УДК 621.391.7

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ ДЛЯ РАДИОТЕЛЕФОННЫХ КАНАЛОВ С МЕЖСИМВОЛЬНОЙ ИНТЕРФЕРЕНЦИЕЙ

ШИШКИН А.В., КОШЕВОЙ В.М.

Национальный университет «Одесская морская академия»
ул. Дидрихсона8, г. Одесса, 65029, Украина
info@onma.edu.ua

ЦИФРОВІ ВОДЯНІ ЗНАКИ ДЛЯ РАДІОТЕЛЕФОННИХ КАНАЛІВ З МІЖСИМВОЛЬНОЮ ІНТЕРФЕРЕНЦІЄЮ

ШИШКІН О.В., КОШЕВИЙ В.М.

Національний університет «Одеська морська академія»
вул. Дідрихсона, 8, м. Одеса, 65029, Україна
info@onma.edu.ua

DIGITAL WATERMARKS FOR RADIOTELEPHONE CHANNELS WITH INTERSYMBOL INTERFERENCE

SHYSHKIN O.V., KOSHEVYY V.M.

National University «Odessa Maritime Academy»,
Didrikson str., 8, 65029, Ukraine, Odessa,
info@onma.edu.ua

Аннотация. *Разработан метод встраивания дополнительных данных в виде цифровых водяных знаков (ЦВЗ) в речевые сообщения, передаваемые в аналоговых радиотелефонных каналах морской подвижной службы. Встраивание данных осуществляется в области коэффициентов дискретного преобразования Фурье (ДПФ) в схеме с информированным кодером. Для повышения устойчивости ЦВЗ к межсимвольным искажениям предложен многоканальный алгоритм передачи данных ЦВЗ в узкополосных частотных каналах по принципу ортогонального частотного мультиплексирования (OFDM). Базовый одноканальный алгоритм формирования ЦВЗ основан на модуляции коэффициента корреляции (КК) вектора коэффициентов ДПФ и некоторого случайного вектора. В результате модуляции вычисляется новый вектор коэффициентов, который имеет ту же евклидову норму, КК с заданным квантованным значением и обладает наименьшим средним квадратом отклонений от исходного вектора. Это позволяет реализовать сохранение физической мощности сигнала в узкой полосе частот для слуховой невосприимчивости вносимых искажений сигнала и обеспечить устойчивость ЦВЗ к амплитудным искажениям. При фиксации уровня искажений из возможных видов модуляции КК амплитудной, фазовой и квадратурно-амплитудной наибольшая помехоустойчивость ЦВЗ обеспечивается для амплитудной модуляции. Проведённые испытания в off-lineрежиме с использованием морских УКВ радиостанций Sailor показали возможность реализации скорости передачи данных ЦВЗ R = 125 бит/с в стандартной полосе радиотелефонии 3 кГц при отношениях ЦВЗ/сигнал WSR = –12,4 дБ и сигнал/шум SNR = 14 дБ. Практическая реализация автоматической идентификации голосовых передач посредством ЦВЗ в УКВ каналах морской радиосвязи может быть осуществлена без замены существующей аппаратуры радиосвязи. К УКВ трансиверу подключается только телефонная трубка с встроенным микрочипом и схема дешифрации ЦВЗ.*

Ключевые слова: *стеганография, автоматическая идентификация, дискретное преобразование Фурье, коэффициент корреляции, дискретизация, квантование, норма сигнала, OFDM, модуляция, помехоустойчивость, УКВ радиоканал.*

Анотація. *Розроблено метод вбудовування додаткових даних у вигляді цифрових водяних знаків (ЦВЗ) в мовні повідомлення, що передаються в аналогових радіотелефонних каналах морської рухомої служби. Вбудовування даних здійснюється в області коефіцієнтів дискретного перетворення Фур'є (ДПФ) в схемі з поінформованим кодером. Для підвищення стійкості ЦВЗ до міжсимвольних спотворень запропонований багатоканальний алгоритм передачі даних ЦВЗ в вузькосму-*

гових частотних каналах за принципом ортогонального частотного мультиплексування (OFDM). Базовий одноканальний алгоритм формування ЦВЗ заснований на модуляції коефіцієнта кореляції (КК) вектора коефіцієнтів ДПФ і деякого випадкового вектора. В результаті модуляції обчислюється новий вектор коефіцієнтів, який має ту ж евклідову норму, КК із заданим квантованим значенням і володіє найменшим середнім квадратом відхилень від вихідного вектора. Це дозволяє реалізувати збереження фізичної потужності сигналу у вузькій смузі частот для слуховий несприйнятливості внесених спотворень сигналу і запровадити стійкість ЦВЗ до амплітудних спотворень. При фіксації рівня спотворень з можливих видів модуляції КК амплітудної, фазової та квадратурного-амплітудної найбільша стійкість ЦВЗ забезпечується для амплітудної модуляції. Проведені випробування в offline режимі з використанням морських УКХ радіостанцій Sailor показали можливість реалізації швидкості передачі даних ЦВЗ R = 125 біт / с в стандартній смузі радіотелефонії 3 кГц при відносинах ЦВЗ / сигнал WSR = –12,4 дБ і сигнал/шум SNR = 14 дБ. Практична реалізація автоматичної ідентифікації голосових передач за допомогою ЦВЗ в УКХ каналах морського радіозв'язку може бути здійснена без заміни існуючої апаратури радіозв'язку. До УКХ трансівера підключається тільки телефонна трубка з вбудованим мікрочіпом і схема дешифрування ЦВЗ.

***Ключові слова**: Стеганографія, автоматична ідентифікація, дискретне перетворення Фур'є, коефіцієнт кореляції, дискретизація, квантування, норма сигналу, OFDM, модуляція, стійкість до перешкод, УКХ радіоканал.*

***Abstract.** A method for embedding additional data in the form of digital watermarks (DWM) in the voice messages transmitted via analog radiotelephone channels of the maritime mobile service has been designed. Data embedding is carried out in the frequency domain of the discrete Fourier transform (DFT) coefficients in a scheme with an informed encoder. In order to increase the resistance of digital watermarks against intersymbol interferences, a multi-channel algorithm for the digital watermarks data transmission in a narrow-band frequency channels according to the orthogonal frequency multiplexing (OFDM) principle has been proposed. The basic single-channel algorithm for the DWM formation is based on the modulation of the correlation coefficient (CC) of the DFT coefficients vector and a certain random vector. As a result of the modulation, a new vector of coefficients is calculated, which has the same Euclidean norm, a CC with a given quantized value and has the smallest mean square root deviation from the original vector. This allows to preserve the physical power of the signal in a narrow frequency band for the auditory immunity of the introduced distortion of the signal and to ensure the robustness of DWM to amplitude distortion. Under fixing the distortion level the possible types of CC modulation amplitude, phase and quadrature-amplitude, the best robustness of the DWM is provided for amplitude modulation. The off-line tests were carried out using the Sailor maritime VHF radio stations showed the possibility of realizing the DWM data transfer rate R = 125 bit/sec in the standard 3 kHz radiotelephony frequency band with the watermark-to-signal ratio WSR = –12.4 dB and signal-to-noise ratio SNR = 14 dB. The practical implementation of the automatic identification of voice transmissions using DWM in the VHF maritime radio channels can be carried out without replacing the existing radio equipment. Only a handset with a built-in microchip and a DWM decryption circuit should be connected to the VHF transceiver.*

