УДК 519.876.5:519.6:004.357 **DOI** 10.15622/sp.51.5

М.В. Гофман

МЕТОДИКА СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ ПРИ СВЯЗИ ЧЕРЕЗ ВОЗДУШНЫЙ АУДИОКАНАЛ

Гофман М.В. **Методика скрытой передачи данных при связи через воздушный аудиоканал.**

Аннотация. В этой статье предлагается методика скрытой передачи информации в слышимой области частотного спектра воздушной среды, а именно — построения, внедрения, выделения и восстановления скрываемого сигнала, когда передача осуществляется через воздушный аудиоканал. Скрываемый сигнал состоит из двух частей. Одна часть используется для синхронизации, а другая часть — информационная. В основе синхронизационной части лежит последовательность Касами, тогда как в основе информационной — кодовое слово кода БЧХ. Обе части скрываемого сигнала получаются путем специального кодирования своих двоичных элементов. При выполнении этого кодирования используются последовательности Голда и RZ коды. В качестве скрывающего или несущего сигнала используется аудиосигнал, который может представлять собой как речь, так и музыку. Построение стегоаудиосигнала выполняется путем внедрения скрываемого сигнала в частотную область скрывающего сигнала. Внедрение представляет собой амплитудную модуляцию отдельных спектральных составляющих скрывающего сигнала. В статье аналитически рассматривается вопрос возможности восстановления скрываемого сигнала, после передачи стегоаудиосигнала через воздушный аудиоканал. Статья снабжена результатами имитационного моделирования и натурных экспериментов передачи стегоаудиосигнала через воздушный аудиоканал.

Ключевые слова: аудиосигнал, стеганография, воздушный аудиоканал, воздушный зазор, последовательность Касами, последовательность Голда, БЧХ код, RZ код.

1. Введение. Компьютеры, которым требуется обеспечить повышенную безопасность, обычно изолируют. Множество видов изоляции объединяют под таким понятием, как «воздушный зазор» (air-gap). Скрытая передача информации через воздушный зазор всегда привлекает к себе внимание исследователей. Классификацию методов сокрытия информации можно найти в статье [1].

Если компьютер, находящийся за воздушным зазором, оснащен динамиком и микрофоном, то их в принципе возможно использовать в качестве средств для скрытой передачи информации. Так, рядом расположенные мобильные телефоны и ноутбуки можно объединить в беспроводную скрытую сеть утечки информации (mesh networks) [2]; чтобы окружающие люди не слышали саму передачу, пока что для таких сетей требуется использовать динамики и микрофоны, способные работать на частотах, близких к ультразвуку, что, конечно, ограничивает круг устройств весьма дорогостоящими.

Вообще задача использования аудиосигналов в качестве «контейнеров» для скрытой передачи дополнительной информации, обычно называемой цифровым водяным знаком, привлекает к себе большое внимание [3, 4, 5, 6, 7]. Есть методики передачи стегоаудиосигналов через радиоканалы и проводные каналы [8]. Однако передача стегоаудиосигналов через воздушный аудиоканал или, иными словами, через слышимый частотный спектр воздушной среды требует разработки и использования таких методик построения сигналов и их внедрения в несущий аудиосигнал, которые были бы устойчивы к воздействию окружающей среды.

В этой статье предлагается методика внедрения информации в аудиосигнал и восстановления внедренной информации после передачи стегоаудиосигнала через воздушный аудиоканал, позволяющая выполнять скрытую передачу данных через такой канал. Особенностью предлагаемой методики внедрения информации в аудиосигнал является то, что информация не будет воспринята человеческим ухом в процессе передачи такого стегоаудиосигнала, тогда как само внедрение информации может быть выполнено в любую частотную область слышимого диапазона. При этом восстановление внедренной информации из принятого стегоаудиосигнала возможно даже при незнании приемником аудиосигнала, в который производилось встраивание.

2. Методика построения, внедрения, выделения и восстановления скрытого сигнала. В предлагаемой методике выполняется построение сигнала, состоящего из двух частей, каждая из которых выполняет свою функцию. Одна используется для установления синхронизации; в ее основе лежит последовательность Касами (Kasami) [9]. Другая часть защищает передаваемую информацию от ошибок; для этого используется код, исправляющий ошибки. При этом элементы этих частей получаются в результате преобразования, в основе которого лежат последовательности Голда (Gold) и RZ коды [8].

Далее, для удобства описания предлагаемой методики как подхода для передачи информации используется терминология и понятия систем передачи данных. Так, кодер и декодер канала используются для построения и восстановления дополнительной информации. Тогда как модулятор и демодулятор используются для

процедур внедрения дополнительной информации в аудиосигнал и выделения ее из принятого сигнала соответственно.

2.1. Передающая сторона. В кодер канала поступает информационная последовательность:

$$\boldsymbol{x} = \left(x(1) \quad x(2) \quad \ldots \quad x\left(N_{\text{X}}\right) \right),$$

где $x(i) \in \{0,1\}$. Кодер канала преобразует информационную последовательность в кодовое слово $(N_{\text{c}}, N_{\text{x}})$ БЧХ кода [10, 11]:

$$\boldsymbol{c}_{\text{БЧХ}} = \left(c_{\text{БЧХ}}(1) \quad c_{\text{БЧХ}}(2) \quad \ldots \quad c_{\text{БЧХ}}(N_{\text{c}}) \right),$$

где $c_{\text{БЧХ}}(i) \in \{0,1\}$; количество исправляемых кодом ошибок обозначим символом N_{t}. Кодер канала, используя вектор $\boldsymbol{c}_{\text{БЧХ}}$, строит кодовое слово следующего вида:

$$\boldsymbol{y} = \left(y(1) \quad y(2) \quad \ldots \quad y(N_{\text{Y}}) \right) = \left(\boldsymbol{y}_{\text{сх}} \quad \boldsymbol{y}_{\text{иф}} \right),$$

которое можно разделить на две части: часть $\boldsymbol{y}_{\text{сх}}$, используемую для установления синхронизации, и часть $\boldsymbol{y}_{\text{иф}}$, которая кодирует вектор $\boldsymbol{c}_{\text{БЧХ}}$. Каждая из этих частей представляет собой вектор, элементы которого — числа из множества $\{-1,1\}$.

Синхронизационная часть $\boldsymbol{y}_{\text{сх}}$ получается в результате кодирования последовательностями Голда элементов последовательности Касами с последующим кодированием RZ кодом. Так, вектор:

$$\boldsymbol{y}_{\text{сх}} = \left(y_{\text{сх}}(1) \quad y_{\text{сх}}(2) \quad \ldots \quad y_{\text{сх}}(N_{\text{K}} N_{\Gamma} N_{\text{RZ}}) \right),$$

где N_{K} — это длина используемой последовательности Касами, N_{Γ} — длина используемых последовательностей Голда, а N_{RZ} — длина кодовых слов используемого RZ кода. Пусть задана последовательность Касами:

$$\boldsymbol{\beta} = \left(\beta(1) \quad \beta(2) \quad \ldots \quad \beta(N_{\text{K}}) \right),$$

где $\beta(i) \in \{-1,1\}$; заданы последовательности Голда:

$$\boldsymbol{g}_1 = \left(g(1,1) \quad g(1,2) \quad \ldots \quad g(1,N_\Gamma)\right),$$
$$\boldsymbol{g}_2 = \left(g(2,1) \quad g(2,2) \quad \ldots \quad g(2,N_\Gamma)\right),$$

где $g(i,j) \in \{-1,1\}$; а также, пусть, задан RZ код из 2-х кодовых слов:

$$\boldsymbol{c}_{\mathrm{RZ}}(1) = \left(c_{\mathrm{RZ}}(1,1) \quad c_{\mathrm{RZ}}(1,1) \quad \ldots \quad c_{\mathrm{RZ}}(1,N_{\mathrm{RZ}})\right),$$
$$\boldsymbol{c}_{\mathrm{RZ}}(2) = \left(c_{\mathrm{RZ}}(2,1) \quad c_{\mathrm{RZ}}(2,1) \quad \ldots \quad c_{\mathrm{RZ}}(2,N_{\mathrm{RZ}})\right),$$

