ПРЕЦИЗІЙНІ ВИМІРЮВАННЯ ТА НОВІТНІ ТЕХНОЛОГІЇ

УДК 004.056.55

І.О. КИРИЛЮК, Ю.В. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

АДАПТИВНИЙ МЕТОД ШИФРУВАННЯ АУДІОФАЙЛІВ СПОСОБОМ ПРЕДСТАВЛЕННЯ ЇХ У ВИГЛЯДІ ЗОБРАЖЕНЬ

В статті проведений аналіз аудіофайлів та методів їх шифрування.

Розглянутий спосіб представлення звуку у вигляді спектрограми. Приведений аналіз деяких методів представлення спектрограми.

Представлений свій програмний метод шифрування аудіофайлів, що дозволить зашифровувати спектрограму самого звуку та передати її по мережі з наступним відтворенням цього звуку. Метод застосовується як до статичних аудіофайлів так і до аудіопотоків.

Ключові слова: аудіофайл, спектрограма, віконні перетворення Фур'є.

IHOR KYRYLIUK, YURIY KHMELNITSKY
Khmelnytskyi National University

ADAPTIVE METHOD OF AUDIO ENCRYPTION OF PRESENTING THEM IN THE IMAGE FORM

It article we analyze audio and methods of their encryption.

The way of presentation of sound as a spectrogram. The analysis of several methods of presentation of spectrogram.

Present own method of encryption audio, allowing you to encrypt spectrogram of the sound and send it over the network with the following reproduction of this sound. Method is applicable to static audio files and to audio streams.

Keywords: audio, spectrogram, sound wave, short-time Fourier transform.

Вступ

Життя сучасної людини так чи інакше пов'язане з мережею. Щодня, по ній передається величезна кількість інформації. І в більшості випадків хочемо щоб інформація була доступна лише тим особам, які мають на це право. Для цього потрібно їх шифрувати. Один з типів інформації – це звукова інформація, аудіофайли. За час широкого розповсюдження IP-телефонії, є телефонні дзвінки, записи яких ми не хочемо щоб були доступні всім. При масовому поширенні аудіозаписів, також є особисті записи, що повинні бути захищеними. Тому шифрування аудіо файлів є досить необхідною задачею. При передачі їх по мережі, чи при простому зберіганні на комп'ютері. Отже, з вищесказаного, можна сформувати наше завдання.

Постановка задачі. На сьогодні існує три види шифраторів: апаратні, програмно-апаратні та програмні. Найдорожчі з них це апаратні, де для шифрування потоку аудіо нам потрібно додаткове апаратне забезпечення, яке буде шифрувати аналогові хвилі і далі вже передавати це по мережі. Далі йдуть програмно-апаратні, і самі дешеві це програмні шифратори.

Загалом, основною метою є використання такого методу для шифрування, що може швидко працювати, достатньо якісно захищати звук від зловмисників, та не шкодити нашим даним. Використання апаратних шифраторів для «домашнього» використання, є дуже дорогим засобом. Використання їх для телефонії, також є задорогим та незручним методом. Тому розробляються нові програмні засоби, що вбудовуються в операційні системи, або використовуються як окремі програми.

Перш за все, нам потрібно знайти такий спосіб, який би не нашкодив нашому аудіо файлу, швидко та якісно виконував шифрування аудіо файлу. Метод не повинен залежати від способу представлення звуку, будь це потік чи вже записаний звук. Має бути економним у використанні. Також сам метод не повинен бути складним чи викликати додаткові непотрібні дії зі сторони користувача. Ми можемо представити звук у вигляді спектрограми – залежності частоти від часу. Далі, виконуючи певні дії над спектрограмою ми можемо шифрувати вміст аудіо файлу. Після отримання зашифрованого зображення, воно має бути надійно захищене, і, при потребі, розшифроване назад без затримок та без значного пошкодження початкового звуку.

Мета статті – опис вирішення задачі шифрування аудіо файлів за допомогою перетворення їх в спектрограму, після цього шифруючи. Перетворення в спектрограму виконується через віконні перетворення Фур'є.

