DOI 10.15276/imms.v15.no4.625
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 4, pp. 625-635

ДОСЛІДЖЕННЯ СТІЙКОСТІ ТРАНСФОРМАНТ ПЕРЕТВОРЕННЯ УОЛША-АДАМАРА ДО СТИСНЕННЯ MPEG3 В ЗАДАЧАХ АУДІОСТЕГАНОГРАФІЇ

[1]А. В. Соколов, [2]М. В. Хименко

[1]Національний університет «Одеська юридична академія»
23, Фонтанська дорога, Одеса, 65009, Україна
[2]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна

Представлено новий напрямок розвитку аудіостеганографії – адаптація та обґрунтування методів кодового управління для підвищення стійкості прихованих повідомлень в аудіоконтейнерах до сучасних атак стисненням, зокрема до MPEG3. Автори проводять системний аналіз сучасних підходів до аудіостеганографії та підкреслюють їхні обмеження – втрату прихованих даних під час стиснення або надмірну вимогливість до обчислювальних ресурсів, що ускладнює використання в мобільних та вбудованих системах. У цьому контексті пропонується адаптувати до аудіоконтейнерів концепцію кодового управління, яка вже продемонструвала високу ефективність для зображень. Такий підхід відкриває можливість здійснювати контрольоване вбудовування даних у стійкі компоненти сигналу, поєднуючи непомітність, стійкість до атак і обчислювальну ефективність. Ключовим внеском роботи є розробка алгоритму ідентифікації трансформант Уолша-Адамара, які мінімально спотворюються під час стиснення MPEG3. Алгоритм послідовно порівнює пари блоків вихідного (FLAC) і стисненого (MPEG3) сигналів, обчислює перетворення Уолша-Адамара, накопичує статистики змін та візуалізує частоти мінімального спотворення трансформант Уолша-Адамара у вигляді гістограм, що дозволяє об'єктивно виділяти пріоритетні позиції для вбудовування. Експерименти виконані на широкому наборі HiFi-аудіозаписів із тестуванням кількох бітрейтів (320, 256, 192, 128 кбіт/с) та різних довжин блоків, що забезпечує репрезентативність та надійність висновків. Результати експериментів демонструють стійку закономірність: трансформанти з індексами 8 і 12 стабільно виявляють найвищу стійкість до спотворень при стисканні і є пріоритетними для вбудовування прихованих даних; при зниженні бітрейту до 192 і 128 кбіт/с окрім зазначених трансформант практично допустимо (і доцільно в ряді сценаріїв) використання трансформант 0 і 4, що розширює набір безпечних позицій для кодового управління. Крім того, при збільшенні довжини блоку до 64 елементів, показано, що стійкою є трансформанта 32. Практична значимість дослідження полягає в тому, що виділені стійкі трансформанти можуть стати основою для створення адаптивних, високоефективних алгоритмів стеганографії з кодовим управлінням: вони дозволяють поєднувати невидимість, стійкість до поширених алгоритмів стиску (включаючи MPEG3) і низькі обчислювальні витрати, що робить запропонований підхід придатним для впровадження в реальні системи. Робота також відкриває перспективи подальших досліджень – розширення аналізу на інші алгоритми стиснення та мультимедійні формати, інтеграцію методів машинного навчання для автоматичної адаптації кодових слів та розробку нових стеганографічних схем.

Ключові слова: аудіостеганографія, кодове управління, перетворення Уолша-Адамара, стеганоповідомлення, стійкість до стиснення, MPEG3-компресія, трансформанти, інформаційна безпека.

Вступ і постановка задачі. Сучасні інформаційні системи дедалі частіше стають об’єктом атак, спрямованих на несанкціоноване отримання, модифікацію чи блокування даних. У таких умовах особливого значення набувають системи стеганографічного захисту інформації. На відміну від криптографії, що забезпечує конфіденційність вмісту повідомлення, стеганографія дозволяє приховати сам факт його існування, що робить її

потужним інструментом у сфері кібербезпеки, цифрових комунікацій та захисту авторських прав [1].

Актуальність стеганографії обумовлена зростанням обсягів мультимедійного контенту, який використовується як контейнер для прихованих повідомлень. Аудіо- та відеофайли, завдяки своїй надмірності та складній структурі, відкривають широкі можливості для вбудовування даних без помітного погіршення надійності сприйняття. Разом із тим, розвиток алгоритмів стиснення з втратами висуває нові виклики, оскільки такі перетворення можуть спотворювати або знищувати стеганографічні вбудовування. Тому дослідження стійкості методів стеганографії до сучасних форматів стиснення є одним із ключових напрямів наукових пошуків сьогодення.

У науковій літературі значна частка досліджень присвячена стеганографії у цифрових зображеннях, що пояснюється їхньою поширеністю та зручністю для вбудовування даних [2]. Проте аудіоконтейнери також відіграють вагому роль у сфері прихованого передавання інформації. Аудіо широко використовується в телекомунікаціях, медіаіндустрії та потокових сервісах, тому вдосконалення методів стеганографії для звукових сигналів є вкрай актуальним. Розробка стійких до стиснення та інших видів атак алгоритмів приховування в аудіо відкриває перспективи для створення більш надійних і практично орієнтованих систем захисту інформації.