***Keywords**: steganography, automatic identification, discrete Fourier transform, correlation coefficient, sampling, quantization, signal rate, OFDM, modulation, robustness, VHF radio channel.*

ВВЕДЕНИЕ

Технологии цифровых водяных знаков (ЦВЗ) и стеганографии– новые направления цифровой обработки сигналов, позволяющие решать задачи защиты информации от несанкционированного копирования, аутентификации и идентификации, секретной связи и другие на основе незаметного, скрытого встраивания информации в передаваемое сообщение или компьютерные файлы (программы, звук, изображение, видео) без увеличения его объёма[1,2].

Разработано большое количество стеганографических методов и их классификаций. Одна из конструктивных классификаций [3] предусматривает деление всех методов на два класса: 1) методы, в которых сигнал-носитель не влияет на встраиваемый сигнал (неинформированный кодер) и 2) методы с учётом сигнала-носителя на встраиваемый сигнал (информированный кодер). К первому классу следует отнести алгоритмы, основанные на независимом суммировании сигнала-носителя с псевдослучайной последовательностью, модулированной скрываемыми данными[4,5]. По аналогии с мобильной связью за такими методами закрепилось название «расширение спектра», хотя в данном случае скрываемый сигнал может занимать ту же полосу частот, что и сигнал-носитель. Для детектирования скрытого сиг-

нала с расширенным спектром используют согласованную фильтрацию. Скрываемый сигнал здесь выступает в роли очень слабого полезного сигнала, а сигнал-носитель – в роли помехи. Для алгоритмов класса 1) количество информации в расчёте на один отсчёт сигнала-носителя, как показано ниже, остаётся незначительным.

Методы, относящиеся ко второму классу, позволяют в принципе устранить мешающее воздействие сигнала-носителя на основе знаний о сигнале. Эти методы связаны с квантованием какого-либо параметра либо функционального преобразования сигнала в соответствии с данными ЦВЗ [6,7]. Указанные методы ориентированы на использование, прежде всего, в компьютерных файлах. Технология автоматической идентификации (АИ) голосовых радиопередач на основе ЦВЗ [8,9] требует дальнейшего развития и исследования с учётом всего комплекса помех для ЦВЗ в реальном радиотелефонном канале.

Настоящая статья посвящена разработке и исследованию метода стеганографического встраивания данных и многоканального алгоритма их передачи на фоне телефонных сигналов в морской радиотелефонии с учётом всего комплекса помех для решения задач скрытной передачи секретной информации и автоматической идентификации передающей станции.

ЦВЗ В МОРСКОЙ РАДИОСВЯЗИ.

В морской подвижной службе (МПС) для радиотелефонной связи в УКВ и ПВ/КВ диапазонах используется аналоговая модуляциясклассами радиоизлучений F3E/G3E и J3Есоответственно. Наиболее интенсивно используемым видом радиосвязи является УКВ радиотелефония, которая во многом определяет навигационную безопасность судоходства. Для оперативного и адресного радиообмена необходима чёткая и однозначно понимаемая идентификация передающей стороны. В то же время автоматическая идентификация (АИ) радиопередач в морских каналах радиосвязи в настоящее время отсутствует. Голосовая идентификация судна путём передачи названия судна, позывного сигнала или его текущих координат может быть получена с задержкой, ошибочно воспринята, или отсутствовать вообще. Кроме того преднамеренно анонимные передачи, особенно на частотах бедствия и безопасности пагубно сказываются на общей безопасности судоходства.

Аналогичная проблема имеет место и в системе радиосвязи с воздушными судами гражданской авиации [10], где также используются аналоговые каналы с голосовой идентификацией.

Другой областью применения стеганографической передачи данных на фоне голосового сообщения может быть ее использование в особых обстоятельствах, например, при террористических атаках.

Кроме собственно самого сигнала-носителя существенными для ЦВЗ в радиотелефонном канале являются следующие помехи:

1) межсимвольные искажения (МСИ);

2) нелинейные искажения, в частности, клиппирование сигнала вследствие нелинейности амплитудной характеристики в схемах низкочастотного усиления;

3) медленная мультипликативная помеха μ;

4) аддитивная помеха n;

5) ошибки синхронизации тактового генератора в приёмнике.

МСИ обусловлены ограниченной частотной полосой приёмопередатчика и многолучевым характером распространения радиоволн. В морской радиотелефонии для передачи речевого сигнала стандартно отводится полоса частот 300 … 3000 Гц, в которой амплитудно-частотная характеристика (АЧХ) канала является существенно неравномерной из-за наличия реактивных элементов в низкочастотных схемах. Многолучевой характер распространения радиоволн обуславливает быстрые частотно-селективные искажения принимаемого сигнала. Таким образом, две разные по своей физической природе причины искажений приводят к

одному и тому же типу линейных или межсимвольных искажений, которые по совокупности моделируются преобразованием линейной фильтрации.

Медленная мультипликативная помеха μ или неселективные замирания имеют место тогда, запаздывания копий сигнала при многолучевом прохождении отличаются незначительно в сравнении с длительностью одного символа и АЧХ канала в этом случае близка к равномерной характеристике. Взаимный фазовый сдвиг копий сигнала в приёмнике приводит к снижению мощности принимаемого сигнала, так называемому плоскому федингу.

Аддитивная помеха объединяет все аддитивные шумы различной физической природы, включая шумы квантования.

Под ошибкой синхронизации в данном случае понимается временной сдвиг отсчётов сигнала в передатчике и приёмнике. Десинхронизация обусловлена тем, что внутренние тактовые генераторы ЦАП и АЦП в передатчике и приёмнике соответственно не имеют общей синхронизации. Поскольку в радиоканале сигнал передаётся в аналоговой форме, то моменты взятия его отсчётов могут быть смещены на величину $\pm 1/(2F_s)$, где F_s - частота дискретизации.