где N_{RZ} — четное число,

$$c_{\mathrm{RZ}}(1,1) = c_{\mathrm{RZ}}(1,2) = \ldots = c_{\mathrm{RZ}}\left(1,\frac{N_{\mathrm{RZ}}}{2}\right) = -1,$$

$$c_{\mathrm{RZ}}\left(1,\frac{N_{\mathrm{RZ}}}{2}+1\right) = c_{\mathrm{RZ}}\left(1,\frac{N_{\mathrm{RZ}}}{2}+2\right) = \ldots = c_{\mathrm{RZ}}(1,N_{\mathrm{RZ}}) = 1,$$

$$c_{\mathrm{RZ}}(2,j) = (-1)\cdot c_{\mathrm{RZ}}(1,j).$$

В этом случае, если -1 кодируется вектором $\boldsymbol{g}_1$, а 1 кодируется $\boldsymbol{g}_2$, то элементы синхронизационной части удовлетворяют следующему равенству:

$$y_{\mathrm{сх}}\left(N_\Gamma N_{\mathrm{RZ}}(i-1) + N_{\mathrm{RZ}}(j-1) + k\right) = c_{\mathrm{RZ}}\left(\frac{g\left(\frac{\beta(i)+1}{2}+1, j\right)+1}{2}+1, k\right),$$

где $i \in \{1,2,\ldots,N_{\mathrm{K}}\}$, $j \in \{1,2,\ldots,N_\Gamma\}$, $k \in \{1,2,\ldots,N_{\mathrm{RZ}}\}$. Таким образом, вначале элементы последовательности Касами подвергаются кодированию последовательностями Голда, элементы которых, в свою очередь, подвергаются кодированию RZ кодом.

Информационная часть:

$$\boldsymbol{y}_{\mathrm{иф}} = \left(y_{\mathrm{иф}}(1) \quad y_{\mathrm{иф}}(2) \quad \ldots \quad y_{\mathrm{иф}}(N_{\mathrm{c}} N_\Gamma N_{\mathrm{RZ}})\right)$$

получается таким же образом, как и синхронизационная часть, но путем кодирования элементов вектора $\boldsymbol{c}_{\text{БЧХ}}$. Так,

$$y_{\text{иф}}\left(N_{\Gamma}N_{\text{RZ}}\left(i-1\right)+N_{\text{RZ}}\left(j-1\right)+k\right)=c_{\text{RZ}}\left(\frac{g\left(c_{\text{БЧХ}}\left(i\right)+1,j\right)+1}{2}+1,k\right),$$

где $i\in\left\{1,2,\ldots,N_{\text{c}}\right\}$, $j\in\left\{1,2,\ldots,N_{\Gamma}\right\}$, $k\in\left\{1,2,\ldots,N_{\text{RZ}}\right\}$.

По длинам векторов $\boldsymbol{y}_{\text{сх}}$ и $\boldsymbol{y}_{\text{иф}}$ видно, что длина итогового вектора $\boldsymbol{y}$ будет удовлетворять равенству:

$$N_{\text{Y}}=\left(N_{\text{c}}+N_{\text{K}}\right)N_{\Gamma}N_{\text{RZ}}.$$

Модулятор выполняет встраивание кодового слова $\boldsymbol{y}$, далее называемого *скрываемым сигналом*, в частотную область *скрывающего сигнала* путем модификации амплитуд спектральных линий скрывающего сигнала. Пусть скрывающий сигнал представляет собой цифровой аудиосигнал:

$$\boldsymbol{z}=\left(z\left(1\right)\quad z\left(2\right)\quad\ldots\quad z\left(k_{\text{Z}}N_{\text{Z}}\right)\right),$$

где $z\left(i\right)$ — отсчеты цифрового аудиосигнала, принимающие значения из диапазона $\left[-1,1\right]$, $k_{\text{Z}}=\left(N_{\text{c}}+N_{\text{K}}\right)N_{\text{RZ}}$, N_{Z} — четное число, для которого выполняется неравенство $N_{\text{Z}}\geq 2\left(N_{\Gamma}+1\right)$.

Смежные блоки элементов вектора $\boldsymbol{z}$, длинами N_{Z}, подвергаются дискретным преобразованиям Фурье, что в итоге дает вместо вещественного вектора $\boldsymbol{z}$, комплексный вектор такой же длины, каждый элемент которого называется спектральной линией. Таким образом *j*-я спектральная линия *i*-го блока равна комплексному числу:

$$Z\left(i,j\right)=\sum_{k=1}^{N_{\text{Z}}}z\left(\left(i-1\right)N_{\text{Z}}+k\right)\exp\left(-\frac{\imath 2\pi\left(k-1\right)\left(j-1\right)}{N_{\text{Z}}}\right),$$

где $i\in\left\{1,2,\ldots,k_{\text{Z}}\right\}$, $j\in\left\{1,2,\ldots,N_{\text{Z}}\right\}$, $\imath=\sqrt{-1}$ — мнимая единица.

Встраивание скрываемого сигнала выполняется путем изменения некоторого подмножества спектральных линий $Z\left(i,j\right)$ с номерами j из диапазона от 1 до $N_{\text{Z}}/2$; при этом мощность модифицируемого

подмножества равна N_Γ. Так, если $\{B(i,1), B(i,2), \ldots, B(i,N_\Gamma)\}$ — это множество номеров спектральных линий *i*-го блока, выбранных для встраивания, при этом $1 < B(i,k) \le N_Z/2$, а $\{A(i,1), A(i,2), \ldots, A(i,N_\Gamma)\}$ — это множество коэффициентов, определяющих силу встраивания (обычно $A(i,k) \ll 1$), то, обозначив результат модификации спектральной линии $Z(i,j)$ как $Z'(i,j)$, само встраивание выполняется по следующему правилу:

$$Z'(i,j) = \begin{cases} Z\big(i,B(i,k)\big)\big(1+A(i,k)\,y(m)\big), & \text{если } j = B(i,k), \\ Z(i,j), & \text{иначе,} \end{cases}$$

где $i \in \{1,2,\ldots,k_Z\}$, $j \in \{1,2,\ldots,N_Z/2\}$, $k \in \{1,2,\ldots,N_\Gamma\}$, m — номер встраиваемого элемента вектора $\boldsymbol{y}$. Значение m зависит и от номера блока i, и от числа k по следующему правилу:

$$m = \big((i-1) \bmod N_{RZ}\big) + 1 + (k-1)\,N_{RZ} + \left[\frac{i-1}{N_{RZ}}\right] N_{RZ} N_\Gamma,$$

где $[a]$ — целая часть вещественного числа a. По правилу зависимости m от i и k видно, что в каждый блок спектральных линий внедряется лишь один элемент каждого кодового слова RZ кода, полученный при кодировании отдельной последовательности Голда. Спектральные линии $Z(i,j)$ с номерами j из диапазона от $(N_Z/2)+1$ до N_Z для сохранения свойства сопряженной симметричности также подвергаются изменениям в соответствии со следующим равенством:

$$Z'(i,j) = \begin{cases} \big(Z'(i,N_Z - j + 2)\big)^*, & \text{если } j \ne (N_Z/2)+1, \\ Z(i,j), & \text{иначе,} \end{cases}$$

где $i \in \{1,2,\ldots,k_Z\}$, $j \in \{(N_Z/2)+1, (N_Z/2)+2, \ldots, N_Z\}$, $(a)^*$ — число, комплексно сопряженное числу a. Выполняя обратное дискретные преобразование Фурье над модифицированными блоками

спектральных линий, будет получен вещественный цифровой аудиосигнал:

$$\boldsymbol{z}' = \left(z'(1) \quad z'(2) \quad \ldots \quad z'(k_Z N_Z)\right),$$

где

$$z'\left((i-1)N_Z + k\right) = \frac{1}{N_Z}\sum_{j=1}^{N_Z} Z'(i,j)\exp\left(\frac{\imath 2\pi(j-1)(k-1)}{N_Z}\right),$$

где $i \in \{1,2,\ldots,k_Z\}$, $k \in \{1,2,\ldots,N_Z\}$, $\imath = \sqrt{-1}$ — мнимая единица.

Значения элементов вектора $\boldsymbol{z}'$ в результате встраивания вектора $\boldsymbol{y}$ могут оказаться вне диапазона $[-1,1]$. Поэтому перед отправкой в канал элементы вектора $\boldsymbol{z}'$ умножаются на нормирующий коэффициент:

$$\theta = \frac{1}{\max\left\{\left|z'(1)\right|,\left|z'(2)\right|,\ldots,\left|z'(k_Z N_Z)\right|\right\}},$$

где $|a|$ — абсолютное значение числа a.