До сучасних стеганографічних методів висувається низка ключових вимог [3]. Насамперед це надійність сприйняття, тобто відсутність помітних змін у контейнері для людини чи стандартних засобів аналізу якості. Важливим критерієм є також стійкість до атак, спрямованих на пошкодження або знищення прихованого повідомлення, а також захищеність від стеганоаналізу, що забезпечує невиявність факту прихованого передавання даних. Сьогодні до цих класичних вимог додається ще один критично важливий аспект – обчислювальна ефективність. Умови використання стеганографії дедалі частіше передбачають реалізацію алгоритмів на пристроях із обмеженими ресурсами, зокрема в системах Інтернету речей та на мобільних платформах. Це вимагає створення методів, які поєднують високу стійкість і невиявність із мінімальними витратами обчислювальних ресурсів.

Наразі запропоновано чимало методів стеганографії для аудіо, від простих бітових модифікацій до сучасних підходів із застосуванням машинного навчання й методів «coverless».

У роботі [4] запропонований метод аудіостеганографії, що базується на модифікації окремих бітів аудіосигналу. Хоча цей підхід простий у реалізації і може бути ефективним при низьких бітрейтах, він страждає від низької стійкості до різних методів аналізу та обробки сигналів. Найменші зміни в аудіофайлі можуть призвести до помітних спотворень, що робить його вразливим до атак і знижує його застосування в реальних умовах.

Запропонований метод coverless аудіостеганографії [5] використовує генеративні змагальні мережі (GAN) для синтезу стеганографічного аудіо без необхідності у вихідному аудіофайлі. Хоча це рішення підвищує скритність, воно вимагає значних обчислювальних ресурсів і може страждати від обмеженої здатності відновлення прихованої інформації. Крім того, якість синтезованого аудіо може змінюватись, що впливає на сприйняття кінцевого користувача.

Метод [6] пропонує сегментацію аудіофайлу на передній та задній плани для більш ефективного вбудовування прихованої інформації. Однак підхід може бути чутливим до різних типів аудіофайлів та умов запису. Крім того, алгоритм може вимагати попереднього аналізу та налаштування для кожного конкретного випадку, що обмежує його універсальність та зручність використання.

Метод [7] поєднує в собі придушення мікромодуляції амплітуди та використання узагальненої аудіо-внутрішньої енергії для підвищення стійкості до спотворень. Однак, незважаючи на поліпшення у скритності та стійкості, метод може бути складним у

реалізації та вимагати значних обчислювальних ресурсів. Крім того, ефективність методу може залежати від характеристик вихідного аудіофайлу, що обмежує його універсальність.

Підхід [8] використовує кластеризацію з диференціальною приватністю для створення стеганографічного аудіо без необхідності у вихідному файлі. Хоча метод забезпечує високий рівень конфіденційності та скритності, він може бути чутливим до якості та різноманітності вихідних даних. Крім того, складність алгоритму та вимоги до обчислювальних ресурсів можуть обмежувати його застосування у реальних умовах.

Як видно з проведеного аналізу представників сучасних стеганографічних методів, жоден із них не позбавлений суттєвих недоліків: одні вразливі до стандартних перетворень і стиснення (що призводить до втрати вбудованої інформації), інші потребують значних обчислювальних ресурсів або мають обмежену універсальність щодо жанру й формату аудіо, ще інші – вразливі до сучасних методів стеганоаналізу. Через це питання створення одночасно стійких, невиявних та ефективних у обчислювальному сенсі аудіостеганографічних методів залишається відкритим і потребує подальших досліджень.

У галузі стеганографії для цифрових зображень справжнім проривом став підхід на основі кодового управління [9]. Використання цієї концепції дозволило вивести стеганографічні методи на новий рівень, забезпечивши одночасне дотримання ключових вимог: надійності сприйняття, стійкості до атак та захищеності від стеганоаналізу. Крім того, алгоритми з кодовим управлінням відзначаються високою обчислювальною ефективністю, що робить їх придатними для практичного застосування навіть на пристроях з обмеженими обчислювальними ресурсами. Це відкриває перспективи поширення даного підходу і на інші мультимедійні контейнери, зокрема аудіосигнали.

Незважаючи на успіхи кодового управління у стеганографії для зображень, на сьогодні цей метод не адаптований для аудіоконтейнерів. Більше того, залишаються невивченими навіть базові характеристики застосування підходу до звукових сигналів. Зокрема, невідомо, які трансформанти аудіо могли б забезпечити найкращу роботу алгоритму, зберігаючи стійкість до атак, захищеність від стеганоаналізу та мінімальні обчислювальні витрати. Це обґрунтовує необхідність проведення фундаментальних досліджень для визначення оптимальних параметрів і стратегій застосування кодового управління у аудіостеганографії.