Одноканальный алгоритм. Разработанный базовый одноканальный алгоритм ЦВЗ принадлежит к классу алгоритмов с информированным кодером и является нечувствительным к амплитудному изменению сигнала. Алгоритм базируется на вычислении коэффициента корреляции сигнального вектора $\boldsymbol{x} = (x_1, x_2, ..., x_L)$ и некоторого случайного вектора $\boldsymbol{u} = (u_1, u_2, ..., u_L)$:

$$\tilde{x} = \frac{(\boldsymbol{x}, \boldsymbol{u})}{\|\boldsymbol{x}\|\|\boldsymbol{u}\|}, \tag{1}$$

где $\|\cdot\|$–эвклидова норма вектора, $\|\boldsymbol{x}\| = \sqrt{x_1 x_1^* + x_2 x_2^* + ... + x_L x_L^*}$,

$*$ – операция комплексного сопряжения,

$(\boldsymbol{x}, \boldsymbol{u}) = x_1 u_1^* + x_2 u_2^* + ... + x_L u_L^*$ – скалярное произведение векторов.

В общем случае векторы $\boldsymbol{x}$ и $\boldsymbol{u}$ лежат в векторном пространстве с комплексными координатами $x \in N^L$, $L \geq 2$. Случайный вектор может использоваться в качестве секретного ключа при конфиденциальной передаче скрытой информации.

Коэффициент корреляции $\tilde{x}$ подвергается квантованию в соответствии с встраиваемым битом ЦВЗ. Возможны следующие варианты квантования $\tilde{x}$ в поле N^L комплексных чисел:

1) квантование мнимой и действительной частей $\tilde{x}$;

2) квантование амплитуды вектора $\tilde{x}$ с сохранением его фазы;

3) квантование фазы вектора $\tilde{x}$ с сохранением его амплитуды.

При квантовании может быть использована числовая решётка, задаваемая, в частности при квантовании амплитуды, формулой:

$$\Lambda_d = \left\{ \Delta m + \frac{\Delta}{2} d + \delta \right\} \bigcap [0,1) \tag{2}$$

где Δ – шаг квантования;

m–последовательность натуральных чисел, включая ноль;

$d = \{0,1\}$ – встраиваемый бит данных;

δ – смещение решётки.

Например, полагая $\Delta = 0,5$, $\delta = 0,1$, числовые решётки 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 стеганографический ключ (стегоключ) наряду со случайным вектором $\boldsymbol{u}$.

В общем случае значение скалярного произведения $\tilde{x}$ является комплексным числом.

Осуществим равномерное квантование $\tilde{x}$ путём скалярного квантования по некоторому правилу Q с шагом Δ и с учётом встраиваемого бита данных d:

$$\tilde{s} = Q(\tilde{x}, \Delta, d). \quad (3)$$

Задачу квантования сформулируем следующим образом. Необходимо найти комплексный вектор стегосигнала $\boldsymbol{s}$, те есть сигнала с встроенным битом ЦВЗ, который удовлетворяет следующим условиям:

1) $\|\boldsymbol{s}\| = \|\boldsymbol{x}\|$ – мощность сигнала сохраняется;

2) $\tilde{s}=(\boldsymbol{s},\boldsymbol{u})/\|\boldsymbol{s}\|\|\boldsymbol{u}\|$ – коэффициент корреляции векторов должен равняться значению $\tilde{s}$, определённому формулой (3), что позволит однозначно определить встроенный бит данных в приёмнике;

3) $\|\boldsymbol{s}-\boldsymbol{x}\| = \min$ – вносимые искажения должны быть минимальными.

Таким образом, имеем классическую задачу минимизации целевой функции по условию 3) при наличии ограничений по условиям 1) и 2).

Эта задача решена из следующих рассуждений. Для геометрического представления решаемой задачи рассмотрим трёхмерное векторное пространство действительных нормированных векторов.

Перенося известную формулу для скалярного произведения векторов на плоскости $(\boldsymbol{s},\boldsymbol{u})=|\boldsymbol{s}|\cdot|\boldsymbol{u}|\cos\vartheta$ в трёхмерное пространство, можно заключить, что искомый вектор $\boldsymbol{s}$ должен образовывать коническую поверхность с вершиной конуса в начале координат и высотой конуса, совпадающей по направлению с вектором $\boldsymbol{u}$. При этом угол раскрыва конуса составляет 2ϑ.

Геометрическая интерпретация для трёхмерного векторного пространства R^3 представлена на рисунке 1. Исходный вектор сигнала-носителя $\boldsymbol{x}$ должен быть трансформирован в вектор стегосигнала $\boldsymbol{s}$ при сохранении нормы $\|\boldsymbol{s}\| = \|\boldsymbol{x}\|$, т.е. длины векторов $\boldsymbol{x}$, $\boldsymbol{s}$ одинаковы. Корректирующий вектор $\boldsymbol{w}$ представляет собой сигнал ЦВЗ, который добавляется к исходному сигналу: $\boldsymbol{s} = \boldsymbol{x} + \boldsymbol{w}$ и является источником вносимых искажений.

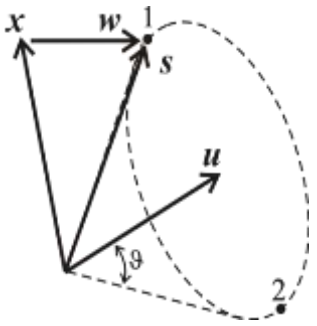


Рисунок 1 – Геометрическая интерпретация векторов в трёхмерном векторном пространстве R^3

В пространстве скалярных векторов скалярное произведение приобретает комплексное значение. В этом случае значение косинуса $\cos\vartheta = \tilde{s}$ также должно быть комплексным числом, что, в общем, имеет место исходя из обобщённого определения функции косинуса комплексного аргумента через гиперболические функции:

$$\cos(x + jy) = \cos(x)\cosh(y) - j\sin(x)\sinh(y).$$

Условие 3) $\|\boldsymbol{w}\| = \min$ накладывает на вектор $\boldsymbol{s}$ требование, что этот вектор находится в плоскости, которая проходит через векторы $\boldsymbol{x}$ и $\boldsymbol{u}$, то есть может быть представлен в виде линейной комбинации этих векторов:

$$\boldsymbol{s} = a\boldsymbol{x} + b\boldsymbol{u}. \quad (4)$$

Необходимо найти коэффициенты a и b. Для их нахождения умножим скалярно обе части уравнения (4) на вектор $\boldsymbol{u} \neq 0$:

$$(\boldsymbol{s},\boldsymbol{u}) = a(\boldsymbol{x},\boldsymbol{u}) + b(\boldsymbol{u},\boldsymbol{u}). \tag{5}$$

