УДК 004.056.55

Кирилюк І.О. (ХмНУ)
к.т.н., доц. **Хмельницький Ю.В.** (ХмНУ)
Берназ Н.М. (ДУТ)

АДАПТИВНИЙ МЕТОД ШИФРУВАННЯ АУДІОФАЙЛІВ СПОСОБОМ ПРЕДСТАВЛЕННЯ ЇХ У ВИГЛЯДІ ЗОБРАЖЕНЬ

В статті проведений аналіз аудіофайлів та методів їх шифрування.

Розглянутий принцип створення цифрового аудіофайлу, його представлення на комп'ютері. Розглянутий спосіб представлення звуку у вигляді спектрограми. Приведений аналіз деяких методів шифрування аудіофайлів.

Представлений свій метод шифрування аудіофайлів, що дозволяє зашифровувати спектрограму самого звуку та передавати її по мережі з наступним відтворенням цього звуку.

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

Вступ. Щодня навколо нас створюються та передаються величезні потоки цифрової інформації. Кожного дня ми стикаємося з музикою, зображеннями, самі створюємо подібні файли. Звісно не всю інформацію ми хочемо видавати у відкритий доступ. Конфіденційність – є однією з найбільших проблем в нашому суспільстві. Створена сьогодні пісня вже завтра може бути доступною у мережі інтернет. Створюючи нові засоби конфіденційного збереження файлів, ми даємо поштовх для створення нових способів злому цих засобів для зловмисників.

Що собою являє звук? Більшість природних звуків представляють собою «чисту» хвилю, для якої ми явно можем побачити шаблон, по якому вона слідує. Синусоїдальна хвиля (sine wave) – це яскравий приклад «чистої» хвилі. Її спади та підйоми змінюються по постійному шаблону[1]. Інші хвилі, такі як людський голос, більш складні – спади та підйоми змінюються швидко, не підпорядковуючись ніякому шаблону. На рисунку 1 показані дві різних звукових хвилі:

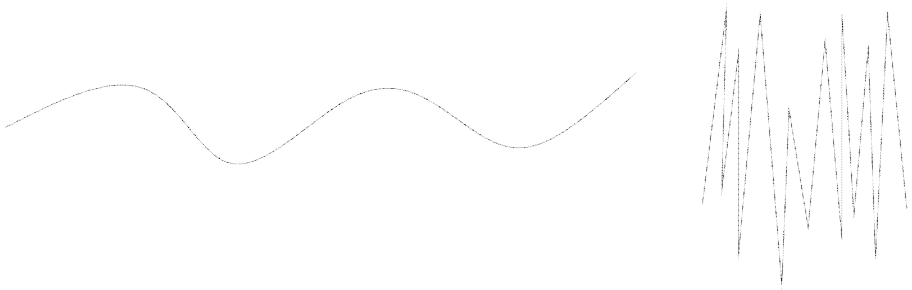

Рис. 1. Різні звукові хвилі

У кожного звуку є унікальні властивості, такі як амплітуда (рівень гучності) і частота. Власне, цифрова форма запису звуку і є записом цих властивостей протягом певного часу.

Основи цифрового запису та відтворення звуків не є дуже складними. В загальному випадку ми беремо звук, наприклад, тривалістю в 2 секунди, і досліджуємо звукову хвилю від початку до кінця з певною частотою (*частотою вибірки* або *частотою дискретизації*) що вимірюється в Герцах (Гц.)

Наприклад, ми хочемо виконати запис звуку тривалістю в дві секунди, з частотою дискретизації 11025 Гц, значить звук буде розділений на 22050 фрагментів (по 11025 фрагментів в секунді). Ці фрагменти називаються *вибірками (samples)*. Для кожної вибірки ми визначаємо амплітуду звукової хвилі в місці надходження вибірки, вимірюючи таким чином рівень гучності в певний момент часу. Записуємо отримане значення і переходимо до наступної вибірки. Записавши рівень гучності для кожної вибірки хвилі, ми отримуємо цифрове представлення звуку.

Це є загальне представлення цифрового звуку. Відповідно будь-який аудіо запис має своє відображення у вигляді графіку частоти та гучності. Записуючи аудіо у вигляді графічного файлу з цим самим графіком, ми матимемо той самий аудіо файл, але який буде зберігатися в зовсім іншому представленні. Перетворюючи назад зображення звукової хвилі, ми отримаємо початковий звук.