У рамках даного дослідження планується дослідити трансформанти аудіосигналів, отримані за допомогою перетворення Уолша-Адамара, з точки зору їхньої стійкості до атак проти прихованого повідомлення. Особлива увага буде приділена впливу стиснення аудіо, оскільки воно є однією з найпоширеніших форм модифікації сигналу, здатною суттєво спотворювати вбудовану інформацію. Результати цього аналізу дозволять визначити, які трансформанти є найбільш підходящими для подальшого застосування методів кодового управління в аудіостеганографії.

Метою цієї роботи є підвищення стійкості стегноповідомлень у аудіо контейнерах на основі кодового управління до атак стисненням шляхом дослідження трансформант перетворення Уолша-Адамара.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Дослідження модальності алгоритмів стиснення аудіо, які можуть виступати як атака на приховане повідомлення.
2. Дослідження вплив алгоритмів стиснення на трансформанти Уолша-Адамара аудіоконтейнерів.
3. Визначення трансформанти Уолша-Адамара, що демонструють найвищу стійкість до атак стисненням.

Розв’язання зазначених завдань закладе фундамент для подальшого застосування методів кодового управління в аудіоконтейнерах. Визначення стійких до стиснення трансформант Уолша-Адамара дозволить розробляти алгоритми приховування

інформації, що поєднують високу стійкість до атак, захищеність від стеганоаналізу та обчислювальну ефективність, необхідну для реалізації на мобільних та вбудованих пристроях. Таким чином, результати цього дослідження стануть основою для створення практично орієнтованих систем аудіостеганографії нового покоління.

Огляд концепції кодового управління та її застосування для аудіоконтейнерів. На сьогодні створена ціла плеяда методів стеганографії з кодовим управлінням. Серед них можна виділити класичний метод, заснований на бінарних кодових словах [9], метод на основі багаторівневих кодових слів [10,11], метод зі сліпим декодуванням [12], а також алгоритми, що забезпечують множинний доступ до прихованої інформації [13]. Кожен із цих підходів по-своєму забезпечує дотримання ключових вимог стеганографії, поєднуючи надійність сприйняття, стійкість до атак і захищеність від стеганоаналізу, при цьому демонструючи високу обчислювальну ефективність.

Основою всіх цих методів є перетворення Уолша-Адамара [14], яке визначається за допомогою наступного співвідношення

$$V = YH_N, \tag{1}$$

де матриця Адамара H_N порядку N задається за допомогою конструкції Сильвестра

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{2}$$

Основна ідея стеганографії з кодовим управлінням полягає у лінійності перетворення Уолша-Адамара, що дозволяє ефективно працювати з трансформантами сигналу, а також у адитивний спосіб вбудовувати приховане повідомлення. Розпишемо цю ідею застосовно до аудіоконтейнерів, для яких доречним є саме одновимірний варіант перетворення Уолша-Адамара. Нехай у черговий вектор блоку аудіоконтейнера Y_i необхідно вбудувати черговий біт інформації d_i, який представляється у вигляді знакового кодування кодового вектора C_i тоді вектор стеганоповідомлення матиме вигляд

$$S_i = Y_i + (-1)^{d_i} C_i. \tag{3}$$

Знаходячи перетворення Уолша-Адамара вектора S_i згідно до (1) та застосовуючи властивість лінійності цього перетворення отримуємо наступне співвідношення

$$V_{S_i} = (Y_i + (-1)^{d_i} C_i) H_N = Y_i H_N + (-1)^{d_i} C_i H_N. \tag{4}$$

Поданий вираз демонструє, що конкретний характер впливу на трансформанти перетворення Уолша-Адамара вектора блоку контейнера Y_i визначається видом кодового слова C_i, яке використовується під час вбудовування. Іншими словами, вибір кодового слова безпосередньо задає, які саме трансформанти будуть модифіковані та яким чином. Якщо ж кодове слово підібране таким чином, щоб воно цілеспрямовано впливало на задані трансформанти перетворення Уолша-Адамара, то з'являється можливість вбудовувати додаткову інформацію саме в ті компоненти, які є найбільш придатними з точки зору стійкості до атак чи невиявності. Це відкриває шлях до побудови адаптивних стеганографічних методів, де управління вбудовуванням здійснюється на рівні структури трансформант.

Методи, засновані на цій ідеї, вже продемонстрували свою ефективність у стеганографії для зображень. Зокрема, вони забезпечують високу стійкість до атак проти вбудованого повідомлення та до атак стеганоаналізу, при цьому вплив на елементи зображення залишається мінімальним і практично непомітним. Важливою перевагою є також те, що завдяки роботі у просторовій області такі методи характеризуються надзвичайно високою швидкодією, що робить їх придатними для використання в реальних системах із жорсткими обмеженнями на обчислювальні ресурси.

Алгоритми стиску аудіосигналів, які можуть застосовуватися для атак. Сучасні алгоритми стиснення аудіо базуються на принципах психоакустики, видаляючи з

сигналу компоненти, малопомітні або нечутні для людського слуху. Це дозволяє істотно зменшити обсяг даних при збереженні задовільної якості звучання. До найбільш відомих підходів належать AAC (Advanced Audio Coding) [15], що забезпечує підвищену ефективність кодування, та OGG Vorbis [16], який виступає відкритою альтернативою комерційним стандартам. Водночас у практичному використанні ключову роль продовжує відігравати алгоритм MPEG3 (MPEG-1 Audio Layer III) [17], який завдяки оптимальному співвідношенню між якістю відтворення та ступенем стиснення залишається найпоширенішим форматом аудіо сьогодні. На рис. 1 подано узагальнену схему роботи алгоритму MPEG3, яка відображає основні етапи обробки сигналу – від аналізу спектра та застосування психоакустичної моделі до квантування і кодування бітового потоку.

