

М.В. ГОФМАН, А.А. КОРНИЕНКО
**ПРЕДЕЛЬНЫЕ БИПОЛЯРНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ
ДЛЯ РОБАСТНОГО МАРКИРОВАНИЯ ЦИФРОВЫХ
АУДИОСИГНАЛОВ ПО МЕТОДУ ЛОСКУТА**

Гофман М.В., Корниенко А.А. Пределные биполярные последовательности для робастного маркирования цифровых аудиосигналов по методу лоскута.

Аннотация. Обеспечение устойчивости маркирования цифровых аудиосигналов в условиях действия помех, различных преобразований и возможных атак является актуальной проблемой. Одним из наиболее используемых и достаточно устойчивых методов маркирования является метод лоскута. Его робастность обеспечивается применением расширяющих биполярных числовых последовательностей при формировании и внедрении маркера в цифровой аудиосигнал и корреляционного детектирования при обнаружении и извлечении маркерной последовательности. Анализ свойств биполярных последовательностей, реализуемых в методе лоскута, показал, что абсолютные значения величины отношения максимума автокорреляционной функции (АКФ) к её минимуму для расширяющих биполярных последовательностей и расширенных маркерных последовательностей, используемых при традиционном маркировании, с высокой точностью приближаются к 2. Это позволило сформулировать критерии для поиска специальных расширяющих биполярных последовательностей, обладающих улучшенными корреляционными свойствами и большей устойчивостью. В статье разработан математический аппарат для поиска и построения предельных расширяющих биполярных последовательностей, используемых при решении задачи робастного маркирования цифровых аудиосигналов по методу лоскута. Пределные биполярные последовательности определены как последовательности, у которых автокорреляционные функции обладают максимально возможными по абсолютному значению отношениями максимума к минимуму. Сформулированы и доказаны теоремы и следствия из них: о существовании верхней границы минимальных значений автокорреляционных функций предельных биполярных последовательностей и о значениях первого и второго лепестков АКФ. На этой основе дано строгое математическое определение предельных биполярных последовательностей. Разработаны метод поиска полного множества предельных биполярных последовательностей на основе рационального перебора и метод построения предельных биполярных последовательностей произвольной длины с использованием порождающих функций. Представлены результаты компьютерного моделирования по оценке значений абсолютной величины отношения максимума к минимуму автокорреляционной и взаимной корреляционных функций исследуемых биполярных последовательностей для слепого приема. Показано, что предложенные предельные биполярные последовательности характеризуются лучшими корреляционными свойствами в сравнении с традиционно используемыми биполярными последовательностями и обладают большей устойчивостью.

Ключевые слова: стеганография, аудиосигнал, метод лоскута, маркирование цифровых объектов, биполярная последовательность, корреляционная функция.

1. Введение. Широкое распространение и использование цифрового аудиоконтента остро ставит вопрос о необходимости его стеганографической защиты для доказательства авторского права,

права собственности, возможности отслеживания сделок и оплаченной рекламы, контроля целостности и решения других задач [1, 2]. Это, в свою очередь, требует развития робастных методов цифрового маркирования и построения аудиостегосистем, устойчивых к атакам, действию помех и преобразованиям. Целью возможных атак может быть удаление, разрушение или нелегитимное извлечение внедренного цифрового маркера (цифрового водяного знака).

Существует достаточно большое количество робастных методов маркирования цифровых аудиосигналов, связанных с погружением цифровых водяных знаков или скрытием передаваемой аудиоинформации [1, 2]. Одним из наиболее используемых и достаточно устойчивых является метод лоскута (от англ. patchwork). Этот метод представляет собой статистический метод маркирования цифровых объектов [3, 4, 5]. Принцип маркирования методом лоскута состоит в следующем. В цифровом объекте в соответствии со стегоключом случайным образом выбирается пара одинаково распределенных элементов. Затем амплитуда одного элемента из каждой пары увеличивается на определенную величину, тогда как амплитуда другого элемента этой пары уменьшается на такую же величину. Путем такой модификации амплитуд можно закодировать, например, один бит внедряемого цифрового маркера (цифрового водяного знака). Этот процесс случайного выбора пар с последующим изменением амплитуд элементов повторяется достаточное количество раз для того, чтобы обеспечивалась статистическая устойчивость внедренного маркера к помехам и предполагаемым атакам на маркированный цифровой объект. Реализация метода лоскута основана на применении биполярных последовательностей.

Метод лоскута и принципы, лежащие в его основе, широко используются для маркирования цифровых аудиосигналов (речь и музыка), цифровых изображений и видео, а также в кодах компьютерных программ [6 – 16]. При этом робастность маркирования методом лоскута обеспечивается применением специальных биполярных последовательностей при формировании и внедрении маркера в покрывающий объект – цифровой аудиосигнал, и корреляционного детектирования при обнаружении и извлечении маркера (выделении информационных битов маркерной последовательности).

В последние годы получило широкое развитие маркирование цифровых аудиосигналов методом лоскута с использованием специальных расширяющих биполярных последовательностей для решения задач, связанных с использованием цифровых водяных

знаков, скрытием передаваемой аудиоинформации, позиционированием маркированными аудиосигналами нелегитимного приемного устройства. В статьях [17–21] изложен традиционный подход к маркированию цифровых аудиосигналов по методу лоскута в частотной области Фурье, когда маркированный аудиосигнал предполагается передавать через воздушный аудиоканал или радиоканал. В этом случае маркер формируется из псевдослучайной биполярной числовой последовательности с почти равномерным распределением элементов (1 и -1) и из расширяющей ее последовательности определенного вида. При этом корреляционные свойства расширенной маркерной последовательности практически не зависят от соответствующих свойств исходной последовательности, а определяются корреляционными свойствами расширяющей биполярной последовательности (РБП). Одно из свойств автокорреляционной функции (АКФ) расширяющей биполярной последовательности – абсолютное значение величины отношения максимума АКФ к её минимуму при этих условиях с высокой точностью приближается к 2. Это позволяет использовать данное свойство как критерий при выборе специальных РБП и построении на их основе специальных маркерных последовательностей с улучшенными корреляционными свойствами, повышающими качество детектирования и устойчивость маркирования цифровых аудиосигналов.

Другие особенности и свойства АКФ расширенной маркерной последовательности накладывают ограничения на выбор расширяющей последовательности при решении задачи позиционирования маркированными аудиосигналами приемного устройства. В работах [21, 22] показано, что для этой задачи наилучшая длина расширяющей последовательности равна двум разрядам. Увеличение длины расширяющей последовательности негативно сказывается на точности определения местоположения нелегитимного приемника с помощью приема и передачи маркированных аудиосигналов.

В статьях [23, 24] предлагается метод маркирования аудиосигналов с использованием выбранных из эвристических соображений расширяющих биполярных последовательностей с улучшенными корреляционными свойствами, повышающими качество детектирования, которым свойственно большее, чем два, по абсолютному значению отношение максимума ее АКФ к минимуму этой функции. Повышение качества детектирования происходит вследствие того, что увеличение абсолютного значения этой величины

обычно приводит к увеличению устойчивости к атакам, и, в частности, к атаке аддитивным белым гауссовским шумом при использовании корреляционного детектора.

В связи с этим представляется актуальной задача разработки математического аппарата построения таких специальных биполярных последовательностей с улучшенными корреляционными свойствами, у которых по абсолютному значению отношение максимума автокорреляционной функции к её минимуму будет максимально возможным.

Целью данной работы является разработка методов поиска и построения нового класса последовательностей – предельных расширяющих биполярных последовательностей, у которых автокорреляционные функции обладают максимально возможными по абсолютному значению отношениями максимума к минимуму, и применение которых повышает устойчивость цифрового маркирования.

Для достижения этой цели:

- Исследованы особенности АКФ расширяющих биполярных последовательностей и сформированных на их основе маркерных последовательностей, используемых при традиционном маркировании цифровых аудиосигналов. Предложены специальные функции для построения РБП с улучшенными корреляционными свойствами для робастного маркирования и предельных биполярных последовательностей, АКФ которых обладают максимально возможными по абсолютному значению отношениями максимума к минимуму. Сформулированы и доказаны теоремы и следствия из них о существовании верхней границы минимальных значений автокорреляционных функций таких последовательностей и о значениях первого и второго лепестков АКФ. На этой основе дано строгое математическое определение предельных биполярных последовательностей.

- Разработаны два метода поиска и построения предельных биполярных последовательностей: с использованием рационального перебора и на основе введенных порождающих функций, функционально связанных с такими последовательностями.

- Проведено компьютерное моделирование по оценке значений абсолютной величины отношения максимума к минимуму автокорреляционной и взаимной корреляционных функций исследуемых биполярных последовательностей для наихудших условий извлечения маркерных последовательностей (слепой прием).

В этом случае искажающим воздействием (шумом) становился сам покрывающий цифровой аудиосигнал.

Теоретический вклад настоящей работы в решение задачи робастного маркирования цифровых аудиосигналов по методу лоскута заключается в разработке математического аппарата для построения предельных расширяющих биполярных последовательностей с улучшенными корреляционными свойствами, более устойчивых к действию помех и искажающих воздействий при обнаружении и извлечении цифровой маркерной последовательности.

2. Традиционное маркирование с использованием расширяющих биполярных последовательностей. Традиционно маркер формируется из псевдослучайной биполярной числовой последовательности:

$$\mathbf{a} = (\alpha_1, \alpha_2, \dots, \alpha_{N_a}), \alpha_i \in \{1, -1\}, \quad (1)$$

где N_a – длина последовательности. После формирования последовательности \mathbf{a} её элементы расширяются путем подстановки вместо них последовательности следующего вида:

$$\gamma = \left(\underbrace{1, \dots, 1}_{N_n}, \underbrace{-1, \dots, -1}_{N_n} \right), \quad (2)$$

где N_n – положительное целое число, определяющее половину длины расширяющей последовательности.