Так как при построении скрываемого сигнала $\boldsymbol{y}$ RZ кодирование выполнялось в последнюю очередь, то ясно, что смежные блоки элементов вектора $\boldsymbol{y}$ длинами N_{RZ} представляют собой кодовые слова RZ кода. А процесс встраивания приведет к тому, что эти кодовые слова последовательно половинами будут встроены в смежные блоки вектора z, длинами N_Z. Выбор величин коэффициентов $A(i,k)$ можно осуществлять, опираясь на значения сигнал-маска, получаемые при помощи психоакустической модели, приведенной в [12, 13].

2.2. Принимающая сторона. Аудиосигнал $\boldsymbol{z}'$ передается через воздушный аудиоканал. Пусть на выходе канала выполняется дискретизация с частотой F_s, равной частоте отправки отсчетов сигнала $\boldsymbol{z}'$ в аудиоканал. Таким образом, на выходе канала получается последовательность отсчетов:

$$\boldsymbol{r} = r(1), r(2), \ldots, r(k_Z N_Z), r(k_Z N_Z + 1), \ldots$$

Приемник разбивает последовательность $\boldsymbol{r}$ на перекрывающиеся блоки длиной $k_Z N_Z$ отсчетов. Для вынесения решения о наличии

скрытого сигнала в некотором блоке или, иными словами, для вынесения решения об установлении синхронизации на некотором блоке приемнику требуется обработать еще $W-1$ такого же размера блоков справа от исследуемого, то есть требуется сделать еще $W-1$ шагов. Шаг составляет один отсчет, поэтому смежные блоки перекрываются настолько, что отличаются лишь в одном элементе. Обозначим блок отсчетов, обрабатываемый на некотором шаге $i_{\text{шаг}} \in \{1,2,\ldots\}$ вектором:

$$\boldsymbol{r}(i_{\text{шаг}}) = \big(r(i_{\text{шаг}}) \quad r(i_{\text{шаг}}+1) \quad \ldots \quad r(i_{\text{шаг}}+k_{\text{Z}}N_{\text{Z}}-1)\big).$$

Вектор $\boldsymbol{r}(i_{\text{шаг}})$ передается в демодулятор. Помимо него в демодулятор поступают множества $\{B(i,1),B(i,2),\ldots,B(i,N_{\Gamma})\}$ номеров спектральных линий, в которые производилось встраивание скрываемого сигнала передатчиком, для всех $i \in \{1,2,\ldots,k_{\text{Z}}\}$. Кроме того, в демодулятор может поступать сам скрывающий сигнал $\boldsymbol{z}$, если известно, что он обычно повышает точность синхронизации и уменьшает вероятность ошибок восстановления символов информационной части. Однако, даже когда скрывающий сигнал $\boldsymbol{z}$ неизвестен приемнику, описываемые в этой работе схемы кодирования и декодирования позволяют выделять скрываемый сигнал $\boldsymbol{y}$ из принятого сигнала; но следует учитывать, что в таком случае сам скрывающий сигнал станет шумом для приемника и будет влиять на качество восстановления скрытого сигнала.

Демодулятор выполняет действия, некоторые из которых обратны выполненным модулятором. Так, он выполняет дискретные преобразования Фурье над смежными блоками элементов вектора $\boldsymbol{r}(i_{\text{шаг}})$, при этом длина блока также равна N_{Z}; например, первый блок можно описать вектором:

$$\big(r(i_{\text{шаг}}) \quad r(i_{\text{шаг}}+1) \quad \ldots \quad r(i_{\text{шаг}}+N_{\text{Z}}-1)\big), \qquad (1)$$

а второй блок — вектором:

$$\big(r(i_{\text{шаг}}+N_{\text{Z}}) \quad r(i_{\text{шаг}}+N_{\text{Z}}+1) \quad \ldots \quad r(i_{\text{шаг}}+2N_{\text{Z}}-1)\big), \qquad (2)$$

и так далее. В результате этих преобразований каждый блок преобразуется в такой же размерности комплексный вектор — вектор спектральных линий. Обозначим *j*-ю спектральную линию *i*-го блока через:

$$R(i,j,i_{\text{шаг}}) = \sum_{k=0}^{N_Z-1} r\left(i_{\text{шаг}} + (i-1)N_Z + k\right) \exp\left(-\frac{\imath 2\pi k(j-1)}{N_Z}\right),$$

где $i \in \{1,2,\ldots,k_Z\}$, $j \in \{1,2,\ldots,N_Z\}$, $\imath = \sqrt{-1}$ — мнимая единица.

Далее вычисляется натуральный логарифм от абсолютных значений тех спектральных линий $R(i,j,i_{\text{шаг}})$, номера которых входят в соответствующее множество $\{B(i,1),B(i,2),\ldots,B(i,N_\Gamma)\}$. Если предположить, что $\boldsymbol{r}(i_{\text{шаг}})$ представляет собой переданный сигнал $\boldsymbol{z}'$, искаженный шумом канала, то:

$$R(i,B(i,k),i_{\text{шаг}}) = \frac{1}{\theta} n(i,B(i,k),i_{\text{шаг}}) Z(i,B(i,k)) \left(1 + A(i,k)\, y(m)\right),$$

где $i \in \{1,2,\ldots,k_Z\}$, $k \in \{1,2,\ldots,N_\Gamma\}$, $n(i,B(i,k),i_{\text{шаг}})$ — коэффициент, появившийся из-за шума в канале связи, и наконец:

$$m = \left((i-1) \bmod N_{RZ}\right) + 1 + (k-1)N_{RZ} + \left[\frac{i-1}{N_{RZ}}\right] N_{RZ} N_\Gamma.$$

В таком случае натуральный логарифм абсолютной величины $\left|R(i,B(i,k),i_{\text{шаг}})\right|$ равен сумме:

$$\ln\frac{1}{\theta} + \ln\left|n(i,B(i,k),i_{\text{шаг}})\right| + \ln\left|Z(i,B(i,k))\right| + \ln\left|1 + A(i,k)\, y(m)\right|.$$

Чтобы удалить влияние спектральной линии скрывающего сигнала $\boldsymbol{z}$, демодулятор вычитает величину $\ln\left|Z(i,B(i,k))\right|$ из этой суммы, но только в том случае, когда ему известен скрывающий сигнал $\boldsymbol{z}$. Если $A(i,k) \ll 1$, то последнее слагаемое будет удовлетворять следующему приближенному равенству:

$$\ln\left|\left(1+A(i,k)\,y(m)\right)\right| \approx A(i,k)\,y(m),$$

то есть приближенно будет пропорционально отсчету скрытого сигнала. При выполнении этих условий можно записать, что выполняется приближенное равенство:

$$\ln\left|R\left(i,B(i,k),i_{\text{шаг}}\right)\right| - \ln\left|Z\left(i,B(i,k)\right)\right| \approx$$
$$\approx \ln\frac{1}{\theta} + \ln\left|n\left(i,B(i,k),i_{\text{шаг}}\right)\right| + A(i,k)\,y(m).$$

Как бы то ни было, когда на вход демодулятора поступает вектор отсчетов $\boldsymbol{r}(i_{\text{шаг}})$, тогда на его выходе, при известном скрывающем сигнале z, будет вектор:

$$\boldsymbol{R}_{\text{В}}(i_{\text{шаг}}) = \left(R_{\text{В}}(1,i_{\text{шаг}}) \quad R_{\text{В}}(2,i_{\text{шаг}}) \quad \ldots \quad R_{\text{В}}(k_{\text{Z}}N_{\Gamma},i_{\text{шаг}})\right),$$

где $R_{\text{В}}(j,i_{\text{шаг}}) = \ln\left|R\left(m,B(m,k),i_{\text{шаг}}\right)\right| - \ln\left|Z\left(m,B(m,k)\right)\right|$, тогда как при неизвестном скрывающем сигнале z будет выполняться равенство:

$$R_{\text{В}}(j,i_{\text{шаг}}) = \ln\left|R\left(m,B(m,k),i_{\text{шаг}}\right)\right|,$$

где $j \in \{1,2,\ldots,k_{\text{Z}}N_{\Gamma}\}$, а зависимость между целыми числами m,k,j определяется следующими равенствами:

$$m = \left\lfloor \frac{j-1}{N_{\Gamma}} \right\rfloor + 1,$$
$$k = \left((j-1) \bmod N_{\Gamma}\right) + 1.$$

Однако на этом работа демодулятора не оканчивается: он таким же образом обрабатывает следующие $W-1$ блоков отсчетов. В итоге он обрабатывает множество $\left\{\boldsymbol{r}(i_{\text{шаг}}), \boldsymbol{r}(i_{\text{шаг}}+1),\ldots,\boldsymbol{r}(i_{\text{шаг}}+W-1)\right\}$ блоков отсчетов и формирует множество:

$$\boldsymbol{\Psi}(i_{\text{шаг}}) = \left\{\boldsymbol{R}_{\text{В}}(i_{\text{шаг}}),\ldots,\boldsymbol{R}_{\text{В}}(i_{\text{шаг}}+W-1)\right\},$$

которое передается декодеру канала.

