УДК 621.396.218

О.В. Шишкін

ФОРМУВАННЯ І ВИЯВЛЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У СИСТЕМІ АВТОМАТИЧНОЇ ІДЕНТИФІКАЦІЇ УЛЬТРАКОРОТКОХВИЛЬОВИХ РАДІОПЕРЕДАЧ

Одеська національна морська академія
вул. Дідріхсона, 8, Одеса, Україна, 65029
E-mail: shishkin@te.net.ua

Розроблено алгоритми формування і виявлення цифрових водяних знаків для системи автоматичної ідентифікації ультракороткохвильових радіотелефонних передач морської і повітряної рухомих служб. Показано, що слухова несприйнятність і завадостійкість убудованих цифрових даних забезпечуються застосуванням технології OFDM спільно з нормованим розподілом спотворень і виявлення пакета даних за хеш-функцією. Проведено експерименти на базі суднової радіостанції RT-2048 Sailor і USB-модуля АЦП-ЦАП типу E14-140M L-CARD в off-line режимі обробки в середовищі Matlab.

Ключові слова: ідентифікація; міжсимвольні спотворення; ультракороткохвильова радіотелефонія; хеш-функція; цифрові водяні знаки.

Постановка проблеми

Натепер в ультракороткохвильових (УКХ) діапазонах морської (156–174 МГц) і повітряної (118–136 МГц) рухомих служб для радіотелефонних передач застосовують аналогову модуляцію (частотну/фазову й амплітудну відповідно). Ідентифікація передавального судна здійснюється шляхом голосової передачі позивного сигналу або цифрового ідентифікатора передавальної станції. Через низку обставин голосової ідентифікації може не бути взагалі, або передаватися із затримкою чи прийматися неправильно. Очевидно, що відсутність або помилки сприйняття голосової ідентифікації в радіотелефонії критичним чином позначаються на загальній безпеці на морському і повітряному транспорті.

Одним із вирішень завдання виключення людського чинника в здійсненні адресної телефонії в системах рухомого радіозв'язку є реалізація автоматичної ідентифікації на основі технології цифрових водяних знаків (ЦВЗ).

Цифровий водяний знак стосовно УКХ радіотелефонії означає вбудовування цифрової інформації безпосередньо в звуковий сигнал і передавання цієї інформації в стандартному радіотелефонному каналі. Автоматична ідентифікація на основі ЦВЗ не потребує заміни штатної апаратури, додаткового частотно-часового ресурсу каналу і зміни процедур радіозв'язку. Крім вирішення основного завдання надійної ідентифікації, передавання цифрової інформації спільно з мовним сигналом дозволяє:

– спрямовувати дані ідентифікації в інші інформаційні системи;

– здійснювати моніторинг радіопередач для виявлення порушників;

– використовувати можливість прихованої передачі інформації в спеціальних застосуваннях, наприклад, у разі терористичних погроз.

Аналіз досліджень і публікацій

Загальним питанням побудови систем цифрової стеганографії і ЦВЗ присвячено праці [1; 4].

Одним із методів вбудовування ЦВЗ з урахуванням сигналу-носія є модуляція індексу квантування (МІК), що ґрунтується на скалярному квантуванні відліків носія (чи його перетворення) і передаванні їх квантованих значень [3]. Проте МІК чутлива до спотворень амплітудного масштабу.

У праці [5] запропоновано поліпшений алгоритм розширення спектра (ISS – Improved Spread Spectrum), який нечутливий до амплітудних спотворень, проте схильний до впливу міжсимвольних спотворень (МСС).

У праці [2] для підвищення завадостійкості ЦВЗ у частотно обмеженому каналі з впливом МСС досліджені алгоритми формування ЦВЗ в амплітудах вузькосмугових сигналів на основі перетворення Гільберта.

Метою роботи є розроблення і дослідження алгоритмів формування і виявлення звукових ЦВЗ, стійких до амплітудних спотворень і МСС.

