} + e \cdot K \cdot K_{\varphi} \cdot \bar{\varphi} = \bar{c} + e \cdot |\alpha| \cdot K_{\varphi} \cdot \bar{\varphi} = \bar{x} - \alpha \cdot K_{\varphi} \cdot \bar{\varphi} + e \cdot |\alpha| \cdot K_{\varphi} \cdot \bar{\varphi} = \bar{x} + (e - sign(\alpha)) \cdot |\alpha| \cdot K_{\varphi} \cdot \bar{\varphi}. \quad (12)$$

Естественно заметить, что при использовании упущенной схемы признаковым пространством кодирования является знак скалярного произведения отрезка и базисной функции. Для изменения знака осуществляется фильтрация базисной функции с удвоенной энергией, при совпадении исходного знака и кодируемого знака фильтрация не осуществляется. В выражении (12) учтено, что требование 4 в случае речевых данных никогда не выполняется, т. е. базисная функция, представленная вектором $\bar{\varphi}$, будет коррелирована с исходным отрезком $\bar{x}$. Степень корреляции базисной функции и исходного отрезка используется как коэффициент, определяющий энергию внедрения $\bar{\varphi}$. Иными словами, использован прием, описанный выражением (6), а в качестве коэффициента пропорциональности, определяющего энергию добавляемой базисной функции, используют результат скалярного произведения (7), это позволяет осуществить скрытное внедрение дополнительной информации, не изменяя в целом энергию исходного отрезка.

Среда кодирования

В качестве среды для стеганографического кодирования будем использовать речевые сигналы (РС), которые являются результатами регистрации значений электромагнитных колебаний на выходе микрофонов при воздействии акустических колебаний на их входах, возникающих в результате речевого обмена [Zhilyakov E.G., 2015].

В основе многих из разработанных подходов используются частотные представления. Стоит отметить, что порождаемые звуками речи отрезки РС обладают свойством концентрации энергии в достаточно «узких» полосах частотной оси (рис. 2).

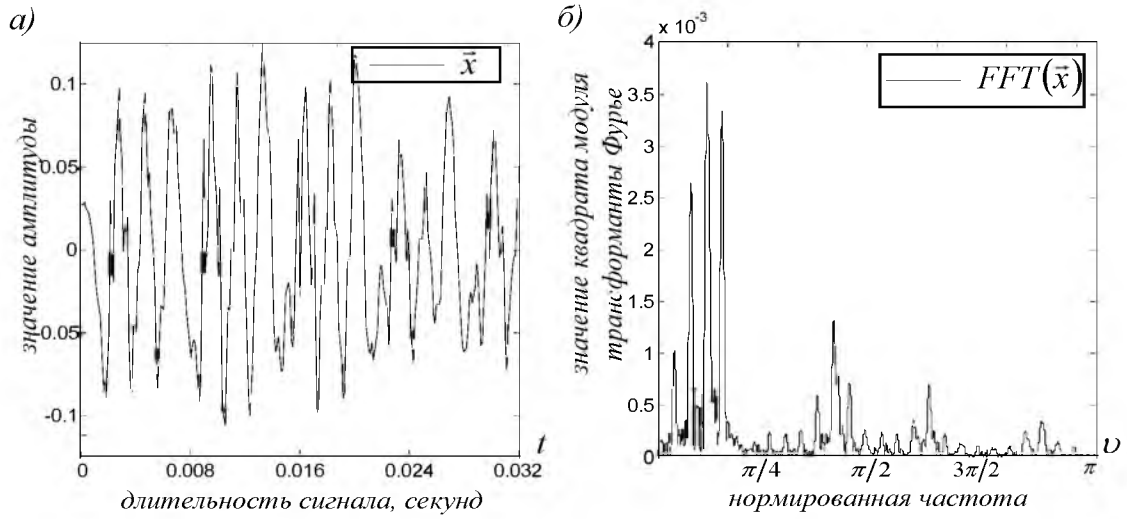

Рис. 2. Отрезок речевого сигнала, соответствующего звуку «а»
Fig. 2. A segment of speech signal corresponding to the sound "a"