Декодер канала, получив множество $\boldsymbol{\Psi}(i_{\text{шаг}})$, каждый из его элементов обрабатывает одинаковым образом. Поэтому для примера далее показана обработка вектора $\boldsymbol{R}_{\text{B}}(i_{\text{шаг}})$ декодером канала.

Вектор $\boldsymbol{R}_{\text{B}}(i_{\text{шаг}})$ форматируется в матрицу $\boldsymbol{D}(i_{\text{шаг}})$ размером $N_{\text{RZ}} \times (N_{\text{c}} + N_{\text{K}}) N_{\Gamma}$:

$$\boldsymbol{D}(i_{\text{шаг}}) = \begin{pmatrix} D(1,1,i_{\text{шаг}}) & D(1,2,i_{\text{шаг}}) & \cdots & D(1,(N_{\text{c}}+N_{\text{K}})N_{\Gamma},i_{\text{шаг}}) \\ D(2,1,i_{\text{шаг}}) & D(2,2,i_{\text{шаг}}) & \cdots & D(2,(N_{\text{c}}+N_{\text{K}})N_{\Gamma},i_{\text{шаг}}) \\ \vdots & \vdots & \ddots & \vdots \\ D(N_{\text{RZ}},1,i_{\text{шаг}}) & D(N_{\text{RZ}},2,i_{\text{шаг}}) & \cdots & D(N_{\text{RZ}},(N_{\text{c}}+N_{\text{K}})N_{\Gamma},i_{\text{шаг}}) \end{pmatrix},$$

где

$$D(i,j,i_{\text{шаг}}) = R_{\text{B}}(k,i_{\text{шаг}}),$$

где $k \in \{1,2,\ldots,k_{\text{Z}}N_{\Gamma}\}$, а зависимость между целыми числами i,j,k выглядит так:

$$i = \left(\left[\frac{k-1}{N_{\Gamma}} \right] \bmod N_{\text{RZ}} \right) + 1,$$

$$j = \left[\frac{k-1}{N_{\Gamma} N_{\text{RZ}}} \right] N_{\Gamma} + \left((k-1) \bmod N_{\Gamma} \right) + 1.$$

Далее отдельно вычисляются суммы верхней половины строк матрицы $\boldsymbol{D}(i_{\text{шаг}})$ и нижней ее половины, в результате получается два вектора-строки, представляющих собой соответствующие суммы, для удобства назовем их верхней и нижней соответственно. А после этого из верхней суммы вычитается нижняя, что дает вещественный вектор $\boldsymbol{\delta}(i_{\text{шаг}})$, длиной $(N_{\text{c}} + N_{\text{K}}) N_{\Gamma}$:

$$\boldsymbol{\delta}(i_{\text{шаг}}) = \left(\delta(1,i_{\text{шаг}}) \quad \delta(2,i_{\text{шаг}}) \quad \ldots \quad \delta\left((N_{\text{c}}+N_{\text{K}})N_{\Gamma}, i_{\text{шаг}} \right) \right),$$

где

$$\delta(j,i_{\text{шаг}}) = \sum_{i=1}^{N_{\text{RZ}}/2} D(i,j,i_{\text{шаг}}) - \sum_{i=(N_{\text{RZ}}/2)+1}^{N_{\text{RZ}}} D(i,j,i_{\text{шаг}}).$$

Если $\boldsymbol{R}_{\mathrm{B}}\left(i_{\text{шаг}}\right)$ содержит скрытый сигнал, то, выполняя такое вычитание, будет нивелировано влияние слагаемого $\ln\theta^{-1}$, которое в некотором роде является шумовым, так как приемнику оно неизвестно.

Оставшаяся шумовая составляющая, входящая в $\delta\left(j,i_{\text{шаг}}\right)$, может быть представлена в виде следующей разности случайных величин:

$$\sum_{i=1}^{N_{\mathrm{RZ}}/2}\ln\left|n\left(i+m,B\left(i+m,k\right),i_{\text{шаг}}\right)\right|-\sum_{i=\left(N_{\mathrm{RZ}}/2\right)+1}^{N_{\mathrm{RZ}}}\ln\left|n\left(i+m,B\left(i+m,k\right),i_{\text{шаг}}\right)\right|,$$

где

$$m=\left\lfloor\frac{j-1}{N_{\Gamma}}\right\rfloor N_{\mathrm{RZ}},$$

$$k=\left(\left(j-1\right)\bmod N_{\Gamma}\right)+1,$$

где $j\in\left\{1,2,\ldots,\left(N_{\mathrm{c}}+N_{\mathrm{K}}\right)N_{\Gamma}\right\}$.

В обычных условиях можно ожидать, что амплитудные спектры шума для смежных блоков отсчетов аудиосигнала, принимаемого микрофоном, будут приближенно одинаковыми; например, можно ожидать приближенное равенство амплитудных спектров, полученных в результате дискретного преобразования Фурье векторов (1) и (2). Зачастую, время, в течение которого состояние канала не меняется, называют временем когерентности канала. Если предположить, что время когерентности канала не меньше времени передачи последовательности из $N_{\mathrm{RZ}}N_{\mathrm{Z}}$ отсчетов сигнала z', то шумовая составляющая в $\delta\left(j,i_{\text{шаг}}\right)$ будет близка к нулю. При выполнении этого условия будет выполняться следующее приближенное равенство:

$$\delta\left(j,i_{\text{шаг}}\right)\approx\sum_{i=1}^{N_{\mathrm{RZ}}/2}A\left(i+m,k\right)y\left(u\right)-\sum_{i=\left(N_{\mathrm{RZ}}/2\right)+1}^{N_{\mathrm{RZ}}}A\left(i+m,k\right)y\left(u\right),$$

где $j\in\left\{1,2,\ldots,\left(N_{\mathrm{c}}+N_{\mathrm{K}}\right)N_{\Gamma}\right\}$, зависимость между целыми числами m,k,u,j определяется следующими равенствами:

$$m = \left[\frac{j-1}{N_\Gamma} \right] N_{\mathrm{RZ}},$$

$$k = \left((j-1) \bmod N_\Gamma \right) + 1,$$

$$u = \left((i+m-1) \bmod N_{\mathrm{RZ}} \right) + 1 + (k-1) N_{\mathrm{RZ}} + \left[\frac{i+m-1}{N_{\mathrm{RZ}}} \right] N_{\mathrm{RZ}} N_\Gamma .$$

К каждому элементу вектора $\boldsymbol{\delta}(i_{\text{шаг}})$ применяется функция:

$$\operatorname{sign}(a) = \begin{cases} 1, & \text{если } a \geq 0, \\ -1, & \text{если } a < 0, \end{cases}$$

что дает вектор $\boldsymbol{s}(i_{\text{шаг}})$, длиной $(N_{\text{с}} + N_{\text{К}}) N_\Gamma$:

$$\boldsymbol{s}(i_{\text{шаг}}) = \left(s(1, i_{\text{шаг}}) \quad s(2, i_{\text{шаг}}) \quad \ldots \quad s\left((N_{\text{с}} + N_{\text{К}}) N_\Gamma, i_{\text{шаг}} \right) \right),$$

где $s(i, i_{\text{шаг}}) \in \{1, -1\}$.