Затем формируется маркерная последовательность:

$$\mathbf{m} = (m_1, m_2, \dots, m_{2N_n N_a}) = \mathbf{a} \otimes \gamma, \quad (3)$$

где \otimes – оператор кронекерова произведения,

$$m_i = (-1)^{\lfloor \frac{i-1}{N_n} \rfloor \bmod 2} \alpha_{\lfloor \frac{i-1}{2N_n} \rfloor + 1}, \quad (4)$$

где $\lfloor x \rfloor$ – ближайшее целое, меньшее или равное числу x .

Прежде чем, перейти к анализу корреляционных свойств маркерной последовательности, определим АКФ произвольной вещественной последовательности:

$$\mathbf{p} = (p_1, p_2, \dots, p_L), \quad (5)$$

как дискретную функцию от целочисленной переменной k , удовлетворяющую следующему равенству:

$$f_{\text{АКФ}}(\mathbf{p}, k) = \sum_{i=1}^L p_i p_{i-k}, \quad (6)$$

где числа p_l являются элементами вещественной последовательности \mathbf{p} , когда индекс $l \in \{1, 2, \dots, L\}$, но для сокращения обозначений будем считать $p_l = 0$, когда индекс $l \notin \{1, 2, \dots, L\}$.

Использование расширяющих последовательностей γ вида, описываемого равенством (2), приводит к тому, что у АКФ сформированной маркерной последовательности \mathbf{m} в соответствии с (3) появляются большие по амплитуде отрицательные значения. Это уменьшает абсолютное значение отношения максимума АКФ к её минимуму по сравнению с таким же значением АКФ для биполярной последовательности \mathbf{a} . При этом абсолютное значение этого отношения оказывается приблизительно равным два в тех случаях, когда исходная псевдослучайная последовательность \mathbf{a} генерируется таким образом, что вероятности появления 1 и -1 оказываются почти равными.

Это свойство АКФ биполярной последовательности, используемой при традиционном маркировании, можно обосновать с помощью следующих рассуждений. Когда в псевдослучайных биполярных последовательностях \mathbf{a} вероятности появления 1 и -1 приблизительно одинаковые, тогда можно получить оценку максимального падения АКФ маркерной последовательности \mathbf{m} , опираясь на среднее значение АКФ маркерной последовательности \mathbf{m} , вычисленное для единичного сдвига от центрального значения АКФ маркерной последовательности \mathbf{m} . Действительно, значение АКФ маркерной последовательности \mathbf{m} , получаемое при единичном сдвиге маркерной последовательности \mathbf{m} относительно центрального значения АКФ, включает в себя все подстановочные (расширяющие)

последовательности $(1, -1)$, значит, падение значения АКФ окажется максимальным. Среднее значение на отдельную подстановку (в зависимости от результатов соседних подстановок) можно вычислить, исходя из значений для каждого из возможных вариантов, составляющих значения АКФ. С учетом симметрии АКФ возможны два варианта составляющих значения, как показано на рисунке 1. Без учета – четыре варианта составляющих, два из которых будут давать такой же вклад в значение АКФ, какой дают элементы другой пары составляющих.

$$\begin{array}{cc}
 \begin{array}{c} \times \\ \hline \end{array} \begin{array}{c} (\dots, 1, -1, \dots) \\ (\dots, -1, 1, \dots) \end{array} & \begin{array}{c} \times \\ \hline \end{array} \begin{array}{c} (\dots, 1, -1, \dots) \\ (\dots, 1, 1, \dots) \end{array} \\
 \dots, \underbrace{-1, -1}, \dots & \dots, \underbrace{1, -1}, \dots \\
 \text{вклад в} & \text{вклад в} \\
 \text{значение} & \text{значение} \\
 \text{АКФ} & \text{АКФ} \\
 \text{равен -2} & \text{равен 0}
 \end{array}$$

Рис. 1. Составляющие значения АКФ

Так как таких составляющих будет в среднем одинаковое количество, то, исходя из них, среднее арифметическое значение оказывается равным единице со знаком минус, что указывает на падение центрального значения АКФ в 2 раза. То есть, если центральное значение АКФ псевдослучайной последовательности после подстановки расширяющей последовательности $(1, -1)$, равно X , то минимальное значение в среднем будет равно $-X/2$.

Например, последовательность Баркера длиной 7:

$$\mathbf{a} = (1, 1, 1, -1, -1, 1, -1), \tag{7}$$

после подстановки последовательности $\gamma = (1, -1)$, станет маркерной последовательностью:

$$\mathbf{m} = (1, -1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1), \tag{8}$$

у которой максимум АКФ равен 14, а минимум -7 и, следовательно, по абсолютной величине их отношение равно $|14 / (-7)| = 2$.

Исходя из этих рассуждений и результатов проведенного моделирования, можно сделать следующие выводы относительно особенностей и свойств АКФ маркерной (расширенной) последовательности, сформированной в соответствии с равенствами (1)–(3). При традиционном маркировании значение этой АКФ оказывается минимальным на «расстоянии» одного сдвига относительно центрального значения, что связано с длиной расширяющей последовательности $(1, -1)$. Максимальное значение АКФ маркерной последовательности m зависит от длины расширяемой псевдослучайной последовательности α и от длины расширяющей последовательности $(1, -1)$. Тогда как минимальное значение АКФ маркерной последовательности m тем ближе по абсолютному значению к половине центрального значения, чем больше длина псевдослучайной последовательности α и чем более равновероятным является появление 1 и -1 в ней. При выполнении последнего условия, когда в качестве расширяемой последовательности α используется псевдослучайная биполярная последовательность, у которой вероятности появления 1 и -1 почти равны, АКФ расширенной последовательности m будет определяться корреляционными свойствами расширяющей последовательности γ , а не корреляционными свойствами расширяемой последовательности α . И еще одно важнейшее свойство АКФ – абсолютное значение величины отношения максимума АКФ к её минимуму с высокой точностью приближается к 2. Это позволяет сформулировать критерии для поиска расширяющих биполярных последовательностей γ , обладающих улучшенными корреляционными свойствами и большей устойчивостью.

С учетом выявленных выше свойств АКФ расширенной биполярной последовательности и в развитие статей [23, 24] далее предлагается метод построения специальных расширяющих биполярных последовательностей для робастного маркирования, позволяющий обеспечить большее, чем 2 по абсолютному значению отношение максимума АКФ маркерной последовательности m к минимуму этой функции.

3. Предельные биполярные последовательности для робастного маркирования. Если вместо традиционной расширяющей последовательности $\gamma = (1, -1)$ в равенстве (3) использовать расширяющую последовательность вида:

$$\gamma = \Phi \otimes \gamma_{\text{трад}}, \quad (9)$$

где:

$$\gamma_{\text{град}} = (1, -1). \quad (10)$$

При этом, когда для формирования γ применяется специально выбираемая биполярная последовательность:

$$\Phi = (\varphi_1, \varphi_2, \dots, \varphi_{N_\varphi}), \varphi_i \in \{1, -1\}, \quad (11)$$

то можно обеспечить превышающее 2 значение абсолютной величины отношения максимума АКФ к её минимуму у маркерной последовательности \mathbf{m} .

Использование биполярной последовательности γ вида (9), вместо биполярной последовательности вида (2), приводит к тому, что маркерная последовательность \mathbf{m} уже не будет определяться уравнением (3), а будет с учетом (1) удовлетворять следующему равенству:

$$\mathbf{m} = (m_1, m_2, \dots, m_{2N_\varphi N_\alpha}) = \alpha \otimes \gamma, \quad (12)$$

где:

$$m_i = (-1)^{(i-1) \bmod 2} \varphi_{\left(\left\lfloor \frac{i-1}{2} \right\rfloor \bmod N_\varphi\right)+1} \alpha_{\left\lfloor \frac{i-1}{2N_\varphi} \right\rfloor + 1}. \quad (13)$$

Например, если:

$$\Phi = (-1, -1, 1, -1), \quad (14)$$

то получится расширяющая последовательность:

$$\gamma = (-1, 1, -1, 1, 1, -1, -1, 1), \quad (15)$$

у которой максимум АКФ равен 8, а минимум -3 , то есть, в этом случае у последовательности γ значение абсолютной величины отношения максимума АКФ к её минимуму равно $|-8/3| = 2.667$.

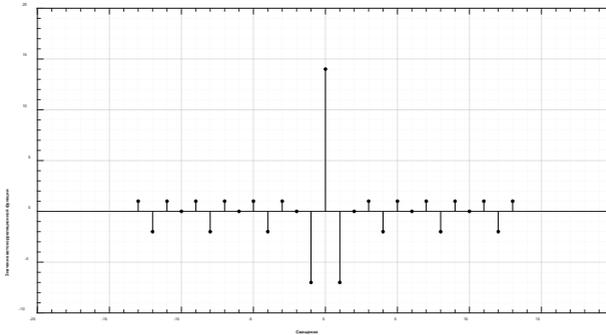


Рис. 3. График автокорреляционной функции маркерной последовательности (8), основанной на традиционной расширяющей последовательности

$$\gamma_{\text{трад}} = (1, -1).$$

Таким образом, с учетом того, что расширяющая последовательность γ в основном определяет автокорреляционные свойства расширенной последовательности \mathbf{m} , когда биполярная последовательность \mathbf{a} является псевдослучайной, то требуется метод получения таких последовательности γ , у которых автокорреляционные функции имеют наибольшие минимумы среди минимумов автокорреляционных функций всех прочих удовлетворяющих равенству (9) биполярных последовательностей такой же длины.