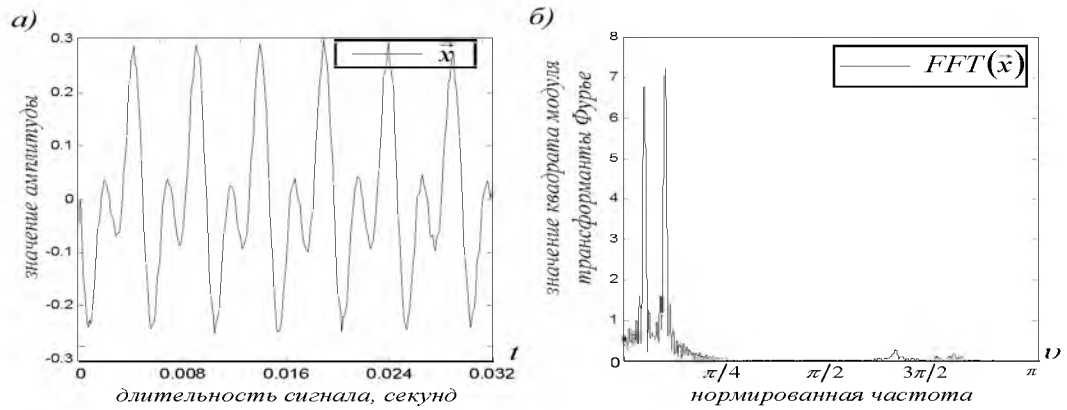

Рис. 3. Отрезок речевого сигнала, соответствующего звуку «и»
Fig. 3. A segment of speech signal corresponding to the sound "e"

В связи с этим можно упомянуть рассматриваемое в литературных источниках разбиение частотной полосы на частотные интервалы [Zhilyakov E.G., 2015], которые опосредованно отражаются на частотных свойствах РС. Таким образом, адекватным подходом к обработке РС является субполосный анализ, когда их свойства соотносятся с некоторым разбиением оси частот на интервалы конечной ширины. Причем ввиду зависимости частотного распределения энергий от вида произносимого звука, анализу необходимо подвергать отрезки РС конечной длительности.

Метод расширения спектра

Рассмотрим метод стеганографического кодирования дополнительной информации, построенный на расширении спектра исходного отрезка [Cox I., 1997; Nedeljko Cvejic, 2004].

$$\vec{y} = \vec{x} + e \cdot K \cdot \vec{u}\,, \tag{13}$$

где $\vec{u}$ – псевдослучайная последовательность $\vec{u} = (u_1, u_2, .., u_i, .., u_N)^T$, описываемая нормальным законом распределения со значениями $u_i \in \{-1, 1\}$.

В методе расширения спектра в качестве базисной функции используют псевдослучайную последовательность (ПСП), представленную на рисунке 4.

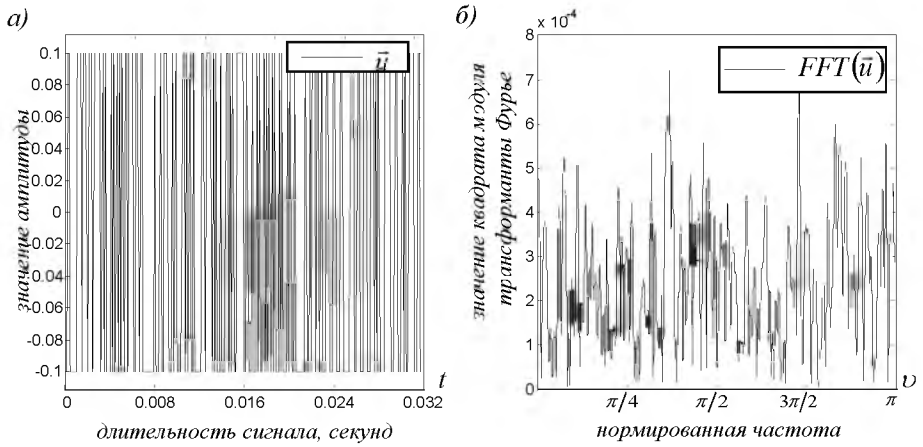

Рис. 4. Отрезок сигнала, соответствующего псевдослучайной последовательности
Fig. 4. A segment of signal corresponding to the pseudo-random sequence

Модификация метода расширения спектра заключается в изменении базисной функции, которая является произведением гармонического сигнала на псевдослучайную последовательность [Грибунин, 2002; Жиляков Е.Г., 2015]:

$$\vec{\phi} = (\phi_1, \phi_2, ..., \phi_i, ..., \phi_N)^T;\ \phi_i = u_i \cdot \cos(2\pi \cdot f_0 \cdot f_\partial \cdot (i-1));\ i = 1, 2, .., N\,, \tag{14}$$

где f_∂ – частота дискретизации; f_0 – центральная частота.