Для выполнения дальнейших действий вектор $\boldsymbol{s}(i_{\text{шаг}})$ выгодно представить в виде матрицы

$$\boldsymbol{S}(i_{\text{шаг}}) = \begin{pmatrix} S(1,1,i_{\text{шаг}}) & S(1,2,i_{\text{шаг}}) & \cdots & S(1,N_\Gamma,i_{\text{шаг}}) \\ S(2,1,i_{\text{шаг}}) & S(2,2,i_{\text{шаг}}) & \cdots & S(2,N_\Gamma,i_{\text{шаг}}) \\ \vdots & \vdots & \ddots & \vdots \\ S(N_{\text{с}}+N_{\text{К}},1,i_{\text{шаг}}) & S(N_{\text{с}}+N_{\text{К}},2,i_{\text{шаг}}) & \cdots & S(N_{\text{с}}+N_{\text{К}},N_\Gamma,i_{\text{шаг}}) \end{pmatrix},$$

где

$$S(i, j, i_{\text{шаг}}) = s(k, i_{\text{шаг}}),$$

где $k \in \{1, 2, \ldots, (N_{\text{с}} + N_{\text{К}}) N_\Gamma\}$, а зависимость между i, j, k определяется следующими равенствами:

$$i = \left[\frac{k-1}{N_\Gamma} \right] + 1,$$

$$j = \left((k-1) \bmod N_\Gamma \right) + 1.$$

Теперь вычисляется значение взаимно-корреляционной функции между последовательностью Голда и теми последовательностями, которые извлечены из $\boldsymbol{R}_{\text{В}}(i_{\text{шаг}})$ — строками матрицы $\boldsymbol{S}(i_{\text{шаг}})$. Для этого используется матрица $\boldsymbol{G}$, размера $N_{\Gamma}\times 2$, составленная из использованных передатчиком последовательностей Голда $\boldsymbol{g}_1$, $\boldsymbol{g}_2$:

$$\boldsymbol{G}=\begin{pmatrix} G(1,1) & G(1,2) \\ G(2,1) & G(2,2) \\ \vdots & \vdots \\ G(N_{\Gamma},1) & G(N_{\Gamma},2) \end{pmatrix},$$

где $G(i,j)=g(j,i)$. Матрица $\boldsymbol{G}$ слева умножается на матрицу $\boldsymbol{S}(i_{\text{шаг}})$, что дает матрицу $\boldsymbol{Y}(i_{\text{шаг}})$, размера $(N_{\text{с}}+N_{\text{К}})\times 2$,

$$\boldsymbol{Y}(i_{\text{шаг}})=\begin{pmatrix} Y(1,1,i_{\text{шаг}}) & Y(1,2,i_{\text{шаг}}) \\ Y(2,1,i_{\text{шаг}}) & Y(2,2,i_{\text{шаг}}) \\ \vdots & \vdots \\ Y(N_{\text{с}}+N_{\text{К}},1,i_{\text{шаг}}) & Y(N_{\text{с}}+N_{\text{К}},2,i_{\text{шаг}}) \end{pmatrix}=\boldsymbol{S}(i_{\text{шаг}})\boldsymbol{G}.$$

Далее вычисляется вектор:

$$\boldsymbol{\gamma}(i_{\text{шаг}})=\begin{pmatrix}\gamma(1,i_{\text{шаг}}) & \gamma(2,i_{\text{шаг}}) & \ldots & \gamma(N_{\text{с}}+N_{\text{К}},i_{\text{шаг}})\end{pmatrix},$$

где

$$\gamma(i,i_{\text{шаг}})=\begin{cases} 1, & \text{если } Y(i,1,i_{\text{шаг}})<Y(i,2,i_{\text{шаг}}), \\ -1, & \text{если } Y(i,1,i_{\text{шаг}})\geq Y(i,2,i_{\text{шаг}}). \end{cases}$$

Каждая из величин $Y(i,1,i_{\text{шаг}})$, $Y(i,2,i_{\text{шаг}})$ — это есть величина взаимно корреляционной функции, поэтому правило вычисления элементов вектора $\boldsymbol{\gamma}(i_{\text{шаг}})$ опирается на то, что большее из значений $Y(i,1,i_{\text{шаг}})$, $Y(i,2,i_{\text{шаг}})$ указывает на большее количество совпадений между принятыми последовательностями и последовательностями Голда $\boldsymbol{g}_1$, $\boldsymbol{g}_2$ соответственно.

Решение об установлении синхронизации будет положительным, если будут выполняться следующие условия, алгебраически зависящие от величины $i_{\text{шаг}}$ номера шага. Во-первых, должно выполняться неравенство:

$$\rho\left(i_{\text{шаг}}\right) \geq \rho_{\text{К}},$$

где $\rho_{\text{К}}$ — пороговое значение, удовлетворяющее неравенству $\rho_{\text{К}} \leq N_{\text{К}}$; $\rho\left(i_{\text{шаг}}\right)$ — скалярное произведение вектора $\boldsymbol{\beta}$, определяющего использованную при передаче последовательности Касами, и первых $N_{\text{К}}$ элементов вектора $\boldsymbol{\gamma}\left(i_{\text{шаг}}\right)$:

$$\rho\left(i_{\text{шаг}}\right) = \sum_{i=1}^{N_{\text{К}}} \gamma\left(i, i_{\text{шаг}}\right)\beta(i).$$

Во-вторых, значение $\rho\left(i_{\text{шаг}}\right)$ должно быть наибольшим среди всех таких же значений, но полученных из остальных элементов множества $\boldsymbol{\Psi}\left(i_{\text{шаг}}\right)$, то есть должно выполнятся равенство:

$$\rho\left(i_{\text{шаг}}\right) = \max\left\{\rho\left(i_{\text{шаг}}\right), \rho\left(i_{\text{шаг}}+1\right), \ldots, \rho\left(i_{\text{шаг}}+W-1\right)\right\},$$

где величины $\rho\left(i_{\text{шаг}}+j\right)$ при $j \in \left\{0,1,\ldots,W-1\right\}$ получены после обработки соответствующих остальных векторов $\boldsymbol{R}_{\text{В}}\left(i_{\text{шаг}}+j\right) \in \boldsymbol{\Psi}\left(i_{\text{шаг}}\right)$.

В-третьих, сумма:

$$\sum_{i=1}^{N_{\text{К}}}\left(N_{\Gamma} - Y\left(i, \frac{\gamma\left(i, i_{\text{шаг}}\right)+1}{2}+1, i_{\text{шаг}}\right)\right)^2$$

должна быть наименьшей, в сравнении с такими же суммами, но полученными для всех остальных элементов множества $\left\{\rho\left(i_{\text{шаг}}\right), \rho\left(i_{\text{шаг}}+1\right), \ldots, \rho\left(i_{\text{шаг}}+W-1\right)\right\}$. В таком варианте третье условие является независимым от результатов применения двух предыдущих условий, что может привести к увеличению времени установления синхронизации. Поэтому для уменьшения времени может быть выгоден другой вариант третьего условия: выполнять сравнение не со всеми остальными элементами множества $\left\{\rho\left(i_{\text{шаг}}\right), \rho\left(i_{\text{шаг}}+1\right), \ldots, \rho\left(i_{\text{шаг}}+W-1\right)\right\}$, а только с равными $\rho\left(i_{\text{шаг}}\right)$

элементами. Второй вариант третьего условия делает это условие зависимым от результатов применения предыдущих условий: если в результате их применения среди остальных элементов не окажется равных $\rho(i_{\text{шаг}})$, то применение этого условия никак не отразится на принятии решения об установлении синхронизации.

Конечно, даже при выполнении всех этих условий не исключается ситуация наличия нескольких элементов в множестве $\{i_{\text{шаг}},\ldots,i_{\text{шаг}}+W-1\}$, которые будут удовлетворять сразу всем этим условиям; тем не менее выбор будет сделан в пользу $i_{\text{шаг}}$. Если же величина $i_{\text{шаг}}$ не удовлетворяет этим условиям, то декодер канала запрашивает от демодулятора множество $\boldsymbol{\Psi}(i_{\text{шаг}}+1)$, и такая же проверка выполняется уже для множества $\{i_{\text{шаг}}+1,\ldots,i_{\text{шаг}}+W\}$ и так далее.

Когда для величины $i_{\text{шаг}}$ все эти условия выполняются, тогда считается, что синхронизация установлена на блоке отсчетов $\boldsymbol{r}(i_{\text{шаг}})$, то есть приемник будет считать, что этот блок отсчетов содержит переданный сигнал. В таком случае выполняется декодирование последних $N_{\text{с}}$ элементов вектора $\boldsymbol{\gamma}(i_{\text{шаг}})$. Для проведения процесса декодирования вычисляется вектор:

$$\boldsymbol{\mu}(i_{\text{шаг}})=\left(\mu(1,i_{\text{шаг}})\quad \mu(2,i_{\text{шаг}})\quad \ldots\quad \mu(N_{\text{с}},i_{\text{шаг}})\right),$$

составленный из 0 и 1 по следующему правилу:

$$\mu(i,i_{\text{шаг}})=\frac{\gamma(N_{\text{К}}+i,i_{\text{шаг}})+1}{2}.$$

Вектор $\boldsymbol{\mu}(i_{\text{шаг}})$ рассматривается декодером канала как искаженное шумом кодовое слово $(N_{\text{с}},N_{\text{х}})$ БЧХ кода. Этот вектор подвергается БЧХ декодированию, что даст битовый вектор:

$$\boldsymbol{x}'(i_{\text{шаг}})=\left(x'(1,i_{\text{шаг}})\quad x'(2,i_{\text{шаг}})\quad \ldots\quad x'(N_{\text{х}},i_{\text{шаг}})\right),$$

где $x'(i,i_{\text{шаг}})\in\{0,1\}$. Когда синхронизация установлена, а количество произошедших ошибок меньше N_{t}, тогда вектор $\boldsymbol{x}'(i_{\text{шаг}})$ совпадет с переданным информационным вектором $\boldsymbol{x}$.