По определению значение АКФ $f_{\text{АКФ}}(\gamma, k)$ последовательности γ , описываемой формулой (9), когда смещение k принадлежит множеству:

$$\{-2N_{\varphi} + 1, -2N_{\varphi} + 2, \dots, -1, 0, 1, 2, \dots, 2N_{\varphi} - 1\}, \quad (18)$$

удовлетворяет следующему равенству:

$$\begin{aligned} f_{\text{АКФ}}(\gamma, k) &= \sum_{i=1}^{2N_{\varphi}-|k|} (-1)^{i-1} \varphi_{\lfloor \frac{i-1}{2} \rfloor + 1} (-1)^{i+|k|-1} \varphi_{\lfloor \frac{i+|k|-1}{2} \rfloor + 1} = \\ &= \sum_{i=1}^{2N_{\varphi}-|k|} (-1)^{2i+|k|-2} \varphi_{\lfloor \frac{i-1}{2} \rfloor + 1} \varphi_{\lfloor \frac{i+|k|-1}{2} \rfloor + 1}, \end{aligned} \quad (19)$$

где $|x|$ – абсолютное значение числа x , а $\lfloor x \rfloor$ – ближайшее целое, меньшее или равное числу x .

Полезно эту АКФ представить в следующем виде:

$$f_{\text{АКФ}}(\gamma, k) = \begin{cases} 2z_{\frac{k}{2}}, & \text{если } k \bmod 2 = 0, \\ -z_{\frac{k-1}{2}} - z_{\lfloor \frac{k-2}{2} \rfloor + 1}, & \text{если } k \bmod 2 = 1 \text{ и } k \neq 2N_{\varphi} - 1, \\ -z_{\frac{k-1}{2}}, & \text{если } k = 2N_{\varphi} - 1, \end{cases} \quad (20)$$

где:

$$z_j = z_{-j} = \sum_{i=1}^{N_{\varphi}-j} \varphi_i \varphi_{i+j}, \quad j \in \{0, 1, \dots, N_{\varphi} - 1\}. \quad (21)$$

При этом, учитывая, что $\varphi_i \in \{1, -1\}$, будет выполняться следующее равенство:

$$z_0 = N_{\varphi}. \quad (22)$$

Так как конкретные значения z_j и z_{-j} (при $j \in \{1, 2, \dots, N_{\varphi} - 1\}$) будут определяться элементами последовательности φ , использованной при формировании последовательности γ , то для z_j и z_{-j} , когда $j \in \{1, 2, \dots, N_{\varphi} - 1\}$, можно указать лишь множества потенциальных значений:

$$z_j, z_{-j} \in \{\pm(a + j - 1), \pm(a + j + 1), \pm(a + j + 3), \dots, \pm(N_{\varphi} - j)\}, \quad (23)$$

где:

$$a = (N_{\varphi} - 1) \bmod 2. \quad (24)$$

Следовательно, количество различных автокорреляционных функций, соответствующих одному и тому же N_{φ} , меньше количества последовательностей γ . Поэтому всё множество последовательностей γ , соответствующих одному и тому же N_{φ} , можно поделить

на непересекающиеся подмножества, в которые попадут последовательности, имеющие одинаковые автокорреляционные функции.

Теорема 1 (О существовании верхней границы для минимального значения АКФ биполярной последовательности γ).

Среди всех биполярных последовательностей ϕ , определенных равенством (11) и имеющих одинаковую длину N_ϕ , нет такой, которая позволяет получить в соответствии с правилом (9) биполярную последовательность γ , у которой АКФ имеет минимум, который больше величины:

$$\left\lfloor \frac{N_\phi - 1}{3} \right\rfloor - N_\phi, \quad (25)$$

то есть для всех таких биполярных последовательностей γ одинаковой длины справедливо неравенство:

$$\min_{\forall k} f_{\text{АКФ}}(\gamma, k) \leq \left\lfloor \frac{N_\phi - 1}{3} \right\rfloor - N_\phi. \quad (26)$$

Доказательство. Так как для $N_\phi = 1$ условие этой теоремы выполняется, поэтому ниже предлагается доказательство для $N_\phi > 1$.

Предположим обратное – а именно, что среди биполярных последовательностей ϕ , определяемых равенством (11), существует такая последовательность, обозначим ее $\hat{\phi}$, из которой в соответствии с правилом (9) получается биполярная последовательность $\hat{\gamma}$, у которой АКФ имеет минимальное значение, которое больше величины (25). В таком случае автокорреляционная функция $f_{\text{АКФ}}(\hat{\gamma}, k)$ (19), (20) последовательности $\hat{\gamma}$, имея максимум, равный $2z_0 = 2N_\phi$, имеет минимум, который больше¹:

¹ Так, например, среди последовательностей ϕ , длиной $N_\phi = 4$, должны были бы существовать такие $\hat{\phi}$, из которых получались бы последовательности $\hat{\gamma}$, у которых минимальное значение автокорреляционной функции было бы больше -3, то есть равнялось бы -2 или -1.

$$\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi. \quad (27)$$

Значит, для этой АКФ обязательно выполняются следующие два неравенства:

$$f_{\text{АКФ}}(\hat{\gamma}, 1) = -z_0 - z_1 > \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi, \quad (28)$$

$$f_{\text{АКФ}}(\hat{\gamma}, 2) = 2z_1 > \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi. \quad (29)$$

Исходя из того, что $z_0 = N_\varphi$, неравенство (28) позволяет заключить, что z_1 должно удовлетворять следующему неравенству:

$$z_1 < -\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor. \quad (30)$$

Тогда как на основании неравенства (29) получается, что:

$$z_1 > \frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2}. \quad (31)$$

Следовательно, величина z_1 должна принадлежать диапазону:

$$\frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} < z_1 < -\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor. \quad (32)$$

Нетрудно показать, что расстояние между правой и левой границами этого диапазона удовлетворяет равенству:

$$-\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - \frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} = \frac{1 + 3 \left\{ \frac{N_\varphi - 1}{3} \right\}}{2},$$

где $\{a\}$ – это дробная часть вещественного числа a . Так как в данном случае выполняется равенство:

$$3 \left\{ \frac{N_\varphi - 1}{3} \right\} = (N_\varphi - 1) \bmod 3, \quad (33)$$

то,

$$\frac{1}{2} \leq \frac{1 + 3 \left\{ \frac{N_\varphi - 1}{3} \right\}}{2} \leq \frac{3}{2}. \quad (34)$$

Таким образом, возможны три ситуации:

$$\frac{1 + 3 \left\{ \frac{N_\varphi - 1}{3} \right\}}{2} = \begin{cases} 1/2, \text{ если } N_\varphi \in \{1, 4, 7, \dots\}, \\ 1, \text{ если } N_\varphi \in \{2, 5, 8, \dots\}, \\ 3/2, \text{ если } N_\varphi \in \{3, 6, 9, \dots\}. \end{cases} \quad (35)$$

В первом и во втором случае, когда расстояние между границами неравенства (32) равно $1/2$ и 1 , соответственно, не существует подходящих целочисленных значений z_1 . Однако, в третьем случае, расстояние между границами неравенства (32) становится наибольшим и оказывается равным $3/2$. Например, когда

$$N_\varphi = 9, \text{ тогда } -\frac{7}{2} < z_1 < -2, \text{ или, когда } N_\varphi = 12, \text{ тогда } -\frac{9}{2} < z_1 < -3.$$

Можно предположить, что, когда $N_\varphi \in \{3, 6, 9, \dots\}$, подходящим значением для z_1 является:

$$\left\lfloor \frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} \right\rfloor, \quad (36)$$

где $\lceil a \rceil$ – ближайшее целое, большее или равное вещественному числу a . Но, в тех случаях, когда число N_φ четно, тогда и величина (36) является четной, однако, в таком случае z_1 не может принимать четные значения (23). И наоборот, когда величина (36) нечетная, тогда и число N_φ также является нечетным, но в таком случае z_1 не может принимать нечетные значения. Следовательно, во всех этих случаях z_1 не может принять значение равно величине (36).

Таким образом, среди биполярных последовательностей φ , определяемых равенством (11), нет такой последовательности $\hat{\varphi}$, из которой в соответствии с правилом (9) получается биполярная последовательность $\hat{\gamma}$, у которой АКФ имеет минимум, больше величины (25).

Следствие из Теоремы 1 (О предельной величине верхней границы отношения по абсолютному значению максимума АКФ биполярной последовательности γ к минимуму этой функции). В пределе с увеличением длины N_φ последовательности φ , абсолютное значение отношения максимума к минимуму АКФ последовательности γ равно 3.

Действительно, проведя преобразования, получим:

$$\lim_{N_\varphi \rightarrow \infty} \left| \frac{2N_\varphi}{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi} \right| = \lim_{N_\varphi \rightarrow \infty} \left| \frac{6N_\varphi}{-2N_\varphi - 1 - 3 \left\{ \frac{N_\varphi - 1}{3} \right\}} \right| = 3, \quad (37)$$

где $\{a\}$ – это дробная часть числа a .

Определение. Предельной биполярной последовательностью γ , удовлетворяющей равенству (9), называется такая (обозначим

ее γ_∞), у которой АКФ имеет минимальное численное значение, равное величине (25):

$$\min_{\forall k} f_{\text{АКФ}}(\gamma_\infty, k) = \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi. \quad (38)$$

Исходя из равенства (38) можно заключить, что у предельных последовательностей γ_∞ автокорреляционные функции такие, что для всех k из множества (18) выполняются неравенства:

$$f_{\text{АКФ}}(\gamma_\infty, k) \geq \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi, \quad (39)$$

которые, с учетом равенства (20) и $z_0 = N_\varphi$, можно свести к следующему (когда $N_\varphi > 1$):

$$\frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} \leq z_j \leq N_\varphi - \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - z_{j-1}, \quad (40)$$

где $j \in \{1, \dots, N_\varphi - 1\}$.