Розроблена система ґрунтується на нових підходах у техніці звукових ЦВЗ:

– використанні технології OFDM;

– нормованому розподілі спотворень, що вносяться у звуковий сигнал;

– обробленні і виявленні в цілому всього пакета даних ЦВЗ на основі обчислення хеш-функції.

Міжсимвольні спотворення зумовлюються обмеженою частотною смугою приймача і багатопроменевим характером поширення радіохвиль.

У радіотелефонії для передавання мовного сигналу стандартно відводиться смуга частот 300–3000 Гц, у якій амплітудно-частотна характеристика каналу є істотно нерівномірною через наявність реактивних елементів у низькочастотних схемах.

Багатопроменевий характер поширення радіохвиль спричиняє швидкі частотно-селективні спотворення прийнятого сигналу. Таким чином, дві різні за своєю фізичною природою причини спотворень призводять до одного і того ж типу лінійних або міжсимвольних спотворень.

Для зниження впливу МСС на формування ЦВЗ запропоновано застосування технології OFDM (Orthogonal Frequency Division Multiplexing), що широко використовується у сучасних системах зв'язку різного призначення і базується на розбитті частотної смуги спектра сигналу на ряд вузькосмугових субканалів з ортогональними підносійними частотами. При цьому швидкий потік даних розщеплюється на ряд повільних потоків, що передаються незалежно в кожному зі смугових субканалів. У межах кожного субканалу амплітудно-частотна характеристика може прийматися постійною, а фазочастотна – лінійною, і тому впливом МСС у кожному субканалі можна нехтувати. Загальна швидкість передавання інформації по всіх каналах залишається незмінною.

Технічно OFDM ґрунтується на використанні прямого і зворотного алгоритмів дискретного перетворення Фурьє (ДПФ).

Одноканальний алгоритм убудовування ЦВЗ описується таким чином. Стегосигнал, тобто сигнал із вбудованими ЦВЗ, формується за формулою

$$\mathbf{s} = \mathbf{x} + \mathbf{w}(\tilde{x}, m), \qquad (1)$$

де $\mathbf{s}, \mathbf{x}, \mathbf{w}$ – вектори довжини L послідовностей відліків стегосигналу, носія і сигналу ЦВЗ відповідно;

$\tilde{x} = (\mathbf{x}, \mathbf{u})$ – скалярний добуток сигналу-носія і деякої псевдовипадкової послідовності $\mathbf{u}$:

$u_i = \{\pm 1\}$;

$m = \{\pm 1\}$ – убудований біт інформації.

Як сигнал-носій застосовують амплітуди частотних коефіцієнтів ДПФ з однаковими індексами.

Координати вектора w у формулі (1) визначають за формулою

$$w_i = \tilde{w} \, |x_i| / \|\mathbf{x}\|_p^{\,p} \, u_i, \qquad (2)$$

де $\|\mathbf{x}\|_p = \sum_{i=1}^{L} |x_i|^p$ $^{1/p}$ – p-норма вектора $\mathbf{x}$.

Значення $\tilde{w}$ обчислюють за формулою

$$\tilde{w} = \begin{cases} 0, & m\tilde{x} \ge \rho, \\ m\rho - \tilde{x}, & m\tilde{x} < \rho, \end{cases} \qquad (3)$$

де ρ – поріг, що визначає стійкість ЦВЗ до дії завад.

Логіка алгоритму (3) пояснюється таким чином. Якщо $m\tilde{x} \ge \rho$, то вносити будь-які спотворення у сигнал для передавання біта ЦВЗ взагалі немає потреби. Потрібний біт буде детектований в приймачі природним чином. Якщо $m\tilde{x} < \rho$, потрібне внесення спотворень, які б скоригували скалярний добуток $\tilde{s} = (\mathbf{s}, \mathbf{u})$ в одне зі значень залежно від біта ЦВЗ:

$$\tilde{s} = \begin{cases} \rho, & m = 1, \\ -\rho, & m = -1. \end{cases} \qquad (4)$$