3. Оценка вероятности ошибки восстановления символов кодового слова, лежащего в основе информационной части скрываемого сигнала. После принятия положительного решения о наличии скрываемого сигнала $\boldsymbol{y}$ в блоке отсчетов $\boldsymbol{r}(i_{\text{шаг}})$ наступает этап декодирования вектора $\boldsymbol{\mu}(i_{\text{шаг}})$. От того, совпадает ли элемент этого вектора с соответствующим элементом кодового слова $\boldsymbol{c}_{\text{БЧХ}}$, зависит правильность восстановления переданного информационного вектора $\boldsymbol{x}$. Поэтому для практического использования предлагаемой методики важно получить оценку вероятности ошибки восстановления элементов кодового слова $\boldsymbol{c}_{\text{БЧХ}}$ или, иными словами, получить оценку вероятности несовпадения элементов вектора $\boldsymbol{\mu}(i_{\text{шаг}})$ с элементами вектора $\boldsymbol{c}_{\text{БЧХ}}$.

Основные параметры предлагаемой в этой работе методики — длина кодового слова RZ кода N_{RZ}, длина кодового слова БЧХ кода N_{c}, количество информационных символов в кодовом слове БЧХ кода N_{x}, исправляющая способность используемого БЧХ кода N_{t}, длина последовательности Касами N_{K}, длина последовательности Голда N_{Γ}, размер блока отсчетов N_{Z}, мощность множества $\boldsymbol{\Psi}(i_{\text{шаг}})$, равная $\left|\boldsymbol{\Psi}(i_{\text{шаг}})\right| = W$, пороговое значение ρ_{K} и, наконец, частота дискретизации F_{s}. Варьируя числовые значения этих параметров, можно влиять на устойчивость к искажающим влияниям канала связи.

Выбор скрывающего сигнала z также имеет значение для надежности передачи. Так, каждый скрывающий сигнал, например, характеризуется своим набором допустимых коэффициентов сил встраивания $A(i,j)$, а также подходящими значениями параметров N_{Z} и N_{RZ}. Выбор значений этих параметров определяется тем, насколько в скрывающем сигнале смежные блоки отсчетов имеют схожие амплитудные спектры.

3.1. Результаты имитационного моделирования. Используем модель канала связи, в которой принятый сигнал — это сумма эхо-сигналов, представляющих собой переданный сигнал, искаженный шумом в частотной области; при этом искажаться будут только спектральные линии, несущие информацию. Отсчет $r(i)$ с выхода

такой модели канала, взятый в i-й момент времени, удовлетворяет следующему равенству:

$$r(i) = r_{\text{эхо}}(i,1) + \sum_{j=2}^{N_{\text{эхо}}} \alpha_{\text{эхо}}(j)\, r_{\text{эхо}}(i,j) + n_{\text{фон}}(i),$$

где i — целое число; $N_{\text{эхо}}$ — максимально возможное количество эхо-сигналов; $r_{\text{эхо}}(i,j)$ — это составляющая отсчета $r(i)$, вносимая j-м эхо-сигналом; $\alpha_{\text{эхо}}(j) \in \{0,1\}$ — коэффициент, указывающий на наличие или отсутствие эхо-сигнала с задержкой на $j-1$ отсчет относительно эхо-сигнала $r_{\text{эхо}}(i,1)$; $n_{\text{фон}}(i)$ — фоновый шум, используемый для моделирования ситуации установления синхронизации и которым можно пренебречь, пока на приемник поступают эхо-сигналы, то есть когда:

$$1 \le i \le k_{\text{Z}} N_{\text{Z}} + \max_{\alpha_{\text{эхо}}(j) \ne 0} \{j\} - 1.$$

Величины $r_{\text{эхо}}(i,j)$ определяются следующим равенством:

$$r_{\text{эхо}}(i,j) = \begin{cases} e_{\text{эхо}}(j)\, r_{\text{эхо,IDFT}}(i,j), & \text{если } 0 \le i-j < k_{\text{Z}} N_{\text{Z}}, \\ 0, & \text{иначе,} \end{cases}$$

где $j \in \{1,2,\ldots,N_{\text{эхо}}\}$, $e_{\text{эхо}}(j) \in [0,1]$ — это доля переданной энергии, которая приходится на j-й эхо-сигнал,

$$r_{\text{эхо,IDFT}}(i,j) = \frac{1}{N_{\text{Z}}} \sum_{k=1}^{N_{\text{Z}}} R_{\text{эхо}}\left(k, \left\lfloor \frac{i-j}{N_{\text{Z}}} \right\rfloor + 1, j\right) \exp\left(\frac{\imath 2\pi (k-1)\left((i-j) \bmod N_{\text{Z}}\right)}{N_{\text{Z}}}\right),$$

где $R_{\text{эхо}}(k,l,j)$ — это комплексное число, определяющее k-ю спектральную линию l-го блока j-го эхо-сигнала. Величины $R_{\text{эхо}}(k,l,j)$ определяются следующим образом:

$$R_{\text{эхо}}(k,l,j) = \begin{cases} Z\left(l, B(l,u)\right)\left(1 + A(l,u)\left(y(m) + n_{\text{блок}}(u,l,j)\right)\right), & \text{если } k = B(l,u), \\ Z(l,k), & \text{иначе,} \end{cases}$$

когда $u \in \{1,2,\ldots,N_\Gamma\}$ и $k \in \{1,2,\ldots,N_Z/2\}$, но

$$R_{\text{эхо}}(k,l,j) = \begin{cases} \left(R_{\text{эхо}}(N_Z - k + 2, l, j)\right)^*, & \text{если } k \neq (N_Z/2)+1, \\ Z(l,k), & \text{иначе,} \end{cases}$$

когда $k \in \{(N_Z/2)+1, (N_Z/2)+2,\ldots,N_Z\}$; в обоих равенствах $l \in \{1,2,\ldots,k_Z\}$; величины A, B и m были определены ранее при указании правила получения спектральных линий Z' переданного сигнала $\boldsymbol{z}'$; $n_{\text{блок}}(u,l,j)$ — это шум в $B(l,u)$-й спектральной линии l-го блока j-го эхо-сигнала. Шум $n_{\text{блок}}(u,l,j)$ отсутствует в тех спектральных линиях $R_{\text{эхо}}(k,l,j)$, которые не несут элемента скрываемого сигнала $\boldsymbol{y}$. Величины $n_{\text{блок}}(u,l,j)$ определяются так:

$$n_{\text{блок}}(u,l,j) = n\left(\left\lfloor \frac{l-1}{N_{RZ}} \right\rfloor N_\Gamma + u, j\right),$$

где $n(\cdot, j)$ — независимые одинаково распределенные гауссовы случайные величины с нулевым математическим ожиданием и дисперсией σ^2.

Особенностью этой модели канала является то, что аддитивный шум $n_{\text{блок}}(u,l,j)$ остается неизменным в каждых N_{RZ} блоках спектральных линий, а значит, он сохраняется в течение $N_{RZ}N_Z/F_s$ секунд. Эту модель аудиоканала можно сравнить с моделью беспроводного канала с независимыми блоковыми замираниями [14, 15], когда замирания в канале имеют блоковый характер — сохраняются в течение времени когерентности канала. Таким образом, если использовать ту же терминологию, то в предлагаемой модели дискретного аудиоканала эхо-сигналы подвергаются независимым блоковым замираниям со временем когерентности, равным времени взятия $N_{RZ}N_Z$ отсчетов, а именно столько времени требуется на передачу $N_{RZ}N_\Gamma$ элементов скрываемого сигнала $\boldsymbol{y}$.