Автокорреляционные функции всех предельных биполярных последовательностей γ_∞ обладают общим свойством, доказательство которого приведено далее в Теореме 2.

Теорема 2 (о значениях первого и второго лепестков АКФ предельной биполярной последовательности). АКФ предельной последовательности γ_∞ является такой, что для неё выполняется либо равенство:

$$f_{\text{АКФ}}(\gamma_\infty, 1) = \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi, \quad (41)$$

либо равенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, 2) = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (42)$$

но не оба сразу.

Доказательство. Так как для $N_{\varphi} = 1$ условие этой теоремы выполняется, поэтому ниже предлагается доказательство для $N_{\varphi} > 1$.

Предположим обратное, что для любой предельной последовательности γ_{∞} при выполнении:

$$\min_{\forall k} f_{\text{АКФ}}(\gamma_{\infty}, k) = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (43)$$

для всех $k \in \{3, 4, \dots, 2N_{\varphi} - 1\}$ выполняется неравенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, k) \geq \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (44)$$

но для всех $k \in \{1, 2\}$ выполняется либо неравенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, k) > \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (45)$$

либо равенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, k) = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}. \quad (46)$$

Если для всех $k \in \{1, 2\}$ выполняется неравенство (45), то в таком случае z_1 должно удовлетворять двойному неравенству (32), для которого при доказательстве Теоремы 1 было показано, что не существует такого z_1 , который удовлетворял бы ему.

Теперь, если будет опровергнуто равенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, 1) = f_{\text{АКФ}}(\gamma_{\infty}, 2), \quad (47)$$

то теорема будет доказана. Предположим обратное, что равенство (47) выполняется, тогда выполняется и равенство:

$$-z_0 - z_1 = 2z_1. \quad (48)$$

В таком случае, с учетом равенства $z_0 = N_{\varphi}$, будет:

$$z_1 = -\frac{N_{\varphi}}{3}. \quad (49)$$

Так как z_1 является целым числом, то это равенство не может выполняться для значений N_{φ} не кратных 3. Тогда, рассмотрим только такие значения N_{φ} , которые кратны 3 – в таких случаях отношение справа от знака равенства (49) будет целым числом. Во-первых, это отношение будет равно нечетному числу, когда N_{φ} равно нечетному числу, кратному 3. Во-вторых, это отношение будет равно четному числу, когда N_{φ} равно четному числу, кратному 3. Но при нечетном N_{φ} число z_1 может быть только четным (23), и, наоборот, – при четном N_{φ} число z_1 может быть только нечетным. Значит, равенство $f_{\text{АКФ}}(\gamma_{\infty}, 1) = f_{\text{АКФ}}(\gamma_{\infty}, 2)$ также не выполняется.

Следствие из Теоремы 2. У предельных последовательностей γ_{∞} , когда $N_{\varphi} > 1$, автокорреляционные функции такие, что:

$$z_1 = \begin{cases} -\left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - 1, & \text{если } (N_{\varphi} + 1) \bmod 3 = 0, \\ -\left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor, & \text{иначе.} \end{cases} \quad (50)$$

Доказательство. Когда для АКФ предельной последовательности γ_{∞} выполняется равенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, 1) = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (51)$$

тогда:

$$-z_0 - z_1 = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}. \quad (52)$$

В таком случае, с учетом равенства $z_0 = N_{\varphi}$, будет выполняться равенство:

$$z_1 = - \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor. \quad (53)$$

Однако это равенство, учитывая свойство (23), может выполняться только, когда четность числа $N_{\varphi} - 1$ совпадает с четностью числа

$\left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor$, то есть равенство (53) выполняется только для тех чисел

N_{φ} , для которых выполняется равенство:

$$(N_{\varphi} - 1) \bmod 2 = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor \bmod 2. \quad (54)$$

Таковыми являются числа $N_{\varphi} \in \{1, 3, 4, 6, 7, 9, 10, 12, 13, \dots\}$. Этим доказана нижняя половина кусочно-определенного равенства (50).

Теперь докажем верхнюю половину (50). Когда для АКФ предельной последовательности γ_{∞} выполняется равенство:

$$f_{\text{АКФ}}(\gamma_{\infty}, 2) = \left\lfloor \frac{N_{\varphi} - 1}{3} \right\rfloor - N_{\varphi}, \quad (55)$$

тогда:

$$z_1 = \frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2}. \quad (56)$$

С одной стороны, правая часть равенства (56) принимает целые значения, только когда $N_\varphi \in \{2, 5, 8, 11, 14, 17, 20, \dots\}$, то есть когда:

$$(N_\varphi + 1) \bmod 3 = 0. \quad (57)$$

С другой стороны, учитывая свойство (23), равенство (56) может выполняться, только когда четность числа $N_\varphi - 1$ совпадает с четностью правой части равенства (56) числа, то есть для таких положительных целых чисел N_φ , для которых выполняется равенство:

$$(N_\varphi - 1) \bmod 2 = \left| \frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} \right| \bmod 2. \quad (58)$$

Но это равенство как раз и выполняется, когда N_φ удовлетворяет равенству (57). При этом, когда N_φ удовлетворяет равенству (57), тогда выполняется равенство:

$$\frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} = - \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - 1. \quad (59)$$

Действительно, если вычесть из левой части этого равенства правую, то получается следующее равенство:

$$\frac{\left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - N_\varphi}{2} + \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor + 1 = \frac{1 - 3 \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor}{2}, \quad (60)$$

где $\{a\}$ – это дробная часть числа a . Но,

$$3 \left\{ \frac{N_\varphi - 1}{3} \right\} = 1, \quad (61)$$

когда N_φ удовлетворяет равенству (57). Значит, когда N_φ удовлетворяет равенству (57), будет выполняться равенство:

$$\frac{1 - 3 \left\{ \frac{N_\varphi - 1}{3} \right\}}{2} = 0. \quad (62)$$

Следовательно, когда N_φ удовлетворяет равенству (57), тогда выполняется равенство (59). Тем самым доказана верхняя половина кусочно-определенного равенства (50).

Следует отметить, что с формальной точки зрения, величина z_1 не определена, когда $N_\varphi = 1$ (21). Но если принять, что $z_1 = 0$, когда $N_\varphi = 1$, то (50) будет выполняться и для случая $N_\varphi = 1$.

4. Метод поиска полного множества предельных последовательностей на основе рационального выбора. Равенство (50) с учетом равенства (21) можно представить в следующем виде:

$$\sum_{i=1}^{N_\varphi-1} \varphi_i \varphi_{i+1} = \begin{cases} - \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor - 1, & \text{если } (N_\varphi + 1) \bmod 3 = 0, \\ - \left\lfloor \frac{N_\varphi - 1}{3} \right\rfloor, & \text{иначе.} \end{cases} \quad (63)$$

Поэтому, опираясь на Следствие из Теоремы 2, можно сказать, что при поиске предельных последовательностей γ_∞ можно ограничиться только множеством Φ из таких биполярных последовательностей φ длиной N_φ , для которых выполняется кусочно-определенное равенство (63).

С учетом равенства (21) числа z_j можно определить как сумму элементов последовательности следующего вида:

$$\mathbf{v}_j = (v_{1,j}, v_{2,j}, \dots, v_{N_\varphi-j,j}), \quad (64)$$

где:

$$v_{i,j} = \varphi_i \varphi_{i+j}. \quad (65)$$

Так как $\varphi_i \in \{1, -1\}$, то $v_{i,j} \in \{1, -1\}$.

Важно отметить, что элементы последовательности \mathbf{v}_j , когда $j \geq 2$, можно вычислить по элементам двух предыдущих последовательностей \mathbf{v}_{j-1} и \mathbf{v}_{j-2} следующим образом:

$$v_{i,j} = v_{i,j-1} v_{i+1,j-2} v_{i+1,j-1}. \quad (66)$$

Действительно, произведение справа от знака этого равенства совпадает с правой частью равенства (65):

$$v_{i,j-1} v_{i+1,j-2} v_{i+1,j-1} = \varphi_i \varphi_{i+j-1} \varphi_{i+1} \varphi_{i+1+j-2} \varphi_{i+1} \varphi_{i+1+j-1} = \varphi_i \varphi_{i+j-1}^2 \varphi_{i+1}^2 \varphi_{i+j} = \varphi_i \varphi_{i+j}.$$

Любой вектор \mathbf{v}_1 связан с двумя биполярными последовательностями Φ . При этом эти две последовательности определяют две последовательности γ , у которых совпадают автокорреляционные функции. Так, когда известен вектор \mathbf{v}_1 , тогда восстановить элементы упомянутых двух биполярных последовательностей Φ , с которыми он связан, можно по следующему правилу:

1) Прямая последовательность Φ : пусть $\varphi_1 = -1$, тогда:

$$\varphi_i = -\prod_{l=1}^{i-1} v_{l,1}, \quad i \in \{2, 3, \dots, N_\varphi\}. \quad (67)$$

2) Инвертированная прямая последовательность Φ : пусть $\varphi_1 = 1$, тогда:

$$\varphi_i = \prod_{l=1}^{i-1} v_{l,1}, \quad i \in \{2, 3, \dots, N_\varphi\}. \quad (68)$$

Таким образом, множество Φ соответствует множеству V_1 из таких последовательностей v_1 , у которых сумма элементов равна числу z_1 , удовлетворяющему равенству (50). А так как $v_{i,j} \in \{1, -1\}$, то мощность множества V_1 равна биномиальному коэффициенту:

$$|V_1| = C_{N_\Phi - 1}^{\frac{N_\Phi - 1 + z_1}{2}}, \quad (69)$$

где:

$$C_{N_\Phi - 1}^{\frac{N_\Phi - 1 + z_1}{2}} = \frac{(N_\Phi - 1)!}{\left(\frac{N_\Phi - 1 + z_1}{2}\right)! \left(\frac{N_\Phi - 1 - z_1}{2}\right)!}. \quad (70)$$

Если некоторая последовательность $v_1 \in V_1$ связана с последовательностью Φ , которая в свою очередь определяет предельную последовательность γ_∞ , тогда сумма элементов каждой из последовательностей множества $\{v_1, v_2, \dots, v_{N_\Phi - 1}\}$ удовлетворяет двойному неравенству (40).

