

СТАТИСТИЧЕСКИЕ ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ ЗВУКОВЫХ СИГНАЛОВ¹

Шишкин А. В., к.т.н., доцент

*Одесская национальная морская академия, Одесса, Украина
ovshyskin@gmail.com*

STATISTICAL DIGITAL WATERMARKS FOR AUDIO SIGNALS

Shishkin O. V., PhD, Associate Professor

Odesa National Maritime Academy, Odesa, Ukraine

Введение

Цифровые водяные знаки (ЦВЗ) [1] звуковых сигналов подразумевают встраивание дополнительной информации непосредственно в аналоговый низкочастотный сигнал. При этом ЦВЗ не оказывают сколь-либо ощутимого влияния на слуховое восприятие звукового сигнала и должны обладать устойчивостью к естественным и преднамеренным искажениям (атакам) сигнала в процессе передачи сигнала через канал. Применение ЦВЗ в системе защиты авторских прав [2] позволяет преодолеть так называемую проблему аналоговой брешы – нелегального копирования законно приобретенного продукта через аналоговый интерфейс с дальнейшим преобразованием его в цифровой формат. Применение ЦВЗ актуально для идентификации радиотелефонных передач в аналоговых УКВ радиоканалах мобильной связи авиационного [3], морского [4] и военного назначения [5].

Система ЦВЗ характеризуется взаимосвязанными параметрами: количество информации, сходство с исходным сигналом, устойчивость к атакам. Лучшее соотношение параметров может быть получено в системе с информированным кодером с использованием квантования какого-либо параметра сигнала-носителя. Однако в процессе квантования неизбежно возникают искажения звукового сигнала. В статье [6] в качестве параметра квантования предложено использовать коэффициент корреляции вектора частотных коэффициентов дискретного преобразования Фурье (ДПФ). Данный метод обеспечивает сохранение мгновенной мощности звукового сигнала в пределах узкой полосы частот и устойчивость ЦВЗ к амплитудным и межсимвольным искажениям.

Целью статьи является разработка алгоритмов статистического встраивания и обнаружения ЦВЗ звуковых сигналов в асинхронном многоканальном режиме. Выбор подходящего фрейма для встраивания ЦВЗ позволяет минимизировать вносимые в сигнал искажения. Обнаружение ЦВЗ ос-

¹ Електронний варіант статті: <http://radap.kpi.ua/radiotechnique/article/view/1071>

новано на скользящем вычислении коэффициентов корреляции векторов коэффициентов ДПФ и оценки максимального правдоподобия вектора расстояний коэффициентов на числовой решетке.

Одноканальный алгоритм

Базовый одноканальный алгоритм ЦВЗ для встраивания одного бита базируется на квантовании коэффициента корреляции сигнального вектора $\mathbf{x} = (x_1, x_2, \dots, x_L)$ и некоторого случайного вектора $\mathbf{u} = (u_1, u_2, \dots, u_L)$. Модуль коэффициента корреляции (или нормированного скалярного произведения) $\tilde{x} = \frac{(\mathbf{x}, \mathbf{u})}{\|\mathbf{x}\| \|\mathbf{u}\|}$ подвергается квантованию числовой решетке, задаваемой формулой

$$\Lambda_m = \left\{ \Delta \mathbb{N} + \frac{\Delta}{2} m + \delta \right\} \cap [0, 1), \quad (1)$$

где Δ – шаг квантования, \mathbb{N} – последовательность натуральных чисел, включая ноль, $m = \{0, 1\}$ – встраиваемый бит данных, δ – смещение решетки.

Например, полагая $\Delta = 0,5$, $\delta = 0,1$, числовые решетки для битов 0 и 1 образуются соответственно последовательностями: $\Lambda_0 = \{0, 1; 0, 6\}$ и $\Lambda_1 = \{0, 35; 0, 85\}$. Параметры Δ , δ могут быть включены в стегоключ наряду со случайным вектором \mathbf{u} .

