УДК 004.056.5

М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко
Одеський національний політехнічний університет,
кафедра інформаційної безпеки

ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У АУДІОФАЙЛИ ЗІ СТИСНЕННЯМ БЕЗ ВТРАТ

Розроблено стеганографічний алгоритм додавання цифрових водяних знаків у частотній області в аудіофайли зі стисненням без втрат з використанням швидкого перетворення Уолша–Адамара, а також перевірено можливість вбудовування цифрових водяних знаків з використанням стиснення залишкового сигналу на прикладі файлів формату FLAC.

Ключові слова: стеганографія, приховування інформації, цифрові водяні знаки.

WATERMARKING OF AN AUDIO SIGNAL WITH LOSSLESS COMPRESSION

In a paper a new steganographic method for watermarking in the frequency domain of an audio signal with lossless compression using a fast Walsh–Hadamard transform is developed. In the example of FLAC format files a possibility of digital watermark embedding using compression of residual signal is checked.

Key words: steganography, data hiding, digital watermarks.

Вступ

Сьогодні методи цифрової стеганографії широко використовуються для захисту інформації та інформаційної безпеки. В їх основу покладено модифікацію цифрових контейнерів – стегоконтейнерів з метою непомітного впровадження певних бітових послідовностей. Основні напрями застосування стеганографічних алгоритмів: надсилання стегоповідомлень, вбудовування цифрових водяних знаків (ЦВЗ) (watermarking) та ідентифікаційних номерів (ІН) (fingerprinting), вбудовування заголовків (captioning) [1].

ЦВЗ здебільшого використовують з метою захисту авторських прав та уникнення незаконного копіювання і використання цифрової інформації. ЦВЗ можуть бути помітними та непомітними. За надійністю ЦВЗ поділяють на крихкі, напівкрихкі та надійні. Надійні ЦВЗ використовуються у системах захисту інформації від несанціонованного копіювання. При цьому ЦВЗ у аудіофайлах повинні бути непомітними для слухової системи людини, щоб забезпечити належну якість звучання, що особливо важливо для комерційного використання. Тому мінімізація викривлень аудіосигналу або застосування слухового маскування є однією з основних умов для практичної реалізації стеганографічного алгоритму для вбудовування ЦВЗ.

Виділяють декілька способів вбудовування ЦВЗ. *Адитивні* методи основані на додаванні до вибраної підмножини відліків оригінального цифрового контейнера згенерованої послідовності псевдовипадкових чисел. В *алгоритмах злиття* у оригінальний контейнер вбудовується певне інформаційне повідомлення значно меншого обсягу. Перевагою таких методів є допустимість незначних викривлень у оригінальному контейнері, а також можливість вбудовування певної корисної інформації, яка є надійнішим підтвердженням прав власності на інформацію, ніж послідовність псевдовипадкових чисел [2].

Аналіз досліджень та публікацій

Проблема вбудовування інформації в аудіофайли з використанням стеганографічних алгоритмів, а також питання стеганографічного аналізу аудіофайлів розглянуто у низці наукових праць. У роботі [3] запропоновано метод приховування інформації з розширенням спектра, що використовує вейвлет-перетворення; в роботі [4] – метод вбудовування інформації зі збереженням гістограми контейнера, який гарантує його точне відтворення; в роботі [5] докладно розглянуто застосування, аналіз та оцінку стеганографічних методів на прикладі аудіофайлів формату WAV. У роботах [6–8] висвітлено різні методи виявлення прихованої інформації у аудіофайлах.

Також було розглянуто вбудовування ЦВЗ в аудіосигнал за допомогою методу розширення спектра в роботі [9]. У [10] запропоновано новий метод вбудовування ЦВЗ на основі перетворень конформної алгебри. Було розглянуто і аналіз властивостей слуху з погляду вбудовування ЦВЗ у аудіофайл у роботі [11]. Отже, існують алгоритми, що забезпечують успішне приховування інформації та додавання цифрових водяних знаків у аудіофайлах. Разом з тим, переважна більшість розроблених методів призначена для використання у аудіофайлах без стиснення. При цьому не була розглянута проблема створення алгоритмів для приховування інформації та додавання цифрових водяних знаків у аудіофайли зі стисненням без втрат (loseless). Отже, залишаються актуальними розроблення та практична реалізація нових стеганографічних методів, що можуть бути застосовані для використання як контейнер подібних аудіофайлів.