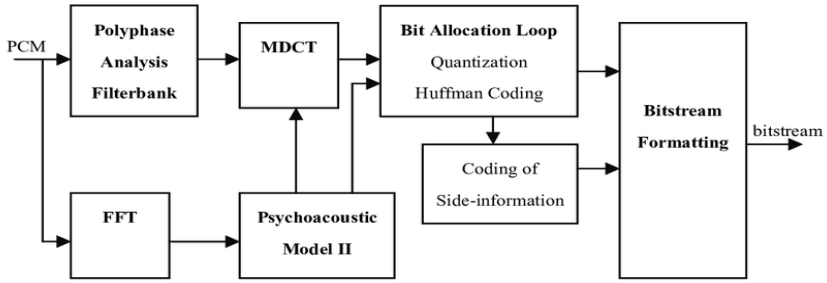

Рис. 1. Схема роботи MPEG3 кодера

На рис. 1 представлено стандартизовану схему роботи MPEG3-кодера, з якої можна виділити такі основні етапи перетворення lossless-файлу (файлу без втрат якості) у формат MPEG3:

– Розбиття, аналіз та квантування. На цьому етапі задається вихідна якість сигналу (як правило частота дискретизації становить 44.1 кГц) та точність квантування (16 біт), що визначають подальшу обробку звуку.

– Перетворення за допомогою MDCT. Вхідна послідовність ділиться на блоки (зазвичай по 576 семплів), після чого кожен блок піддається модифікованому косинусному перетворенню (MDCT).

– Швидке перетворення Фур'є (FFT – Fast Fourier Transform) [8]. Використовується для аналізу спектра та переходу між часовою та частотною областями представлення сигналу.

– Частотне маскування та психоакустичне моделювання [9]. На цьому кроці відкидаються частоти, нечутні для людини, а також ті, що неістотно впливають на якість сприйняття, що суттєво зменшує розмір файлу.

– Квантування та кодування за допомогою коду Гаффмана [10]. Частотні компоненти квантизуються залежно від їхньої важливості (на основі психоакустичних моделей), після чого застосовується кодування Гаффмана для подальшого зменшення обсягу даних.

Для формування вихідного MP3-файлу ключову роль відіграє модифіковане дискретне косинусне перетворення (MDCT). Воно застосовується до послідовності, що попередньо пройшла обробку за допомогою 32-смугового багатофазового квадратурного фільтра (PQF). Завдяки цьому поєднанню забезпечується перехід від часової області до частотної з урахуванням перекриття блоків, що дозволяє зменшити спотворення на межах сегментів та досягти високої якості відтворення при суттєвому зменшенні обсягу даних.

Вектор трансформант p_k перетворення MDCT [18] для заданого блоку $\{x_k\}$ задається як

$$p_k = \sum_{n=0}^{2N-1} x_n \cos\left(\frac{\pi}{N}\left(n+\frac{1}{2}+\frac{N}{2}\right)\left(k+\frac{1}{2}\right)\right). \quad (5)$$

Запропонований алгоритм дослідження. Для проведення експериментів було використано набір із 155 звукових фрагментів та музичних композицій у HiFi-якості у форматі FLAC [11]. Для оцінки ефективності стиснення застосовувався алгоритм з різними бітрейтами.

У більшості випадків стандартним вважається бітрейт 192 Кбіт/с, який забезпечує оптимальний баланс між якістю звучання та розміром вихідного файлу. При такому рівні стиснення звук зберігає повну розбірливість і не втрачає помітних деталей навіть при відтворенні на стандартних пристроях прослуховування.

За основу для пошуку було взято набір з 108 звуків та пісень HiFi якості у форматі FLAC. Алгоритм стискає вхідні файли з бітрейтами 320 Кбіт/с, 256 Кбіт/с, 192 Кбіт/с, 128 Кбіт/с.

Для демонстрації ефективності роботи алгоритму MP3-кодування було проведено експериментальне стиснення набору аудіофайлів у форматі FLAC із подальшим порівнянням їхніх розмірів у вихідному (нестисненому) вигляді та після перетворення з різними бітрейтами.

У табл. 1 наведено приклад значення розмірів набору файлів у мегабайтах для різних бітрейтів, що дозволяє оцінити співвідношення між ступенем стиснення обсягом пам’яті, який займатимуть аудіофайли.

Таблиця 1.