А теперь, для примера выполним поиск всех предельных последовательностей γ_∞ для $N_\Phi = 4$. Поиск представлен в виде следующей последовательности действий:

1) Так как $N_\Phi = 4$, то, в соответствии с равенством (50), выполняется следующее равенство: $z_1 = -1$.

2) Так как $N_\Phi = 4$ и $z_1 = -1$, то поиск подходящих последовательностей v_1 длиной $N_\Phi - 1 = 3$, следует вести среди всех таких биполярных последовательностей, у которых сумма элементов равна -1 .

3) В соответствии с равенством (69), множество V_1 проверяемых последовательностей v_1 , длиной $N_\Phi - 1 = 3$, имеет мощность $|V_1| = 3$.

С учетом того, что в это множество должны войти все последовательности \mathbf{v}_1 длиной 3, у которых сумма элементов равна -1 , то оно будет следующим:

$$\mathbf{V}_1 = \{(-1, -1, 1), (-1, 1, -1), (1, -1, -1)\}.$$

4) Определим по формуле (66) для каждой из этих трех последовательностей последующие за ними последовательности \mathbf{v}_2 и \mathbf{v}_3 : для последовательности $\mathbf{v}_1 = (-1, -1, 1)$, это будут: $\mathbf{v}_2 = (1, -1)$ и $\mathbf{v}_3 = 1$; для последовательности $\mathbf{v}_1 = (-1, 1, -1)$: $\mathbf{v}_2 = (-1, -1)$ и $\mathbf{v}_3 = 1$; для последовательности $\mathbf{v}_1 = (1, -1, -1)$, последующими будут: $\mathbf{v}_2 = (-1, 1)$ и $\mathbf{v}_3 = 1$.

5) Так как сумма элементов последовательности \mathbf{v}_j равна величине z_j , то можно проверить, определяет ли какая-то из последовательности множества \mathbf{V}_1 предельную последовательность γ_∞ . Учитывая, что $z_1 = -1$ и, что у предельных последовательностей γ_∞ выполняются двойные неравенства (40). Следует проверить выполняются ли два двойных неравенства:

$$-\frac{3}{2} \leq z_2 \leq 4, \quad -\frac{3}{2} \leq z_3 \leq 3 - z_2.$$

– Выполним проверку для вектора $\mathbf{v}_1 = (-1, -1, 1)$.

Суммы элементов векторов \mathbf{v}_2 и \mathbf{v}_3 равны $z_2 = 0$ и $z_3 = 1$, соответственно. Оба двойных неравенства удовлетворяются. Следовательно, вектор $\mathbf{v}_1 = (-1, -1, 1)$ успешно проходит проверку, так как определяет предельные последовательности γ_∞ .

– Выполним проверку для вектора $\mathbf{v}_1 = (-1, 1, -1)$.

Суммы элементов векторов \mathbf{v}_2 и \mathbf{v}_3 равны $z_2 = -2$ и $z_3 = 1$, соответственно. Первое двойное неравенство не удовлетворяются. Следовательно, вектор $\mathbf{v}_1 = (-1, 1, -1)$ не проходит проверку, так как не определяет предельные последовательности γ_∞ .

– Выполним проверку для вектора $\mathbf{v}_1 = (1, -1, -1)$.

Суммы элементов векторов v_2 и v_3 равны $z_2 = 0$ и $z_3 = 1$, соответственно. Оба двойных неравенства удовлетворяются. Следовательно, вектор $v_1 = (1, -1, -1)$ успешно прошел проверку, так как определяет предельные последовательности γ_∞ .

б) Используя вектора, которые прошли проверку, восстановим по правилам (67)–(68) биполярные последовательности Φ :

- Для вектора $v_1 = (-1, -1, 1)$:
 - прямая последовательность $\Phi_{1,1} = (-1, 1, -1, -1)$;
 - инвертированная прямая последовательность $\Phi_{1,2} = (1, -1, 1, 1)$.
- Для вектора $v_1 = (1, -1, -1)$:
 - прямая последовательность $\Phi_{2,1} = (-1, -1, 1, -1)$;
 - инвертированная прямая последовательность $\Phi_{2,2} = (1, 1, -1, 1)$.

Видно, что последовательность $\Phi_{2,1}$ получается из последовательности $\Phi_{1,1}$ путем обращения порядка всех элементов, тогда как последовательность $\Phi_{2,2}$ получается из $\Phi_{1,1}$ путем обращения порядка элементов с последующим инвертированием их значений. А так как последовательность $\Phi_{1,2}$ получается из последовательности $\Phi_{1,1}$ путем инвертирования значений всех элементов, то, получается, что все три последовательности $\Phi_{1,2}$, $\Phi_{2,1}$ и $\Phi_{2,2}$ можно получить из $\Phi_{1,1}$.

7) Теперь по последовательностям $\Phi_{1,1}$, $\Phi_{1,2}$, $\Phi_{2,1}$ и $\Phi_{2,2}$, в соответствии с правилом (9), вычислим биполярные последовательности, которые являются предельными:

$$\gamma_{\infty,1,1} = (-1, 1, 1, -1, -1, 1, -1, 1),$$

$$\gamma_{\infty,1,2} = (1, -1, -1, 1, 1, -1, 1, -1),$$

$$\gamma_{\infty,2,1} = (-1, 1, -1, 1, 1, -1, -1, 1),$$

$$\gamma_{\infty,2,2} = (1, -1, 1, -1, -1, 1, 1, -1).$$

Все эти четыре последовательности имеют одну и ту же автокорреляционную функцию $f_{\text{АКФ}}(\gamma_{\infty}, k)$:

$$-1, 2, -1, 0, 1, -2, -3, 8, -3, -2, 1, 0, -1, 2, -1.$$

5. Метод построения предельных биполярных последовательностей с использованием порождающих функций.

С ростом величины N_{φ} возрастает и мощность множества V_1 (69) последовательностей-кандидатов, среди которых находятся те, которые связаны с предельными последовательностями γ_{∞} . Поэтому если найти функциональную зависимость между предельными последовательностями и значениями специальных функций, которые далее называются порождающими, то можно будет сразу определять некоторое подмножество предельных последовательностей для любого заданного значения N_{φ} (без необходимости выполнения поиска предельных последовательностей на основе рационального перебора).

Каждой биполярной последовательности φ (11) можно сопоставить целое неотрицательное число a , по следующему правилу:

$$a = \sum_{i=1}^{N_{\varphi}} 2^{N_{\varphi}-i} \left(\frac{\varphi_i + 1}{2} \right). \quad (71)$$

Например, биполярной последовательности $\varphi = (1, -1, -1, -1, 1)$, будет сопоставлено число $a = 17$.

Среди целых неотрицательных чисел a , в контексте решения задачи нахождения предельных последовательностей γ_{∞} , особый интерес представляют такие целые неотрицательные числа, которые соответствуют последовательностям φ , лежащим по правилу (9) в основе предельных последовательностей γ_{∞} . Например, когда $N_{\varphi} = 5$, тогда такие целые числа a образуют последовательность: 5, 9, 11, 13, 18, 20, 22, 26. Видно, что минимальным среди них является число 5, значит, числа с 1 по 4 не связаны с предельными последовательностями.

Целое неотрицательное число a , соответствующее биполярной последовательности Φ , определенной равенством (11) и имеющей длину N_Φ , которая позволяет получить в соответствии с правилом (9) биполярную последовательность, которая является предельной последовательностью γ_∞ , можно вычислить с помощью следующей рекуррентной функции:

$$f_1(N_\Phi) = \begin{cases} f_1(N_\Phi - 1), & \text{если } N_\Phi \in \{3, 6, 9, \dots\}, \\ 2f_1(N_\Phi - 1), & \text{если } N_\Phi \in \{4, 7, 10, \dots\}, \\ 2f_1(N_\Phi - 1) + 1, & \text{если } N_\Phi \in \{2, 5, 8, \dots\}, \\ 0, & \text{если } N_\Phi = 1. \end{cases} \quad (72)$$

Например, пусть $N_\Phi = 19$, тогда:

$$\begin{aligned} a = f(19) &= 2f(18) = 2(f(17)) = 2(2f(16) + 1) = \\ &= 2(2(2f(15)) + 1) = \dots = 2730. \end{aligned} \quad (73)$$

В двоичном представлении в девятнадцатиразрядной двоичной сетке (так как $N_\Phi = 19$) это число выглядит так:

$$2730_{10} = 00000001010101010_2. \quad (74)$$

Значит, искомая биполярная последовательность будет:

$$\begin{aligned} \Phi = (-1, -1, -1, -1, -1, -1, -1, 1, -1, \\ 1, -1, 1, -1, 1, -1, 1, -1, 1). \end{aligned} \quad (75)$$

Этой последовательности Φ соответствует биполярная последовательность:

$$\begin{aligned} \gamma = (-1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, \\ 1, -1, -1, 1, 1, -1, -1, 1, 1, -1, -1, 1, \\ 1, -1, -1, 1, 1, -1, -1, 1, 1, -1, -1, 1), \end{aligned} \quad (76)$$

у которой абсолютное значение отношения максимума к минимуму АКФ равно:

$$\left| \frac{2N_{\varphi}}{\frac{N_{\varphi}-1}{3} - N_{\varphi}} \right| = \frac{38}{13} \cong 2,92, \quad (77)$$

что является максимально достижимым значением, когда $N_{\varphi} = 19$ в формуле (26). Значит последовательность (76) является предельной последовательностью.