Основний матеріал. Отже, нам потрібно наш звук представити перш за все у вигляді спектрограми. При вирішенні задачі перетворення звуку в спектрограму, використовується віконне перетворення Фур'є. Спектрограма – це двовимірний графік, де на горизонтальній осі йде представлення

часу, на вертикальній – частота. Третій вимір – амплітуда, представлена інтенсивністю або кольором кожної точки в зображенні[1]. Спектрограми зазвичай створюються одним з двох способів: апроксимуються, як набір фільтрів, отриманих з серії смугових фільтрів (це, власне, був єдиний метод до появи сучасних методів цифрової обробки сигналів), або розраховуються по сигналу часу, використовуючи віконні перетворення Фур'є. Для цифрової обробки, зазвичай, використовуються саме віконні перетворення Фур'є (відмінність віконного перетворення від звичайного перетворення Фур'є полягає в тому, що віконне перетворення є функцією від часу, частоти та амплітуди, в той час як звичайне перетворення є функцією лише від частоти, що не дозволяє визначати час в який ми фіксуємо ту чи іншу частоту звуку), що визначаються наступним чином:

$$F(t,\omega) = \int_{-\infty}^{\infty} f(\tau) W(\tau - t) e^{-i\omega t} d\tau ,$$

де $W(\tau - t)$ – деяка віконна функція.

Виконується цифрова вибірка даних в деякій часовій області. Сигнал розбивається на частини, які, як правило, перекриваються, а після цього проводиться перетворення Фур'є, для того щоб розрахувати величину частотного спектру для кожної частини. Ці частини відповідають вертикальній лінії на зображенні – значення амплітуди в залежності від частоти в кожний момент часу[2].

Суть віконного перетворення полягає в тому, що ми наш звук розбиваємо на частини – вибірки, після чого до цих вибірок застосовується перетворення Фур'є і, після перетворення ці частини разом утворюють повну спектрограму. Існує багато різних видів цих вибірок, їх ще називають вікнами. Зазвичай використовуються вікна Ханна, Хемінга, Блекмана.

Для прикладу, візьмемо вікно Ханна. Воно характеризується наступною формулою:

$$W(n) = 0.5 * \left(1 - \cos\left(\frac{2\pi n}{N-1}\right)\right),$$

де $N - 1$ – вибірка. На рисунку 1 представлений загальний вигляд вікна Ханна.

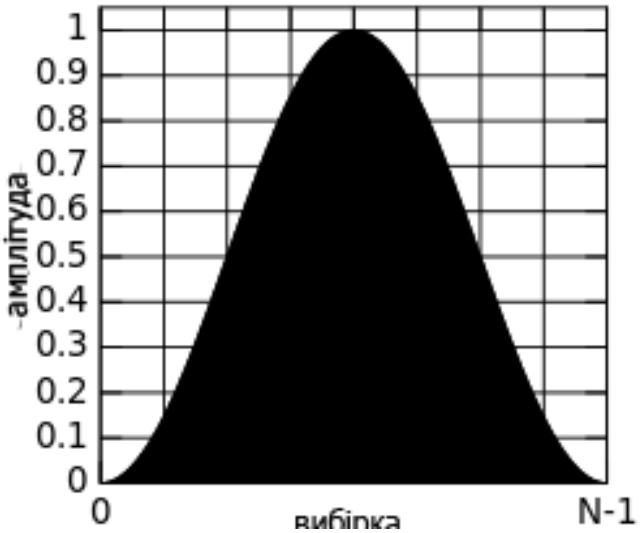

Рис. 1. Вікно Ханна

Перевагою вікна Ханна є дуже низький рівень, так званого, аліасингу. Це явище накладання або нечіткості різних безперервних сигналів. Наприклад накладання високих частот на низькі в результаті чого сигнал спотворюється. Якщо вікно Ханна використовується в якості вибірки сигналу, для перетворення Фур'є, то при зворотному перетворенні в нас буде утворюватися мінімальна кількість спотворень. Спочатку весь наш звуковий файл буде поділений на ці вікна, в залежності від того, на скільки багато вибірок (вікон) ми зробимо, буде залежати на скільки якісно наш звук буде перетворений у спектрограму. Тобто ми зможемо більш детальніше зобразити всі переходи амплітуди та частоти звуку.