Залежність розміру вихідного набору даних від коефіцієнту збереження якості при стисненні

Бітрейт	Без стиснення (.flac)	320 Кбіт/с (.mp3)	256 Кбіт/с (.mp3)	192 Кбіт/с (.mp3)	128 Кбіт/с (.mp3)
Розмір	2.92 ГБ	1.2 ГБ	1.03 ГБ	878 МБ	699 МБ

Як можна побачити з даних табл. 1, застосування алгоритмів стиснення є надзвичайно важливим інструментом як для ефективного зберігання аудіоінформації, так і для її передачі через канали зв’язку. Використання MPEG3-кодування дозволяє суттєво зменшити обсяг даних без критичної втрати якості, що робить цей підхід базовим стандартом у більшості сучасних мультимедійних систем.

Представимо у вигляді конкретних кроків алгоритм дослідження, який дозволяє визначати трансформанти перетворення Уолша-Адамара аудіоконтейнерів, що є найбільш вразливими до стиснення MPEG3. Застосування цього алгоритму дасть змогу ідентифікувати ті компоненти сигналу, які зазнають найбільших змін під час компресії, а отже, є критично важливими для забезпечення стійкості стеганографічних методів.

Крок 1. Ініціалізувати вектор

$$\begin{array}{r|cccc} i & 0 & 1 & \dots & N-1 \\ \hline \textit{Кількість} & 0 & 0 & \dots & 0 \end{array}. \qquad (6)$$

Крок 2. Обрати та зчитати аудіофайл у форматі без втрат FLAC. Здійснити стиснення обраного аудіофайлу із заданим бітрейтом і зберегти його у форматі з втратами MPEG-3.

Крок 3. Розбити обидві послідовності (без стиснення та із стисненням) на блоки розміру N. Знайти перетворення Уолша-Адамара згідно з (1) для блоків вихідної послідовності та блоків послідовності після стиснення алгоритмом MPEG-3.

Крок 4. Знайти різницю між трансформантами перетворення Уолша-Адамара блоків вихідної послідовності та послідовності із стиском.

Крок 5. Обрати трансфрманту перетворення Уолша-Адамара, яка зазнала найменших змін, інкрементувати значення кількості у (6), що відповідає номеру зазначеної трансформанти.

Крок 6. Якщо оброблено всі аудіофайли, зупин, інакше перейти до Кроку 2.

Крок 7. Здійснити представлення вектора (6) у вигляді стовпчикової діаграми.

Для наочності та кращого розуміння роботи запропонованого підходу алгоритм

дослідження стійкості трансформант перетворення Уолша-Адамара до стиснення MPEG3 буде представлено у вигляді блок-схеми (рис. 2). Такий графічний опис дозволяє чітко простежити послідовність етапів обробки аудіосигналу, від підготовки вхідних файлів і застосування перетворення до аналізу впливу стиснення на окремі трансформанти.

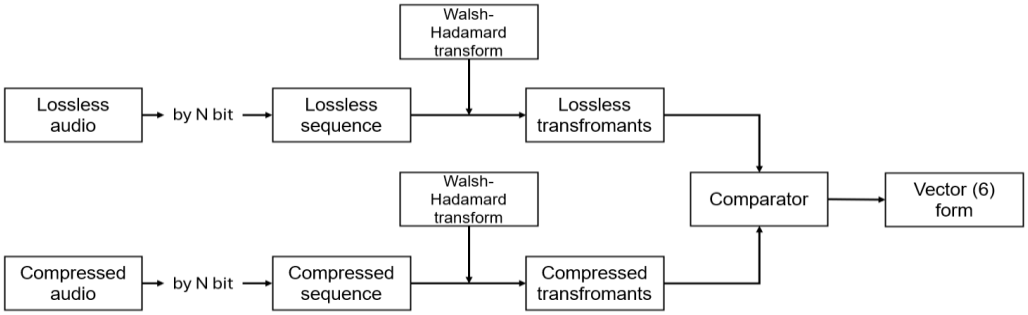

Рис. 2. Схема розробленого алгоритму пошуку трансформант перетворення Уолша-Адамара, що зазнають найбільшого спотворення через стиснення

Як видно з рис. 2, алгоритм обробки отримує два потоки аудіоданих: один у форматі FLAC, інший – у форматі MPEG3. Кожен з них розбивається на послідовності довжиною N елементів. Далі до кожної пари блоків застосовується перетворення Уолша-Адамара [12], основна мета якого – визначити позиції в послідовності, що найменше або найбільше змінюються під час атаки стисненням.

Індекси позицій, які зазнали найменших змін, інкрементуються у відповідному векторі (6), на основі якого будується діаграма частоти появи позицій у блоці, що найменше піддавалися змінам у процесі обробки всього набору даних. У цьому контексті менші значення на гістограмі вказують на статистично більшу стійкість позиції до змін під час стиснення, що дозволяє ідентифікувати трансформанти, найбільш придатні для вбудовування прихованої інформації.

На рис. 3 представлено графічне відображення результатів дослідження стійкості трансформант перетворення Уолша-Адамара до стиснення MPEG3.