В общем случае значение \tilde{x} является комплексным числом. Его квантованная версия \tilde{s} представляется в виде $\tilde{s} = A_s \exp(j\varphi_s)$, где амплитуда определяется формулой $A_s = \arg \min_{\lambda \in \Lambda_m} d(\lambda, |\tilde{x}|)$, а фаза сохраняется такой же как и в \tilde{x} : $\varphi_s = \varphi_x$. В статье [6] получено преобразование вектора исходного сигнала \mathbf{x} в стегосигнал \mathbf{s} в виде:

$$\mathbf{s} = \alpha \mathbf{x} + \beta \mathbf{u} \frac{\|\mathbf{x}\|}{\|\mathbf{u}\|}, \quad (2)$$

где $\alpha = \sqrt{(1 - \tilde{s} \tilde{s}^*) / (1 - \tilde{x} \tilde{x}^*)}$, $\beta = \tilde{s} - \alpha \tilde{x}$.

Преобразование (2) обеспечивает минимизацию вносимых искажений $\|\mathbf{x} - \mathbf{s}\| = \min$ при сохранении нормы $\|\mathbf{s}\| = \|\mathbf{x}\|$. Физически сохранение нормы сигнала означает сохранение его мощности.

Оценка скрытого бита ЦВЗ осуществляется на решетке (1) исходя из критерия максимального правдоподобия по формуле:

$$\hat{m} = \arg \min_{\lambda \in \Lambda_m} \text{dist}(|\tilde{y}|, \lambda), \quad (3)$$

где $\tilde{y} = (\mathbf{y}, \mathbf{u}) / (\|\mathbf{y}\| \|\mathbf{u}\|)$ – коэффициент корреляции принятого вектора \mathbf{y} .

ЦВЗ по данному алгоритму нечувствительны к искажениям амплитудного масштаба несмотря на наличие операции квантования.

Система ЦВЗ звуковых сигналов с информированным кодером показана на рис. 1. Кодер ЦВЗ располагается в разрыве низкочастотной цепи непосредственно за микрофоном (точки 1 – 2). Под каналом здесь понимается весь комплекс стандартного радиооборудования, который осуществляет типовые преобразования сигналов: квантование, усиление, модуляцию, сжатие и другие операции, а также соответствующие им обратные преобразования, включая собственно эфирный радиоканал с присущими ему помехами. Выходной сигнал для извлечения ЦВЗ снимается с выхода звукового сигнала (точка 3).

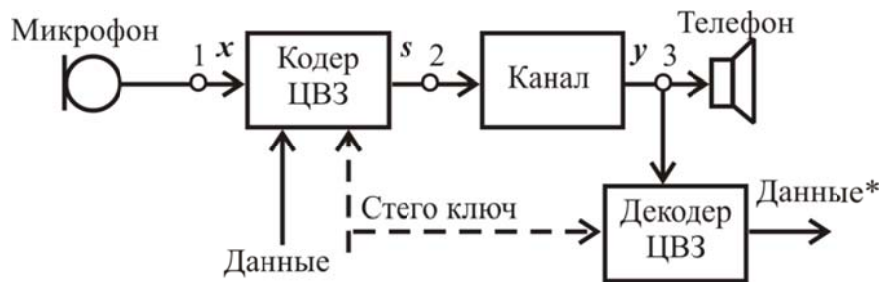


Рис. 1. Система ЦВЗ звуковых сигналов

Многоканальный алгоритм

Для повышения и помехоустойчивости ЦВЗ к межсимвольным искажениям применен многоканальный алгоритм. В многоканальном алгоритме каждый бит информационного пакета ЦВЗ передается в узкой частотной полосе спектра звукового сигнала. Тем самым реализуется принцип технологии частотного ортогонального мультиплексирования (OFDM). Для передачи одного бита используется сигнальный вектор длиной L , который образован соседними частотными коэффициентами ДПФ. Минимальная длина вектора, при котором одноканальный алгоритм (1) – (3) работоспособен, равен $L = 2$. В принципе, чем больше L , тем более помехоустойчив алгоритм. Однако стремление к узкой субканальной полосе частот ограничивает размер вектора. С точки зрения слухового восприятия изменение мощности соседних гармоник, образующих вектор, не ощущаются на слух, так как сохраняется общая мощность (или норма) сигнального вектора.

В предложенном n -канальном алгоритме при частоте дискретизации $F_s = 8$ кГц и длине фрейма (и размерности ДПФ) $N = 512$ длины субканальных векторов лежат в диапазоне от 2 до 7 при общем числе субканалов $n = 63$ и занимаемой полосе частот (15,6 – 3000) Гц. Длины векторов рассчитывались на основе мел-шкалы с увеличением длины от минимальной $L = 2$ до $L = 7$. Для формирования 63 векторов задействованы коэффициенты ДПФ с 1-го по 193, нулевой коэффициент (постоянная составляющая) не используется. Ширина полосы каждого субканала определяется очевид-

ным соотношением $\Delta f_i = L_i F_s / N$.