Після застосування до обраної вибірки перетворення Фур'є, зображення набуде кінцевого спектрографічного вигляду. Приклад зображення показано на рисунку 2.

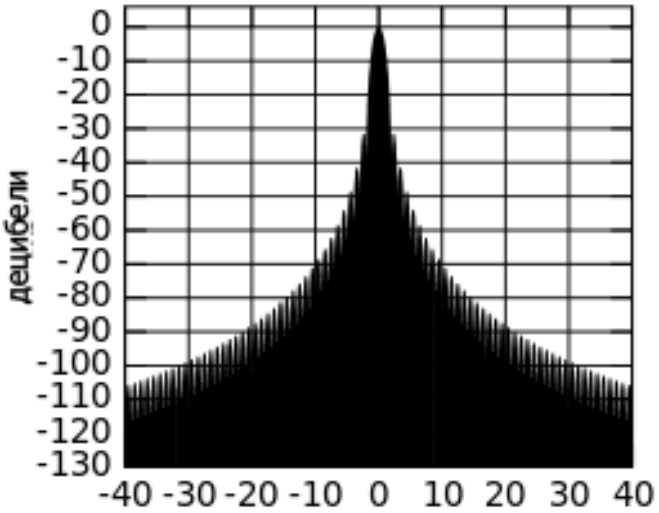

Рис. 2. Вибірка, з перетворенням Фур'є

Отже ми маємо аудіо файл. Спочатку розділяємо весь вміст файлу на вікна. Після цього, за допомогою перетворень Фур'є, звуковий потік представляємо у вигляді спектрограми. Під час перетворення, після обчислення віконної функції, змінюватимемо значення цієї функції на певну величину – Z. Цю величину можна зберігати різноманітними стеганографічними способами. Наприклад, значення цієї величини буде окремо зберігатися і передаватися разом із зображенням, а саме вбудовуватиметься в зображення шляхом поміщення цієї величини в молодші біти зображення. Таким чином при розшифровуванні зображення ми спочатку зчитуємо перші молодші біти зображення, отримуємо необхідне число, після цього відбуватиметься декодування спектрограми назад у звук.

Потрібно зазначити, що при застосуванні шифрування до аудіопотоку, наприклад в системі передачі цифрового звуку, сам потік буде розділятися на блоки. Певна частина звуку буде записуватися в буфер, потім до цієї частини буде застосоване шифрування, і вже після цього, зашифроване повідомлення буде відправлене до отримувача. Зі сторони отримувача знову ж таки буде так саме. Спочатку розшифровується частина звукозапису – прийнятий буфер, після цього розшифроване повідомлення поступає на аудіовихід до користувача. Для забезпечення вищого рівня надійності, до кожного блоку відправленого в потоці, можна застосовувати різну величину числа Z. І в разі, якщо зловмисник отримує одну частину блока з відомим йому одним секретним числом, то іншу частину він не зможе розшифрувати.

Після проведення шифрування ми отримає щось на зразок зображеного на рисунку 3. Це взятий довільний аудіо файл та побудована спектрограма з нього.