Постановка задачі

З метою розроблення методу непомітного для слухової системи людини вбудовування ЦВЗ у аудіофайли зі стисненням, на прикладі аудіофайлів формату FLAC, необхідно розробити стеганографічний алгоритм вбудовування інформації в аудіофайли зі стисненням, провести моделювання його роботи, визначити викривлення оригінального аудіосигналу в разі додавання ЦВЗ та можливість їх зменшення, що і є предметом дослідження, висвітленого в цій статті.

Загальна будова аудіофайла формату FLAC

Структура аудіофайла формату FLAC містить такі основні елементи:

- Рядок “fLaC” у ASC-II кодуванні (0x66 0x4C 0x61 0x43).
- Обов’язковий блок метаданих STREAMINFO, який містить інформацію про основні властивості аудіопотоку – кількість каналів, частоту дискретизації, кількість відліків у аудіопотоці, кількість бітів у відліку, розмір фрейму, а також md5 хеш-суму оригінального аудіосигналу.
- Інші блоки метаданих у кількості до 128, що можуть містити текстові коментарі, зображення, відступи, інформацію про треки тощо.
- Один чи декілька фреймів (кадрів) аудіоданих.
- Структуру кадру даних наведено на рис. 1. У кожному підкадрі зберігаються дані одного каналу. Власне аудіодані у файлі формату FLAC можуть записуватися такими способами:

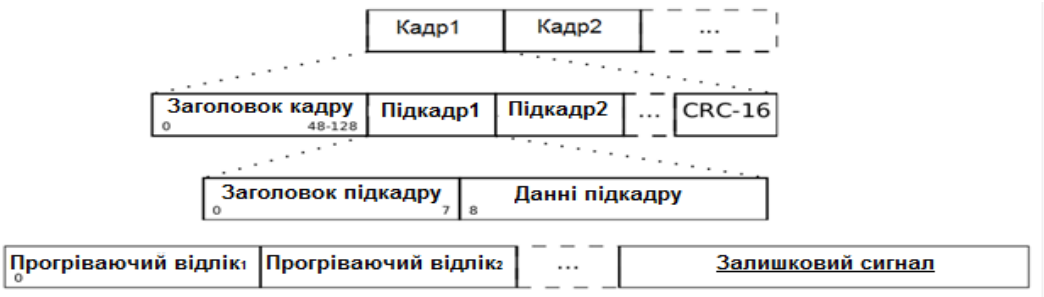

Рис. 1. Структура кадру даних аудіофайла формату FLAC

- SUBFRAME_CONSTANT – для декількох відліків оригінального сигналу, що містять те саме значення, зберігається лише саме значення та кількість таких відліків.
- SUBFRAME_VERBATIM – містить некодований оригінальний сигнал.

- SUBFRAME_FIXED – містить оригінальний сигнал, стиснутий з використанням визначених лінійних предикторів. Відмінність між оригінальним та передбаченим за допомогою предикторів сигналами – залишковий сигнал кодується кодами Райса.
- SUBFRAME_LPC – подібний до попереднього, але лінійні предиктори вибирають під час кодування, інформація про них зберігається у підкадрі [12].

Вбудовування ЦВЗ за рахунок стиснення залишкового сигналу

У разі вбудовування ЦВЗ у оригінальний сигнал за допомогою певного алгоритму виникають викривлення корисного сигналу. Якщо в разі передавання вбудованої інформації за допомогою стегоконтейнера помітні викривлення можна замаскувати за допомогою накладання додаткового шуму або навіть ігнорувати, у випадку вбудовування ЦВЗ необхідний інший підхід, який дозволить зберегти якість звучання аудіосигналу на необхідному рівні.