Внесение ЦВЗ сопровождается определенными искажениями сигнала-носителя. Эти искажения могут проявляться в большей или меньшей степени в зависимости от близости значения коэффициента корреляции к квантованному значению в каждом канале $d_i = |\tilde{x}_i - \tilde{s}_i|$. В идеальном случае, когда $\tilde{s}_i = \tilde{x}_i$, как следует из (2), никаких искажений в i -м субканале вообще не потребуется. Поэтому подходящий для встраивания фрейм может быть оценен вектором расстояний $\mathbf{d} = (d_1, d_2, \dots, d_n)$.

Статистические ЦВЗ подразумевают предварительную оценку пригодности скользящего звукового фрейма для встраивания информации в коде-ре ЦВЗ. Оценка текущего фрейма для встраивания ЦВЗ сводится к следующему правилу: Если норма вектора \mathbf{d} не превышает некоторого порога ρ_1 , т.е. $\|\mathbf{d}\| \leq \rho_1$, то осуществляется встраивание ЦВЗ, в противном случае – отказ от ЦВЗ в текущем фрейме и продвижение фрейма на один отсчет вперед.

Для стабилизации вносимых искажений к уровню громкости звукового сигнала предложено использовать плавающий порог по формуле:

$$\rho_1 = h \Delta \frac{\sigma_{\text{long}}}{\sigma_{\text{frame}}}, \quad (4)$$

где – $h=0,5 \dots 8$ – коэффициент, задающий интенсивность встраивания ЦВЗ, Δ – шаг квантования на числовой решетке, σ_{long} , σ_{frame} – среднеквадратические отклонения (СКО) звукового сигнала, вычисленные соответственно на длительном (3 – 5) секунд и коротком в течение одного фрейма интервалах.

В результате предварительной оценки возможности встраивания ЦВЗ удастся существенно уменьшить вносимые искажения и, соответственно, слуховую восприимчивость ЦВЗ. Передача ЦВЗ при этом происходит в асинхронном режиме.

Обнаружение ЦВЗ

Процедура обнаружения и декодирования ЦВЗ построена на оценке скользящего фрейма, составленного из N последовательных отсчетов принятого сигнала и может быть пояснена следующим образом. Первоначально вычисляется ДПФ текущего фрейма. Далее производится вычисление коэффициентов корреляции \tilde{y}_i принятых векторов \mathbf{y}_i в частотной области и случайных последовательностей \mathbf{u}_i . Для вычисления расстояний используются те же решетки Λ_0 , Λ_1 и что и при кодировании. Затем вычисляют наименьшие субканальные расстояния модулей коэффициентов корреляции принятого вектора частотных коэффициентов до узлов объеди-

ненных решеток $\Lambda_{10} = \Lambda_0 \cup \Lambda_1$:

$$d_i = \min_{\lambda \in \Lambda_{10}} \text{dist}(|\tilde{y}_i|, \lambda). \quad (5)$$

Решение об обнаружении ЦВЗ выносится на основании сравнения нормы вектора расстояний \mathbf{d} с порогом: если $\|\mathbf{d}\| \leq \rho_2$, то ЦВЗ обнаружен, в противном случае – нет.

Оценка встроенного бита в каждом субканале осуществляется по формуле:

$$\hat{m}_i = \arg \min_{\lambda \in \Lambda_m} d(|\tilde{y}_i|, \lambda). \quad (6)$$

Обоснуем возможность такого подхода к обнаружению ЦВЗ. Найдем законы распределения вероятности случайной величины $\|\mathbf{d}\|$ при отсутствии и наличии ЦВЗ. Положим, что расстояние $d_i = \xi$ является случайной величиной, распределенной по равномерному закону на интервале $(-\Delta/4, \Delta/4)$ с плотностью вероятности $w(\xi) = 2/\Delta$. Обозначим дисперсию случайной величины ξ при отсутствии ЦВЗ через σ_0^2 . Для равномерного закона распределения она равна $\sigma_0^2 = (\Delta/2)^2/12 = \Delta^2/48$. Найдем среднее значение и дисперсию нормы вектора расстояний $\|\mathbf{d}\| = \left(\sum_{i=1}^n d_i^2\right)^{1/2}$.