Отсюда коэффициент b выразится следующим образом:

$$b = \frac{(\boldsymbol{s},\boldsymbol{u}) - a(\boldsymbol{x},\boldsymbol{u})}{\|\boldsymbol{u}\|^2}. \tag{6}$$

После скалярного умножения обеих частей уравнения (4) на вектор $\boldsymbol{s}$ и учитывая свойство эрмитовой симметричности $(\boldsymbol{x},\boldsymbol{y}) = (\boldsymbol{y},\boldsymbol{x})^*$, в результате тождественных преобразований, последовательно получим:

$$\begin{aligned}
\|\boldsymbol{s}\|^2 &= a\left((a\boldsymbol{x} + b\boldsymbol{u}),\boldsymbol{x}\right)^* + b(\boldsymbol{s},\boldsymbol{u})^* = \\
&= a\left(a(\boldsymbol{x},\boldsymbol{x}) + b(\boldsymbol{u},\boldsymbol{x})\right)^* + b(\boldsymbol{s},\boldsymbol{u})^* = \\
&= a\left(a\|\boldsymbol{x}\|^2 + b(\boldsymbol{x},\boldsymbol{u})^*\right)^* + b(\boldsymbol{s},\boldsymbol{u})^* = \\
&= aa^*\|\boldsymbol{x}\|^2 + ab^*(\boldsymbol{x},\boldsymbol{u}) + b(\boldsymbol{s},\boldsymbol{u})^*.
\end{aligned}$$

Подставляя в последнее тождество выражение для коэффициента b из формулы (4), получим:

$$\|\boldsymbol{s}\|^2 = aa^*\|\boldsymbol{x}\|^2 + a\frac{(\boldsymbol{s},\boldsymbol{u})^* - a^*(\boldsymbol{x},\boldsymbol{u})^*}{\|\boldsymbol{u}\|^2}(\boldsymbol{x},\boldsymbol{u}) + \frac{(\boldsymbol{s},\boldsymbol{u}) - a(\boldsymbol{x},\boldsymbol{u})}{\|\boldsymbol{u}\|^2}(\boldsymbol{s},\boldsymbol{u})^*. \tag{7}$$

Учитывая, что $\|\boldsymbol{s}\| = \|\boldsymbol{x}\|$, далее получим:

$$1 = aa^* + a\frac{(\boldsymbol{s},\boldsymbol{u})^* - a^*(\boldsymbol{x},\boldsymbol{u})^*}{\|\boldsymbol{u}\|^2\|\boldsymbol{s}\|^2}(\boldsymbol{x},\boldsymbol{u}) + \frac{(\boldsymbol{s},\boldsymbol{u}) - a(\boldsymbol{x},\boldsymbol{u})}{\|\boldsymbol{u}\|^2\|\boldsymbol{s}\|^2}(\boldsymbol{s},\boldsymbol{u})^*.$$

$$1 = aa^* + a\left(\tilde{s}^* - a^*\tilde{x}^*\right)\tilde{x} + \left(\tilde{s} - a\tilde{x}\right)\tilde{s}^*.$$

$$1 = aa^* + a\tilde{s}^*\tilde{x} - aa^*\tilde{x}\,\tilde{x}^* + \tilde{s}\,\tilde{s}^* - a\tilde{x}\,\tilde{s}^*.$$

$$1 = aa^* - aa^*\tilde{x}\,\tilde{x}^* + \tilde{s}\,\tilde{s}^*.$$

Откуда получаем решение для коэффициента a в виде:

$$a_{1,2} = \pm\sqrt{\frac{1 - \tilde{s}\,\tilde{s}^*}{1 - \tilde{x}\,\tilde{x}^*}}. \tag{8}$$

В формуле (8) для коэффициента a радикал должен быть взят со знаком плюс, что соответствует ближайшему к вектору $\boldsymbol{x}$ решению (точка 1 на рисунке 1). Точка 2 даёт решение для наиболее удалённого вектора в случае отрицательного значения коэффициента a.

Коэффициент b, следуя (6), вычисляется по формуле

$$b = \left(\tilde{s} - a\tilde{x}\right)\frac{\|\boldsymbol{x}\|}{\|\boldsymbol{u}\|}. \tag{9}$$

Таким образом, получены коэффициенты для вычисления вектора $\boldsymbol{s}$.

Окончательно вектор $\boldsymbol{s}$ вычисляется по формуле (4) по известным векторам $\boldsymbol{x}$ и $\boldsymbol{u}$ с подстановкой в неё коэффициентов a и b.

Вектор $\boldsymbol{s}$ обеспечивает минимизацию вносимых искажений $\|\boldsymbol{x}-\boldsymbol{s}\|=\min$ при сохранении нормы $\|\boldsymbol{s}\|=\|\boldsymbol{x}\|$. Физически сохранение нормы сигнала означает сохранение его мощности.

Формулы (4), (8), (9) позволяют сформировать сигнал с ЦВЗ, который минимально (по среднему квадрату отклонения) отличается от исходного сигнала и имеет ту же мощность, что исходный сигнал. При том обеспечивается требуемое значение скалярного произведения $\tilde{s}=(\boldsymbol{s},\boldsymbol{u})/\|\boldsymbol{s}\|\|\boldsymbol{u}\|$, равное квантованному значению $\tilde{x}$. Инвариантность нормы сигнала к ЦВЗ позволяет в конечном итоге обеспечить их нечувствительность к амплитудным искажениям в канале передачи.

Для передачи дополнительной информации на фоне звукового сигнала необходима модуляция какого-либо параметра этого сигнала. Таким параметром выбран коэффициент корреляции сигнального и опорного векторов.

Коэффициент корреляции нечувствителен к амплитуде сигналов. Поэтому его использование позволяет добиться устойчивости ЦВЗ в каналах с амплитудными искажениями сигналов. К таким каналам относятся все реальные аналоговые радиотелефонные каналы МПС.

МОДУЛЯЦИЯ КОЭФФИЦИЕНТА КОРРЕЛЯЦИИ.