Вибір оптимального значення параметра норми p у формулі (2) має визначатися з суб'єктивного сприйняття спотворень, що вносяться у звуковий сигнал. У загальному випадку $p > 0$. У разі $p = 1$ значення коригування $\tilde{w}$ розподіляється пропорційно амплітудам координат вектора $\mathbf{x}$:

$$w_i = \tilde{w} \frac{|x_i|}{\|\mathbf{x}\|_1} u_i. \qquad (5)$$

Якщо $p \to 0$, $\tilde{w}$ розподіляється рівномірно на всі відліки x_i. Саме для такого випадку алгоритм ISS застосовано у праці [5]. Для рівномірного розподілу формула (2) набуває вигляду

$$w_i = \frac{\tilde{w}}{L} u_i.$$

У класі сигналів з $\tilde{w} = \text{const}$ рівномірний розподіл мінімізує середній квадрат унесених спотворень, проте суб'єктивне слухове сприйняття внаслідок маскувального впливу великих амплітуд і зниження шумового ефекту в паузах свідчить на користь вибору значень p у діапазоні 0,5–1.

Вектор, що приймається, дорівнює

$$\mathbf{y} = \mathbf{x} + \mathbf{w} + \mathbf{n},$$

де $\mathbf{n}$ – вектор шуму.

У приймачі обчислюється скалярний добуток $\tilde{y} = (\mathbf{y}, \mathbf{u})$, що еквівалентний обчисленню кореляції прийнятого й опорного сигналів.

Детектований біт оцінюється за знаком скалярного добутку:

$$\hat{m} = \operatorname{sign}(\mathbf{y}, \mathbf{u}).$$

У матричній формі для багатоканального випадку алгоритм (1) можна подати у вигляді

$$\mathbf{S} = \mathbf{X} + \mathbf{W}(\tilde{\mathbf{X}}, \mathbf{M}),$$

де $\mathbf{X}, \mathbf{W}$ – матриці розмірності $(B \times L)$ амплітуд частотних коефіцієнтів сигналу-носія і ЦВЗ відповідно;

$\tilde{\mathbf{X}}$ – вектор $(B \times 1)$ скалярних добутків;

$\mathbf{M}$ – вектор $(B \times 1)$ убудованих цифрових даних ідентифікації.

Елементи верхньої частини матриці комплексних коефіцієнтів $\dot{S}_b$ обчислюються таким чином:

$$\dot{S}_b = \begin{cases} X_b, & b = 0, B+1, \ldots, N/2; \\ S_b \exp(j\varphi_b), & b = 1,2,\ldots,B, \end{cases} \qquad (6)$$

де φ_b – фази коефіцієнтів X_b.

Для зберігання дійсного характеру відліків в часової області необхідно представить нижню частини матриці $\mathbf{S}$ у вигляді комплексного спряження верхньої частини:

$$\dot{S}_{b+N/2} = \dot{S}_{N/2-b}, \quad b = 1,2,\ldots, N/2-1. \qquad (7)$$

Для спрощення запису індексація відповідних стовпців $l = 1,2,\ldots,L$ у формулах (6) і (7) випущена.

Формування ЦВЗ пояснюється схемою на рисунку для значень $N = 8$, $L = 5$, $B = 2$. Довжина блока, що обробляється, для цих значень становить 40 відліків для двох бітів ЦВЗ. Послідовність відліків сигналу-носія у часовій області зображено квадратиками (див. рисунок, *а*). Блок з 40 відліків переформатується по стовпцях у вигляді матриці розмірності 8×5 (див. рисунок, *б*). Далі обчислюються частотні коефіцієнти ДПФ по стовпцях матриці. Частотні коефіцієнти зображено кружками (див. рисунок, *в*). Верхній рядок відповідає сталим складовим ДПФ.

