

ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КВАЛІФІКАЦІЙНА РОБОТА

Другий (магістерський) рівень

**НА ТЕМУ: Метод перевірки цілісності аудіоданих на
основі цифрових водяних знаків**

Автор:
Студент гр. КСМм-22-1
Бондарчук П. С.

Керівник:
доц. Мартовицький В.О

ХАРКІВ
2024р.

1

Метою кваліфікаційної роботи є дослідження та розробка методу перевірки цілісності аудіоданих на основі цифрових водяних знаків

❖ Об'єктом дослідження є процес автентифікації аудіофайлів.

❖ Предметом дослідження полягає в методи перевірки цілісності аудіоданих .

2

Актуальність

1.Забезпечення вірності і точності: Якщо аудіодані втрачають цілісність через помилки при передачі чи збереженні, це може призвести до втрати чи спотворення інформації. Перевірка цілісності допомагає уникнути таких проблем і забезпечити вірність даних.

2.Захист від змін та зловживань: Якщо аудіодані можуть бути змінені без вашого відома чи зловживані, це може вплинути на їхнє використання та вірогідність. Перевірка цілісності допомагає виявити будь-які неправомірні зміни та втручання.

3.Гарантує вірну роботу аудіосистем: У випадку використання аудіоданих в професійних або важливих застосуваннях (наприклад, в медицині, судовій експертизі або аудіозаписах), важливо впевнитися, що дані залишаються недоторканими і їх можна довіряти.

4.Безпека та відповідність: У деяких випадках, особливо коли йдеться про звукові дані, які відносяться до особистої інформації або даних, що підпадають під регуляторні вимоги, перевірка цілісності може бути важливою для виконання вимог щодо безпеки та конфіденційності.

5.Попередження втрати даних: Перевірка цілісності може служити інструментом для попередження втрати аудіоданих через помилки, випадки видалення чи інші проблеми.

3

Існуючі методи забезпечення цілісності

Хеш-суми (MD5, SHA-1, SHA-256)

CRC (циклічний надлишковий код)

Аудіо-сигнатури

Редундантність даних

Файлові характеристики

4

Стеганографія в аудіофайлах

1.Заміна менших бітів (Least Significant Bit, LSB): Цей метод включає в себе приховування інформації, замінюючи менш важливі біти аудіосемплів на біти прихованого повідомлення. Зазвичай це не помітно для вуха людини, але при аналізі може бути виявлено зміни.

2.Фазова модифікація: Іншим методом є зміна фази аудіосигналу, що може бути використаною для приховування інформації. Малі зміни у фазі можуть бути використані для передачі бітів повідомлення.

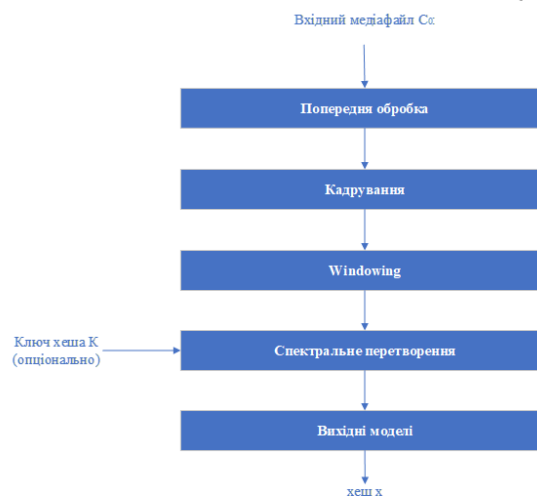
3.Вставка інших звуків: Можливо вставити в аудіоданий вже існуючий звуковий шум, який не буде помітний для слухача, але містить в собі приховану інформацію.

4.Часовий зсув (Time-domain techniques): Цей метод використовує зміни у часовому представленні аудіосигналу для приховування інформації.

5.Використання непримітних частот: Деякі методи можуть використовувати непримітні частоти для приховування інформації, особливо в участках аудіосигналу, які менше чутливі для вуха.