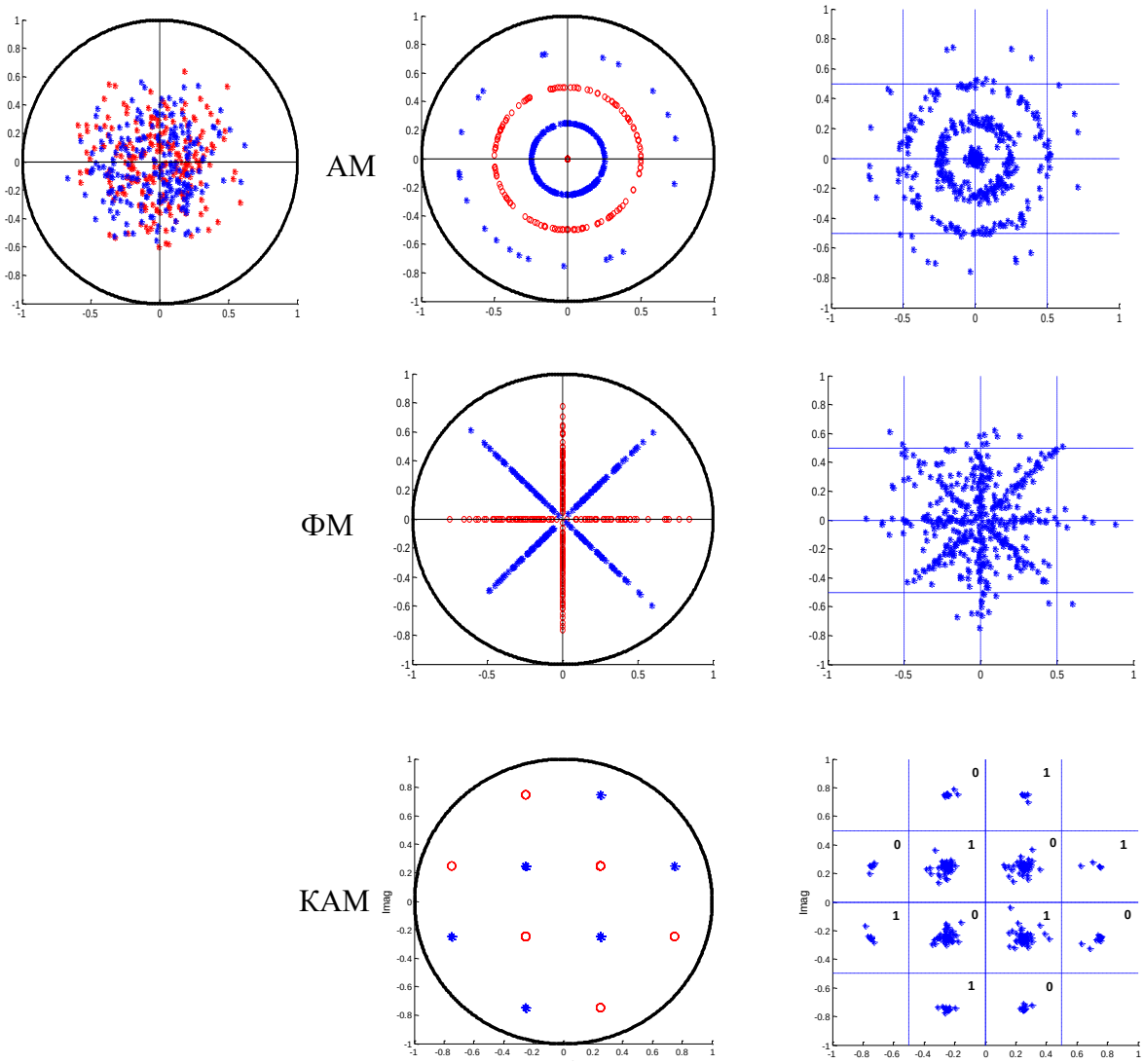
Ключевой операцией в технике формирования ЦВЗ является операция квантования. Коэффициент корреляции в общем случае является комплексным числом. Поэтому возможны, как минимум, следующие варианты квантования: а) амплитуды, б) фазы, в) реальной или мнимой частей коэффициента корреляции, г) одновременное квантование реальной и мнимой составляющих. Наибольший интерес представляют варианты а), б) и г).

Соответственно встраивание ЦВЗ на основе таких способов модуляции коэффициента корреляции названо амплитудной модуляцией (АМ), фазовой модуляцией (ФМ) и квадратурной амплитудной модуляцией (КАМ) коэффициента модуляции по аналогии с известными традиционными видами модуляции в системах радиосвязи. Однако при обычной модуляции изменению подвергаются параметры несущего колебания – амплитуда, фаза или совместно оба этих параметра. В нашем же случае изменению подвержен коэффициент корреляции сигнального и опорного векторов.

В результате такой модуляции один встраиваемый бит ЦВЗ приводит к модификации всех координат вектора сигнала-носителя $\boldsymbol{x}$. При этом энергия сигнала ЦВЗ, переносящего один бит информации равномерно распределяется по всей длине вектора сигнала-носителя во временно*м* измерении. Если же использовать в качестве сигнала-носителя $\boldsymbol{x}$ коэффициенты преобразования Фурье, то вся мощность сигнала $\boldsymbol{w}$ для одного бита ЦВЗ будет распределена в частотно-временной плоскости. Такой подход формирования ЦВЗ отвечает устоявшейся концепции синтеза сложных сигналов в современных широкополосных системах радиосвязи и радиолокации.

На рисунке 2 представлены созвездия коэффициентов корреляции (КК) при АМ, ФМ и КАМ на комплексной плоскости, полученные для встраивания ЦВЗ в частотной области дискретного преобразования Фурье (ДПФ) некоторого тестового звукового сигнала и случайной последовательности двоичных данных. Исходные КК $\tilde{x}$ хаотически распределены в круге единичного радиуса. В результате модуляции путём дискретизации (3) формируется значение КК $\tilde{s}$ в соответствии с законом АМ, ФМ или КАМ. Значения $\tilde{s}$ после модуляции располагаются на концентрических окружностях, радиальных линиях или узловых точках для АМ, ФМ и КАМ соответственно. В результате воздействия некоторой помехи положения КК $\tilde{y}$ в приёмнике смещаются, что проиллюстрировано на рисунке 2 в) для соответствующего вида модуляции.

В приёмнике оценка скрытого бита ЦВЗ $\hat{d}$ осуществляется исходя из критерия максимального правдоподобия по формуле:



а) б) в)

Рисунок 2 – Созвездия коэффициентов корреляции при АМ, ФМ и КАМ на комплексной плоскости: а) исходные коэффициенты корреляции $\tilde{x}$ до модуляции; б) $\tilde{s}$ в передатчике после модуляции; в) $\tilde{y}$ в приёмнике Рисунок 1 – Геометрическая

$$\hat{d} = \arg\min_{\lambda \in \Lambda_d} dist\left(\tilde{y}, \lambda\right), \tag{10}$$

где $\tilde{y} = \dfrac{(\boldsymbol{y},\boldsymbol{u})}{\|\boldsymbol{y}\|\|\boldsymbol{u}\|}$ – коэффициент корреляции принятого вектора;

Λ_d – геометрическое место точек $\tilde{s}\left(d\right)$.

