ПРОБЛЕМЫ СРАВНЕНИЯ АУДИОФАЙЛОВ

Золотарев А.А., Панин Д.В.

АНОО ВО «Воронежский институт высоких технологий», Воронеж, e-mail: bbosly@yandex.ru

Рассматриваемая задача посвящена численной оценке схожести аудиофайлов на основе алгоритмов нечеткого поиска. На сегодняшний день задача сравнения мелодий является актуальной в свете резкого скачка в развитии технологий цифровой обработки сигналов, их распознавания и сравнения. Многие крупные компании музыкально-технологической сферы занимаются исследованиями в данной области, разработкой и совершенствованием новых алгоритмов, технологий и программного обеспечения.

Цель работы состоит в подведении теоретической базы и реализации процесса сравнения содержимого аудиофайлов на основе алгоритма нечеткого поиска с использованием метрики Левенштейна. Объектом для исследования был избран формат .wav.

Рассматриваемая задача сводится к считыванию данных из двух WAV-файлов, их преобразованию и анализу схожести двух мелодий.

В общем случае оценить схожесть двух наборов каких-либо значений можно с помощью алгоритмов нечеткого поиска. Задача нечеткого поиска в общем виде формулируется следующим образом: «По заданному «слову» найти в тексте или словаре размера n все «слова», совпадающие с этим словом (или начинающиеся с этого слова) с учетом k возможных различий».

На вход подаются два аудиофайла с расширением .wav. Функционал программы должен включать [1]:

• разбор этих файлов и извлечение из них последовательностей значений амплитуд звукового сигнала;

• преобразование полученных амплитудных значений в частотные путем применения БПФ;

• перевод числовых последовательностей значений частот в символьные последовательности и сравнение их с помощью алгоритма Левенштейна.

На выходе мы получаем числовую оценку схожести содержимого данных аудиофайлов.

Цифровой звук – это аналоговый звуковой сигнал, представленный посредством дискретных численных значений его амплитуды.

Звуковая волна имеет три основных характеризующих ее параметра: амплитуда, частота и фаза. Два последних являются функцией времени, тогда как амплитуда определяет динамический диапазон. Отсюда следует, что для корректного представления звукового сигнала в цифровой форме необходимо сохранить изменения амплитуды как функцию времени.

Для получения спектра звукового сигнала наиболее часто используются дискретное преобразование Фурье и вейвлет-преобразование. Интегральное преобразование и ряды Фурье лежат в основе спектрального анализа. Однако несмотря на популярность преобразования Фурье для частотного представления сигнала, существует ряд фундаментальных ограничений, которые привели к появлению оконного преобразования Фурье и стимулировали развитие вейвлетного преобразования. Основные из них [2,3]:

• Ограниченная информативность анализа нестационарных сигналов и практически полное отсутствие возможностей анализа их особенностей (сингулярностей), т. к. в частотной области происходит «размазывание» особенностей сигналов (разрывов, ступенек, пиков и т. п.) по всему частотному диапазону спектра.

• Гармонические базисные функции разложения не способны в принципе отображать перепады сигналов с бесконечной крутизной типа прямоугольных импульсов, т. к. для этого требуется бесконечно большое число членов ряда. При ограничении числа членов ряда Фурье в окрестностях скачков и разрывов восстановленного сигнала возникают осцилляции (явление Гиббса).

Несмотря на очевидные ограничения классического дискретного преобразования Фурье, на начальном этапе разработки программного решения задачи было выбрано именно оно (точнее, его оптимизированная вариация, называемая быстрым преобразованием Фурье). Этот метод наиболее интуитивен на начальных этапах изучения теоретического базиса спектрального анализа, имеет множество реализаций на разных языках программирования и оставляет пространство для дальнейшего расширения функциональности программной реализации, добавления других методов преобразования для сравнения их эффективности.

Стоит отметить, что на данном этапе работы программное решение удовлетворяет лишь частному случаю постановки задачи. Сравнение будет эффективно при малой длительности целевых аудиофайлов (приблизительно до 1с), поскольку без применения оконной функции при преобразовании Фурье теряется информация о времени, когда прозвучала та или иная частота. Для сравнительной оценки частотного спектра коротких аудиосигналов можно использовать алгоритмы нечеткого поиска. В отличие от прямого сравнения, нечеткий поиск дает возможность получить оценку схожести приблизительно похожих отрывков, что позволит в некоторой степени пренебречь возможными помехами, повреждениями хранящихся в аудиофайлах данных и другими незначительными отличиями различной природы.

В силу того, что классические алгоритмы нечеткого поиска подразумевают работу с сим-

вольными последовательностями, встает вопрос о выборе принципа применения этих алгоритмов к данной предметной области. Здесь существует два пути.