Важно отметить, что числа, получаемые из значения $f_1(N_{\varphi})$, путем инвертирования всех двоичных разрядов, путем обращения всех двоичных разрядов, а также путем обращения и инвертирования всех двоичных разрядов также соответствуют последовательностям φ , определяющим предельные последовательности γ_{∞} . Например, если такие операции выполнить с числом $f_1(19) = 2730$, представленном в 19-разрядной сетке, соответственно получатся следующие числа: 521557, 174720, 349567. Этим трем числам, также как и числу 2730 (73)–(77), соответствуют предельные последовательности γ_{∞} . И все они будут иметь одинаковые автокорреляционные функции.

Когда $N_{\varphi} \in \{1, 2, 3, 4\}$, тогда с помощью порождающей функции $f_1(N_{\varphi})$, определенной равенством (72), можно получить все возможные предельные последовательности γ_{∞} . Однако, когда $N_{\varphi} \geq 5$, среди предельных последовательностей γ_{∞} появляются такие, которые уже не получаются с помощью порождающей функции $f_1(N_{\varphi})$. Так, например, при $N_{\varphi} = 5$ существует предельные последовательности γ_{∞} , связанные с числами 9, 13, 18, 22, тогда как с помощью порождающей функции $f_1(N_{\varphi})$ можно получить числа: 5, 11, 20, 26. Число 9 является вторым по порядку в этой последовательности из 8 чисел. Если проанализировать вторые по порядку числа для $N_{\varphi} \geq 5$, можно получить вторую порождающую функцию:

$$f_2(N_\varphi) = \begin{cases} f_2(N_\varphi - 1), & \text{если } N_\varphi \in \{6, 9, 12, \dots\}, \\ 2f_2(N_\varphi - 1), & \text{если } N_\varphi \in \{7, 10, 13, \dots\}, \\ 2f_2(N_\varphi - 1) + 1, & \text{если } N_\varphi \in \{8, 11, 14, \dots\}, \\ 9, & \text{если } N_\varphi = 5. \end{cases} \quad (78)$$

Функции $f_1(N_\varphi)$ (для значений $N_\varphi \in \{1, \dots, 10000\}$) и $f_2(N_\varphi)$ (для значений $N_\varphi \in \{5, \dots, 10000\}$) успешно прошли проверку на то, что они действительно вычисляют подходящие числа a , с помощью которых можно получить предельные последовательности γ_∞ . Таким образом, с помощью порождающих функций f_1 и f_2 можно получать предельные последовательности в тех случаях, когда вычислительная сложность поиска предельных последовательностей в соответствии с предложенным выше методом неприемлемо велика.

6. Результаты компьютерного моделирования. Выше было доказано, что абсолютное значение отношения максимума АКФ маркерной последовательности \mathbf{m} к минимуму АКФ, когда используется предельная последовательность γ_∞ , превышает число 2 и в пределе равно 3. В то время как абсолютное значение этого отношения, когда используется традиционная расширяющая последовательность $\gamma_{\text{трад}}$ при построении маркерной последовательности \mathbf{m} , с достаточно высокой точностью равно 2. Применение предложенных предельных последовательностей с улучшенными корреляционными свойствами позволяет повысить качество детектирования и, как следствие, устойчивость маркирования цифровых аудиосигналов к действию помех, преобразованиям и деструктивным воздействиям.

Важно выполнить экспериментальную оценку того, насколько применение предельных биполярных последовательностей отражается на корреляционных свойствах извлекаемого из стегоаудиосигнала маркера для наихудших (и часто реальных) условий приема, характеризующих прежде всего слепой прием. Напомним, что при слепом приеме аудиосигнал, в который внедряется маркер, неизвестен авторизованному получателю. В этом случае в процессе обнаружения и извлечения маркера из стегоаудиосигнала исходный (покрывающий) аудиосигнал становится шумом, влияющим на качество корреляционного детектирования.

Для этого необходимо, прежде всего, оценить то, насколько при слепом приеме изменяется взаимная корреляция между извлеченной из маркированного аудиосигнала последовательностью и внедренной маркерной последовательностью \mathbf{m} при варьировании тех или иных параметров, а также провести сравнительную оценку абсолютных значений отношений максимумов к минимумам взаимных корреляционных функций (ВКФ), характеризующих эту корреляцию, для традиционно используемой последовательности $\gamma_{\text{трад}}$ и предложенной предельной последовательности γ_{∞} .

В процессе проведенного компьютерного моделирования в качестве покрывающих аудиосигналов использовались 100 популярных музыкально-песенных композиций из различных направлений музыки. Маркированные аудиосигналы не подвергались никаким дополнительным цифровым преобразованиям. Поэтому исходный цифровой аудиосигнал в условиях слепого приема выступал единственным искажающим воздействием (шумом). Варьируемым параметром была сила внедрения маркера, определяющая коэффициент масштабирования амплитуды частотной составляющей спектра Фурье блока отсчетов при внедрении элементов маркера. Оценивались два показателя – отношение сигнал-маркер и абсолютное значение отношения максимума взаимной корреляционной функции к ее минимуму. Оба этих показателя позволяли делать выводы об устойчивости (в условиях слепого приема) маркерных последовательностей, сформированных на основе предельных последовательностей γ_{∞} , и традиционно используемых маркерных последовательностей, основанных на $\gamma_{\text{трад}}$.

Для внедрения, обнаружения и извлечения маркерной последовательности методом слепого приема использовались процедуры, предложенные в работе [24].

При формировании маркерных последовательностей \mathbf{m} для компьютерного моделирования последовательность \mathbf{a} представляла собой биполярную последовательность длиной 64449 элементов, получаемую в результате кронекерова произведения двух псевдослучайных последовательностей:

$$\mathbf{a} = \mathbf{a}_1 \otimes \mathbf{a}_2,$$

где \mathbf{a}_1 – это биполярная последовательность Касами (длиной 1023 элемента), \mathbf{a}_2 – это биполярная последовательность Голда (длиной 63 элемента). В качестве расширяющей последовательности

использовалась либо биполярная последовательность $\gamma_{\text{трад}}$, определяемая равенством (10), соответствующая традиционному методу формирования маркерной последовательности по правилу (3), либо предельная биполярная последовательность:

$$\gamma_{\infty} = (1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1, -1, 1, 1, -1)$$

соответствующая предлагаемому робастному методу формирования маркерной последовательности по правилу (12).

В результате, при использовании традиционного подхода к формированию маркерной последовательности вычисленное абсолютное значение отношения максимума АКФ к её минимуму составило:

$$\left| -\frac{128898}{64417} \right| \cong 2.001,$$

а при использовании предлагаемого подхода с использованием предельных биполярных последовательностей, это отношение равнялось:

$$\left| -\frac{1675674}{580009} \right| \cong 2.889.$$

Поскольку при слепом приеме покрывающий аудиосигнал становится шумом для процесса извлечения внедренных маркеров и вычисления ВКФ, то абсолютные значения этих отношений для ВКФ будут определяться отношением сигнал-маркер, которое в свою очередь, зависит от силы внедрения элементов маркера.

Результаты компьютерного моделирования по оценке абсолютной величины отношения максимума ВКФ к ее минимуму в зависимости от основных параметров маркирования представлены в Таблицах 1 и 2. Приняты следующие обозначения столбцов таблицы: [А] – сила внедрения маркера; [Б] – среднее значение отношения сигнал-маркер (единица измерения – дБ); [В] – среднее значение абсолютной величины отношения максимума ВКФ к минимуму этой функции, характеризующей корреляцию между извлеченной последовательностью и внедренной маркерной последовательностью.

Традиционно считается [25, 26, 27, 28], что, когда отношение сигнал-маркер больше 20 дБ, тогда акустические артефакты, появляющиеся в результате внедрения маркера в аудиосигнал, будут

не слышимы человеческим ухом. Поэтому при моделировании максимальная сила внедрения равнялась 0.1, что обеспечивает отношение сигнал-маркер больше 20 дБ.

Анализ полученных результатов показал, что при силе внедрения 0.1 абсолютное значение величины отношения максимума ВКФ к ее минимуму уменьшается по сравнению с этим же показателем, полученным для АКФ (2.001), почти на 0.12 (традиционное маркирование), тогда как для робастного маркирования, основанного на использовании предельной последовательности, это отличие составляет всего лишь около 0.05 (при значении для АКФ, равном 2.889). Традиционный маркер становится не отличим от белого шума, когда сила внедрения будет меньше 0.01, тогда как маркер, построенный на основе предельной последовательности, будет не отличим от белого шума только тогда, когда сила внедрения будет меньше 0.003.

Таким образом, при слепом приеме маркирование цифровых аудиосигналов с использованием предельных биполярных последовательностей, по сравнению с традиционным маркированием, не только обеспечивает большее по абсолютной величине отношение максимума ВКФ к ее минимуму, но и является на порядок более устойчивым к искажающему воздействию покрывающего аудиосигнала.