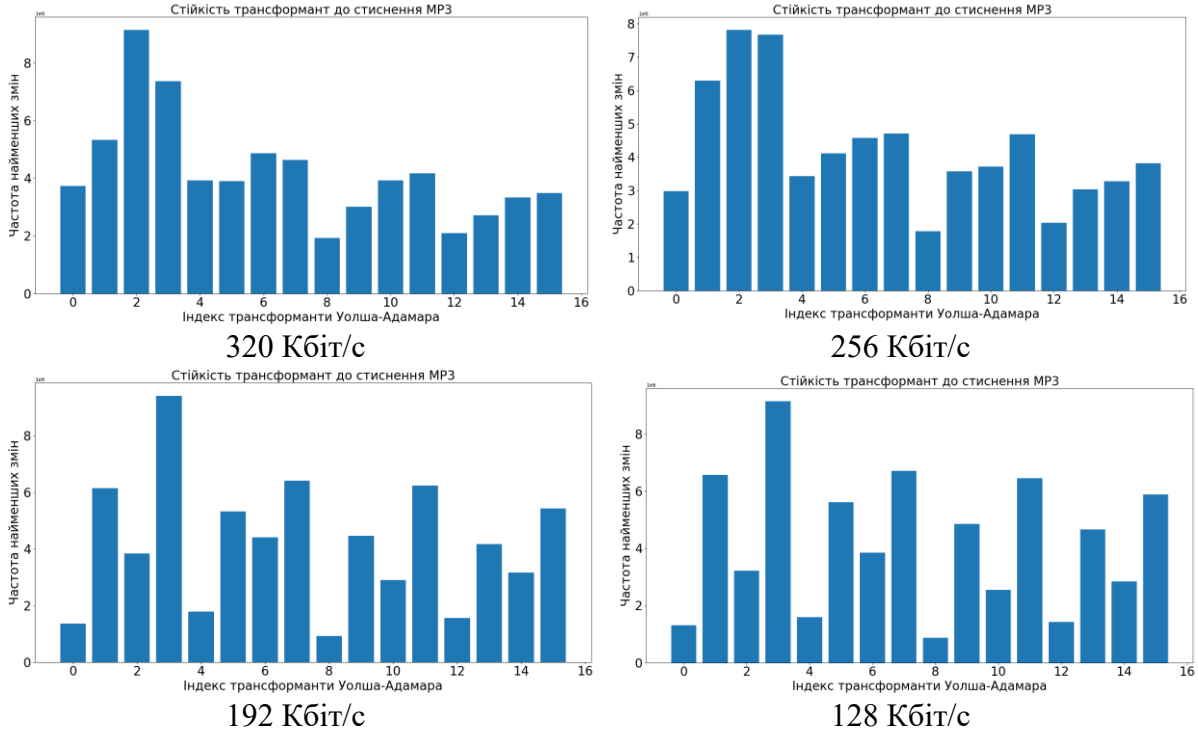

Рис. 3. Зміни трансформант перетворення Уолша-Адамара у аудіофайлах при стисненні MPEG3 для довжини блока $N = 16$

Аналіз представлених на рис. 3 гістограм показав закономірності зміни трансформант при стисненні MPEG3 з різними бітрейтами. Для бітрейтів 256 Кбіт/с і вище найменшому пошкодженню піддаються трансформанти з індексами 8 та 12, що робить їх пріоритетними для вбудовування додаткової інформації. При зниженні бітрейту до 192 та 128 Кбіт/с виявляється можливим також використовувати трансформанти 0 та 4 для вбудовування, проте навіть у цих умовах основною та найбільш стійкою залишається трансформанта 4. Таким чином, результати дослідження дозволяють виділити трансформанти, які забезпечують максимальну стійкість до втрат при стисненні та можуть бути рекомендовані для подальшого застосування методів кодового управління у аудіоконтейнерах. Відзначимо також, що дослідження змін трансформант перетворення Уолша-Адамара в аудіофайлах під впливом MPEG3-стиснення для більших довжин блока (наприклад, $N = 64$) є вкрай важливими. Збільшення розміру блока змінює спектральну роздільну здатність перетворення, по-іншому розподіляє енергію між трансформантами й може виявити інші, більш стійкі до компресії компоненти сигналу, що потенційно збільшує стійкість стеганографічного методу.

Для стислості ми наводимо на рис. 4 гістограму змін трансформант перетворення Уолша-Адамара, побудовану згідно до запропонованого нами алгоритму для бітрейту 128 Кбіт/с і довжини блока $N = 64$.