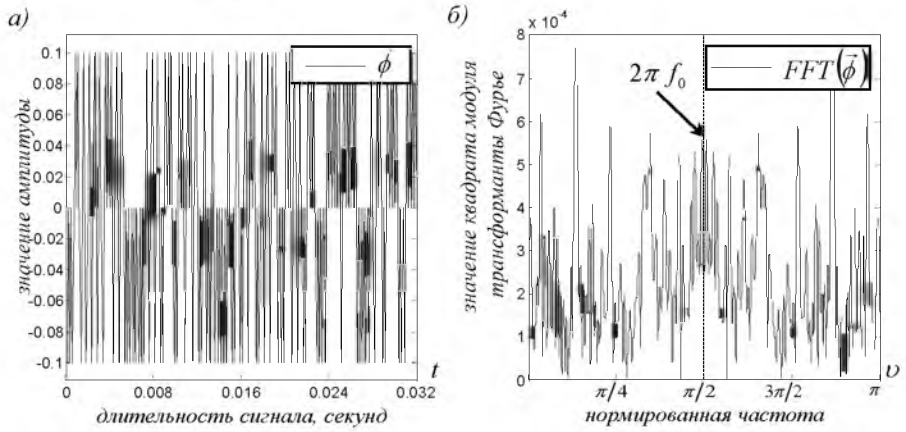

Рис. 5. Отрезок сигнала, соответствующего произведению псевдослучайной последовательности и гармонического сигнала

Fig. 5. A segment of signal corresponding to the multiplication of the pseudo-random sequence and the harmonic signal

Стеганографическое кодирование дополнительной информации модифицированным методом расширения спектра:

$$\bar{y} = \bar{x} + \left(e - sign(\alpha)\right) \cdot |\alpha| \cdot \vec{\phi}\ ;\ \alpha = \langle \bar{x}, \vec{\phi} \rangle . \tag{15}$$

Декодирование дополнительной информации, при условии, что при кодировании использовалась базисная функция вида (14):

$$\tilde{e} = sign\left(\langle \bar{y}, \vec{\phi} \rangle\right) = sign\left(\sum_{i=1}^{N} y_i \cdot \phi_i\right). \tag{16}$$

Особенности использования стеганографического метода расширения спектра для кодирования дополнительной информации:

– изменения происходят во всем частотном диапазоне, что не учитывает природу сигнала;

– для восстановления декодированной информации необходимо хранить данные для восстановления ПСП;

– из рассмотренных методов обладает наименьшей емкостью.

Метод дискретно-косинусного внедрения

Рассмотрим один из распространённых методов стеганографического кодирования использующий прямое разложение отрезка аудио-сигнала $\bar{x}$, на DCT-коэффициенты вида [Malvar H. S., 1992]:

$$\alpha_1 = \frac{\sqrt{2}}{N} \sum_{i=1}^{N} x_i \tag{17}$$

$$\alpha_k = \frac{2}{N} \sum_{i=0}^{N-1} x_i \cdot \cos\left(\frac{(2i+1) \cdot k \cdot \pi}{2N}\right);\ k = 2,3,\ldots, N . \tag{18}$$

$$\alpha = (\alpha_1, \alpha_2, .., \alpha_k, .., \alpha_N)^T , \tag{19}$$

где x_i – значение амплитуды сигнала $x_i \in \bar{x}$; m – номер DCT-коэффициента; α_k – DCT-коэффициент $k = 0,1,\ldots,(N-1)$.

Кодирование осуществляется путем замены знака коэффициента разложения:

$$\tilde{\alpha}_k = sign(e) \cdot |\alpha_k|\ ;\ k \in \{1,2,\ldots,(N-1)\};\ \vec{\alpha} = (\alpha_1, \alpha_2, .., e \cdot |\alpha_k|, .., \alpha_N)^T = (\alpha_1, \alpha_2, .., \tilde{\alpha}_k, .., \alpha_N)^T \tag{20}$$

так как гармонический сигнал можно представить в виде вектора (функция и спектр гармонического сигнала приведены на рисунке 6.):

$$\bar{g} = (g_1, g_2, ..., g_i, ..., g_N)^T ,\ g_i = \cos\left(\frac{2 \cdot i \cdot k \cdot \pi}{2 \cdot N}\right);\ i = 0,1,..,(N-1);\ k \in \{1,2,..,(N-1)\}. \tag{21}$$

то кодирование можно осуществить путем использования соотношения:

$$\bar{y} = \bar{x} + \left(e - sign(\alpha)\right) \cdot |\alpha| \cdot \bar{g}\,, \quad \alpha = \langle \bar{x}, \bar{g} \rangle\,. \tag{22}$$

в котором в качестве базисной функции используют гармонический сигнал, представленный на рисунке 6.