Распределение квадрата случайной величины $\eta = \xi^2$ может быть получено через якобиан нелинейного преобразования [7]:

$$W(\eta) = \frac{1}{\sqrt{\eta}} \left[w(\sqrt{\eta}) + w(-\sqrt{\eta}) \right] = \frac{2}{\Delta\sqrt{\eta}}.$$

Среднее и дисперсия η непосредственно определяются из формул:

$$m_\eta = \int_{-\Delta/4}^{\Delta/4} \xi^2 w(\xi) d\xi = \frac{\Delta^2}{48},$$

$$\sigma_\eta^2 = \int_{-\Delta/4}^{\Delta/4} (\eta - m_\eta)^2 w(\xi) d\xi = \frac{\Delta^2}{720}.$$

Распределение суммы n независимых случайных величин в силу центральной предельной теоремы при достаточно большом числе n аппроксимируется нормальным законом:

$$\gamma = \left(\sum_{i=1}^n \eta_i\right) \sim N(nm_\eta, n\sigma_\eta^2).$$

И, наконец, распределение нормы вектора $\|\mathbf{d}\|$ может быть получено путем нелинейного преобразования $\|\mathbf{d}\| = g(\gamma)$ типа \sqrt{x} посредством линейной аппроксимации нелинейной функции [7]. Случайная величина $\|\mathbf{d}\|$ выражается через величину γ в окрестности точки $C = m_\gamma$ следующим об-

разом:

$$\|d\| = a_0 + a_1(\gamma - C),$$

где $a_0 = g(C)$, $a_1 = \left. \frac{dg}{d\gamma} \right|_{\gamma=C} = \frac{1}{2\sqrt{C}}$.

Имеем линейное преобразование нормальной величины γ . После несложных операций получим следующие искомые значения среднего и дисперсии при отсутствии ЦВЗ:

$$m_{\|d\|,0} = \sigma_0 \sqrt{n} = \frac{\Delta}{4} \sqrt{\frac{n}{3}}, \quad \sigma_{\|d\|,0}^2 = \frac{\sigma_0^2}{5} = \frac{\Delta^2}{240}. \quad (7)$$

Существенным выводом, следующим из формул (7) является то, что дисперсия распределения нормы не зависит от числа субканалов n , а среднее значение возрастает пропорционально \sqrt{n} .

В случае присутствия ЦВЗ на интервале наблюдения закон распределения расстояний d_i может быть принят нормальным с нулевым средним и дисперсией σ_1^2 . Строго говоря «хвосты» распределения зеркально отражаются в точках $\xi = \pm\Delta/4$. Для нормального закона распределения, основываясь на результатах из [6] и проделав аналогичные вычисления, получим среднее значение и дисперсию равными соответственно:

$$m_{\|d\|,1} = \sigma_1 \sqrt{n}, \quad \sigma_{\|d\|,1}^2 = \sigma_1^2 / 2.$$

Принимая во внимание зеркальное отражение кривой распределения в точках $\xi = \pm\Delta/4$, очевидно, что СКО расстояний в случае наличия ЦВЗ σ_1 никак не может превышать значение СКО σ_0 в случае отсутствия ЦВЗ, т.е. $\sigma_1 \leq \sigma_0$.



Рис. 2. Функции распределения вероятностей нормы вектора расстояний

ошибок 1-го и 2-го рода.

Соответственно $m_{\|d\|,1} \leq m_{\|d\|,0}$ и с ростом n кривые распределений удаляются друг от друга при сохранении дисперсий. Таким образом, вычисление $\|d\|$ и сравнение ее с порогом позволяет обнаружить ЦВЗ вне зависимости от его информационного наполнения без использования каких-либо специальных меток. Плотности вероятности $\|d\|$ при отсутствии/наличии ЦВЗ представлены на рис. 2 вместе с иллюстрацией

Для повышения достоверности декодирования ЦВЗ предложено использовать блочный корректирующий код Боуза-Чоудхури-Хоквингема (БЧХ) [8] с параметрами (63, 30, 6). Код БЧХ(63, 30, 6) имеет общую длину блока $n = 63$, число информационных битов $k = 30$ и максимальное число исправляемых ошибок на блок $t = 6$.

В морской радиосвязи для опознавания судов и береговых станций используется 9-тизначный идентификатор морской подвижной службы (ИМПС). В двоичной кодировке ИМПС представляется 30-ю двоичными разрядами. Поэтому для передачи ИМПС в системе автоматической идентификации голосового сообщения достаточно одного блока кода БЧХ(63, 30, 6).