При выборе вида модуляции КК следует руководствоваться следующими соображениями. Помехоустойчивость ЦВЗ определяется расстоянием $d_{01} = dist\left(\tilde{s}\left(d=0\right), \tilde{s}\left(d=1\right)\right)$ между линиями (точками) расположения $\tilde{s}$ для противоположных значений встраиваемого бита. Как видно из рисунка 2 для ФМ КК это расстояние уменьшается вплоть до нуля в области

малой корреляции, что не гарантирует помехоустойчивость ЦВЗ даже для сильного сигнала-носителя.

Сравним АМ и КАМ по показателям вносимые искажения и помехоустойчивость. Для объективного сравнения следует зафиксировать вносимые искажения по СКО при АМ и КАМ и найти минимальные расстояния между линиями положений КК $\tilde{s}$.Проделанный анализ показал, что

$$d_{01\text{АМ}} = 2d_{01\text{КАМ}}. \qquad 11)$$

Таким образом, минимальное расстояние между векторами с противоположными битами ЦВЗ в 2 раза больше для АМ, чем для КАМ при одинаковом уровне вносимых искажений.

Исследования показали, что наибольшее деструктивное влияние на ЦВЗ в радиотелефонных каналах МПС оказывает межсимвольная интерференция. Ее влияние особенно сильно сказываются в КВ диапазоне из-за хаотичных отражений в ионосферном слое. В УКВ диапазоне отражения не характерны и основным путём распространения является путь в направлении прямой видимости передающей и приёмной антенн. Однако источником МСИ здесь является неравномерность амплитудно-частотной характеристики (АЧХ) сквозного тракта УКВ трансивера.

АЧХ приёмо-передающего тракта связных трансиверов морского применения не нормируется. Поэтому для каждой пары передатчик-приёмник она может иметь свои особенности. В современных технологиях радиосвязи широко применяется метод ортогонального частотного мультиплексирования (Orthogonal frequency division multiplexing (OFDM)). Основной сферой применения OFDM являются радиоканалы с многолучевым распространением сигналов.

МНОГОКАНАЛЬНЫЙ АЛГОРИТМ

Для повышения помехоустойчивости ЦВЗ к межсимвольным искажениям предложен многоканальный алгоритм [11], реализующий идею параллельной передачи данных ЦВЗ по многим СК в стандартной полосе УКВ связи. В многоканальном алгоритме каждый бит информационного пакета ЦВЗ передаётся в узкой частотной полосе спектра звукового сигнала. Общий поток данных ЦВЗ разделяется на ряд параллельных потоков, каждый из которых передаётся независимо с низкой скоростью. Тем самым реализуется принцип технологии OFDM[12].

В матричной форме многоканальный алгоритм формирования стегосигнала для АМ в каждом канале записывается в виде:

$$\mathbf{S} = \mathbf{X} + \mathbf{W}\left(\tilde{\mathbf{X}}, \mathbf{D}\right), \qquad (12)$$

где $\mathbf{X}$ – $(B \times L)$ матрица амплитуд ДПФ,

$\mathbf{W}$ – $(B \times L)$ матрица амплитуд сигнала ЦВЗ,

$\tilde{\mathbf{X}}$ – вектор-столбец коэффициентов корреляции длиной B,

$\mathbf{D}$ – вектор-столбец данных длиной B.

Логика преобразований пакета в формате «короткого» ДПФ поясняется рисунком 3 для следующих числовых значений параметров пакета: $NL = 40$, $N = 5$, $L = 8$, $B = 2$. Таким образом, 2 бита данных ЦВЗ инкапсулируются в 40 отсчётов сигнала-носителя во временной области. Отсчёты во временной и частотной областях обозначены квадратиками и кружками соответственно. Исходные отсчёты даны без заполнения, а отсчёты, подверженные модификации, выделены серым.

Альтернативный вариант формирования пакета ЦВЗ в формате «длинного» ДПФ, представлен на рисунке 4 для следующих числовых значений параметров пакета ЦВЗ: $NL = 16$ - размерность ДПФ и длина пакета, $L = 2$ – длина векторов, $B = 2$ – число битов встроенной

информации. На рисунке координаты каждого вектора – коэффициенты ДПФ – обведены пунктирными линиями.

Как видно из сравнения рисунков 3 и 4 формирование векторов сигнала-носителя $\boldsymbol{x}_i, i = 1...B$ в первом случае осуществляется по горизонтали, т.е. из коэффициентов с одинаковыми индексами 5-ти коротких ДПФ, во втором – по вертикали из группы смежных коэффициентов одного длинного ДПФ. (Для упрощения рисунка длина векторов $\boldsymbol{x}_i$ принята равной двум).

С точки зрения противодействия МСИ оба варианта равноценны. Однако применение «длинного» ДПФ предпочтительнее для уменьшения влияния ошибки синхронизации в приёмнике. Ошибка синхронизации лежит в интервале $\pm 1/(2F_s)$, где F_s – частота дискретизации звукового сигнала в передатчике и приёмнике. Чем больше размерность ДПФ, тем меньше влияние на его результат будет иметь замена одного крайнего отсчёта во временной после-

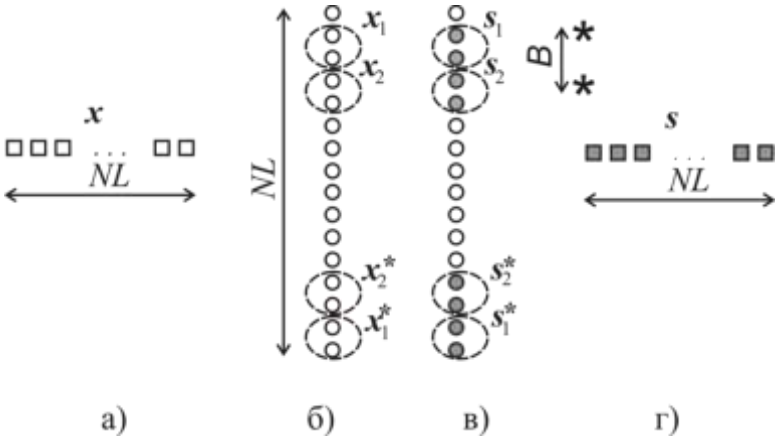


Рисунок 4 – Обработка пакета ЦВЗ в формате «длинного» ДПФ: а) – исходная последовательность временных отсчётов; б) – матрица $N \times L$ временных отсчётов сигнала-носителя; в) – матрица $N \times L$ частотных коэффициентов ДПФ; г) – модифицированные коэффициенты ДПФ