Декодирование дополнительной информации, при условии, что при кодировании использовалось дискретно-косинусная трансформация для коэффициента $k \in \{1, 2, .., (N-1)\}$, осуществляется следующим образом:

$$\mathscr{e} = sign\left(\frac{2}{N}\sum_{i=2}^{N} x_i \cdot \cos\left(\frac{i \cdot k \cdot \pi}{N}\right)\right). \tag{23}$$

Особенности использования стеганографического метода кодирования дополнительной информации, основанного на дискретно-косинусной трансформации:

– изменение происходит на строго определённых частотах;

– пространство кодирования меньше, чем у рассматриваемых методов, и зависит от длительности отрезка, что облегчает разрушение дополнительной информации;

– емкость зависит от свойств сигнала и выбранной психоакустической модели.

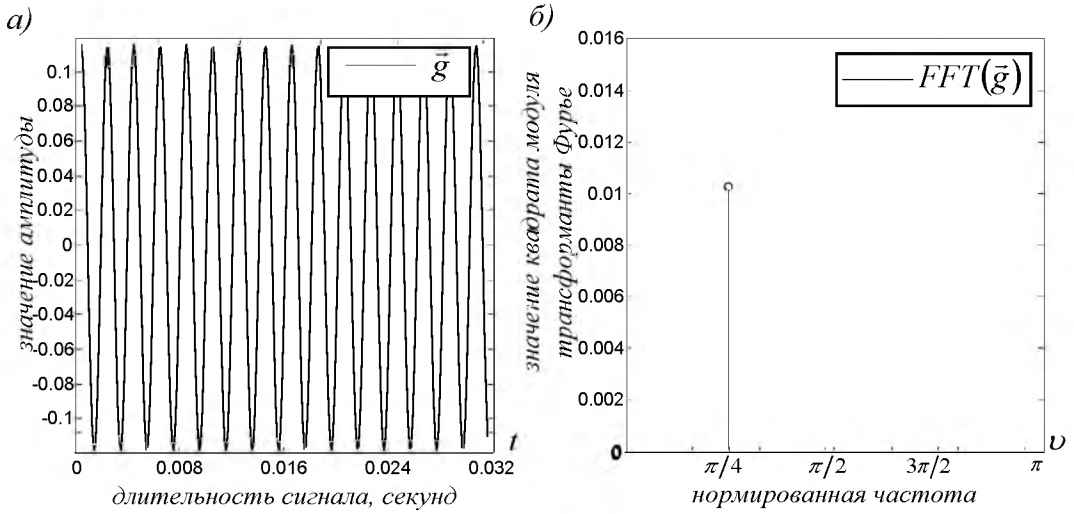

Рис. 6. Отрезок, соответствующий гармоническому сигналу
Fig. 6. Interval corresponding to the harmonic signal

Оптимальный субполосный метод

Субполосная матрица A_r симметрична и положительно определенна, поэтому для неё можно найти N собственных векторов и соответствующих им собственных чисел [Zhilyakov E.G., 2015]:

$$diag\left(\lambda_k\right) \cdot \bar{q}_k = A_r \cdot \bar{q}_k\,; \quad k = 1,2,..,N\,, \tag{24}$$

где $\bar{q}_k$ – собственный вектор субполосной матрицы A_r; λ_k – собственное число, соответствующее $\bar{q}_k$ собственному вектору субполосной матрицы, принимающее значение: $0 < \lambda_k \le 1$.

Важным свойством собственных векторов субполосной матрицы, найденных для одной субполосы, можно отнести условие ортонормальности:

$$\left\langle \bar{q}_i\,, \bar{q}_k \right\rangle = \begin{cases} 1, & i = k \\ 0, & i \neq k \end{cases};\ i,k \in \{1,2,..,N\}\,, \tag{25}$$

в котором в качестве базисной функции используют собственный вектор субполосной матрицы, представленный на рисунке 7.