Известно, что коды БЧХ не принадлежат к классу совершенных кодов, для которых любая произвольная последовательность из n бит обязательно декодируется в какое-либо разрешенное кодовое слово. При невозможности декодирования БЧХ декодер устанавливает флажок отказа от декодирования. Вероятность такого отказа от декодирования при случайном выборе кодового слова может быть получена из формулы:

$$P_{\text{од}} = \frac{2^n - 2^k (1 + \sum_{i=1}^t C_n^i)}{2^n}, \quad (8)$$

где $C_n^i = \frac{n!}{i!(n-i)!}$ – биномиальные коэффициенты.

Для кода БЧХ(63,30,6) из формулы (8) получим $P_{\text{од}} = 0,9912$.

В приложениях ЦВЗ необходимо минимизировать ошибки 2-го рода, иначе будут получены искаженные данные идентификации о передающем судне. Ошибки 1-го рода, т.е. пропуск ЦВЗ не являются столь критичными, поскольку данные идентификации повторяется многократно в течении передачи сигнала. При установке порога обнаружения $\rho_2 = m_0 - 5\sigma_0$ вероятность ошибки 2-го рода (false-negative) составляет $P_{FN} \approx 2 \times 10^{-7}$ для параметров $\Delta = 1, n = 63$.

Декодер БЧХ дополнительно снижает вероятность ошибки 2-го рода за счет отказа от декодирования отсутствующего ЦВЗ. Результирующая ошибка 2-го рода составит величину $P_{\text{ош}2} = P_{FN} (1 - P_{\text{од}}) \approx 2 \times 10^{-9}$.

Результаты моделирования

Разработанные алгоритмы исследовались на реальных речевых сигналах в среде Матлаб.

Влияние шага квантования Δ и коэффициента интенсивности h на скорость передачи скрытой информации (бит/с) и качество сигнала (дБ) представлено в табл. 1 в виде пары значений R / SWR .

Скорость информации рассчитывалась как средняя скорость передачи

інформації на протяженні речевого сигналу по формуле:

$$R = \frac{N_{\text{TX}} k}{l_{\text{wav}} F_s}, \quad (9)$$

где N_{TX} – число переданих фреймов; l_{wav} – количество отсчетов в тестируемом сигнале wav-формата; k – количество информационных бит в одном ЦВЗ.

Для оценки качества сигнала использовалось отношение SWR мощностей сигнала-носителя и вносимых искажений, рассчитываемое в частотно-временной плоскости спектрограммы ($N_{SP} \times T_{SP}$) по формуле:

$$SWR = 10 \lg \frac{\sum_{j=1}^{T_{SP}} \sum_{i=1}^{N_{SP}} X_{ij}^2}{\sum_{j=1}^{T_{SP}} \sum_{i=1}^{N_{SP}} (X_{ij} - S_{ij})^2}. \quad (10)$$

В соответствии со стандартом Международной федерации фонографической промышленности (IFPI) [2] внесение ЦВЗ не должно снижать качество звукового сигнала ниже 20 дБ. Удовлетворяющие этому требованию характеристики отделены в табл. 1 жирной линией.

Таблица 1

Шаг квантования Δ	Коэффициент интенсивности h				
	0,5	1	2	4	8
0,25	93/48,8	136/41,5	238/32,6	390/24,8	458/21,4
0,5	93/43,1	136/34,5	221/26,1	348/19,5	458/14,4
1,0	85/38,9	136/30,4	229/21,2	331/14,6	450/ 8,7
2,0	93/34,6	144/24,3	212/16,8	348/ 9,8	450/ 5,4

В монографии [2] приведены показатели звуковых ЦВЗ, полученные методом сингулярного разложения (singular value decomposition) матриц коэффициентов вейвлет и косинусного преобразований, которые позиционируются как лучшие на текущий момент. Указанный метод разработан для сигналов в полосе частот до 18 кГц музыкального содержания и позволяет получить скорость передачи данных ЦВЗ 172 бит/с при отношении SWR около 40 дБ. В нашем случае скорость передачи данных для $SWR \approx 40$ дБ составляет (85 – 136) бит/с.