Первый подразумевает модификацию классических алгоритмов для обработки числовых (в т. ч. и комплексных) данных. Это самый очевидный путь. В то же время он довольно трудоемкий, требует глубокого и детального изучения математической базы и может повлечь за собой непредвиденные сложности в связи с дальнейшей оптимизацией.

Второй вариант кажется более затратным по времени и вычислительным мощностям, но, на мой взгляд, оправдывает себя простотой реализации. Он состоит в переводе числовой последовательности в некую эквивалентную ей последовательность символов, к которой затем можно применить классический алгоритм поиска без каких-либо дополнительных манипуляций с данными или модификаций самого алгоритма.

Список литературы:

1. Попов В.Н. и др. Подготовка набора данных для обучения нейронной сети, используемой в задачах сравнения аудиофайлов // Проблемы правовой и технической защиты информации. 2021. №. 9. С. 22-27.

2. Юрченко Н.Ю. Аудио- и видеоматериалы из интернета: трудности и возможности // Вестник УМЦ. 2017. № 15-2. URL: https://cyberleninka.ru/article/n/audio-i-videomaterialy-iz-interneta-trudnosti-i-vozmozhnosti (дата обращения: 15.01.2025).

3. Слепой ABX тест звучания аудиофайлов. URL: https://hamsterilla.ru/slepoj-abx-test-zvuchaniya-audiofajlov/ (дата обращения: 15.01.2025).

ДЕТЕКТИРОВАНИЕ ПРИЗНАКОВ ФИШИНГОВЫХ АТАК НА ОСНОВЕ ВСТРОЕННЫХ СРЕДСТВ ЗАЩИТЫ ПОЧТОВЫХ СЕРВИСОВ

Конанов О.И.

Российский экономический университет имени Г.В. Плеханова, Москва, e-mail: 2310.Oleg.Konanov@gmail.com

Статистические отчеты различных организаций показывают, что почтовый фишинг является одной из самых распространенных и эффективных техник кибератак, использующихся как при атаках на почтовую инфраструктуру организаций, так и на частные почтовые ящики. По данным отчета ФБР IC3 Report за 2021 год, на долю фишинговых атак приходится почти 22% всех случаев утечки данных, что подтверждает их позицию как одного из самых распространенных киберпреступлений. В отчете Verizon за 2022 год говорится, что 36% всех случаев утечки данных связаны с фишингом. По оценкам специалистов, к 2022 году атаки с использованием выкупа или фишинга будут происходить каждые 11 секунд [1].

Кроме того, несмотря на кажущуюся простоту почтового фишинга, данная техника непрерывно совершенствуется злоумышленниками. Исследования показывают, что более 80% фишинговых рассылок осуществляются с помощью специализированного программного обеспечения. Также злоумышленники стали активно применять технологии машинного обучения, например, получившие в последнее время широкое распространение языковые модели, для формирования правдоподобных фишинговых писем и обхода существующих средств защиты почтовых сервисов [2].

В статье рассмотрены актуальные техники фишинговых атак, в том числе предложены дополнительные фишинговые подтехники, не представленные в матрице Mitre Att&ck, выделены признаки того, что письмо является фишинговым, механизмы детектирования данных признаков, а также эффективность встроенных средств защиты почтовых сервисов по детектированию данных признаков.

Показано, что существующие встроенные средства защиты почтовых сервисов не детектируют все фишинговые признаки и требуют дальнейшего совершенствования.

Анализ техник фишинговых атак и их признаков

Почтовый фишинг может быть разделен на целевой (направленный на конкретного сотрудника, узкую группу сотрудников в рамках одной организации, частный почтовый ящик конкретного пользователя) и массовый (может быть направлен на всех сотрудников одной организации, сотрудников различных организаций, частные почтовые ящики широкого круга пользователей). В рамках настоящего исследования были рассмотрены целевые фишинговые атаки.

С точки зрения фреймворка Mitre Att&ck, фишинг входит в тактику Initial Access. Целью злоумышленника на данном шаге является получение несанкционированного доступа к ИС.

С точки зрения Mitre Att&ck, злоумышленник может выполнить поставленные задачи на данном шаге с помощью следующих подтехник, связанных с почтовым фишингом [3]:

1. Целевой фишинг с вложением – к письму прикрепляется вредоносное вложение, например, исполняемый файл, архив, документ Microsoft Office с вредоносным расширением и т.д.

2. Целевой фишинг с ссылкой – в текст письма помещается вредоносная ссылка, ведущая, например, на поддельный корпоративный ресурс (как правило с формой авторизации с целью получения логина и пароля сотрудника), загрузчик вредоносного ПО и т.д.

3. Целевой фишинг с помощью стороннего сервиса – данная подтехника зачастую комбинируется с подтехниками целевого фишин-