В этой модели отношение сигнал-шум SNR для отдельного эхо-сигнала можно посчитать следующим образом. Так как элемент скрываемого сигнала всегда имеет одинаковое абсолютное значение

$|y(\cdot)|=1$, то при известном приемнику скрывающем сигнале z можно определить отношение сигнал-шум (выраженное в дБ) SNR на спектральную линию, опираясь на величину дисперсии σ^2:

$$\mathrm{SNR}=10\lg\left(\frac{1}{\sigma^2}\right).$$

Основные параметры канала: максимально возможное количество $N_{\text{эхо}}$ эхо-сигналов; двоичный вектор:

$$\boldsymbol{\alpha}_{\text{эхо}}=\left(1 \quad \alpha_{\text{эхо}}(2) \quad \ldots \quad \alpha_{\text{эхо}}(N_{\text{эхо}})\right),$$

определяющий существование соответствующего эхо-сигнала; вещественный вектор:

$$\boldsymbol{e}_{\text{эхо}}=\left(e_{\text{эхо}}(1) \quad e_{\text{эхо}}(2) \quad \ldots \quad e_{\text{эхо}}(N_{\text{эхо}})\right),$$

элементы которого — это доли переданной энергии, переносимые соответствующими эхо-сигналами, величина дисперсии σ^2 шума. Остальные параметры, использованные при описании модели канала, определяются по параметрам передаваемого вектора z'.

Предположим, что распространению звука до микрофона ничего не мешает, а также предположим, что в области распространения звука нет никаких отражающих его объектов, и, наконец, предположим, что расстояние между микрофоном и динамиком такое, что можно пренебречь ослаблением звука. В таком случае микрофона достигнет только один эхо-сигнал, энергия которого приблизительно равна переданной. Поэтому параметры модели канала будут иметь следующие значения: $N_{\text{эхо}}=1$; $\alpha_{\text{эхо}}(1)=1$, остальные $\alpha_{\text{эхо}}(j)=0$; $e_{\text{эхо}}(1)=1$, остальные $e_{\text{эхо}}(j)=0$. В таком случае отсчет сигнала на выходе канала, взятый в *i*-й момент времени, будет удовлетворять следующему равенству:

$$r(i)=r_{\text{эхо}}(i,1)+n_{\text{фон}}(i),$$

где $n_{\text{фон}}(i)$ — фоновый шум, представляющий собой независимые одинаково распределенные нормальные случайные величины с математическим ожиданием, равным нулю, и дисперсией, равной единице, когда $k_{\text{Z}}N_{\text{Z}}<i\le 0$, но $n_{\text{фон}}(i)=0,$ когда $1\le i\le k_{\text{Z}}N_{\text{Z}}$.

В таблице 1 приводятся результаты имитационного моделирования представленной методики для случая, когда канал описывается этой моделью. Моделирование выполнялось с фоновым шумом перед приемом и после приема переданного сигнала, чтобы промоделировать процесс установления синхронизации. По результатам моделирования, полученным, когда скрывающий сигнал z неизвестен, видно, что, несмотря на уменьшение отношения сигнал-шум, вероятность ошибки не уменьшается, а колеблется возле некоторой величины; это происходит из-за того, что сам скрывающий сигнал z становится шумом и мешает восстановлению переданных символов. Когда же скрывающий сигнал z известен приемнику, тогда вероятность ошибки восстановления меньше 10^{-2} уже при отношении сигнал-шум -28 дБ.

Таблица 1. Сводная таблица результатов использования предлагаемой методики для модели канала с одним эхо-сигналом

Отношение сигнал-шум SNR, дБ	Вероятность ошибки восстановления символа переданного кодового слова $c_{\text{БЧХ}}$	
	Первый вариант третьего условия	Второй вариант третьего условия
Скрывающий сигнал известен приемнику		
-40	0.262	0.264
-35	0.131	0.13
-34	0.104	0.1
-33	0.08	0.075
-32	0.06	0.056
-31	0.035	0.037
-30	0.023	0.023
-29	0.011	0.012
-28	0.006	0.006
-27	0.002	0.003
-26	0.001	0.0006
-25	0.0003	0.0002
Скрывающий сигнал не известен приемнику		
-25	0.265	0.225
-20	0.083	0.081
-19	0.069	0.067
-18	0.068	0.057
-17	0.05	0.052
-16	0.043	0.046
-15	0.042	0.038
-14	0.039	0.039
-13	0.037	0.037
-12	0.037	0.04
-11	0.043	0.043

Параметры методики: $N_{RZ} = 20$, $N_c = 63$, $N_x = 7$, $N_t = 15$, $N_K = 255$, $N_\Gamma = 127$, $N_Z = 256$, ρ_K=100 , W=1500 . Результаты, приведенные в этой таблице, учитывают вероятность установления синхронизации.

3.2. Результаты натурных экспериментов. В качестве значения ρ_K , используемого методикой как порогового при вынесении решения об установлении синхронизации, будем использовать число 101. Таким образом, если в процессе передачи через канал изменятся более 77 символов из 255 символов последовательности Касами, то выбранный порог не будет превышен.

Остальные параметры методики будут такими: $N_c = 63$, $N_K = 255$, $N_\Gamma = 127$, $N_Z = 2(N_\Gamma + 1) = 256$, $F_s = 32000$ Гц, $W = 1500$. Величину N_{RZ} при проведении экспериментов будем варьировать. Для примера рассчитаем, сколько времени потребуется для передачи скрытого сигнала с этими параметрами и $N_{RZ} = 20$. Так, для встраивания такого скрываемого сигнала потребуется модифицировать:

$$k_Z = (N_c + N_K) N_{RZ} = 6360$$

непересекающихся блок отсчетов, при этом каждый блок состоит из $N_Z = 256$ отсчетов. Следовательно, во времени, при частоте дискретизации равной $F_s = 32$ кГц, потребуется:

$$\frac{k_Z N_Z}{32000} = 50.88$$

секунд на передачу скрываемого сигнала $\boldsymbol{y}$.

Используем следующую аппаратуру для выполнения натурного эксперимента. В качестве динамиков будем использовать наушники Sennheiser MX170. Микрофоном будет Philips SBC ME570. И, наконец, аудиокарта ASUS Xonar Essence STX/A.

Запись будет продолжаться некоторое время и после окончания передачи аудиосигнала. Удлинение времени записи должно быть достаточным, чтобы передаваемый аудиосигнал распространился от динамика до микрофона. Запись будем выполнять в нешумном помещении.

Конечно, в зависимости от шума в реальном канале, а также от выбранного скрывающего сигнала z, значения вероятности ошибки восстановления каждого отдельного случая будут своими. Тем не менее содержимое таблицы 2, полученное в результате ряда натурных экспериментов, дает некоторую оценку того, насколько знание скрывающего сигнала приемником и вычитание его из принятого сигнала может повлиять на вероятность ошибки восстановления символа кодового слова. Например, при $N_{\mathrm{RZ}} = 20$ вероятность ошибки восстановления меньше более чем в два раза, когда скрывающий сигнал z известен приемнику, в сравнении со случаем, когда он не известен приемнику.

Таблица 2. Сводная таблица результатов натурных экспериментов по оценке вероятности ошибки восстановления символов кодового слова при различных значениях параметров методики

Значение N_{RZ}	4	8	12	16	20
Вероятность ошибки восстановления символа переданного кодового слова $c_{\text{БЧХ}}$ (скрывающий сигнал известен приемнику)	0.16	0.1	0.06	0.05	0.03
Вероятность ошибки восстановления символа переданного кодового слова $c_{\text{БЧХ}}$ (скрывающий сигнал не известен приемнику)	0.2	0.19	0.1	0.12	0.09

Скрывающий сигнал — речь. Вещание ведется в нешумном помещении. Расстояние между микрофоном и динамиком ≈ 2.5 см. Мощность динамика 40% от номинальной. Значения основных параметров: ρ_{K}=101, $W = 1500$, $N_{\Gamma} = 127$, N_{Z}=256, N_{K}=255, F_{s}=32 кГц.

4. Заключение. В этой работе предложена методика построения, внедрения и восстановления скрытого сигнала при передаче через воздушный аудиоканал. Методика имеет следующие характерные черты. Во-первых, ее можно использовать даже при передаче стегоаудиосигнала через воздушный аудиоканал. Во-вторых, внедрение и восстановление скрываемого сигнала возможно и в том случае, когда скрывающий сигнал является речевым сигналом. В-третьих, синхронизационная часть скрываемого сигнала во времени передается отдельно. В-четвертых, внедрение скрываемого сигнала выполняется в неперекрывающиеся блоки отсчетов скрывающего сигнала. В-пятых, используется правило вынесения решения об установлении синхронизации, основанное на проверке трех условий, которые обычно ликвидируют ситуации неоднозначного выбора.