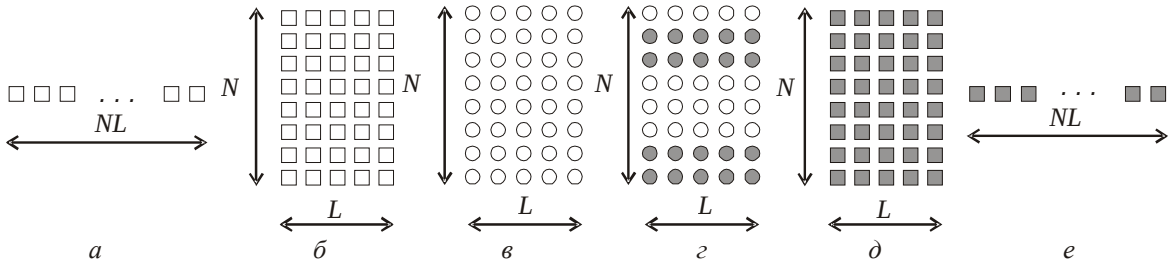
Потім здійснюється модифікація амплітуд частотних коефіцієнтів за викладеним алгоритмом відповідно до формул (1)–(5) (див. рисунок, *г*). Модифіковані за амплітудою частотні коефіцієнти виділено сірим кольором.

На рисунку модифікації підлягають амплітуди першої і другої гармонік (другий і третій рядки відповідно). Рядки 7 і 8 є комплексно-зв'язаними відносно рядків 3 і 2 відповідно. Наступним кроком здійснюється зворотне ДПФ також по стовпцях матриці. У зворотного ДПФ сформовано відліки стегосигналу, які також помічено сірим (див. рисунок, *д*).

З матриці 8×5 регістра відліки стегосигналу читаються по стовпцях (див. рисунок, *е*).

Виявлення цифрових водяних знаків і синхронізація

Виявлення ЦВЗ ґрунтується на обчисленні кореляційної суми (скалярного додатка) амплітуд ДПФ прийнятої послідовності відліків і опорної ПВП. Для коректного детектування необхідно синхронізувати роботу корелятора із вхідною послідовністю. Вирішуватимемо завдання синхронізації і детектування спільно шляхом оброблення усієї послідовності відліків, яка відповідає одному пакету ЦВЗ.



Формування ЦВЗ

Під пакетом ЦВЗ розумітимемо послідовність власне даних ЦВЗ і деякої хеш-функції, вичисленої за даними ЦВЗ. У приймачі пакет ЦВЗ вважається виявленим і правильно детектованим, якщо вичислене значення хеш-функції збігається з прийнятими даними.

Такий спосіб виявлення ЦВЗ не потребує додаткового передавання синхронізуючої послідовності, маркера початку даних і контрольної суми. Усі ці відповідні завдання вирішуються шляхом оброблення усієї послідовності одного пакета і порівняння прийнятої і переданої хеш-функцій. Вирішується також проблема впливу неточності синхронізації на достовірність виявлення. Достовірність правильного виявлення при цьому визначається довжиною хеш-функції. Достатньою довжиною хеш-функції є 15 біт. У цьому випадку ймовірність помилкового виявлення становить 2^{-15}.

Витратами такого підходу є затримка виявлення в приймачі на довжину одного пакета і досить великий обсяг обчислень, який має вироблятися із частотою дискретизації.

Результати моделювання

Випробування проводилися в реальному УКХ радіоканалі на частоті 156,850 МГц (17-й канал) з використанням двох комплектів суднової радіостанції RT-2048 Sailor і USB-модуля аналого-цифрового перетворювача і цифро-аналогового перетворювача типу E14-140M L-CARD.

У тестовий мовний фрагмент у середовищі Matlab багаторазово вносився блок даних ЦВЗ довжиною B=15 біт, сформований за розробленим алгоритмом. Частота дискретизації F_s = 8 кГц, ширина смуги субканалу Δf =125 Гц за розмірності ДПФ N=64.

Оброблений файл передавався через цифро-аналоговий перетворювач на вхід УКХ радіостанції, випромінювався в ефір, приймався другим комплектом УКХ радіостанції і через аналого-цифровий перетворювач записувався в прийнятий звуковий файл.