Однако для объективной сравнительной оценки количества встраиваемой информации следует учитывать ширину полосы частот сигнала-носителя ЦВЗ и рассчитывать не усредненную скорость передачи скрытой информации в составе ЦВЗ, а ее плотность в плоскости частота – время, измеренную в (бит/с)/Гц. Тогда с учетом отличающихся в $18/3 = 6$ раз по ширине частотных полосах сигнала-носителя плотность данных ЦВЗ в разработанных алгоритмах превышает примерно в (3 – 5) раз плотность скрываемой информации по методу [2] при том же уровне искажений. При

этом следует подчеркнуть, что в табл. 1 приведены сведения по количеству полезной и исправленной от ошибок информации (30 бит на один пакет ЦВЗ), а не всей встраиваемой информации с учетом избыточности (63 бита на пакет ЦВЗ).

Помехоустойчивость ЦВЗ к атакам в канале оценивалась отношением числа обнаруженных и верно декодированных пакетов ЦВЗ к общему числу встроенных пакетов. В качестве атак принимались следующие: компрессия – растяжение по амплитуде по μ -закону, фильтрация, отражающая неравномерность амплитудно-частотной характеристики сквозного тракта, аддитивный гауссовский шум, измеренный по отношению к средней мощности звукового сигнала, квантование по амплитуде последовательности сигнальных отсчетов на 256 уровнях и преобразование цифровых форматов и битрейтов wav (64 кбит/с) – mp3 (8 кбит/с) – wav (64 кбит/с). Результаты в зависимости от шага квантования коэффициента корреляции сведены в табл. 2.

Таблица 2

Шаг квантования	Компандирование	Фильтрация	Аддитивный шум, дБ			Квантование	MP3 сжатие
			-40	-30	-20		
0,125	0,76	0,13	0,23	0	0	0,5	0,62
0,25	1	0,36	0,75	0,1	0	0,63	0,87
0,5	1	0,82	1	0,37	0,09	0,84	1
1	1	1	1	1	0,43	1	1
2	1	1	1	1	0,68	1	1

Выводы

Реализация статистического подхода к встраиванию ЦВЗ в звуковой сигнал на основе оценки вносимых искажений позволяет эффективно решить задачу количество информации – искажения. Применение асинхронного режима встраивания ЦВЗ в «удобные» фреймы совместно с алгоритмом квантования коэффициента корреляции, узкополосной многоканальной обработки и помехоустойчивого кодирования позволило получить характеристики, превосходящие известные.

Алгоритм обнаружения и декодирования ЦВЗ позволяет обойтись без использования каких-либо маркерных и синхронизирующих сигналов.

Несмотря на большой объем вычислений, разработанные алгоритмы статистических ЦВЗ могут быть достаточно просто реализованы для работы в реальном времени, так как хорошо векторизуются и используют стандартные процедуры БПФ и помехоустойчивого кодирования.

Устойчивость разработанных ЦВЗ к квантованию и преобразованию цифровых форматов позволяет применять их не только в аналоговых, но и цифровых каналах передачи информации.

Перечень ссылок

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
2. Dhar P.K. Advances in Audio Watermarking Based on Singular Value Decomposition / P.K. Dhar, T. Shimamura. – Springer, 2015. – 58 p.
3. Hofbauer K. Speech Watermarking for Analog Flat-Fading Bandpass Channels / K., Hofbauer G. Kubin, W. B. Kleijn // *IEEE Trans on Audio, Speech, and Language Processing*. – 2008. – Vol. 17, No 8. – pp 1624 – 1637.
4. Шишкин А. В. Идентификация радиотелефонных передач в УКВ диапазоне морской радиосвязи // *Известия вузов. Радиоэлектроника*. – 2012. – Т. 55, № 11. – С. 11 – 20.
5. Piotrowski Z. Electromagnetic Compatibility of the Military Handset with Hidden Authorization Function Based on MIL-STD-461D Results / Z. Piotrowski, L. Nowosielski, L. Zagodzinski, P. Gajewski // *PIERS Online*. – 2008. – Vol. 4, No. 5. – pp. 566 – 570.
6. Шишкін О.В. Прихована цифрова модуляція звукових сигналів / О. В. Шишкін // *Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування*. – 2014. – № 58. – с. 129-138.
7. Горяинов В.Т. Примеры и задачи по статистической радиотехнике / В.Т. Горяинов, А.Г. Журавлев, В.И. Тихонов; под ред. В.И. Тихонова. – М. : Советское радио, 1970, 600 с.
8. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение: пер. с англ. / Р. Морелос-Сарагоса. – М. : Техносфера, 2005.– 320 с.