Таблица 1. Результаты моделирования для случая, когда использовалась традиционная биполярная последовательность $\gamma = (1, -1)$

[A]	[B]	[B]
0.1	22.6537914407729	1.89400133362661
0.09	23.5689087161114	1.88940377072308
0.08	24.5919137027463	1.88378546192023
0.07	25.7516863726654	1.87676523118745
0.06	27.0905201404766	1.86774872443684
0.05	28.6739760385219	1.85576203481233
0.04	30.6118656605248	1.83912315246444
0.03	33.1099713242667	1.80857006872274
0.02	36.6298991976145	1.66904242496330
0.01	42.6405797512073	1.22115540454256
0.009	43.5527289528179	1.17197219241071
0.008	44.5716571653026	1.12916956984856
0.007	45.7256236763519	1.09483301588215
0.006	47.0558026726118	1.06745248183093
0.005	48.6255673720736	1.04974406741366
0.004	50.5399521171489	1.03956744534308
0.003	52.9924466534771	1.03586059278761
0.002	56.4032438747814	1.03275100298008
0.001	62.0084277052975	1.03056260054767

Таблица 2. Результаты моделирования для случая, когда использовалась предельная биполярная последовательность

$$\gamma_{\infty} = (1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1 - 1).$$

[A]	[B]	[B]
0.1	22.9756767301182	2.84137761957072
0.09	23.8908264049154	2.83731141890393
0.08	24.9138766626027	2.83226677555242
0.07	26.0737153223891	2.82584064373021
0.06	27.4126506827211	2.81737334369541
0.05	28.9962748847080	2.80570558153818
0.04	30.9344738175417	2.78840201614555
0.03	33.4332456738216	2.75516799839706
0.02	36.9550626144124	2.67636860609201
0.01	42.9756178969781	2.44763217519363
0.009	43.8907537349459	2.39680709039650
0.008	44.9137846437648	2.33405951225665
0.007	46.0735950750664	2.24683845587408
0.006	47.4124869330215	2.10918146136329
0.005	48.9960389735402	1.90539412353207
0.004	50.9341050426052	1.64397752034035
0.003	53.4325898308898	1.33580638954599
0.002	56.9535867943209	1.10082579442145
0.001	62.9697239736851	1.00904942996361

7. Заключение. В статье разработан математический аппарат для поиска и построения предельных биполярных последовательностей, используемых при решении задачи робастного маркирования цифровых аудиосигналов по методу лоскута. Предельные биполярные последовательности определены как расширяющие последовательности с улучшенными корреляционными свойствами, у которых автокорреляционные функции обладают максимально возможными по абсолютному значению отношениями максимума к минимуму.

Сформулированы и доказаны теоремы и следствия из них: о существовании верхней границы минимальных значений автокорреляционных функций предельных биполярных последовательностей и о значениях первого и второго лепестков АКФ. На этой основе дано строгое определение предельных биполярных последовательностей и показано, что в пределе значение абсолютной величины отношения максимума АКФ таких последовательностей к её минимуму стремится к 3. Разработаны метод поиска полного множества предельных биполярных последовательностей на основе рационального перебора и метод построения предельных биполярных

последовательностей произвольной длины с использованием порождающих функций.

Представлены результаты компьютерного моделирования по оценке значений абсолютной величины отношения максимума к минимуму автокорреляционной и взаимной корреляционных функций исследуемых биполярных последовательностей для наихудших условий приема – слепого приема. Их анализ показал, что предложенные предельные биполярные последовательности характеризуются лучшими корреляционными свойствами в сравнении с традиционно используемыми биполярными последовательностями и обладают большей устойчивостью.

Литература

1. Алексеев В.Г., Коржик В.И. Погружение цифровых водяных знаков в аудиосигналы с помощью использования частотно селективного изменения фазы // Научные технологии в космических исследованиях Земли. 2019. Т. 11. № 6. С. 22–29.
2. Шелухин О.И., Рыбаков С.Ю., Магомедова Д.И. Скрытие информации в аудиосигналах с использованием детерминированного хаоса // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 1. С. 80–91.
3. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding // IBM systems journal. 1996. vol. 35. № 3.4. pp. 313–336.
4. Wendzel S., Caviglione L., Mazurczyk W., Mileva A., Dittmann J., Krätzer C., Kevin L., Claus V., Laura H., Jorg K., Tom N., Sebastian Z. A Generic Taxonomy for Steganography Methods. TechRxiv. Preprint. IEEE. 2022. DOI: 10.36227/techrxiv.20215373.v2.
5. Makhdoom I., Abolhasan M., Lipman J. A Comprehensive Survey of Covert Communication Techniques, Limitations and Future Challenges // Computers & Security. 2022. vol. 120. DOI: 10.1016/j.cose.2022.102784.
6. Yeo I., Kim H. Modified patchwork algorithm: A novel audio watermarking scheme // IEEE Transactions on speech and audio processing. 2003. vol. 11. № 4. pp. 381–386.
7. Liu Z., Huang Y., Huang J. Patchwork-based audio watermarking robust against desynchronization and recapturing attacks // IEEE transactions on information forensics and security. 2018. vol. 14. № 5. pp. 1171–1180.
8. Chincholkar Y., Ganorkar S. Audio watermarking algorithm implementation using patchwork technique // 2019 IEEE 5th International Conference for Convergence in Technology (I2CT). IEEE. 2019. pp. 1–5.
9. Chincholkar Y., Kude S. Effective robust patchwork method to the vulnerable attack for digital audio watermarking // ICTACT Journal on Image & Video Processing. 2018. vol. 8. № 4. pp. 1753–1758.
10. Li Q., Wang X., Pei Q. Compression Domain Reversible Robust Watermarking Based on Multilayer Embedding // Security and Communication Networks. 2022. vol. 2022. Article ID 4542705. 13 p. DOI: 10.1155/2022/4542705.
11. Saritas O., Ozturk S. A color channel multiplexing approach for robust discrete wavelet transform based image watermarking // Concurrency and Computation: Practice and Experience. 2022. e7255. DOI: 10.1002/cpe.7255.
12. Zhu X., Lai Z., Zhou N., Wu J. Steganography with High Reconstruction Robustness: Hiding of Encrypted Secret Images. Mathematics. 2022. vol. 10. № 16: 2934. DOI: 10.3390/math10162934.

13. Paul S., Mishra D. Hiding images within audio using deep generative model // *Multimedia Tools and Applications*. 2022. pp. 1–24. DOI: doi.org/10.1007/s11042-022-13034-4.
14. Luo X., Goebel M., Barshan E., Yang F. LECA: A Learned Approach for Efficient Cover-agnostic Watermarking // *arXiv preprint arXiv:2206.10813*. 2022. DOI: 10.48550/arXiv.2206.10813.
15. Ghosal S., Roy S., Basak R. LSB Steganography Using Three Level Arnold Scrambling and Pseudo-random Generator // Eds.: Giri D., Mandal J., Sakurai K., De D. In: *Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems*. 2022. vol. 481. pp. 105–116. DOI: 10.1007/978-981-19-3182-6_9.
16. Rai D.K. Invisible Unicode Programming // *International Journal of Research Publication and Reviews*. vol. 3. № 4. pp. 1–19. DOI: 10.55248/gengpi.2022.3.4.1.
17. Nakashima Y., Tachibana R., Babaguchi N. Watermarked movie soundtrack finds the position of the camcorder in a theater // *IEEE Transactions on Multimedia*. 2009. vol. 11. № 3. pp. 443–454.
18. Tachibana R. Sonic watermarking // *EURASIP Journal on Advances in Signal Processing*. 2004. vol. 2004. № 13. DOI: 10.1155/S1110865704403138.
19. Tachibana R. Audio watermarking for live performance // *Security and Watermarking of Multimedia Contents V. SPIE*, 2003. vol. 5020. pp. 32–43. DOI: 10.1117/12.476832.
20. Zhang Z., Wu X. An audio covert communication system for analog channels // *International Conference on Electrical and Control Engineering. IEEE*, 2010. pp. 3279–3282. DOI: 10.1109/iCECE.2010.800.
21. Kaneto R., Nakashima Y., Babaguchi N. Real-time user position estimation in indoor environments using digital watermarking for audio signals // *20th International Conference on Pattern Recognition. IEEE*, 2010. pp. 97–100.
22. Гофман М.В., Корниенко А.А., Глухов А.П. Методика позиционирования маркированными аудиосигналами // *Проблемы информационной безопасности. Компьютерные системы*. 2018. № 4. С. 120–129.
23. Гофман М.В. Методика скрытой передачи данных при связи через воздушный аудиоканал // *Труды СПИИРАН*. 2017. Вып. 51. С. 97–122.
24. Гофман М.В. Помехоустойчивое маркирование цифровых аудиосигналов в аудиостегосистемах с множественным входом и множественным выходом // *Проблемы информационной безопасности. Компьютерные системы*. 2021. Вып. 3. С. 83–95.
25. Özer H., Sankur B., Memon N., Avcıbaşı İ. Detection of audio covert channels using statistical fingerprints of hidden messages // *Digital Signal Processing*. 2006. vol. 16. № 4. pp. 389–401.
26. Su Z., Zhang G., Yue F., Chang L., Jiang J., Yao X. SNR-constrained heuristics for optimizing the scaling parameter of robust audio watermarking // *IEEE Transactions on Multimedia*. 2018. vol. 20. № 10. pp. 2631–2644.
27. Appadurai E., Bhatt M., Geetha D. Semi Fragile Audio Crypto-Watermarking based on Sparse Sampling with Partially Decomposed Haar Matrix Structure // *Acta Cybernetica*. 2020. vol. 24. № 4. pp. 679–697.
28. Khillare A., Malviya A. Reversible Digital Audio Watermarking Scheme Using Wavelet Transformation // *Journal of Engineering Research and Application*. 2018. vol. 8(7). pp 62–72.

Гофман Максим Викторович — канд. техн. наук, доцент, кафедра «информатика и информационная безопасность», Петербургский государственный университет путей сообщения Императора Александра I. Область научных интересов: информационная

безопасность. Число научных публикаций — 45. maxgof@gmail.com; Московский проспект, 9, 190031, Санкт-Петербург, Россия; р.т.: +7(812)310-3472.