Принципи цифрового представлення звуку загалом досить прості:

- спочатку перетворюємо аналоговий сигнал в цифровий, це робить пристрій – аналогово-цифровий перетворювач (АЦП)
- робимо збереження отриманих цифрових даних на носій
- якщо нам потрібно відтворити отриманий файл, то для цього проводиться зворотне перетворення з цифрового в аналоговий звук за допомогою цифро-аналогового перетворювача (ЦАП)

Від того як часто програмно ми будемо зчитувати ці вибірки, так як ми їх будемо редагувати, залежить те на скільки якісний буде звук при оцифровуванні. Формат представлення звукових даних залежить від способу квантування АЦП, ну і формат самого файлу зі звуком залежить від структури та особливостей записаних аудіо даних. Виділяють загалом три групи аудіо форматів:

- аудіоформати без стиснення (WAV, AIFF)
- аудіоформати з стисненням без втрат (APE, FLAC)
- аудіоформати з стисненням з втратами (mp3)

Це є найпоширеніші аудіо формати.

В сучасному світі, аудіо файли використовуються у багатьох сферах діяльності людей. Це не лише записи пісень, а і записи телефонних розмов (при широкому поширенню IP-телефонії в наш час) чи особисті голосові записи. І за різних причин ми можемо не бажати щоб ці записи потрапили у чужі руки. Для цього можна проводити шифрування самих аудіо файлів.

Постановка задачі. По-перше нам потрібно знайти спосіб зашифрувати необхідні файли від зловмисників. Чи то при передачі цього файлу чи навіть просто при зберіганні.

По-друге, цей спосіб повинен бути зручним і надійним.

По-третє, використання цього способу не повинно нашкодити нашим даним.

Візьмемо до прикладу IP-телефонію. Звук відразу ж оцифровується і передається по каналам зв'язку від одного комп'ютеру до іншого. Відповідно на цьому етапі вже можна проводити шифрування необхідного нам цифрового потоку.

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. Але нам потрібна легка програмна реалізація, для якої не потрібне буде додаткове обладнання, де шифрування буде проходити непомітно для користувача.

На програмному рівні є варіанти шифрування даних під час передачі по мережі. Наприклад SRTP (Secure Real-Time Transport Protocol) – безпечний протокол передачі даних в реальному часі призначений для шифрування в однонаправлених та багатонаправлених передачах медіа та програм [2]. Це окремий протокол для мережі, шифрування в ньому проводиться за допомогою AES шифру що може працювати в двох режимах, що перетворюють початково блочний шифр AES в потоковий шифр. Недоліком цього методу є те, що працює він лише для передачі в реальному часі даних, немає можливості зберегти передані аудіо дані в зашифрованому вигляді якщо потрібно їх буде передати/перенести на інших носій.

Звісно завжди залишається варіант звичайного шифрування аудіофайлу, де ми поблоково можемо шифрувати частини даних будь-яким шифром що нам потрібно, але така методика також не допоможе зберегти проміжні результати шифрування для майбутнього їх відтворення з іншого носія або зручного перенесення.

Реалізувати зручний спосіб шифрування вхідного аудіопотоку, чи шифрування вже збереженого файлу можна за допомогою представлення цього звуку у вигляді зображення. Зображення і буде проміжним результатом при передачі від клієнта до клієнта, чи перенесенні з одного носія на інший. І навіть при зломі цього проміжного результату, буде важко відтворити аудіофайл без ключів.

Як представлялось вище, цифровий звук – це є графік амплітуди коливань та частоти. Якщо взяти звукозапис, перетворити його в цей графік в нас вийде звичайне зображення хвилі. Але якщо при запису цієї хвилі до прикладу використати ключ, що буде змінювати цифрове значення амплітуди на певну величину, та значення гучності, файл неможливо буде прослухати без «повернення» цих значень в початковий стан.

Для посилення шифрування можна використовувати зображення спектрограми нашого звуку. 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. На рисунку 2 показаний приклад спектрограми.