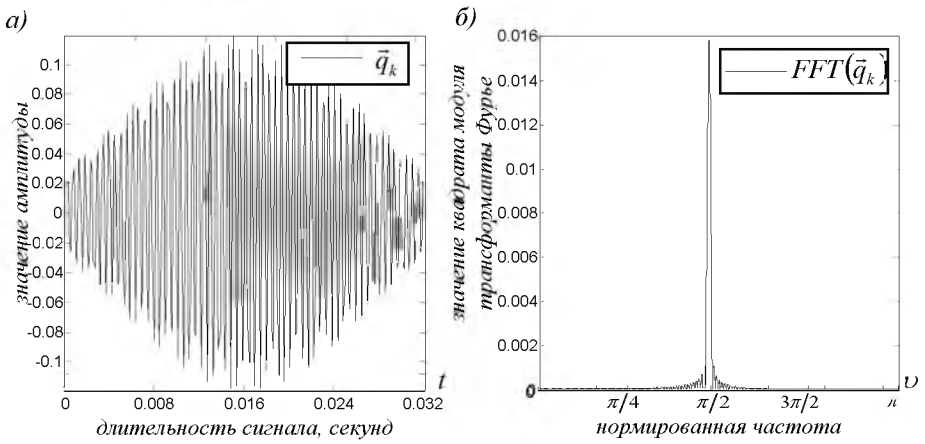

Рис. 7. Отрезок сигнала, соответствующего псевдослучайной последовательности
Fig. 7. A segment of signal corresponding to the pseudo-random sequence

Стеганографическое кодирование дополнительной информации модифицированным методом расширения спектра:

$$\bar{y} = \bar{x} + (e - sign(\alpha)) \cdot |\alpha| \cdot \bar{q}_k, \ \alpha = \langle \bar{x}, \bar{q}_k \rangle . \quad (26)$$

Декодирование дополнительной информации, при условии, что при кодировании использовалась базисная функция вида (14):

$$\tilde{e} = sign\left(\langle \bar{y}, \bar{q}_k \rangle\right) = sign\left(\sum_{i=1}^{N} y(i) \cdot q_k(i)\right). \quad (27)$$

Особенности использования стеганографического субполосного метода кодирования дополнительной информации:

– во время кодирования и декодирования необходимо детектировать паузы или частотные компоненты, содержащие энергию, при кодировании в которую восстановление информации не происходит;

– для оптимального кодирования необходима своя психоакустическая модель;

– необходимы решающие правила для выбора центральной частоты и ширины частотного интервала.

Подходы к оценке работоспособности методов

Мера, отражающая абсолютное изменение энергии отрезков во временной области (*mean square error*), [Vercoe B.L. 1995; Iser B., 2008]:

$$MSE = \sum_{i=1}^{N} (x_i - y_i)^2 . \quad (28)$$

Оценка, определяющая порядок изменения энергии по отношению к общей энергии исходного сигнала (*signal-to-noise ratio* – SNR) [Vercoe B.L. 1995; Iser B., 2008]:

$$SNR = 10 \cdot \log_{10} \frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N} (x_i - y_i)^2} . \quad (29)$$

Степень структурной схожести синтезированного и исходного отрезка оценим с использованием корреляции ρ [Vercoe B.L. 1995; Furui, Sadaoki. 2000; Iser B., 2008]:

$$\rho = \frac{\left(\sum_{i=1}^{N} (x_i - \bar{x}) \cdot \sum_{i=1}^{N} (y_i - \bar{y})\right)}{\sqrt{\sum_{i=1}^{N} (x_i - \bar{x})^2 \cdot \sum_{i=1}^{N} (y_i - y)^2}} . \quad (30)$$

Нормированное среднеквадратическое отклонение [Жиляков, Е.Г., 2014]:

$$\sigma = \sqrt{\sum_{i=1}^{N}(x_i - k \cdot y_i)^2} \Big/ \sqrt{\sum_{i=1}^{N} x_i^2} \; ; \; k = \sum_{i=1}^{N} x_i \cdot y_i \Big/ \sum_{i=1}^{N} x_i^2 \; . \quad (31)$$

Вероятность ошибки (bit error rate) [Vercoe B.L. 1995; ; Iser B., 2008]:

$$BER = \frac{1}{M} \sum_{m=1}^{M} (((sign(e_m)+1)/2) \oplus ((sign(\tilde{e}_m)+1)/2)). \quad (32)$$

где M - количество кодируемых бит; $\oplus$ - операция «сумма по модулю два».