Для повного вирішення цієї проблеми треба повністю відновити оригінальний сигнал після зчитування вбудованої інформації. Цього можливо досягти або вилучивши ЦВЗ із сигналу перед його відтворенням, або не додаючи ЦВЗ до корисного сигналу, а зберігаючи його інакше.

Зберігання цифрового підпису або іншої інформації, що становить ЦВЗ, у метаданих файла є ненадійним, оскільки його легко видалити. Надійнішим може бути вбудовування ЦВЗ у кадр даних. Так, якщо залишковий чи оригінальний сигнал буде стиснуто за допомогою певного алгоритму стиснення даних, ЦВЗ може бути дописаний до сигналу так, що загальна довжина отриманої бітової послідовності збігатиметься із довжиною нестиснутого сигналу.

Для реалізації такого алгоритму необхідно перевірити можливість стиснення залишкового аудіосигналу або його частини, тобто його надлишковість. Для цього проведено стиснення послідовності останніх бітів залишкового сигналу кадру даних спеціально вибраного аудіосигналу за допомогою деяких поширених алгоритмів стиснення. Моделювання роботи алгоритму проведемо у середовищі математичних обчислень Matlab 2010a. Як контейнер використаємо файл, створений за допомогою програми FLAC-Frontend 2.0 з налаштуванням рівня стиснення = 5. Для отримання файла формату FLAC використаємо спеціально записаний файл формату WAV. Кількість відліків у файлі N = 4096, кожний відлік кодується n = 16 біт, частота дискретизації f_d = 44,1 кГц, файл моноканальний. Також проведено експерименти з модифікованою послідовністю, отриманою з оригінальної виконанням логічної операції XOR кожного біта, крім останнього з попереднім. Мета такого перетворення – довести, що результати стиснення інваріантні щодо попередньої обробки послідовності. Для експериментів використано програму 7-Zip. Результати моделювання наведено у табл. 1.

Отже, стиснення цієї частини залишкового сигналу неможливе, а його надлишковість мінімальна. Тому необхідно розробити стеганографічний алгоритм, що дасть змогу провести занурення ЦВЗ безпосередньо у залишковий сигнал аудіофайла формату FLAC.

Таблиця 1

Результати стиснення послідовності, вилученої із залишкового сигналу

Алгоритм стиснення	Розмір для оригінальної послідовності, байт	Розмір для модифікованої послідовності, байт
Без кодування	511	511
Арифметичне кодування	512	512
LZMA	645	644
LZMA2	623	623
PPMd	671	670
Bzip2	743	740

Вбудовування ЦВЗ у залишковий сигнал

Вбудовування ЦВЗ у залишковий або некодований оригінальний сигнал можливо виконувати у просторовій або у частотній області. Для вбудовування у просторовій області використаємо метод найменшого значущого біта (НЗБ). З метою додавання ЦВЗ у частотній області сигналу розробимо стеганографічний алгоритм вбудовування інформації. Для переходу до частотної області необхідно виконати певне перетворення над сигналом. Найчастіше використовується перетворення Фур'є [13]. Оскільки це перетворення потребує значного обсягу обчислень, у цьому випадку доцільнішим буде

використання простіших та швидших алгоритмів, наприклад швидкого перетворення Уолша–Адамара (ШПУА) [14]. Можливе також використання рекомендацій з [10].

Для моделювання використаємо те саме середовище математичних обчислень та файл-контейнер, що і у розділі 2. Алгоритм забезпечує вбудовування інформації модифікуванням значень певних коефіцієнтів ШПУА [15]. Як секретний ключ розглядаються номери коефіцієнтів *m*, *n*, поріг розпізнавання *T* та значення ступеня стиснення *C*. Стегоповідомлення розглянемо як бітову послідовність $p_1, p_2,..., p_t$ де $p_i \in \{0, 1\}$, $i = 1, 2,..., t$. Пропускна здатність стегоканалу, утвореного за допомогою цього методу, становитиме

$$C = \frac{f_d}{8 \cdot j}, \tag{1}$$

де f_d – частота дискретизації аудіофайла-контейнера, Гц; j – розмір блока масиву коефіцієнтів ШПУА.