5

Основні етапи перцептивного аудіохешування можуть включати в себе наступні етапи:



6

(1)

Етапи створення перцептивного аудіохеша

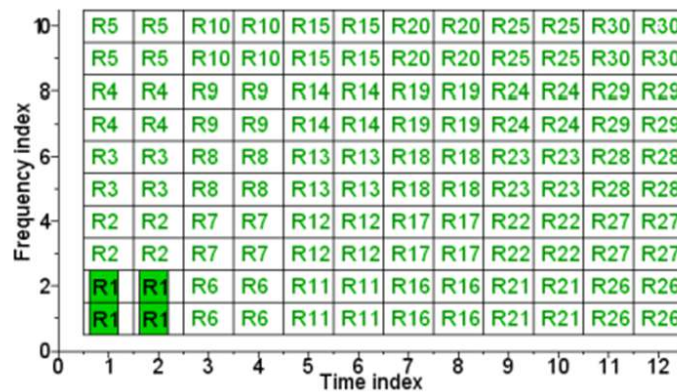
- аудіосигнал представляється в цифровому вигляді семплами і аналізується в досить великих кадрах $L=214 = 16384$ семплів.
- Дані кадру спочатку зважуються за допомогою вікна Хеммінга, щоб уникнути ефектів витоку спектра. Потім обчислюється перетворення Фур'є.
- Потім коефіцієнти амплітуди Фур'є $\{r_k\}$ повторно дискретизуються відповідно до логарифмічно масштабованої вісню частот

$$d_{i,t} := e_{i,t} - e_{i,t-1} - [e_{i+1,t} - e_{i+1,t-1}], i = 1 \dots 32. \quad (1)$$

$$H_{i,t} = \begin{cases} 1 & \text{if } d_{i,t} \geq 0 \\ 0 & \text{if } d_{i,t} < 0 \end{cases} \quad (2)$$

7

Схема виділення ознак



8

Етапи вбудови ЦВЗ

Спочатку, для вбудовування кожного окремого біта повідомлення використовуються дві незв'язні підмножини

$$A := \{a_i\} \quad B := \{b_j\} \quad , \quad A \cap B = \{\} \quad , \quad i, j = 1 \dots N \quad (3)$$

$$\bar{a} := 1/N \sum_{i=1}^N a_i \quad \bar{b} := 1/N \sum_{j=1}^N b_j \quad (4)$$

Тоді, для вбудовування бітового символу повідомлення $m = "1"$, кожне значення вибірки в A трохи збільшується, тоді як кожне значення вибірки в B трохи зменшується; і навпаки, якщо $m = "0"$, відповідно.

Модифіковані коефіцієнти нарешті записуються назад до даних обкладинки, замінюючи оригінальні значення на їхні місця.

9

Алгоритм вбудови ЦВЗ

Вхідні дані: Вхідні аудіодані слід подавати у вигляді інтервалів Імпульсно-кодової модуляції у часовій області. Файл або потік Імпульсно-кодової модуляції розбито на кадри по $L=2048$ відліків. При частоті дискретизації 44.1 кГц L становить 46 мілісекунд тривалості. На практиці загальна кількість модифікованих кадрів T становить кілька сотень (ш дорівнює кільком секундам).

Windowing: Семпли кадру перемножуються поелементно за допомогою вікна Хеммінга

Перетворення Фур'є: Дані віконного кадру перетворюються на спектральну область за допомогою швидкого перетворення Фур'є (ШПФ), отримуючи коефіцієнти $L/2$ абсолютних значень (τ_k) і фазові коефіцієнти (ϕ_k).