Вычислительные эксперименты

Для проверки работоспособности методов использовались фрагменты аудиосигнала с частотой дискретизации 8 кГц и разрядностью 16 бит [ГОСТ 16600-72]. Общая длительность речевого материала составила 23 минуты, с длительностью 0,032 с., (из материала были исключены отрезки, соответствующие паузе). В результате моделирования было внедрено 10^9 бит, результаты моделирования представлены в таблице.

Таблица
Table

Оценка работоспособности методов
Performance evaluation methods

Стеганографический метод	MSE	SNR	ρ	σ	BER	V , бит/с
Метод расширения спектра (SSp), [Cox I., 1997]	0.152	20.3	0.873	0.015	0.31	32
Модифицированный метод расширения спектра (SSp), [Грибунин В.Г., 2002]	0.011	37.4	0.992	$0.1 \cdot 10^{-3}$	$3.2 \cdot 10^{-4}$	32
Метод дискретно-косинусной трансформации (DCT), [Bender W., 1996]	0.030	50.1	0.987	$1.1 \cdot 10^{-16}$	$2.1 \cdot 10^{-6}$	128
Субполосный метод, (SubBand), [Жиляков, 2015]	0.03	47.5	0.993	$1.2 \cdot 10^{-16}$	$3.2 \cdot 10^{-6}$	218

Заключение

Методы стеганографии базируются на математическом аппарате и соответствующей психоакустической модели, разработанной для данного математического аппарата. В процессе исследований были выявлены преимущества и несовершенства методов и подходов стеганографического кодирования.

Стоит отметить, что важным моментом использования алгоритмов стеганографического кодирования дополнительной информации является обеспечение скрытности (характеризуемой мерами MSE, SNR, ρ, σ) при достоверности её восстановления, характеризуемой вероятностью ошибки (BER). Выполнение требований скрытности и достоверности напрямую сопряжено с использованием базисных функций, которые должны учитывать время-частотную структуру исходных сигналов. Выбор базисной функции определяет вид искажений в синтезируемом сигнале. Степень коррелированности исходного сигнала и базисной функции влияет на возможность безошибочного декодирования и скрытность. Следующим этапом, после выбора базисных функций, является разработка принципов определения весового коэффициента (1). Значение весового коэффициента определяет величину искажений, вызываемых в синтезируемом сигнале. Завершающим этапом является определение области допустимых значений, которые может принимать декодируемая информация и, соответственно, в совокупности с вышеописанным влияет на однозначность восстановления кодируемой информации, при этом наиболее часто используют подход (10).

Методы стеганографии, базирующиеся на расширении спектра, не позволяют адекватно использовать частотные свойства речевого сигнала. Под адекватностью в данном случае понимается внесение изменений в строго выделенной частотной полосе. Как известно, речевые сигналы сосредоточены в узкой полосе (рис. 2 и рис. 3), поэтому адекватное кодирование и выбор полосы является важным моментом.

После проведенного анализа реализованных методов стеганографии, с учетом того, что в коммерческих организациях существенную долю оперативно передаваемой информации составляют речевые сообщения, авторами сделан вывод о том, что наиболее приемлемыми методами аутентификации речевого сообщения являются методы, базирующиеся на субполосном синтезе и DCT-преобразовании. Стоит отметить, что методы, построенные на субполосном синтезе, имеют большую в шесть раз пропускную способность по сравнению с методами дискретно-косинусной трансформации.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 15-07-01570-а.

Список литературы
References

1. ГОСТ 16600-72. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений [Звукозапись] / ГОСТ 16600-72; исп.: Д.И. Библев. Белгород: НИУ БелГУ, 2016. 1380 сек. – Режим доступа: https://www.researchgate.net/publication/312167036_Recording_Gost_16600-72 DOI: 10.13140/RG.2.2.33677 .74720

GOST 16600-72. Peredacha rechi po traktam radiotelefonnoj svyazi. Trebovaniya k razborchivosti rechi i metody artikulyacionnyh izmerenij [Zvukozapis'] / GOST 16600-72; isp.: D.I. Biblev. – Belgorod: NIU BelGU, 2016. 1380 sek. URL: https://www.researchgate.net/publication/312167036 _Recording_Gost_16600-72 DOI: 10.13140/RG.2.2.33677.74720

2. Грибунин В.Г., Оков И.Н., Туринцев И.В., 2002. Цифровая стеганография. Аспекты защиты. М., Солон-Пресс, 261.