У цьому алгоритмі виконуються такі кроки [15].

Крок 1. Аудіофайл розбивається на окремі кадри, визначається їх тип.

Крок 2. Для кожного кадру, який має залишковий сигнал (ЗС), ЗС зчитується та декодується.

Крок 3. Для масиву значень залишкового сигналу виконується ШПУА.

Крок 4. Масив коефіцієнтів ШПУА розбивається на блоки розміром 1×8 (2):

$$X_j = (X_{1,j}, X_{2,j}, ..., X_{8,j}), \tag{2}$$

де j – номер відповідного коефіцієнта ШПУА.

Крок 5. Вибирають пару коефіцієнтів ШПУА: $X_{m,j}$ та $X_{n,j}$ так, щоб зменшити помітність внесених викривлень. Якщо ж $p_i = 0$, то $X_{m,j}$ корегується так, щоб виконувалась умова (3). У іншому випадку корегується $X_{n,j}$ так, щоб виконувалась умова (4).

$$|X_{m,j}| - |X_{n,j}| > P, \tag{3}$$

$$|X_{m,j}| - |X_{n,j}| < -P, \tag{4}$$

де j – номер відповідного коефіцієнта ШПУА.

Крок 6. Виконується збирання блоків у масив коефіцієнтів ШПУА.

Крок 7. Виконується зворотне ШПУА масиву коефіцієнтів.

Крок 8. Здійснюється кодування ЗС, запис його у кадр аудіофайла.

Крок 9. Коригуються контрольні суми кадрів та хеш-сума аудіоданих.

Зчитування вбудованої інформації здійснюється так [15].

Крок 1. Аудіофайл ділять на окремі кадри, визначається їх тип.

Крок 2. Для кожного кадру, який має ЗС, ЗС зчитується та декодується.

Крок 3. Для масиву значень ЗС виконується ШПУА.

Крок 4. Масив коефіцієнтів ШПУА розбивається на блоки розміром 1×8 (3.1).

Крок 5. У випадку, якщо виконується умова (5), то $p_i = 0$; інакше приймаємо, що $p_i = 1$.

$$|X_{m,j}| > |X_{n,j}|, \tag{5}$$

де j – номер відповідного коефіцієнта ШПУА.

Значення основних показників викривлення сигналу в разі вбудовування ЦВЗ певної довжини *t* наведено у табл. 2.

Таблиця 2

Основні показники викривлення сигналу

Назва параметра викривлення	Значення за $t = 200$	Значення за $t = 500$	Значення з використанням алгоритму НЗБ
Максимальна різниця, MD	774	1197	1
Середня максимальна різниця, AD	167,3125	274,537	0,4916
Нормована середня максимальна різниця, nAD	0,2020	0,331	$5{,}93 \cdot 10^{-4}$
Середньоквадратична похибка, MSE	$4{,}526 \cdot 10^4$	$1{,}217 \cdot 10^5$	0,4916
Нормована середньоквадратична похибка, NMSE	0,0087	0,023	$9{,}41 \cdot 10^{-8}$
Співвідношення “сигнал/шум”, SNR	115,4617	42,935	$1{,}06 \cdot 10^7$
Максимальне співвідношення “сигнал/шум”, PNSR	$1{,}189 \cdot 10^4$	$4{,}421 \cdot 10^3$	$1{,}09 \cdot 10^9$
Якість звучання, AF	0,991	0,977	1
Нормована взаємна кореляція, NC	1,001	1,011	1
Якість кореляції, CQ	$2{,}226 \cdot 10^6$	$2.248 \cdot 10^6$	$2{,}23 \cdot 10^6$
Структурний зміст, SC	0,991	0,958	1

Цей алгоритм можливо модифікувати з метою занурення крихкого ЦВЗ. Цифровий підпис правовласника додаватиметься до блока метаданих APPLICATION разом з іншою службовою інформацією програми, за допомогою якої створюється файл. У залишковий сигнал буде вбудовуватися спеціально згенерована псевдовипадкова бітова послідовність, ключем для генерації якої буде значення певної хеш-функції для ЦВЗ. Отже, у разі вилучення або модифікації ЦВЗ відновлення оригінального сигналу буде неможливим.