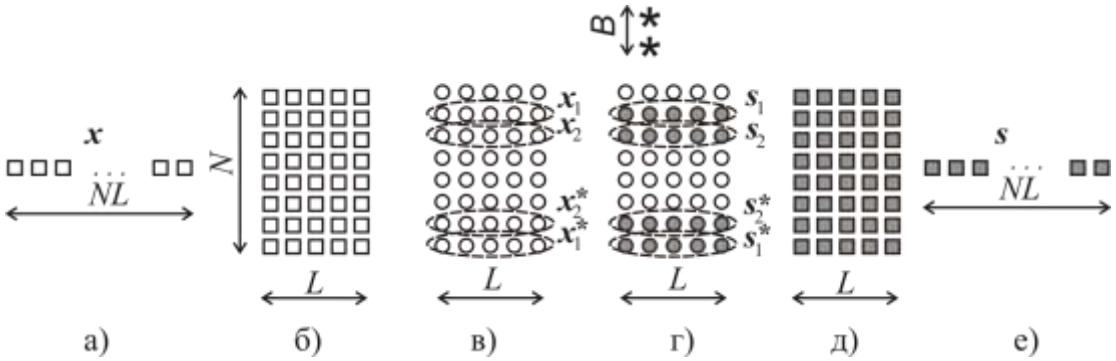


Рисунок 3 - Обработка пакета ЦВЗ в формате «короткого» ДПФ:а) – исходная последовательность временных отсчётов; б) – матрица $N \times L$ временных отсчётов сигнала-носителя; в) – матрица $N \times L$ частотных коэффициентов ДПФ; г) – модифицированные коэффициенты ДПФ; д) – матрица $N \times L$ временных отсчётов стегосигнала; е) – последовательность временных отсчётов стегосигнала

довательности, что и подтверждается результатами экспериментов.

Результаты эксперимента и моделирования. Экспериментальные испытания макета программно-аппаратного комплекса проводились в реальном УКВ радиоканале на частоте 156,850 МГц (17-й канал МПС). Испытания проводились в offline режиме с использованием двух комплектов судовой радиостанции RT-2048 Sailor и USB-модуля АЦП-ЦАП типа E14-140 L-CARD. Схема проведения испытаний представлена на рисунке 4, на котором обозначены: ПК – персональный компьютер, ЦАП – цифро-аналоговый преобразователь, АЦП – аналого-цифровой преобразователь, ИМПС – идентификатор морской подвижной службы

Методика испытаний следующая: в тестовый речевой фрагмент в среде MATLAB многократно вносился блок данных ЦВЗ длиной 15 бит. Далее подготовленный файл передавался через канал ЦАП – УКВ р/станция (передатчик) – радиотрасса 20 км – УКВ р/станция (приёмник) – АЦП и записывался в принятый звуковой файл

Принятый файл обрабатывался в среде MATLAB. В условиях эксперимента при следующих параметрах:

– отношение сигнал ЦВЗ/сигнал-носитель $WSR = -12{,}4$ дБ;
– отношение сигнал-носитель/шум $SNR = 14$ дБ;
– скорость передачи данных ЦВЗ $R = 125$ бит/с;
– все блоки ЦВЗ на длине речевого фрагмента детектировались устойчиво верно.

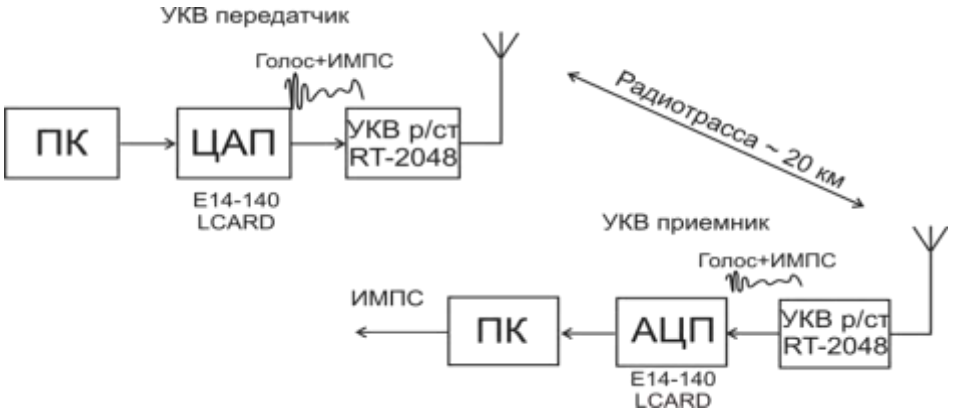


Рисунок 4 - Схема проведения испытаний устройства АИ

Таблица 1 –Относительное число верно декодированных пакетов ЦВЗ

Шаг квантования	Компандирование	Фильтрация	Аддитивный шум, дБ			Квантование, Q=256	Клиппирование 50%	Медленные замирания	Комплексная помеха
			40	30	20				
	(1)	(2)	(3)			(4)	(5)	(6)	(7)
0,125	0,76	0,13	0,23	0	0	0,5	0,9/1	0,13	0
0,25	1	0,26	0,6	0,1	0	0,63	0,93/1	0,37	0
0,5	1	0,72	0,72	0,37	0	0,84	0,94/1	0,5	0,03
1	1	0,94	0,86	0,71	0.14	1	0,97/1	1	0,43
2	1	1	1	0,74	0.37	1	1	1	0,68

Компьютерное моделирование для исследования влияния всевозможных помех на достоверность восстановления ЦВЗ проводилось в среде MATLAB. Помехоустойчивость ЦВЗ к атакам в канале оценивалась отношением числа обнаруженных и верно декодированных пакетов ЦВЗ к общему числу встроенных пакетов. Результаты в зависимости от шага квантования коэффициента корреляции сведены в таблицу 1.

Спецификация моделируемых помех канала радиосвязи приводится ниже.

(1) Сжатие-расширение (компаундирование): сигнал с ЦВЗ проходит стандартную процедуру компаундирования в соответствии с μ-законом. Соответствующие процедуры в MATLABlin2mu(s), mu2lin(y).

(2) Фильтрация: сигнал с ЦВЗ пропускался через полосовой фильтр Баттерворта порядка 2 с граничными частотами 400 Гц и 2 кГц. Соответствующие процедуры в MATLAB butter (1,[.1,0.5]), filter(bb,aa,s).

(3) Аддитивный белый гауссов шум (АБГШ): АБГШ добавлен к сигналу ЦВЗ на уровне, измеренном для всего фрагмента сигнала. Awgn (s,SNR,'measured'), filter(bb,aa,s).