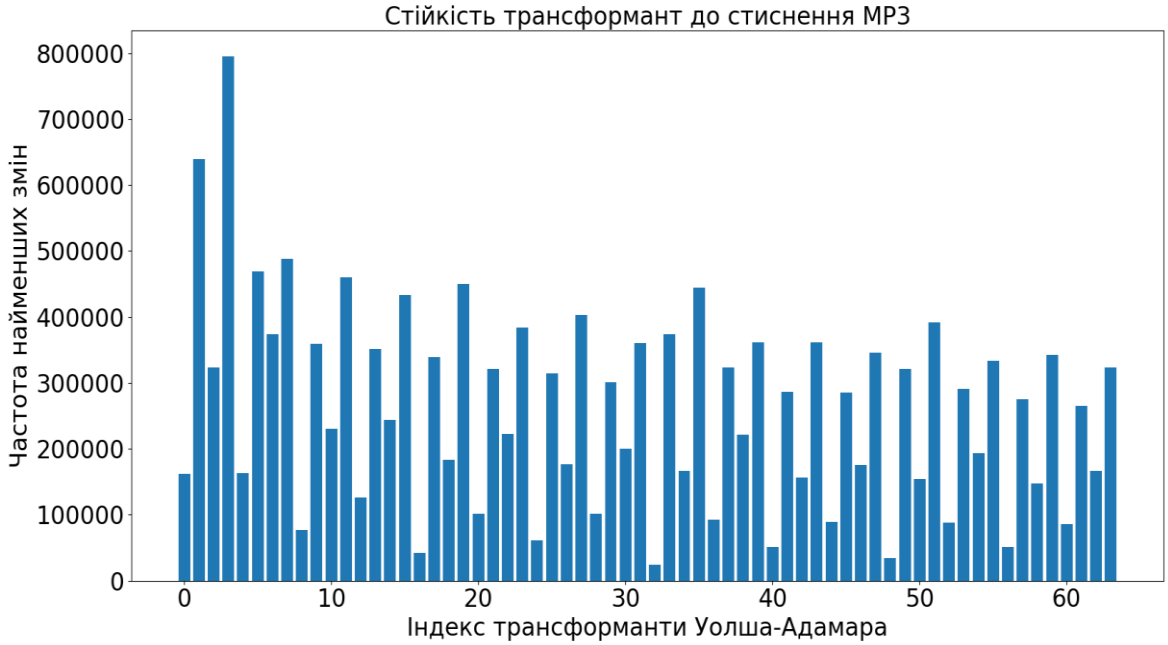

Рис. 4. Зміни трансформант перетворення Уолша-Адамара у аудіофайлах при стисненні MPEG3 для довжини блока $N = 64$

Аналіз представленої на рис. 4 гістограми для блоку довжиною 64 та бітрейту 128 кбіт/с показує, що найбільш стійкою до MPEG3-стиснення є трансформанта номер 32. Саме її рекомендується використовувати для вбудовування додаткової інформації. Водночас трансформанти 16, 24, 40, 48 та деякі інші також демонструють відносну стійкість і можуть слугувати альтернативними позиціями для вбудовування, проте вони поступаються трансформанті 32 за стабільністю та частотою найменших змін.

Висновки. Розв’язано важливу науково-прикладну задачу дослідження стійкості трансформант перетворення Уолша-Адамара в аудіоконтейнерах до атак стисненням на прикладі алгоритму MPEG3. Отримані результати дозволяють сформулювати такі висновки:

1. Проведено ґрунтовний аналіз сучасних методів аудіостеганографії, що показав наявність істотних недоліків існуючих рішень – низьку стійкість до атак

стисненням, значні обчислювальні витрати або обмежену універсальність. Це обґрунтувало доцільність дослідження нових підходів, зокрема методів на основі кодового управління.

2. Запропоновано та реалізовано алгоритм ідентифікації найбільш стійких до стиснення MPEG3 трансформант перетворення Уолша-Адамара. Алгоритм дозволяє статистично визначати ті компоненти спектру сигналу, які зазнають мінімальних змін під час компресії та, відповідно, є найбільш придатними для приховування інформації.

3. Експериментальні дослідження на базі широкого набору аудіофайлів у форматі HiFi довели, що трансформанти з індексами 8 та 12 стабільно демонструють найвищу стійкість до спотворень незалежно від бітрейту стиснення. Разом із тим, при нижчих бітрейтах (192 та 128 Кбіт/с) можливим є також використання трансформант 0 та 4, які зберігають відносну стійкість у цих умовах. Для блоків більшої довжини (64 елементи) найвищу стабільність до компресії показала трансформанта 32. Отримані результати підтверджують залежність оптимального вибору трансформант від параметрів стиснення та розміру блока.

4. Отримані результати підтверджують перспективність використання кодового управління в аудіостеганографії. Ідентифіковані стійкі трансформанти перетворення Уолша-Адамара можуть слугувати основою для побудови адаптивних алгоритмів приховування інформації, що поєднують високу стійкість до атак стисненням, невиявність та обчислювальну ефективність.

Таким чином, розроблений підхід формує науково обґрунтовану базу для подальшої розробки практично орієнтованих систем аудіостеганографії нового покоління, здатних забезпечувати надійний захист інформації навіть у середовищах із жорсткими обмеженнями на обчислювальні ресурси та активним застосуванням алгоритмів стиснення.