Рис. 2. Вигляд спектрограми

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:

$$F(t,\omega) = \int_{-\infty}^{\infty} f(\tau)W(\tau - t)e^{-i\omega\tau}d\tau, \quad (1)$$

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[3].

Взагалі є багато варіантів представлення: деколи вертикальна та горизонтальна вісь відображені так, що час відображається в обидва боки – вверх та вниз, деколи амплітуда представлена вершинами в тривимірному просторі, а не кольором чи інтенсивністю. Саме для цього методу шифрування найкраще використовувати перший метод що описаний вище, а саме відображення амплітуди інтенсивністю на загальному графіку. Змінюючи значення параметрів цих трьох вимірів що відображаються на спектрограмі ми можемо керувати на скільки наш аудіофайл буде можливо прослухати при зворотному перекодуванню.

При потоковій передачі аудіопотоку, ми можемо розбивати на блоки буфер з аудіопотоком, і цей буфер далі конвертувати у вигляд зображення спектрограми. За допомогою ключа змінити на певну величину значення амплітуди/частоти та відправити дане зображення до отримувача нашого повідомлення, там за допомогою зворотного кодування ми повертаємо спектрограмі початковий вигляд, і після цього перекодовуємо назад в аудіопотік, який відтворюється отримувачем. Якщо це вже є збережений файл зі звуком, ми можемо не розбивати на блоки а відразу ж весь файл перетворити у вигляд спектрограми, після чого застосувати зміну параметрів звуку, і надалі утворити зображення спектрограми з новими параметрами.

Ключ для шифрування можна приховати за допомогою звичайного вбудовування ключа в перші біти в зображенні. При потоковій передачі ключ можна передати або з першим зображенням буферу, або можна ключ змінювати для підвищення надійності шифру, при кожній передачі буферу, відповідно записуючи його в перші біти нашого зображення.

Створена програма що приймає на вхід або аудіо потік, або готовий звуковий файл, за допомогою перетворень створює зашифровану спектрограму повідомлення. Далі вона або передається далі по каналу зв'язку або просто зберігається на носії. При потоковій передачі, весь запис розбивається на частини в залежності від вказаної величини буферу, і вбудовується ключ що дасть змогу розшифрувати наш аудіофайл. Якщо це готовий звуковий файл можемо обрати чи розбити його на частини чи повністю представити у вигляді спектрограми. Програма – одержувач, спочатку зчитую ключ з перших бітів зображення, далі перетворює спектрограму за допомогою цього ключа в звичайний звук і відтворює.

Висновки. Даний спосіб дозволить передавати зашифровані аудіоповідомдлення по незашифрованих каналах зв'язку, і допоможе зменшити шанс на те, що навіть якщо наші дані дістануться зловмиснику, то він не зможе їх відтворити. Для цього йому потрібно мати ключ, і всі частини зображення якщо це потокова передача.

ЛІТЕРАТУРА:

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

2. Крюков Ю.С. Безопасность VoIP-контента / Ю.С. Крюков // Защита информации. INSIDE. – 2008. - №3. – С.83-84.

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

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

Кирилюк И.О., к.т.н., доц. Хмельницкий Ю.В., Берназ Н.М.

АДАПТИВНЫЙ МЕТОД ШИФРОВАНИЯ АУДИОФАЙЛОВ СПОСОБОМ ПРЕДСТАВЛЕНИЯ ИХ В ВИДЕ ИЗОБРАЖЕНИЙ

В статье приведен анализ аудиофайлов и методов их шифрования.

Рассмотрен принцип создания цифрового аудиофайла, его представление на компьютере. Рассмотрен способ представления звука в виде спектрограммы. Приведен анализ некоторых методов шифрования аудиофайлов.

Представлен свой метод шифрования аудиофайлов, что позволяет зашифровать спектрограмму самого звука и передавать ее по сети з последующим воспроизведением этого звука.

Ключевые слова: аудиофайл, спектрограмма, звуковая волна, оконные преобразования Фурье.

Kyryliuk I.O., Ph.D. Khmelnitsky Yu.V., Bernaz N.M.

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

It article we analyze audio and methods of their encryption.

The principles of creation of digital audio file, its representation on the computer. The way of presentation of sound as a spectrogram. The analysis of several audio file encryption methods.

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.

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