Gribunin V.G., Okov I.N., Turintsev I.V., 2002. Tsifrovaya steganografiya. Aspektyi zaschityi. M., Solon-Press, 261.

3. Жиляков Е.Г., 2015. Оптимальные субполосные методы анализа и синтеза сигналов конечной длительности. Автоматика и телемеханика. М., Академический научно-издательский, производственно-полиграфический и книгораспространительский центр Российской академии наук. Издательство "Наука, 4: 51-66.

Zhilyakov E.G., 2015. Optimalnyie subpolosnyie metodyi analiza i sinteza signalov konechnoy dlitelnosti. Avtomatika i telemehanika. M.: Akademicheskiy nauchno-izdatelskiy, proizvodstvenno-poligraficheskiy i knigorasprostranitelskiy tsentr Rossiyskoy akademii nauk. Izdatelstvo Nauka, 4: 51-66

4. Жиляков Е.Г., Пашинцев В.П., Белов С.П., Лихолоб П.Г., 2015. О методе скрытного кодирования контрольной информации в речевые данные. Инфокоммуникационные технологии. 13(3): 325-333.

Zhilyakov E.G., Pashincev V.P., Belov S.P., Likholob P.G., 2015. O metode skrytnogo kodirovaniya kontrol'noj informacii v rechevye dannye. Infokommunikacionnye tekhnologii. 13(3): 325-333. (Russian)

5. Жиляков Е.Г., Лихолоб П.Г., Медведева А.А., Прохоренко Е.Н., 2016. Исследование чувствительности некоторых мер качества скрытия информации в речевых сигналах. Научные ведомости БелГУ. Сер. Экономика. Информатика. 9(230): 174-179.

Zhilyakov E.G., Liholob P.G., Medvedeva A.A., Prohorenko E.N., 2016. Research of sensitivity of some measures quality assessment hidden information in the speech signal. Nauchnye vedomosti BelGU. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. Economics Information technologies]. 9(230): 174-179. (in Russian)

6. Жиляков Е.Г., Чадюк П.В., Иванов О.Н., 2014. Алгоритм субполосной фильтрации эмпирических данных Вопросы радиоэлектроники. Серия: Электронная и вычислительная техника М.: ОАО «ЦНИИ «Электроника». 2(4): 109-117.

Zhilyakov E.G., Chadyuk P.V., Ivanov O.N., 2014. Algoritm subpolosnoj fil'tracii ehmpiricheskih dannyh. Voprosy radioehlektroniki. Seriya: EHlektronnaya i vychislitel'naya tekhnika. M.: OAO «CNII «EHlektronika», 2(4): 109-117. (in Russian)

7. Bender W. et al. Techniques for data hiding. IBM Syst. J. 1996. 35(3.4): 313–336.

8. Cox I. J., Kilian J., Leighton F. T., Shamoon T., 1997. Secure spread spectrum watermarking for multimedia. IEEE transactions on image processing. 6(12): 1673-1687.

9. Fridrich J., 2012. Steganography in digital media: Principles, algorithms, and applications. Steganography in Digital Media, 1-441.

10. Furui, Sadaoki., 2000. Digital speech processing, synthesis, and recognition. 2nd ed., rev. and expanded.

11. Iser B., Schmidt G., Minker W., 2008. Bandwidth extension of speech signals. Springer Science & Business Media.

12. Malvar H.S., 1992. Signal processing with lapped transforms. Boston: Artech House.

13. Nedeljko Cvejic, Tapio Seppanen, 2004. Spread spectrum audio watermarking using frequency hopping and attack characterization. Signal Processing 84: 207-213.

14. Swanson M.D., Kobayashi M., Tewfik A.H. Multimedia data-embedding and watermarking technologies. Proc. IEEE. 1998. 86(6): 1064–1087.

15. Vercoe B.L. 1995. Csound: A Manual for the Audio-Processing System, MIT Media Lab, Cambridge.

16. Zhilyakov E.G. Belov S.P., Belov A.S. Firsova A.A., 2015, On the division of speech signals on homogeneous segments. International Journal of Applied Engineering Research, 10(24): 45271-45275.