Список літератури

1. Babando A. K., Ahmad B. M. Data security using steganography. *LC International Journal of STEM*. 2022. Vol. 3, No. 4. P. 12-24.
2. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. *IEEE Access*. 2020. No. 8. P. 166589-166611. doi: 10.1109/ACCESS.2020.3022779
3. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2010. 251 с.
4. Gopalan K. Audio steganography using bit modification. *International Conference on Multimedia and Expo. ICME'03. Proceedings. IEEE*. 2003. Vol. 1. P. I-629. DOI: 10.1109/icme.2003.1220996
5. Li J., Wang K., Jia X. A coverless audio steganography based on generative adversarial networks. *Electronics.* 2023. Vol. 12, No. 5. P. 1253. DOI 10.3390/electronics12051253
6. Wang J., Wang K. A novel audio steganography based on the segmentation of the foreground and background of audio. *Computers and Electrical Engineering*. 2025. Vol. 123. P. 110026. DOI 10.1016/j.compeleceng.2024.110026
7. Su W. et al. Efficient audio steganography using generalized audio intrinsic energy with micro-amplitude modification suppression. *IEEE Transactions on Information Forensics and Security*. 2024. Vol. 19. P. 6559-6572. DOI: 10.1109/tifs.2024.3417268
8. Feng Y. et al. A robust coverless audio steganography based on differential privacy clustering. *IEEE Transactions on Multimedia*. 2025. DOI: 10.1109/tmm.2025.3543107
9. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. No. 4 (52). P. 115-130. DOI: 10.52254/1857-0070.2021.4-52.11
10. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. *Radiotekhnika.* 2021. 4(207). P. 27–39. DOI: 10.30837/rt.2021.4.207.02.

11. Kobozeva A.A., Sokolov A.V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. *Radioelectronics and Communications Systems*. 2023.Vol. 66, No. 4. P. 173-189. DOI: 10.3103/s0735272723040052
12. Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. Problems of regional energetics. 2024. Vol. 62, No. 2. P. 121-137. DOI: 10.52254/1857-0070.2024.2-62.11
13. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3. P. 147-161. DOI: 10.15276/imms.v11.no3.147
14. Ahmed N., Rao K. R. Walsh-Hadamard transform. Orthogonal transforms for digital signal processing. Berlin, Heidelberg : Springer Berlin Heidelberg, 1975. P. 99-152.
15. Bosi M. et al. ISO/IEC MPEG-2 advanced audio coding. *Journal of the Audio engineering society*. 1997. Vol. 45, No. 10. P. 789-814.
16. Kosaka A. et al. Design of Ogg Vorbis decoder system for embedded platform. *IEICE Transactions on Fundamentals*. 2005. Vol. 88, No. 8. P. 2124-2130. DOI: 10.1093/ietfec/e88-a.8.2124
17. Shlien S. Guide to MPEG-1 audio standard. *IEEE Transactions on Broadcasting*. 2002. Vol. 40, No. 4. P. 206-218. DOI: 10.1109/11.362938
18. Wang Y., Vilermo M. Modified discrete cosine transform: Its implications for audio coding and error concealment. *Journal of the Audio Engineering Society.* 2003. Vol. 51, No. 1/2. P. 52-61.

RESEARCH OF THE ROBUSTNESS OF WALSH-HADAMARD TRANSFORMANTS AGAINST MPEG3 COMPRESSION FOR AUDIO STEGANOGRAPHY

[1]A.V. Sokolov, [2]M.V. Khymenko

[1]National University "Odesa Law Academy"
23, Fontanska doroha, Odesa, 65009, Ukraine
[2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine

The paper presents a new direction in the development of audio steganography – adaptation and justification of code control methods to increase the resistance of covert messages in audio containers to modern compression attacks, in particular to MPEG3. The authors perform a systematic analysis of modern approaches to audio steganography and emphasize their limitations – loss of covert data during compression or excessive demands on computing resources, which complicates their use in mobile and embedded systems. In this context, it is proposed to adapt the concept of code control to audio containers, which has already demonstrated high effectiveness for images. This approach opens up the possibility of controlled data embedding into stable signal components, combining stealth, resistance to attacks and computational efficiency. The key contribution of the paper is the development of an algorithm for identifying Walsh-Hadamard transformants, which are minimally distorted during MPEG3 compression. The algorithm sequentially compares pairs of blocks of the original (FLAC) and compressed (MPEG3) signals, calculates the Walsh-Hadamard transform, accumulates statistics of changes and visualizes the frequencies of minimum distortion of the Walsh-Hadamard transformants in the form of histograms, which allows to objectively highlight priority positions for embedding. The experiments were performed on a wide set of HiFi audio recordings with testing of several bitrates (320, 256, 192, 128 kbit/s) and different block lengths, which ensures the representativeness and reliability of the conclusions. The experimental results demonstrate a stable pattern: transformants with indices 8 and 12 consistently exhibit the highest resistance to distortion during compression and are prioritized for embedding hidden data; when the bitrate is reduced to 192 and 128 kbit/s, in addition to the above transformants, it is practically permissible (and advisable in a number of scenarios) to use transformants 0 and 4, which expands the set of safe positions for code control. In addition, when the block length is increased to 64 elements, it is shown that transformant 32 is stable. The practical significance of the research is that the selected stable transformants can become the basis for creating adaptive, highly effective steganography algorithms with code control: they allow combining invisibility, resistance to common compression algorithms (including MPEG3) and low computational costs, which makes the proposed approach suitable for implementation in real systems. The paper also opens up prospects for further research – expanding the analysis to other compression algorithms and multimedia formats, integrating machine learning methods for automatic adaptation of codewords and developing new steganographic schemes.

Keywords: audio steganography, code control, Walsh-Hadamard transform, steganographic message, compression robustness, MPEG3 compression, transformants, information security.