Для оценки вероятности ошибки восстановления символов кодового слова предложена модель воздушного аудиоканала. Результаты имитационного моделирования, полученные с ее помощью, для различных значений отношения сигнал–шум позволяют оценить требуемую исправляющую способность кода для использования при построении информационной части скрываемого сигнала. Натурные эксперименты показывают применимость предлагаемой методики для передачи в реальном воздушном аудиоканале.

Литература

1. *Petitcolas F.A.P., Anderson R.J., Kuhn M.G.* Information hiding – a survey // Proceedings of the IEEE. 1999. vol. 87. no. 7. pp. 1062–1078.
2. *Hanspach M., Goetz M.* On covert acoustical mesh networks in air // Journal of Communications. 2013. vol. 8. no. 11. pp. 758–767.
3. *Мирончиков Е.Т., Гофман М.В., Вихарев С.О.* Методика построения цифровых водяных знаков, устойчивых к сбоям синхронизации // Известия Петербургского Университета Путей Сообщения. 2016. Т. 13. Вып. 1(46). С. 60–67.
4. *Wu S., Huang J., Huang D., Shi Y. Q.* Efficiently self-synchronized audio watermarking for assured audio data transmission // IEEE Transactions on Broadcasting. 2005. vol. 51. no. 1. pp. 69–76.
5. *Hua G. et al.* Twenty years of digital audio watermarking – a comprehensive review // Signal Processing. 2016. vol. 128. pp. 222–242.
6. *Roy S., Sarkar N., Chowdhury A.K., Iqbal S.M.A.* An efficient and blind audio watermarking technique in DCT domain // 18th International Conference on Computer and Information Technology (ICCIT). IEEE. 2015. pp. 362–367.
7. *Cui D., Gong Y., Liu M.* Design and Performance Evaluation of Robust Digital Audio Watermarking under Low Bits Rates // 2nd International Conference on Information Science and Control Engineering (ICISCE). IEEE. 2015. pp. 194–197.
8. *Zhang Z., Wu X.* An Audio Covert Communication System for Anolog Channels // 2010 International Conference on Electrical and Control Engineering (ICECE). IEEE. 2010. pp. 3279–3282.
9. *Torrieri D.* Principles of spread-spectrum communication systems. Springer. 2015. 641 p.
10. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки: монография // М.: Мир. 1976. 594 с.
11. *Кудряшов Б.Д.* Основы теории кодирования: учеб. пособие // СПб.: БХВ-Петербург. 2016. 400 с.
12. ГОСТ Р 54711-2011: Звуковое вещание цифровое. Кодирование сигналов звукового вещания с сокращением избыточности для передачи по цифровым каналам связи. MPEG-1 часть III (MPEG-1 audio) // М.: Стандартинформ. 2014. 169 с.
13. *Spanias A., Painter T., Atti V.* Audio signal processing and coding // John Wiley & Sons. 2007. 464 p.
14. *Collins A., Polyanskiy Y.* Dispersion of the coherent MIMO block-fading channel // IEEE International Symposium on Information Theory (ISIT). IEEE. 2016. pp. 1068–1072.
15. *Гофман М.В.* Помехоустойчивое пространственное блоковое кодирование // LAP Lambert Academic Publishing. 2013. 176 с.

Гофман Максим Викторович — к-т техн. наук, доцент кафедры информатики и информационной безопасности, Петербургский государственный университет путей сообщения Императора Александра I. Область научных интересов: системы связи, системы передачи данных. Число научных публикаций — 10. maxgof@gmail.com; Московский пр., 9, Санкт-Петербург, 190031; р.т.: +7(812)310-34-72, Факс: +7(812)570-76-68.

DOI 10.15622/sp.51.5

M.V. GOFMAN

A METHOD OF HIDDEN DATA TRANSMISSION IN COMMUNICATION VIA AIR AUDIO CHANNEL

Gofman M.V. **A Method of Hidden Data Transmission in Communication via Air Audio Channel.**

Abstract. This article proposes a method for secure data transmission in the audible domain of the frequency spectrum of the air environment. Specifically, it proposes the method of construction, embedding, extraction and recovery of a hidden signal transmitted through the air audio channel. The hidden signal consists of two parts. One part is used for synchronization, and the other one is used for carrying information. The basis of the synchronization part is the Kasami sequence, whereas the basis of the information part is a code word of the binary BCH code. Both parts of the hidden signal are obtained through special encoding of their binary elements. The encoding uses Gold sequences and RZ codes. Speech or music are used as a carrier signal. The hidden signal is embedded in the frequency domain of the carrying signal. The embedding is based on amplitude modulation of individual spectral components of the carrying signal. The article discusses the possibility of restoring the hidden signal after the transmission of the stego-audio signal through the air audio channel. The article presents the results of simulation modeling and field experiments of transmission of the stego-audio signal through the air audio channel.

Keywords: audio signal, steganography, air audio channel, air-gap, Kasami sequence, Gold sequence, BCH code, RZ code.

References

1. Petitcolas F.A.P., Anderson R.J., Kuhn M.G. Information hiding – a survey. Proceedings of the IEEE. 1999. vol. 87. no. 7. pp. 1062–1078.
2. Hanspach M., Goetz M. On covert acoustical mesh networks in air. *Journal of Communications*. 2013. vol. 8. no. 11. pp. 758–767.
3. Mironchikov E.T., Gofman M.V., Viharev S.O. [A method for building synchronization fault-tolerant digital watermarks]. *Izvestija Peterburgskogo Universiteta Putej Soobshhenija – Proceedings of Petersburg Transport University*. 2016. vol. 13. no. 1(46). pp. 60–67. (In Russ.).
4. Wu S., Huang J., Huang D., Shi Y. Q. Efficiently self-synchronized audio watermarking for assured audio data transmission. *IEEE Transactions on Broadcasting*. 2005. vol. 51. no. 1. pp. 69–76.
5. Hua G. et al. Twenty years of digital audio watermarking – a comprehensive review. *Signal Processing*. 2016. vol. 128. pp. 222–242.
6. Roy S., Sarkar N., Chowdhury A. K., Iqbal S. M. A. An efficient and blind audio watermarking technique in DCT domain. 18th International Conference on Computer and Information Technology (ICCIT). IEEE. 2015. pp. 362–367.
7. Cui D., Gong Y., Liu M. Design and Performance Evaluation of Robust Digital Audio Watermarking under Low Bits Rates. 2nd International Conference on Information Science and Control Engineering (ICISCE). IEEE. 2015. pp. 194–197.
8. Zhang Z., Wu X. An Audio Covert Communication System for Anolog Channels // 2010 International Conference on Electrical and Control Engineering (ICECE). IEEE. 2010. pp. 3279–3282.
9. Torrieri D. Principles of spread-spectrum communication systems. Springer. 2015. 641 p.

10. Peterson W.W., Weldon E.J. *Error-correcting codes.* Cambridge. MA: MIT. 1972. 571 p. (Russ. ed.: Piterson U., Ujeldon Je. *Kody, ispravljajushhie oshibki.* M: Mir. 1976. 594 p.).
11. Kudrjashov B.D. Osnovy teorii kodirovanija [Basics of Coding Theory]. SPb.: BHV-Peterburg. 2016. 400 p. (In Russ.).
12. GOST R 54711-2011 [Digital sound broadcasting. Coding of sound broadcasting signals with redundancy for transfer on digital communication channels. MPEG-1 part III (MPEG-1 audio)]. M.: Standartinform. 2014. 169 p. (In Russ.).
13. Spanias A., Painter T., Atti V. Audio signal processing and coding. John Wiley & Sons. 2007. 464 p.
14. Collins A., Polyanskiy Y. Dispersion of the coherent MIMO block-fading channel. IEEE International Symposium on Information Theory (ISIT). IEEE. 2016. pp. 1068–1072.
15. Gofman M.V. Pomehoustojchivoe prostranstvennoe blokovoe kodirovanie [Noiseproof space-time block coding]. LAP Lambert Academic Publishing. 2013. 176 p. (In Russ.).

Gofman Maksim Viktorovich — Ph.D., associate professor of informatics and information security department, Emperor Alexander I st. St. Petersburg State Transport University. Research interests: communication systems, systems of data transmission. The number of publications — 10. maxgof@gmail.com; 9, Moskovsky pr., Saint Petersburg, 190031; office phone: +7(812)310-34-72, Fax: +7(812)570-76-68.