Прийнятий файл оброблявся в середовищі Matlab для виявлення ЦВЗ. Таким чином, передавався сигнал у реальному радіоканалі з програмним обробленням в off-line режимі.

Результати експерименту при відношенні сигнал–шум у радіоканалі 15 дБ зведено в таблицю.

Усі блоки ЦВЗ на довжині мовного фрагменту з 27 000 відліків детектувалися стійко правильно.

Результати експерименту

WSR , дБ	-16,5	-14,6	-12,1
L	31	15	7
R , біт/с	60	125	268

Примітка. *WSR* (Watermark-to-Signal Ratio) – відношення ЦВЗ/сигнал-носій, *L* – довжина псевдовипадкової послідовності, *R* – швидкість даних ЦВЗ.

Швидкість передавання прихованої інформації визначається за формулою

$$R = \frac{B\,F_s}{N\,L}.$$

Моделювання алгоритму в середовищі Matlab показало стійкість ЦВЗ також до нелінійних спотворень типу «кліпування» сигналу аж до рівня 0,5.

Висновки

Для забезпечення стійкості звукових ЦВЗ до міжсимвольної інтерференції з метою вирішення проблеми автоматичної ідентифікації УКХ радіотелефонних передач у морському радіозв'язку запропоновано використовувати OFDM технологію спільно з відомим поліпшеним алгоритмом прямого розширення спектра (ISS). Алгоритм OFDM-ISS вбудовування ЦВЗ в аналоговий звуковий сигнал забезпечує стійкість ЦВЗ до міжсимвольної інтерференції, нелінійних спотворень і адитивного шуму за потужності спотворень сигналу за рахунок ЦВЗ нижче від рівня природного шуму в радіоканалі. Слухова несприйнятність ЦВЗ досягається розподілом його енергії в частотно-часовій площині сигналу-носія і правильним заданням параметра p норми сигналу.

Можливість гнучкого вибору параметрів N, L, B і ρ забезпечує компромісне вирішення завдання реалізації характеристик системи ЦВЗ.

Виявлення ЦВЗ здійснюється шляхом оброблення в цілому усього пакета відліків на основі порівняння хеш-функцій. Такий підхід дозволяє взагалі обійтися без передавання синхронізуючої послідовності, маркера і контрольної суми.

Практична реалізація системи ідентифікації на основі ЦВЗ може бути здійснена без заміни існуючої апаратури УКХ радіозв'язку. Штатний УКХ трансивер має бути доповнений мікросхемою з прошиванням даних ідентифікації, яка встановлюється безпосередньо в телефонну трубку і мінідисплеєм, підключеним до стандартного низькочастотного виходу звукового сигналу приймача для візуалізації ідентифікатора передавальної станції.

Література

1. *Конахович Г.Ф.* Компьютерная стеганография. Теория и практика / *Г.Ф. Конахович, А.Ю. Пузыренко.*– К.: МК-Пресс, 2006. – 288 с.

2. *Шишкин А.В.* Устойчивые цифровые водяные знаки для звуковых сигналов / А.В. Шишкин // Известия вузов. Радиоэлектроника. – 2011. – Т. 54, № 3. – С. 30–38.

3. Chen, B.; Wornell, G.W. 2001. *Quantization index modulation: a class of provably good methods for digital watermarking and information embedding*. IEEE Transactions on Information Theory. Vol. 47, N 4. May: 1423–1443.

4. Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J.; Kalker, T. 2008. *Digital watermarking and steganography*. Second Edition – Morgan Kaufmann Publishers. 594 p.

5. Malvar, H.S.; Florencio, D.A. 2003. *Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking*. IEEE Transactions on Signal Processing. Vol. 51, N 4. April: 898–905.

References

1. Konahovych, G.F.; Puzyrenko, A.Yu. 2006. *Computer steganography. Theory and practice*. Kyiv, MK-Press. 288 p. (in Russian).

2. Shishkin, A.V. 2001. *Robust digital watermarks for audio signals.* Izvestiya vuzov. Radioelectronic. Vol. 54, N 3: 30–38 (in Russian).