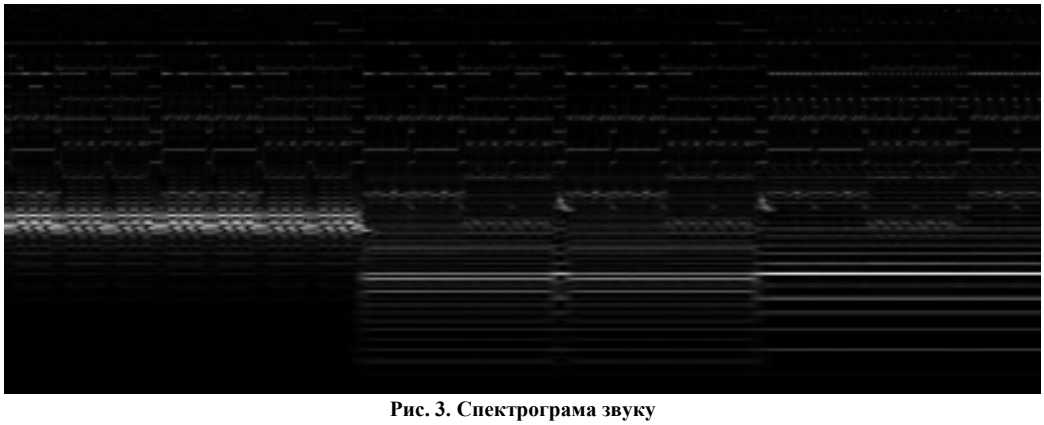

Рис. 3. Спектрограма звуку

Як бачимо з рисунку, білий колір позначає амплітуду частоти, вертикальне розташування білого кольору показує саму частоту відповідно. Чим інтенсивніше колір тим вища амплітуда. Саме це зображення і буде передаватися по мережі, або зберігатися на комп'ютері. В початковому коді цього зображення буде зашифроване секретне число Z, що використовується для безпосереднього шифрування. Заміняючи початкові біти зображення, воно не буде спотворювати саму спектрограму, через що можемо не переживати за якість переданого повідомлення.

Якщо ми просто зберігаємо зашифрований аудіо файл на комп'ютері, то просто для розшифрування

ми завантажуємо обрану спектрограму в програму, і отримуємо початковий аудіо файл. Якщо шифрування відбувалося під час передачі аудіо сигналу по мережі, то в отримувача при надходженні зашифрованого зображення, так само в програмі розшифровується воно, і подається для отримувача в початковому вигляді з дуже малими спотвореннями. Якість розшифрованого звуку буде залежати від величини вибірки, що використовувалась для створення спектрограми. Відповідно чим більше вибірок тим краще буде якість зашифрованого повідомлення.

Висновки. Представлений метод шифрування аудіо файлу у вигляді спектрограми дозволить зберегти необхідні аудіо дані від зловмисників, шляхом зміни представлення шифрованого файлу. Найкраще, цей метод покаже себе при шифруванні розмов по ір-телефонії, між невеликою кількістю комп'ютерів, наприклад у невеликій корпоративній мережі. Так як метод являється повністю програмним, він є економічно вигідним, тому що для нього не потрібно буде додаткових витрат для придбання спеціалізованого апаратного забезпечення. Частини програми можна вбудовувати у власні, вже готові програмні розробки цифрової телефонії, і використовувати ці частини для шифрування. Можна використовувати не частини програми а весь представлений метод у вигляді цілісної програми без вбудовування в інше, глобальне забезпечення. Програму можна буде запустити на необхідних комп'ютерах, між якими і буде постійний обмін голосовими повідомленнями. Якщо ж використовуватися метод буде в особистих цілях, тоді готова програма дозволить просто завантажувати в себе необхідний звук, і видавати зашифровану спектрограму, з якою користувач може виконувати будь-які дії.

Література

1. Радзишевский А.Ю. Основы аналогового и цифрового звука / А.Ю. Радзишевский – М.: Вильямс, 2006. – 288с.

2. [Електронний ресурс] // Дата оновлення 7.07.2014. URL: https://ru.wikipedia.org/wiki/Спектрограмма (дата звернення: 16.09.2014)

References

1. Radzishevskiy A.Y. Fundaments of analog and digital sound / A.Y. Radzishevskiy – Moskow.: Williams, 2006. – 288p.

2. https://ru.wikipedia.org/wiki/Спектрограмма (check: 16.09.2014)

Рецензія/Peer review : 3.12.2014 р. Надрукована/Printed :2.1.2015 р.