Вибір Patchwork шаблону: У спектрі кожного кадру виділимо дві непересічні підмножини $A = \{a_i\} := \{a_{i_n}\}$ та $B = \{b_j\} := \{b_{j_n}\}$ з N абсолютними коефіцієнтами Фур'є, кожен з яких "вибирається" псевдовипадково зі спектру $\{\tau_k\}$. Формальний вибір коефіцієнтів здійснюється шляхом псевдовипадкового вибору відповідних N індексів i_n та j_n з можливого діапазону $i_n, j_n \in \{1 \dots L/2\} \in \mathbb{N}$ та присвоєння їх множинам індексів A та B :

10

Алгоритм вбудови ЦВЗ

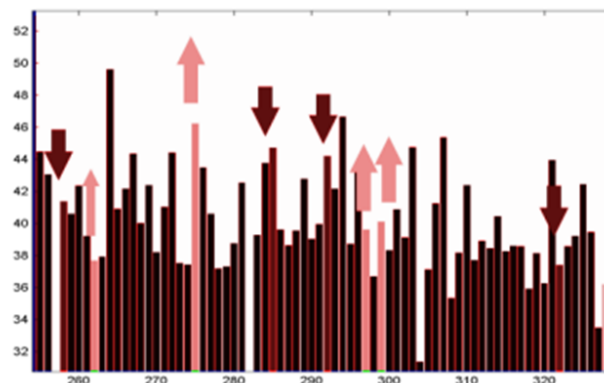
Patchwork Вбудовування: Для вбудовування біта повідомлення коефіцієнти Фур'є модифікуються відповідно до принципу Patchwork, описаного на попередньому слайді збільшення/зменшення аналітично здійснюється експоненціальному представленні з технічних причин:

Модифіковані коефіцієнти записуються назад у спектр величин шляхом заміни вихідних значень на місці, і виходить спектр із водяним знаком.

Зворотне перетворення Фур'є: нарешті, модифікований звуковий спектр (перетворюється назад у спектральну область за допомогою зворотного ШПФ).

11

Принцип Patchwork вбудовування в спектр Фур'є



12

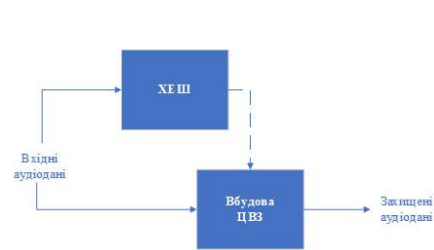


Рисунок 1 – Модель вразливого до вмісту водяного знаку - етап захисту/вбудовування

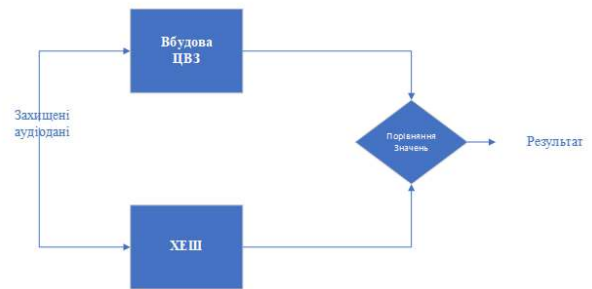


Рисунок 2 – Модель вразливого до зміни вмісту водяного знаку - етап перевірки/виявлення

13

Результати експеременту

Інтервал атаки	Додавання шуму	Вирізання	Переквантування	Змішування з іншим аудіо
1/8 s	0.89	0.49	0.88	0.78
1/4 s	0.85	0.49	0.84	0.74
1/2 s	0.77	0.50	0.77	0.68
1 s	0.71	0.50	0.74	0.66
2 s	0.61	0.50	0.66	0.61
4 s	0.55	0.51	0.59	0.57
8 s	0.50	0.52	0.52	0.54

14

ВИСНОВКИ

- проведено аналіз вучасних методів перевірки цілісності аудиофайлів.
- проведено аналіз методів стеганографії для аудиофайлів.
- реалізовано алгоритм перцептивного аудіохеша .
- реалізовано алгоритм Patchwork вбудови ЦВЗ.
- Реалізовано комбінований метод перевірки цілісності аудіоданих на основі алгоритму перцептивного аудіохеша та алгоритму Patchwork вбудови ЦВЗ .

Апробація результатів роботи була на міжнародній конференції:

Бондарчук П. С., et al. " Аналіз вучасних методів перевірки цілісності аудиофайлів." InterConf (2023): 44-52.