Висновки

Розроблено стеганографічний алгоритм приховування інформації у частотній області залишкового сигналу аудіофайла зі стисненням без втрат формату FLAC, який дає змогу вбудовувати ЦВЗ у аудіосигнал. Здійснено моделювання роботи алгоритму в середовищі Matlab, визначено значення основних показників викривлення аудіосигналу в разі вбудовування ЦВЗ у частотну область та у просторову з використанням методу НЗБ. Такі викривлення порівняно незначні й можуть бути прийнятними для забезпечення якості звучання на рівні форматів зі стисненням із втратами. Для зменшення викривлень можливе використання принципів аудіомаскування та відповідна модифікація алгоритму. Також можливо модифікувати алгоритм з метою використання крихких ЦВЗ.

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-пресс, 2002. 2. Григорьян А. К. Аветисова Н. Г. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор // Информационно-управляющие системы № 2 / том 45 / 2010 3. Андрианова О. С., Губенко Н. Е. Метод скрытой передачи больших массивов информации путем стегокодирования звуковых и графических файлов // Материалы 3-й международной научно-технической конференции "Моделирование и компьютерная графика-2009". Донецк, 7–9 октября 2011 г. – С. 389–392. 4. Жарких А. А., Гурин А. В., Пластунов В. Ю. Точно обратимый метод встраивания данных в аудиофайл с сохранением гистограммы контейнера // Вестник МГТУ. – 2010. – Т.13, № 4/2. – С. 1048–1051. 5. Хабес Альхрейсат. Сокрытие информации внутри WAV-файлов: применение, анализ и оценка // Известия СПбГЭТУ "ЛЭТИ". – 2006. – Т. 3 – С. 48–56. 6. Жилкин М. Ю., Меленцова Н. А. Метод выявления скрытой информации, базирующийся на сжатии // Вычислительные технологии. – 2007. – Т.12, № 4. – С. 26–31. 7. Кокорин П. П. О методах стегоанализа в аудиофайлах // Труды СПИИРАН, Вып. 4. – СПб.: Наука, 2007. – С. 239–246. 8. Алексеев А. П., Аленин А. А., Михайлов В. И. Выявление стеганографических вложений в WAV-файлах с помощью спектрального анализа // Инфокоммуникационные технологии. – 2011. – Т.9. № 2. – С. 53–57. 9. Коробейников Г. А., Даурских А. Г., Павлова Н. В. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра // Научно-технический вестник СпбГУ ИТМО – 2009. – №1(59). – С. 82–87. 10. Жарких А. А., Пластунов В. Ю. Новый метод внедрения водяного знака в аудиосигнал // Вестник МГТУ. – 2009. – Т.12, № 2. – С. 206–211. 11. Антипов И. Е., Тендитник В. А. Анализ свойств слуха с точки зрения интеграции цифровых водяных знаков // Матеріали VI Міжнародної науково-практичної конференції "Сучасні проблеми і досягнення в галузі радіоелектроніки, телекомунікацій та інформаційних технологій", 19–21 вересня 2012 р., Запоріжжя. – С. 303–305. 12. FLAC format. [Електроний ресурс] // Xiph.org Foundation. – 2014. – Режим доступу: https://xiph.org/flac/format.html. 13. Залманзон Л. А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 584 с. 14. Айфичер Э. С., Барри У. Д. Цифровая обработка сигналов. – М.: Вильямс, 2004. – 989 с. 15. Калашніков М., Яковенко О., Кушніренко Н. Вбудовування цифрових водяних знаків у аудіофайли зі стисненням без втрат // Матер. III Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем", 5–6 червня 2014 р., Львів. – С. 96–97.