Корниенко Анатолий Адамович — д-р техн. наук, профессор кафедры, кафедра «информатика и информационная безопасность», Петербургский государственный университет путей сообщения Императора Александра I. Область научных интересов: информационная безопасность. Число научных публикаций — 421. kaa.pgups@yandex.ru; Московский проспект, 9, 190031, Санкт-Петербург, Россия; р.т.: +7(812)310-3472.

M. GOFMAN, A. KORNIENKO
**LIMIT BIPOLAR SEQUENCES FOR PATCHWORK-BASED
ROBUST DIGITAL AUDIO WATERMARKING**

Gofman M., Kornienko A. Limit Bipolar Sequences for Patchwork-Based Robust Digital Audio Watermarking.

Abstract. Ensuring the robustness of digital audio watermarking under the influence of interference, various transformations and possible attacks is an urgent problem. One of the most used and fairly stable marking methods is the patchwork method. Its robustness is ensured by the use of expanding bipolar numerical sequences in the formation and embedding of a watermark in a digital audio and correlation detection in the detection and extraction of a watermark. An analysis of the patchwork method showed that the absolute values of the ratio of the maximum of the autocorrelation function (ACF) to its minimum for expanding bipolar sequences and extended marker sequences used in traditional digital watermarking approach 2 with high accuracy. This made it possible to formulate criteria for searching for special expanding bipolar sequences, which have improved correlation properties and greater robustness. The article developed a mathematical apparatus for searching and constructing limit-expanding bipolar sequences used in solving the problem of robust digital audio watermarking using the patchwork method. Limit bipolar sequences are defined as sequences whose autocorrelation functions have the maximum possible ratios of maximum to minimum in absolute value. Theorems and corollaries from them are formulated and proved: on the existence of an upper bound on the minimum values of autocorrelation functions of limit bipolar sequences and on the values of the first and second petals of the ACF. On this basis, a rigorous mathematical definition of limit bipolar sequences is given. A method for searching for the complete set of limit bipolar sequences based on rational search and a method for constructing limit bipolar sequences of arbitrary length using generating functions are developed. The results of the computer simulation of the assessment of the values of the absolute value of the ratio of the maximum to the minimum of the autocorrelation and cross-correlation functions of the studied bipolar sequences for blind reception are presented. It is shown that the proposed limit bipolar sequences are characterized by better correlation properties in comparison with the traditionally used bipolar sequences and are more robust.

Keywords: steganography, digital audio, patchwork method, digital watermarking, bipolar sequences, correlation function.

References

1. Alekseev V.G., Korzhik V.I. [Embedding of digital watermark signals with the use of a frequency selective phase changing]. *Naukoemkie tehnologii v kosmicheskikh issledovaniyah Zemli – H&ES Research*. 2019. vol. 11. № 6. pp. 22–29. DOI: 10.24411/2409-5419-2018-10292. (In Russ.).
2. Sheluhin O.I., Rybakov S.Y., Magomedova D.I. [Audio steganography method using determined chaos]. *Naukoemkie tehnologii v kosmicheskikh issledovaniyah Zemli – H&ES Research*. 2021. vol. 13. № 1. pp. 80–91. DOI: 10.36724/2409-5419-2021-13-1-80-91. (In Russ.).
3. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding. *IBM systems journal*. 1996. vol. 35. № 3.4. pp. 313–336.
4. Wendzel S., Caviglione L., Mazurczyk W., Mileva A., Dittmann J., Krätzer C., Kevin L., Claus V., Laura H., Jorg K., Tom N., Sebastian Z. A Generic Taxonomy for

- Steganography Methods. TechRxiv. Preprint. IEEE. 2022. DOI: 10.36227/techrxiv.20215373.v2.
5. Makhdoom I., Abolhasan M., Lipman J. A Comprehensive Survey of Covert Communication Techniques, Limitations and Future Challenges. *Computers & Security*. 2022. vol. 120. DOI: 10.1016/j.cose.2022.102784.
 6. Yeo I., Kim H. Modified patchwork algorithm: A novel audio watermarking scheme. *IEEE Transactions on speech and audio processing*. 2003. vol. 11. № 4. pp. 381–386.
 7. Liu Z., Huang Y., Huang J. Patchwork-based audio watermarking robust against desynchronization and recapturing attacks. *IEEE transactions on information forensics and security*. 2018. vol. 14. № 5. pp. 1171–1180.
 8. Chincholkar Y., Ganorkar S. Audio watermarking algorithm implementation using patchwork technique. *IEEE 5th International Conference for Convergence in Technology (I2CT)*. IEEE. 2019. pp. 1–5.
 9. Chincholkar Y., Kude S. Effective robust patchwork method to the vulnerable attack for digital audio watermarking. *ICTACT Journal on Image & Video Processing*. 2018. vol. 8. № 4. pp. 1753–1758.
 10. Li Q., Wang X., Pei Q. Compression Domain Reversible Robust Watermarking Based on Multilayer Embedding. *Security and Communication Networks*. 2022. vol. 2022, Article ID 4542705. 13 p. DOI: doi.org/10.1155/2022/4542705.
 11. Saritas O., Ozturk S. A color channel multiplexing approach for robust discrete wavelet transform based image watermarking. *Concurrency and Computation: Practice and Experience*. 2022. e7255. DOI: doi.org/10.1002/cpe.7255.
 12. Zhu X., Lai Z., Zhou N., Wu J. Steganography with High Reconstruction Robustness: Hiding of Encrypted Secret Images. *Mathematics*. 2022. vol. 10. № 16:2934. DOI: doi.org/10.3390/math10162934.
 13. Paul S., Mishra D. Hiding images within audio using deep generative model. *Multimedia Tools and Applications*. 2022. pp. 1–24. DOI: 10.1007/s11042-022-13034-4.
 14. Luo X., Goebel M., Barshan E., Yang F. LECA: A Learned Approach for Efficient Cover-agnostic Watermarking. *arXiv preprint arXiv:2206.10813*. 2022. DOI: 10.48550/arXiv.2206.10813.
 15. Ghosal S., Roy S., Basak R. LSB Steganography Using Three Level Arnold Scrambling and Pseudo-random Generator. Eds.: Giri D., Mandal J., Sakurai K., De D. In: *Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems*. 2022. vol. 481. pp. 105–116. DOI: 10.1007/978-981-19-3182-6_9.
 16. Rai D. Invisible Unicode Programming. *International Journal of Research Publication and Reviews*. vol. 3. № 4. pp. 1–19. DOI: 10.55248/gengpi.2022.3.4.1.
 17. Nakashima Y., Tachibana R., Babaguchi N. Watermarked movie soundtrack finds the position of the camcorder in a theater. *IEEE Transactions on Multimedia*. 2009. vol. 11. № 3. pp. 443–454.
 18. Tachibana R. Sonic watermarking. *EURASIP Journal on Advances in Signal Processing*. 2004. vol. 2004. № 13. DOI: 10.1155/S1110865704403138.
 19. Tachibana R. Audio watermarking for live performance. *Security and Watermarking of Multimedia Contents V*. SPIE. 2003. vol. 5020. pp. 32–43. DOI: 10.1117/12.476832.
 20. Zhang Z., Wu X. An audio covert communication system for analog channels. *International Conference on Electrical and Control Engineering*. IEEE. 2010. pp. 3279–3282. DOI: 10.1109/iCECE.2010.800.
 21. Kaneto R., Nakashima Y., Babaguchi N. Real-time user position estimation in indoor environments using digital watermarking for audio signals. *20th International Conference on Pattern Recognition*. IEEE. 2010. pp. 97–100.

22. Gofman M.V., Kornienko A.A., Glukhov A.P. [A Positioning Method Based On Digital Audio Watermarking]. Problemy informacionnoj bezopasnosti. Komp'juternye sistemy – Problems of information security. Computer systems. 2018. № 4. pp. 120–129. (In Russ.).
23. Gofman M.V. [A Method of Hidden Data in Communication via Air Audio Channel] Trudy SPIIRAN – SPIIRAS Proceedings. 2017. № 2(51). pp. 97–122. (In Russ.)
24. Gofman M.V. [Noisproof Digital Audio Watermarking In MIMO Audio Stegosystems]. Problemy informacionnoj bezopasnosti. Komp'juternye sistemy – Problems of information security. 2021. № 3. pp. 83–95. (In Russ.).
25. Özer H., Sankur B., Memon N., Avcıbaş İ. Detection of audio covert channels using statistical footprints of hidden messages. Digital Signal Processing. 2006. vol. 16. № 4. pp. 389–401.
26. Su Z., Zhang G., Yue F., Chang L., Jiang J., Yao X. SNR-constrained heuristics for optimizing the scaling parameter of robust audio watermarking. IEEE Transactions on Multimedia. 2018. vol. 20. № 10. pp. 2631–2644.
27. Appadurai E., Bhatt M., Geetha D. Semi Fragile Audio Crypto-Watermarking based on Sparse Sampling with Partially Decomposed Haar Matrix Structure. Acta Cybernetica. 2020. vol. 24. № 4. pp. 679–697.
28. Khillare A., Malviya A. Reversible Digital Audio Watermarking Scheme Using Wavelet Transformation. Journal of Engineering Research and Application. 2018. vol. 8(7). pp 62–72.

Gofman Maksim — Ph.D., Associate Professor of the Department, Department «informatics and information security», Emperor Alexander I St. Petersburg State Transport University. Research interests: information security. The number of publications — 45. maxgof@gmail.com; 9, Moskovsky Av., 190031, St. Petersburg, Russia; office phone: +7(812)310-3472.

Kornienko Anatolij — Ph.D., Dr.Sci., Professor of the department, Department «informatics and information security», Emperor Alexander I St. Petersburg State Transport University. Research interests: information security. The number of publications — 421. kaa.pgups@yandex.ru; 9, Moskovsky Av., 190031, St. Petersburg, Russia; office phone: +7(812)310-3472.