(4) Квантование: сигнал с ЦВЗ квантован по амплитуде на Q уровней. 1/Q*round(s*Q).

(5) Клиппирование: сигнал с ЦВЗ ограничен по амплитуде сверху и снизу на уровне 50% от максимального значения.

(6) Медленные замирания: сигнал с ЦВЗ подвергался амплитудной модуляции с частотой 3 Гц и глубиной модуляции 0,5.

(7) Комплексная помеха: Сигнал одновременно подвергался воздействию 3-х помех (4) + (5), *SNR*=30 дБ + (8).

ЗАКЛЮЧЕНИЕ.

Разработанный алгоритм формирования ЦВЗ с сохранением нормы сигнала обеспечивает их устойчивость к амплитудным искажениям в канале передачи и слуховую нечувствительность вносимых искажений, поскольку происходит лишь перераспределении мощности смежных гармоник спектра при сохранении из суммарной мощности.

Из трёх возможных видов модуляции коэффициента корреляции – АМ, ФМ, КАМ – наилучший результат по соотношению вносимые искажения – помехоустойчивость даёт амплитудная модуляция коэффициента корреляции.

Формирование ЦВЗ в частотной области позволяет использовать технологию частотного ортогонального мультиплексирования (OFDM) для эффективного противодействия МСИ. ЦВЗ на основе OFDM могут формироваться в формате «длинного» и «короткого» ДПФ, причём формат «длинного» ДПФ предпочтительнее с точки зрения уменьшения ошибок синхронизации.

Проведённые эксперимент и компьютерное моделирование подтверждают возможность практического использования технологии ЦВЗ для автоматической идентификации радиопередач и применения в особых условиях, например, при террористических атаках для скрытной передачи информации на фоне голосового сообщения.

ЛИТЕРАТУРА

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
2. Cox I.J. et al. Digital watermarking and steganography. Second Edition. Morgan Kaufmann Publishers, USA. 2008. - 594 p.
3. Chen B., Wornell G.W. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*. Vol. 47, No. 4, 2001.pp. 1423-1443.
4. Malvar H.S., Florencio D.A. Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking. *IEEE Transactions on Signal Processing.* Vol. 51, No 4. 2003.pp. 898 – 905.

5. Шишкин А.В. Цифровые водяные знаки с расширением спектра для аудиосигналов при использовании информации о сигнале-носителе. *Известия вузов – Радиоэлектроника*. Т. 51, № 6. 2008. С. 22 – 32.
6. Шишкин А.В., Кошевой В.М. Устойчивая к атакам масштабирования стеганографическая передача информации с исключением мешающего влияния сигнала-носителя. *Известия вузов – Радиоэлектроника*. Т. 50, № 6.2007. С. 3 – 15.
7. Zareian M. and Tohidypour H. R. A Novel Gain Invariant Quantization-Based Watermarking Approach IEEE Transactions on Information Forensics and Security, vol. 9, No. 11, November 2014, pp. 1804 – 1813.
8. Шишкин А. В. Идентификация радиотелефонных передач в УКВ диапазон морской радиосвязи. Известия вузов – Радиоэлектроника. Т. 55, № 11. 2012. С. 11 – 20.
9. Шишкін О.В. Формування і виявлення цифрових водяних знаків у системі автоматичної ідентифікації ультракороткохвильових радіопередач. Вісник Національного авіаційного університету, № 2 (55), 2013.С. 57 – 61.
10. HofbauerK., KubinG., andKleijnW. B. Speech Watermarking for Analog Flat-Fading Bandpass Channels, IEEE Transaction Audio, Speech, and Language Processing. Vol. 17, No 8, 2008.pp 1624 – 1637.
11. Shishkin A.V., Lyashko A.A. Hash-based Detection of OFDM Watermarking Symbol for Radiotelephone Identification. Proceedings of IEEE East-West Design & Test Symposium (EWDTS'12). 2012. Kharkov, Ukraine, September 14-16, pp. 389 – 392.
12. Ипатов В.В. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. – М.: Техносфера, 2007. – 488 с.

REFERENCES

1. Konahovich G. F., PuzyrenkoA.Yu. Komp’uternaya steganografiay. Teoriay i praktika. – K.: MK-Press, 2006. – 288 p.
2. Cox I.J. et al. Digital watermarking and steganography. Second Edition. Morgan Kaufmann Publishers, USA. 2008. - 594 p.
3. Chen B., Wornell G.W. Quantizationindex modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*. Vol. 47, No. 4, 2001.pp. 1423-1443.
4. Malvar H.S., Florencio D.A. Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking. *IEEE Transactions on Signal Processing.* Vol. 51, No 4. 2003.pp. 898 – 905.
5. Shishkin A. V. Digital watermarks with spectrum spreading for audio signals using the signal carrier information.*Radioelectronics and Communications Systems.* Vol. 51, No 6, 2008. pp308-315.
6. ShishkinA. V., Koshevoy V. M.Steganographic data transmission robust against scaling attacks (resistant-to-scaling-attacks) and eliminating the hampering effect of signal-carrier. *Radioelectronics and Communications Systems.* Vol. 50, No 6, 2007. Pp289-297.
7. Zareian M. and Tohidypour H. R. A Novel Gain Invariant Quantization-Based Watermarking Approach *IEEE Transactions on Information Forensics and Security*, vol. 9, No. 11, November 2014, pp. 1804 – 1813.
8. Shishkin A. V. Identification of radiotelephony transmissions in VHF band of maritime radio communications.*Radioelectronics and Communications Systems.* Vol. 55, No 11, 2012. Pp482-489.
9. Shyshkin O.V.Formuvannya I vyyavlennya cyfrovyh vodyanyh znakiv u systemi avtomatychnoi identyficacii ultrakorotkohvylnovyh radioperedech. Visnyk Nacional’nogo aviaciynogo universytetu, № 2 (55), 2013. pp. 57 – 61.
10. Hofbauer K., Kubin G., and Kleijn W. B. Speech Watermarking for Analog Flat-Fading Bandpass Channels, *IEEE Trans on Audio, Speech, and Language Processing*. Vol. 17, No 8, 2008. pp 1624 – 1637.
11. Shishkin A.V., Lyashko A.A. Hash-based Detection of OFDM Watermarking Symbol for Radiotelephone Identification. *Proceedings of IEEE East-West Design & Test Symposium (EWDTS'12).* 2012. Kharkov, Ukraine, September 14-16, pp. 389 – 392.
12. Ipatov V.P. Spread Spectrum and CDMA. Principles and Applications. – Jons Wiley & Sons Ltd, 2005M.: Техносфера, 2007.