References

1. Konakhovich G.F. and Puzyrenko A.Yu. (2006) *Kompyuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press, 288 p.
2. Dhar P.K. and Shimamura T. (2015) *Advances in Audio Watermarking Based on Singular Value Decomposition*, Springer, 58 p.
3. Hofbauer K., Kubin G., and Kleijn W. B. (2008) Speech Watermarking for Analog Flat-Fading Bandpass Channels, *IEEE Trans on Audio, Speech, and Language Processing*, Vol. 17, No 8, pp. 1624 – 1637.
4. Shishkin A.V. (2012) Identification of radiotelephony transmissions in VHF band of maritime radio communications. *Radioelectronics and Communications Systems*, Vol. 55, No 11, pp. 482 – 489.
5. Piotrowski Z., Nowosielski L., Zagodzinski L., and Gajewski P. (2008) Electromagnetic Compatibility of the Military Handset with Hidden Authorization Function Based on MIL-STD-461D Results. *PIERS Online*, Vol. 4, No. 5, pp. 566 – 570.
6. Shishkin A.V. (2014) Hidden Digital Modulation of Audio Signals. *Visn. NTUU KPI, Ser. Radiotekh. Radioaпаратobuduv.*, No 58, pp. 129-138. (in Ukrainian)
7. Goryainov V.T., Zhuravlev A.G. and Tikhonov V.I. eds. (1970) *Primery i zadachi po statisticheskoy radiotekhnike* [Examples and problems of statistical radio engineering], Moscow, Sovetskoe radio, 600 p.
8. Morelos-Zaragoza R.H. (2006) *The Art of Error Correcting Coding*. John Wiley & Sons Ltd., 263 p.

Шишкин А. В. Статистические цифровые водяные знаки звуковых сигналов. Разработаны алгоритмы встраивания и обнаружения цифровых водяных знаков в звуковые сигналы на основе анализа скользящего фрейма в частотной области. Алгоритмы обеспечивают минимизацию искажений сигнала, обнаружение и декодирование ЦВЗ в асинхронном режиме без использования каких-либо маркеров и синхросигналов. Для обеспечения помехоустойчивости ЦВЗ применена узкополосная многоканальная передача и помехоустойчивое кодирование.

Ключевые слова: цифровые водяные знаки, идентификация, коэффициент корреляции, квантование, норма сигнала, дискретное преобразование Фурье, кодирование с исправлением ошибок.

Шишкін О. В. Статистичні цифрові водяні знаки звукових сигналів. Розроблені алгоритми вбудовування і виявлення цифрових водяних знаків в звукові сигнали на основі аналізу ковзаючого фрейма у частотній області. Алгоритми забезпечують мінімізацію спотворень сигналу, виявлення і декодування ЦВЗ в асинхронному режимі без використання яких-небудь маркерів і синхросигналів. Для забезпечення завадостійкості ЦВЗ застосована вузькосмугова багатоканальна передача і завадостійке кодування.

Ключові слова: цифрові водяні знаки, ідентифікація, коефіцієнт кореляції, квантування, норма сигналу, дискретне перетворення Фур'є, кодування з виправленням помилок.

Shyshkin O. V. Statistical Digital Watermarks of Audio Signals.

Introduction. Digital watermarks (DWM) refer to embedding additional information directly into audio signal for digital right management and automatic identification of radiotelephone transmissions in aeronautical, maritime and military VHF communication.

The main part. The designed embedding algorithm is based on evaluation of sliding frame to embed information or no regarding to distortions introduced by DWM. Watermark location is grounded calculation of distances norm between received and maximum likelihood estimated signal vectors in the domain of Discreet Fourier Transform and doesn't need for any marking and synchronizing measures. Robustness of DWM against quantization, filtering, additive Gaussian noise, digital format conversion is provided by multichannel narrowband DWM transmission and application of BCH (63,30,6) error-correction code. The proposed algorithm demonstrates watermark inaudibility because of preserving signal power before and after data embedding and searching the most suitable frames for DWM positioning.

Conclusion. The proposed algorithms provide advanced compromising solution of audio watermarking process: data payload – inaudibility – robustness. The designed algorithms are applicable both in analog and digital channels for transmission monitoring and digital right management.

Keywords: digital watermarks, identification, correlation coefficient, quantization, signal norm, discrete Fourier transform, error correcting coding.