3. Chen, B.; Wornell, G.W. 2001. *Quantization index modulation: a class of provably good methods for digital watermarking and information embedding*. IEEE Transactions on Information Theory. Vol. 47, N 4. May: 1423–1443.

4. Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J.; Kalker, T. 2008. *Digital watermarking and steganography*. Second Edition – Morgan Kaufmann Publishers. 594 p.

5. Malvar, H.S.; Florencio, D.A. 2003. *Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking*. IEEE Transactions on Signal Processing. Vol. 51, N 4. April: 898–905.

Стаття надійшла до редакції 05.04.2013.

Шишкін Олександр Володимирович. Кандидат технічних наук. Доцент. Кафедра морського радіозв'язку, Одеська національна морська академія, Одеса, Україна. Освіта: Одеський політехнічний інститут (1977); Одеська державна морська академія, Одеса, Україна (2001). Напрям наукової діяльності: цифрова обробка сигналів, системи цифрових водяних знаків, навігаційна і інформаційна безпека на морському транспорті, глобальна морська система зв'язку у разі лиха та для безпеки мореплавства. Кількість публікацій: 60, 8 патентів. E-mail: shishkin@te.net.ua

O. Shishkin. Forming and detection of digital watermarks in the System for Automatic Identification of VHF Transmissions

Odessa National Maritime Academy, Didrikhson street 8. Odessa, Ukraine, 65029
E-mail: shishkin@te.net.ua

Forming and detection algorithms for digital watermarks are designed for automatic identification of VHF radiotelephone transmissions in the maritime and aeronautical mobile services. An audible insensitivity and interference resistance of embedded digital data are provided by means of OFDM technology jointly with normalized distortions distribution and data packet detection by the hash-function. Experiments were carried out on the base of ship's radio station RT-2048 Sailor and USB ADC-DAC module of type E14-140M L-CARD in the off-line processing regime in Matlab medium.

Keywords: digital watermarks; hash-function; identification; intersymbol interference; VHF radiotelephony.

Shishkin Oleksandr. Candidate of Engineering. Associate Professor. Maritime Radio Communication Department, Odessa National Maritime Academy, Odessa, Ukraine. Education: Odessa Polytechnic Institute (1977); Odessa National Maritime Academy, Odessa, Ukraine (2001). Research area: digital signal processing, systems of digital watermarks, navigation and information security on marine transport, global maritime distress and safety system (GMDSS).
Publications: 60, patents 8. E-mail: shishkin@te.net.ua

А.В. Шишкин. Формирование и обнаружение цифровых водяных знаков в системе автоматической идентификации ультракоротковолновых радиопередач

Одесская национальная морская академия, ул. Дидрихсона, 8, Одесса, Украина, 65029
E-mail: shishkin@te.net.ua

Разработаны алгоритмы формирования и обнаружения цифровых водяных знаков для системы автоматической идентификации ультракоротковолновых радиотелефонных передач морской и воздушной подвижных служб. Показано, что слуховая невосприимчивость и помехоустойчивость встроенных цифровых данных обеспечиваются технологией OFDM совместно с нормированным распределением искажений и обнаружения пакета данных по хеш-функции. Проведены эксперименты на базе судовой радиостанции RT-2048 Sailor и USB-модуля АЦП-ЦАП типа E14-140M L-CARD в off-line режиме обработки в среде Matlab.

Ключевые слова: идентификация; межсимвольные искажения; ультракоротковолновая радиотелефония; хеш-функция; цифровые водяные знаки.

Шишкин Александр Владимирович. Кандидат технических наук. Доцент. Кафедра морской радиосвязи, Одесская национальная морская академия. Образование: Одесский политехнический институт (1977); Одесская государственная морская академия, Одесса, Украина (2001). Направление научной деятельности: цифровая обработка сигналов, системы цифровых водяных знаков, навигационная и информационная безопасность на морском транспорте, глобальная морская система связи при бедствии и для безопасности мореплавания. Количество публикаций: 60, 8 патентов. E-mail: shishkin@te.net.ua